Safety Instrumented Function Verification: The Three Barriers

Iwan van Beurden, CFSE
exida
vanbeurden@exida.com

W. M. Goble, PhD, CFSE
exida
Sellersville, PA 18960, USA
wgoble@exida.com

J. V. Bukowski, PhD
Villanova University
Villanova, PA 19085, USA
julia.bukowski@villanova.edu

November 2017 V2R1

Abstract

The three constraints (systematic capability constraint, architectural constraint, and probabilistic performance metric constraint) that are implied by requirements per international safety standards IEC 61511 [1] and IEC 61508 [2] to determine the safety integrity level (SIL) of a safety instrumented function (SIF) are described and discussed. Examples of their applications are presented. For low demand mode SIF operation, the importance of including numerous key variables in the computation of average probability of failure on demand (PFDavg) is noted.

Introduction

Many members of the functional safety community *erroneously* believe that the SIL of a SIF is determined solely by the PFDavg of the SIF in low demand mode and solely by the probability

of (dangerous) failure per hour (PFH) of the SIF in continuous/high demand mode. Actually, the overall SIL of a SIF is determined by the minimum SIL achieved by the SIF considering three different constraints, viz., a systematic capability (SC) constraint, an architectural constraint (SILac), and the achievable PFDavg or PFH. exida calls these constraints the "three barriers." Additionally, for a SIF intended to operate in low demand mode, if a risk reduction factor (RRF) was specified in the SIF requirements, then 1/PFDavg must also meet or exceed the stated RRF. Thus, SIL determination is significantly more complicated than simply calculating a PFH or PFDavg and performing a table look-up to establish the corresponding SIL level.

While this paper assumes that the reader has at least a rudimentary knowledge of functional safety, some fundamental information is reviewed and references are provided to more detailed information for the reader who is not conversant with the fundamental information presented. After a Notation section, this paper

- presents basic information about SIF,
- provides some historical context for the development of the three constraints,
- describes and discusses the three constraints,
- indicates the importance of recognizing all pertinent variables that impact SIL and appropriately including them in required computations,
- provides an illustrative example of the using all three constraints in verifying the SIL of a SIF.

IEC 61508 is a fundamental standard whose first edition predates the many later standards that are derived from IEC 61508. These later standards emphasize the specific needs of individual industries. IEC 61511 is based on the principles of IEC 61508 but is specific to the process industries. Since this white paper is addressed to the process industries, IEC 61511 is the principal reference with material from IEC 61508 included when such material is especially relevant to the discussion about IEC 61511.

Notation

C_{PT}	proof test coverage
DD	dangerous detected
DI	demand interval
DTI	diagnostic test interval
DU	dangerous undetected
HFT	hardware fault tolerance
IEC	International Electrotechnical Commission
koon	k-out-of-n architectural structure where k of the n devices must correctly operate in order that the koon structure is operational
MDT	mean time to detect a failure
MRT	mean time to restore from a failure
MTTR	mean time to restore
nX	n times

PDC	partial diagnostic credit
PFDavg	average probability of failure on demand
PFH	probability of failure per hour, also known as average frequency of dangerous failure
RRF	risk reduction factor
SC	systematic capability
SD	safe detected
SFF	safe failure fraction
SIF	safety instrumented function
SIL	safety integrity level
SILac	SIL architectural constraint
SSI	site safety index
SU	safe undetected
TI	time interval between successive proof tests
λ_D	assumed constant failure rate for dangerous failures
λ_{DD}	assumed constant failure rate for dangerous failures detected by automatic diagnostics
λ_{DU}	assumed constant failure rate for dangerous failures undetected by automatic diagnostics
λ_S	assumed constant failure rate for safe failures
λ_{SD}	assumed constant failure rate for safe failures detected by automatic diagnostics
λ_{SU}	assumed constant failure rate for safe failures undetected by automatic diagnostics

Basics of Safety Instrumented Functions

Generally, a SIF consists of sensor elements, a logic solver element, and final elements. The SIF monitors a process, determines if the process is operating within acceptable limits, and intervenes appropriately if the process strays outside its acceptable limits. The SIF itself is subject to failure and can fail in one of two ways. The SIF can erroneously determine that a correctly operating process is outside of its acceptable limits and inappropriately intervene in the process operation. This is called a safe failure of the SIF. Alternately, the SIF can fail such that it is incapable of determining if the process is within acceptable limits and/or such that it is incapable of appropriately intervening when the process strays outside its acceptable limits. This is called a dangerous failure of the SIF.

It is usually assumed that safe and dangerous failures of the SIF are reasonably described by constant failure rates denoted λ_S and λ_D, respectively. If the SIF contains automatic self-diagnostics which detect some of the SIF failure states, then λ_S and λ_D can be further decomposed into

$$\lambda_S = \lambda_{SD} + \lambda_{SU}$$

and

$\lambda_D = \lambda_{DD} + \lambda_{DU}$

where the subscripts SD, SU, DD, and DU mean safe detected, safe undetected, dangerous detected and dangerous undetected, respectively. Dangerous failures not detected by automatic diagnostics may be found only during proof testing, i.e., periodic testing and maintenance. The time interval between successive proof tests, TI, impacts SIF safety.

When a process strays outside its acceptable limits such that SIF intervention is required, the process is said to place a demand on the SIF. A SIF's design and implementation must take into account both the consequences of the SIF's failure to respond appropriately (dangerous failure) to a demand and how frequently a demand will be placed on the SIF. The more significantly negative the consequences, the greater the safety that must be provided by the SIF. This concept of measuring SIF safety via risk reduction is called the SIL of the SIF and is measured by four order-of-magnitude levels 1 through 4 with 4 being the level of highest safety. The SIL assigned to a SIF is determined by the many requirements of IEC 61511 and IEC 61508. If the SIF experiences a demand frequently, faster than any practical proof test, the SIF is said to operate in high/continuous demand mode. If the SIF experiences a demand less than twice any practical proof test interval, the SIF is said to operate in low demand mode.

The reader who is unfamiliar with any of the above material is referred to [3] for more detailed information.

Historical Perspectives

Prior to the release of the first edition of IEC 61508, SIF were subject to prescriptive architectural requirements and standardized designs in order to achieve various SIL levels. IEC 61508 was the first IEC standard to introduce the concept of performance based assessment and allowed for any appropriate SIF designs that could justify/demonstrate their safety performance to a given SIL as measured by various safety performance metrics and a few other constraints. The most important performance metric for SIF in continuous/high demand mode is PFH which, for non-redundant SIF, depends on λ_D and, if the SIF is configured to move to a safe failure state upon detection of a DD failure by automatic diagnostics, also depends on the ratio of the frequency with which automatic diagnostics are executed to the frequency of demand on the SIF. The most important performance metric for SIF in low demand mode is PFDavg which, at the time IEC 61508 was first written, was usually calculated based on

- λ_{DD},
- λ_{DU},
- the mean time to restore (MTTR) the SIF from a DD failure and
- the time interval between successive proof tests, TI.

However, the IEC 61508 committee was cautious about having a SIL determined solely based on probabilistic performance metrics which largely depended on λ_{DD} and λ_{DU}, principally because

of a concern that some analysts would generate very low failure rates (overly optimistic failure rates) resulting in overly optimistic performance metrics and consequently unsafe designs. Some committee members insisted that certain architectural constraints (redundancy associated with minimum levels of hardware fault tolerance (HFT)) needed to be in place at least for the higher SIL to protect against their concerns about overly optimistic failure rates. Thus, certain architectural constraints were added to the determination of SIL; in this paper these are referred to as SILac.

Other committee members expressed concerns that redundancy alone is not sufficient to address the issues because, about that time, new information came to light [4] which clearly indicated that redundant architectures could be subject to high percentages of common cause failures. These committee members wanted a quality measure of the strength of a device's design and manufacture which would guard against common cause failures due to systematic weaknesses that would otherwise obviate the benefits of redundancy. This led to an additional constraint on SIL determination which IEC 61508 called systematic capability (SC).

As it turned out, the committee's concerns about some analysts generating overly optimistic failure rates were correct. Further, another unanticipated issue arose. Over the years it became increasing obvious that PFDavg was significantly impacted by parameters other than λ_{DD}, λ_{DU}, MTTR and TI [5]. Using only the aforementioned four parameters often results in optimistic PFDavg calculation and, potentially, unsafe designs for low demand SIF applications. Therefore, the cautionary requirements of three constraints in determining SIL have indeed been appropriate.

It should be noted that, in theory, if realistic values for λ_{DD} and λ_{DU} are used to compute PFDavg and if all parameters impacting PFDavg are included in the PFDavg computations, then the additional SILac constraint will no longer be needed to accurately determine the SIL of a SIF operating in low demand. But until such practices are largely uniform in the functional safety community, the three barriers serve an important and useful function in the determination and verification of SIL for a SIF.

Three Barriers to SIL Determination

While historically the three constraints which determine SIL assignment developed in the order of probabilistic performance metric, SILac and SC, they are here treated in reverse order representing the order in which a SIF designer needs to consider them. The three barriers/constraints are summarized below.

The achieved SIL level of the SIF is the minimum of:

Barrier 1 - **SIL level based on Systematic Capability (SC) of each device used in a SIF.** SC is a measure of design quality that shows sufficient protection against systematic design faults. SC is achieved either by choosing a certified part with SC to the given SIL level or greater or by completing a

prior use justification to the given SIL level or greater. The lowest SC for any device in the SIF determines the SIL level for the SIF with respect to SC.

Barrier 2 - **SIL level based on minimum architecture constraints (SILac) for each element (sub-system) in a SIF**. There are different tables that can be used to establish architecture constraints; one is in IEC 61511 [1], and two alternatives are in IEC 61508 [2] (Route 1_H or Route 2_H). The lowest SILac for any SIF subsystem determines the SIL level for the SIF with respect to SILac.

Barrier 3 - **SIL level based on a PFH (high demand), or a PFDavg (low demand) for the entire SIF.**

All three of these design barriers must achieve or exceed the target SIL level. If a SIF design meets *only two* of the barriers then the worst case (lowest) SIL determines the SIL level for the SIF. Additionally, for SIF in low demand mode, the designer must ensure that 1/PFDavg exceeds the RRF if this metric has been specified in the SIL requirement specification.

Barrier 1 – Systematic Capability

As noted above, the SC is determined either by choosing an IEC61508 certified device for use in the SIF or by providing a prior use justification (also known as proven-in-use justification) for the device. These two different methods of determining SC are described and discussed next. At this juncture, a note about terminology is in order. The constraint provided by Barrier 1 is known as SC – systematic capability. When a device is certified through the process described below, it is genenerally said to have a certified rating of SC x where x is 1 through 4 corresponding to a SIL level. When a device meets the SC constraint through prior justification, the device is generally said to meet SIL x by prior use justification or to be proven-in-use up to SIL x. The use of these two different terms (SC or SIL) generally distinguishes the method used in evaluating the degree to which a device meets the SC constraint.

Use of Certified Devices

IEC 61511 uses the IEC 61508:2010 requirements for device certification. In the IEC 61508 standard, systematic capability is a measure of design quality as specified by a series of tables that stipulate design and test techniques. More stringent design and test methods are required as the SIL level increases. These methods reflect the committee opinion of necessary and effective “fault avoidance techniques.” The objective is to reduce the number of design mistakes that might result in a dangerous failure of the device.

IEC 61508:2010 has nearly 400 requirements for compliance and 29 tables of design, test, and documentation techniques. Each line of a table describes a technique and gives a category for four columns which represent the four SIL levels. The categories are normally R (recommended, the designer should consider this method or justify an alternative) or HR (highly recommended, the designer must use this technique or equivalent).

As an example, Figure 1 shows a portion of Table A.2 from IEC 61508:2010, Part 3. Different software design techniques are specified for each SIL level. In line 11b, semi-formal methods are recommended for SIL1 and SIL 2 but highly recommended for SIL 3 and SIL 4.

		Technique/Measure *	Ref.	SIL 1	SIL 2	SIL 3	SIL 4
Fault Avoidance	7	Modular approach	Table B.9	HR	HR	HR	HR
	8	Use of trusted/verified software elements (if available)	C.2.10	R	HR	HR	HR
	9	Forward traceability between the software safety requirements specification and software architecture	C.2.11	R	R	HR	HR
	10	Backward traceability between the software safety requirements specification and software architecture	C.2.11	R	R	HR	HR
	11a	Structured diagrammatic methods **	C.2.1	HR	HR	HR	HR
	11b	Semi-formal methods **	Table B.7	R	R	HR	HR
	11c	Formal design and refinement methods **	B.2.2, C.2.4	---	R	R	HR
	11d	Automatic software generation	C.4.6	R	R	R	R
	12	Computer-aided specification and design tools	B.2.4	R	R	HR	HR
	13a	Cyclic behaviour, with guaranteed maximum cycle time	C.3.11	R	HR	HR	HR
	13b	Time-triggered architecture	C.3.11	R	HR	HR	HR
	13c	Event-driven, with guaranteed maximum response time	C.3.11	R	HR	HR	-
	14	Static resource allocation	C.2.6.3	-	R	HR	HR
	15	Static synchronisation of access to shared resources	C.2.6.3	-	-	R	HR

Figure 1. Methods table from IEC 61508:2010, Part 3, Table A.2. Note: R = Recommended and HR = Highly Recommended. Copyright IEC 2010.

As another example, Figure 2 shows a table for software module test techniques. The differences between methods required for each SIL level are shown. More testing is needed to achieve higher design quality for the higher SIL levels.

	Technique/Measure *	Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Test case execution from boundary value analysis	C.5.4	R	HR	HR	HR
2	Test case execution from error guessing	C.5.5	R	R	R	R
3	Test case execution from error seeding	C.5.6	---	R	R	R
4	Test case execution from model-based test case generation	C.5.27	R	R	HR	HR
5	Performance modelling	C.5.20	R	R	R	HR
6	Equivalence classes and input partition testing	C.5.7	R	R	R	HR
7a	Structural test coverage (entry points) 100 % **	C.5.8	HR	HR	HR	HR
7b	Structural test coverage (statements) 100 %**	C.5.8	R	HR	HR	HR
7c	Structural test coverage (branches) 100 %**	C.5.8	R	R	HR	HR
7d	Structural test coverage (conditions, MC/DC) 100 %**	C.5.8	R	R	R	HR

Figure 2. Methods table from IEC 61508:2010, Part 3, Table B.2. Note: R = Recommended and HR = Highly Recommended. Copyright IEC 2010.

The collection of these tables defines the systematic capability rating given during a certification assessment. All SIL 3 HR methods or equivalent must be used on new designs to achieve a SC rating of SC 3 (SIL 3). Similarly, all SIL 2 HR methods must be used on a new design for that device to achieve a SC 2.

Devices which are certified per IEC 61508 have undergone an auditing process by an accredited third party which assures that nearly 400 IEC 61508 requirements for compliance with various design, test and documentation have been satisfied to the certified SC level. The existence of many different types of certified devices from various manufacturers makes the use of certified devices over a wide range of functional needs a very appealing alternative to the work required to create a prior-use or proven-in-use justification.

Prior Use Justification

Most companies agree that if a user company has many years of *documented* successful experience (sufficiently low number of dangerous failures) with a particular version of a particular instrument this can provide justification for using that instrument even if it is not safety certified. Most agree that prior use requires that a system be in place to record all field failures and failure modes at each end-user site. Version records of the instrument hardware and software must be kept as significant design changes may void prior use experience. Operating conditions must be recorded and must be similar to the proposed safety application.

Clause 11.5.3 of IEC 61511:2016 provides requirements for the selection of various devices based on prior use. While it does not give specific details as to what the criteria for "prior use" are, it does state that "Appropriate evidence shall be available that the devices are suitable for use in the [Safety Instrumented System] SIS." Four bullet items are provided:

- consideration of the manufacturer's quality, management, and configuration management systems;
- adequate identification and specification of the devices;
- demonstration of the performance of the devices in similar operating environments;
- the volume of operating experience.

Consideration of the manufacturer's quality, management, and configuration management systems requires verification of a quality certification like ISO 9000 or equivalent on a periodic basis. In addition, an audit of manufacturers design process including testing and documentation procedures should be performed. For SIL 3 applications, an audit of the manufacturer per the requirements of IEC 61508 should be performed.

Adequate identification and specification of the devices require that the manufacturer maintains a version control system for device production. Changes in the hardware or software must be reflected in a version identification system with version changes clearly marked on the product or provided with a digital command. The reason this is so important is that field performance of a particular version may not be the same as the performance of a new version. For higher SIL levels, an audit of the manufacturer's version history and the manufacturer's warranty failure history is needed.

A demonstration of the performance for the devices in a similar operating environment requires the equipment be installed in non-critical applications and monitored. For dangerous failures, proof testing may be the only way to detect failures. A proof test must be designed to detect all potentially dangerous failures not detected by automatic diagnostics. Proof test records must be kept. Failures detected must be analyzed to root cause. All "alerts" or other diagnostic failure detection alarms must be recorded and resolved. Operating conditions should be recorded and all model numbers and version numbers must be recorded.

The volume of operating experience is not specified but most systems require a minimum of 100,000 unit operating hours for a particular version of each device.

Barrier 2 – Architectural Constraints

Architectural constraints refer to the minimum hardware fault tolerance (HFT) required to attain a particular SILac. HFT is the number of redundant devices in a SIF element which can fail and have that SIF element remain functional. HFT is not the same as redundancy. Table 1 lists various SIF safety architectures and their corresponding HFT.

Table 1. Safety architectures versus hardware fault tolerance provided

Architecture	HFT
1oo1	0
1oo2	1
2oo2	0
1oo3	2
2oo3	1
3oo3	0

IEC 61511 describes three ways that a SIF may satisfy the architectural constraints. Clause 11.4.3 states that:
"The HFT of the SIS or its SIS subsystems shall be in accordance with;
• 11.4.5 to 11.4.9 of clause 11 or,
• the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
• the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.
NOTE The route developed in IEC 61511 is derived from route 2H of IEC 61508-2:2010"

Now it is important to note that IEC 61511 Clauses 11.4.5 – 11.4.9 ("the route developed in IEC 61511") are for practical purposes the same as IEC 61508-2:2010 Route 2_H. Further, based on the above language it is clear that the analyst may choose any of the three (really two) methods. Thus, logically, one should choose the method that will result in the higher possible SILac rating. Finally, there are currently only two products on the market (logic solvers with SFF > 99%) where Route 1_H results in a higher SILac rating than does Route 2_H. Thus, as a practical matter, the method described as IEC 61508 Route 2_H should be the primary method for determining SILac. This paper describes that method below. Note, however, that IEC 61508 Route 2_H also requires the availability of quality field failure data. In the absence of quality field

failure data, IEC 61508 Route 1_H must be used and this will generally lead to a lower SILac rating. The IEC 61508 Route 1_H method is included in the Appendix.

Architectural Constraints – Route 2_H

Route 2_H was added to the second edition (2010) of IEC 61508 in Part 2, Clause 7.4.4.3. Since architectural constraints were created as a defense against unrealistically low failure rate data, Route 2_H recognized that the probabilistic approach would answer the real need for redundancy *if* the failure rates were realistic. Therefore, failure rate quality criteria were established.

The stated failure rate quality criteria are "the reliability data used when quantifying the effect of random hardware failures (see Clause 7.4.5) shall be:

a) "based on field feedback for elements in use in a similar application and environment; and
b) based on data collected in accordance with international standards (e.g. IEC 60300-3-2 [6] or ISO 14224 [7]); and
c) evaluated according to:
    i) the amount of field feedback; and,
    ii) the exercise of expert judgement; and where needed,
    iii) the undertaking of specific tests;

    in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval) of the probability distribution of each reliability parameter (e.g., failure rate) used in the calculations."

There is no restriction on where the approach is applied. Therefore the failure rate quality criteria can be applied to devices or components. Using this approach, a device consisting of components which are all categorized as 2_H may be classified as 2_H [8]. To make certain the components in the new device are in a similar operating environment, the device should have at least one year of field operation.

Text from clause 7.4.4.3.1 of IEC 61508:2010 can be used to construct a table of HFT. Although there are specific conditions and special cases described, the overall approach is shown in Table 2. IEC 61511:2016 clearly states that its minimum HFT requirements were derived from IEC 61508:2010 Route 2_H.

Table 2. IEC 61508 Route 2_H HFT requirements.

SIL	Mode	Minimum HFT
1	Any	0
2	Low Demand	0
2	High or Continuous	1
3	Any	1
4	Any	2

EXAMPLE 1
A simple SIF was designed with a pressure switch hardwired to a two-way solenoid valve. The pressure switch opens on a high pressure demand and de-energizes the solenoid which will take the process to a safe state. According to the architecture limits of IEC 61511 and IEC 61508, Route 2_H to what SIL does this SIF design qualify?
Answer: Each element (pressure switch for sensing and solenoid for final element) have HFT = 0. Assuming the SIF operates in low demand mode, per Table 2 each element qualifies to SIL 2 and therefore the overall SIF (operating in low demand mode) qualifies for SILac to SIL 2. Note the Route 2_H requirement that quality field failure data be available for each device.

EXAMPLE 2
Two transmitters are used in a SIF sensor element design. The logic solver is programmed to trip if either transmitter indicates a dangerous condition (1oo2). To what SIL level is this sensor element design qualified per IEC 61511 and IEC 61508, Route 2_H HFT requirements?
Answer: The sensor design has a HFT of 1 since one transmitter can fail dangerously and the SIF can still perform the safety function. Per Table 2 the sensor element design qualifies for a SILac of SIL 3 for any SIF operational mode. Note the Route 2_H requirement that quality field failure data be available for the transmitter device.

Barrier 3 – Probabilistic Performance Metrics

As noted above, there are two separate probabilistic performance measures – PFH used for continuous/high demand SIF operation and PFDavg used for low demand SIF operation.

Probability of Failure per Hour – PFH

The metric PFH is often thought of as a failure rate. This is not quite correct. **If** the failure rate governing the *overall* SIF is *truly* a constant (as will be the case for a series configuration where all constituent devices/elements are governed by truly constant failure rates), then PFH is equal to that constant failure rate and is itself a failure rate. However, if the failure rate governing the *overall* SIF behavior is time dependent, say $\lambda(t)$, (as may well be the case in a redundant configuration *even if* the constituent devices/elements are governed by truly constant failure rates), then PFH is defined as the average of $\lambda(t)$ over a given interval [0, TI] [3].

Because of the complexities introduced by redundant configurations operating in continuous/high demand mode**, in this paper, only non-redundant systems will be discussed with regard to computing PFH.**

When a SIF is functioning in continuous demand mode, a demand is either always present or occurs so frequently that neither automatic diagnostics nor proof testing serve to improve safety. Consequently, both λ_{DD} and λ_{DU} impact PFH. In a non-redundant device/element, PFH represents the equivalent dangerous constant failure rate for the SIF, i.e.,

$$PFH = \lambda_{DD} + \lambda_{DU}. \quad (1)$$

When a SIF is functioning in high demand mode, automatic diagnostics may lower the probability of dangerous failure if the diagnostics are running fast enough compared to the demand rate **and** the system is programmed to initiate transition to the safe state upon a diagnosed failure. IEC 61508:2010 defines the term diagnostic test interval (DTI) as the "interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage." Most consider that if the diagnostics are run 100 times or more within the average demand interval, i.e., if DI ≥ 100X DTI, then full diagnostic credit can be given. In that case, PFH = λ_{DU}. In a non-redundant system, if the automatic diagnostics run at a slower rate, partial diagnostic credit (PDC) can be given as [9]

$$PDC \approx (\lambda_{Diag}/\lambda_{Demand})\ (1 - \exp[-\lambda_{Demand}/\lambda_{Diag}]) \qquad (2)$$

where

λ_{Diag} equals the automatic diagnostic rate = 1/DTI
λ_{Demand} equals the demand rate = 1/Demand Interval, i.e. 1/DI.

Note that when the statement is made that DI = nX DTI, $\lambda_{Diag}/\lambda_{Demand} = n$.

For non-redundant systems, PFH for high demand is calculated with Equation 3 as

$$PFH = (1\text{-}PDC)\ \lambda_{DD} + \lambda_{DU}. \qquad (3)$$

For both continuous and high demand, the calculated PFH value is compared to the Continuous / High Demand target frequency of dangerous failures from IEC 61511 to determine the SIL achieved by the design. This chart is shown in Table 4.

Table 3. Continuous/High demand mode dangerous probability limits per SIL

Safety Integrity Level	Target Frequency of Dangerous Failures per Hour
SIL 4	**>=10^{-9} to < 10^{-8}**
SIL 3	**>=10^{-8} to < 10^{-7}**
SIL 2	**>=10^{-7} to < 10^{-6}**
SIL 1	**>=10^{-6} to < 10^{-5}**

EXAMPLE 3

A set of non-redundant (HFT = 0) safety equipment is used to implement a SIF with a demand expected every 50 milliseconds. Once a demand occurs, it takes 100 milliseconds for an incident to occur. (Therefore the process safety time is 100 milliseconds.) The safety manual for each device was reviewed. The longest diagnostic time interval is given as 500 milliseconds. After a failure is detected the SIF equipment set requires 20 milliseconds to shut down the process. The following failure rate data are obtained for the equipment set by adding the failure rates of the categories of all devices:

$\lambda_{DD} = 8.5 * 10^{-6}$ failures per hour

λ_{DU} = 0.5 * 10^{-6} failures per hour
What SIL level is achieved by this design based on PFH requirements?
Answer: All dangerous failures will cause an incident within 150 milliseconds. The failure detection and response time of 520 milliseconds is not fast enough to bring the process to a safe state. Therefore, λ_{DD} and λ_{DU} are added together to obtain the total dangerous failure rate, λ_D. Using Equation 1, the PFH equals λ_D and is 9 * 10^{-6} failures per hour which meets the requirements for SIL1 per Table 3.

EXAMPLE 4
A set of non-redundant (1oo1, HFT = 0) safety equipment is used to implement a SIF. The DTI is 100 milliseconds. The system is programmed to take the process to a safe state when a diagnostic indicates an internal failure. The SIF response time to achieve a safe state is 50 milliseconds. The process safety time is 500 milliseconds. An average demand interval is 1 second. The following failure rate data are obtained for the equipment set by adding the failure rates of the categories of all components:
λ_{DD} = 8.5 * 10^{-6} failures per hour
λ_{DU} = 0.5 * 10^{-6} failures per hour
What SIL level is achieved by this design based on PFH requirements?
Answer: DI = 1 second and DTI = 100 milliseconds. DI = 10X DTI. This SIF is operating in high demand mode and will receive partial diagnostic credit. DTI plus the SIF response time equals 150 milliseconds which is within the process safety time of 500 milliseconds. Therefore, a portion of dangerous detected failures are likely to be converted to safe failures. Since the ratio of diagnostic rate to demand rate is 10, Equation 2 gives a credit for the diagnostics:

$$PDC \approx (\lambda_{Diag}/\lambda_{Demand})\,(1 - \exp[-\lambda_{Demand}/\lambda_{Diag}])$$
$$= 10 * (1-\exp[-0.1]) = 0.9516$$

Equation 3 is used to calculate the PFH:

$$PFH = (1 - 0.95) * \lambda_{DD} + \lambda_{DU}$$
$$= (0.05 * 8.5 * 10^{-6}) + 0.5 * 10^{-6}$$
$$= 0.925 * 10^{-6} \text{ failures per hour.}$$

That meets the requirements for SIL 2 per Table 3.

Average Probability of Failure on Demand - PFDavg

When a SIF operates in low demand mode, the probabilistic metric is PFDavg. Although many analysts rely on so called “simplified equations” to calculate PFDavg, it has become increasing clear that this approach is inadequate to compute realistic values of PFDavg. Simplified equations, such as those presented in IEC 61508 Part 6, contain only four of the nine variables known to impact the computed value of PFDavg. A companion white paper [5] details these nine key variables. Table 4 summarizes the key variables, their sources, and their applicability.

Of special note are the proof test coverage (C_{PT}) which measures the percentage of DU failures which can be discovered in proof testing and the site safety index (SSI) which adjusts the other key variables to reflect differences in maintenance and testing practices and safety culture in general from site to site. In [5], an example is provided which illustrates that under quite realistic parameter values, the decision to include only those parameters used in the "simplified equations" produces a value for PFDavg that is optimistic by a full SIL level compared to the PFDavg computed using all key variables! The authors strongly advise analysts to use certified or well vetted tools for the computation of PFDavg in order to obtain realistic values for PFDavg which support safe designs. The interested reader is referred to the latest version of [5] for full details.

Table 4. Summary of Key Variables for PFDavg Calculations

Variable Number	Description	Source	Applicability
1	Failure rates, λ_{DD} and λ_{DU}	Manufacturer	Always
2	Mission Time, MT	End User	Always
3	Proof Test Intervals, IT	End User	Always
4	Proof Test Effectiveness, C_{PT}	End User	Always
5	Mean Time to Restore, MTTR Note: MTTR = MRT + MDT see [9] for details	End User	For failures due to λ_{DD}, if automatic diagnostics do not trigger an automatic process shutdown For failures due to λ_{DU}, if proof testing is performed with process operating
6	Proof Test Duration, PTD	End User	If proof test performed with process operating
7	Probability of Initial Failure, PIF	End User	If equipment not 100% tested after installation
8	Site Safety Index, SSI	End User	Always
9	Redundancy / Common Cause	System Designer	HFT ≥1

Once PFDavg is appropriately determined, the corresponding SIL level for the SIF is provided by Table 5.

Table 5. SIL Level related to PFDavg

Safety Integrity Level	PFDavg Low Demand Mode of Operation
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$

SIL 1	**≥ 10^{-2} to < 10^{-1}**

Applying the 3 Barriers to Verify SIL Level for a High Pressure SIF

This section provides an example of applying the three barriers to a realistic low demand SIF example in order to verify the SIF SIL level. Table 6 provides the data required arranged according to the key variables for computing PFDavg. Table 7 summarizes the findings which are detailed below.

Table 6. Parameter values for key variables for high pressure SIF SIL verification example

Failure Rates (1/hr)						
		SD	SU	DD	DU	
Sensors						
	Safety Pressure Transmitter Composite[1] Certified SC 3	3.01E-7	1.74E-7	-	4.4E-8	
Logic Solver						
	Generic PLC2 (1oo2D) Certified SC 3	1.19E-5	1.36E-7	3.97E-6	2.50E-7	[10]
Final Element						
	Generic 3-way solenoid	-	1.01E-6	-	5.85E-7	[10]
	Generic Air Operated Ball Valve, Close on Trip Proven-in-use to SIL 2	-	5.00E-7	-	1.98E-6	[10]
Mission Time (MT)						
The equipment is expected to operate for 15 years before replacement and/or refurbishment and restoration in as new condition.						
Proof Test Interval (TI)						
Sensors	3 years					
Logic Solver	5 years					
Final Element	1 year					
Proof Test Coverage (C_{PT})						
Sensors	90%					[11]
Logic Solver	90%					[11]
Final Element	69%					[11]
Mean Time To Restore (MRT_{DD})						
Sensors	N/A automatic shutdown implemented for diagnosed failures					
Logic Solver	12 hours					
Final Element	N/A no diagnosed failures					
Proof Test Duration (PTD)						
All proof testing will be performed with the process shutdown implying PTD = 0 and MRT_{DU} = 0.						
Probability of Initial Failure (PIF)						
All components of the SIF are completely tested once installed implying PIF= 0.						
Site Safety Index (SSI)						
SSI 2 included in the failure rates						
Redundancy (HFT) / Common Cause (beta factor)						
Sensors	2oo3 / 2%					
Logic Solver	1oo2D / 2%					[10]
Final Element	1oo2 / 5%					
[1] Base failure rates are converted to standard failure rate categories assuming: high trip, internal transmitter detected failures are driven under range, all out of range values are detected and flagged as transmitter faults, trip delay is implemented to avoid false trips, all detected failures lead to automatic shutdown. [2] Individual module failure rates are combined into a single set of failure rates for the logic solver.						

Table 7. Summary of SIL Verification Calculations for High Pressure SIF Example

SIF Element	Overall SIL	Safety Integrity	Architectural Constraints	PFDavg	TI (years)
Sensors	3	Certified SC 3	HFT = 1 SIL 3	2.72E-05	3
Logic Solver	3	Certified SC 3	HFT = 1 SIL 3	1.95E-04	5
Final Element	2	Proven-in-use SIL 2	HFT = 1 SIL 3	7.21E-03	1
ENTIRE SIF	**2**	**SIL 2**	**SIL 3**	**7.43E-03**[1] **SIL 2**	

[1] The model used to compute PFDavg for this example contains both fail dangerous and fail safe states. The addition to the model of the fail safe state reduces the overall PFDavg and consequently, the PFDavg for the entire SIF is less than the sum of the individual PFDavg for each SIF element.

SC - Systematic Capability

As provided in Table 6, the transmitters and logic solver are devices certified to SC 3 while the final element is proven-in-use up to SIL 2. This allows the overall SIL to qualify per systematic capability to SIL 2.

SILac - Architectural Constraints

The SILac is verified using IEC 61508 Route 2_H. The sensor element of the SIF has a HFT of 1. Per Table 2, the sensor element may be used in SIF up to SIL 3. The logic solver element of the SIF has a HFT of 1. Therefore, per Table 2, the logic solver element may also be used in SIF up to SIL 3. The SIF's final element has a HFT of 1. Per Table 2, the final element may be used in SIF up to SIL 3. As a result, the SILac allows for the use of the SIF up to SIL 3.

SIF PFDavg Calculation

The PFDavg calculations were performed using SIL verification software [11]. Note that TI is different for each SIF element. The PFDavg for the entire SIF is 7.43E-03. The RRF is 135. Per Table 5, this qualifies for SIL 2 provided that, if a RRF is specified, it is less than or equal to 135.

Overall SIL Verification

Based on the outcomes of the three different constraint evaluations, i.e., Systematic Capability (SIL 2), SILac (SIL 3), and PFDavg (SIL 2), the entire SIF qualifies for use up to SIL 2. Even if

proven-in-use justification is provided for the final element up to SIL 3, the PFDavg limits the SIF. This is common if realistic failure rates are used.

Revision History

V0R1	Draft	Bukowski, van Beurden	July 2016
V1R1	Initial Release	Bukowski, Goble	December 2016
V2R1	Update	Goble	November 2017

References

1. IEC 61511, *Application of Safety Instrumented Systems for the Process Industries*, 2nd Edition, Geneva: Switzerland, 2016.

2. IEC 61508, *Functional Safety of electrical / electronic / programmable electronic safety related systems*, Geneva: Switzerland, 2010.

3. van Beurden, I. and Goble, W.M., *Safety Instrumented System Design: Techniques and Design Verification,* Research Triangle Park, N.C., International Society of Automation, 2018

4. Rutledge, P.J. and Mosleh, A., "Dependent-Failures in Spacecraft: Root Causes, Coupling Factors, Defenses, and Design Implications," *Proc. Ann. Reliability & Maintainability Symposium*, Washington, DC, January 1995, pp. 337-342.

5. Van Beurden, I. and Goble, W.M., *The Key Variables Needed for PFDavg Calculation,* exida White Paper, PA: Sellersville, www.exida.com, April 2017.

6. IEC 60300-3-2, *Dependability management - Part 3-2: Application guide - Collection of dependability data from the field,* Geneva: Switzerland, 2004.

7. ISO 14224, *Petroleum, petrochemical and natural gas industries -- Collection and exchange of reliability and maintenance data for equ*ipment, International Organization for Standardization, Geneva, Switzerland, 2016.

8. *Criteria for the Application of IEC 61508:2010 Route 2_H*, exida White Paper, PA: Sellersville, www.exida.com, December 2016.

9. Bukowski, J.V. and Goble, W. M., "Properly Crediting Diagnostics in Safety Instrumented Functions for High Demand Processes," *2017 Proceedings Annual Reliability and Maintainability Symposium*, Orlando, FL, January 2017, pp. 1-6.

10. Safety Equipment Reliability Handbook, Fourth Edition, exida.com LLC, PA: Sellersville, PA, USA, 2015, ISBN-13: 978-1-934977-156

11. exida exSILentia® SILver™ embedded proof test coverage calculator based on Safety Equipment Reliability Handbook data [10].

12. Yokogawa MAGLOG and Hima PLANAR

Appendix

This appendix presents the IEC 61508 Route 1H method for determining SILac which usually results in a SILac rating less than or equal to the SILac rating achieved using Route 2_H. Route 1_H must be used when quality field failure data are not available.

Some historical perspective regarding the development of the Route 1_H method of assessing architectural constraints is useful. Currently, Route 1_H distinguishes two types of devices, Type A and type B. Type A devices use technologies for which significant operational histories are available. Type B devices use new or newer technologies for which significant operational history is not available. Originally, the Route 1_H constraint was intended to apply only to Type B devices but was later extended to Type A devices.

In assessing the SILac that could be attained by an element (sensor, logic solver, or final element), and by extension by the entire SIF, based on architectural considerations, it became apparent that newer technologies, especially those incorporating automatic diagnostics, offered opportunities for greater safety based on how extensive the diagnostic capabilities were and how they were utilized. To account for this, Route 1_H was *initially* designed to set architectural constraints (determine the minimum SIF element HFT) for Type B equipment based on the ratio of $\lambda_{DD}/(\lambda_{DD} + \lambda_{DU})$ where the ratio was calculated based on all of the devices which comprised the SIF element. The ratio is often referred to as the dangerous diagnostic coverage and represents the percentage of dangerous failures that will be detected by automatic diagnostics. However, some technologies (which did not include automatic diagnostics at all) existed where almost all failures were safe failures [12]. The ratio $\lambda_{DD}/(\lambda_{DD} + \lambda_{DU})$ did not appropriately apply to these devices so a new metric, safe failure fraction (SFF), was devised. SFF was defined as

$$SFF = \left(\frac{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}}{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}+\lambda^{DU}}\right). \quad \text{(A.1)}$$

The SFF measures the natural tendency of a SIF device or element to fail safely or to detect dangerous failures, therefore, the greater the SFF the better. The SFF is calculated for each "element." Although there are disagreements as to what is included in an element, most consider an element to be a collection of devices that perform a sensing safety function, a logic solver safety function, or a final element safety function.

Based on the SFF, a look-up table provided the corresponding minimum HFT required for the various SILac. This table is reproduced below as part of Table A.1. Note how, for a given SFF

range, SILac begins with a SIL level for HFT = 0 and then the SIL increases by 1 for each increase in HFT (up to SIL 4). For example, for SFF 60% < 90%, in the portion of Table A.1 for Type B devices, the SILac begins at SIL 1 for HFT = 0 and increases by 1 SIL level each for HFT = 1 and HFT = 2. Recall that originally the Route 1_H method was intended only for use with Type B devices. Later, the Route 1_H method was extended to include Type A devices. The Route 1_H look-up table for Type A devices was derived from the Route 1_H table for Type B devices. Note that for a given SFF range the SILac for Type A devices begins with a SIL level for HFT = 0 that is 1 SIL level greater than the corresponding SILac assigned to Type B devices for HFT = 0 (except for Type A with SFF > 99% where some HFT is required for SIL 4). After that the SIL increases by 1 for each increase in HFT (up to SIL 4).

Table A.1. Minimum Fault Tolerance to Achieve SILac Based on SFF

SFF	TYPE A Minimum Hardware Fault Tolerance			TYPE B Minimum Hardware Fault Tolerance		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	Not allowed	SIL 1	SIL 2
60% < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

In order to illustrate the application of the Route 1_H method, it is first necessary to clarify the definitions of Type A and B devices. Devices are classified as Type A "if, for the components required to achieve the safety function:

- The failure modes of all constituent components are well defined; and
- The behavior of the subsystem [element] under fault conditions can be determined; and
- There is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met."

Examples of products typically classified as Type A include relays, solenoids, pneumatic boosters, actuators, valves and even simple electronic modules with resistors, capacitors, op amps, etc. The Type A language was meant to emphasize the need for failure data quality.

Any device that does not meet the Type A criteria is classified as Type B. Examples are devices with a microprocessor, complex Application Specific Integrated Circuits (ASIC), or other new technology components. These are classified Type B because of their complex designs in combination with a relatively short operational history for any given generation. By the time enough experience begins to accumulate, a new generation of technology is introduced!

The two examples of determining the SILac used in the body of the paper when IEC 61508 Route 2H was applied are repeated here for the purpose of comparison. Note that in each case, Route 2H produces a higher SILac rating than does Route 1H.

EXAMPLE A.1

A simple SIF was designed with a pressure switch hardwired to a two-way solenoid valve. The pressure switch opens on a high pressure demand and de-energizes the solenoid which will

take the process to a safe state. This SIF has no automatic diagnostics, no complex new technology, and both devices are considered Type A. The failure rates are given below.

Pressure Switch:

$\lambda^{SD} = 0 * 10^{-6}$ failures per hour

$\lambda^{SU} = 2.4 * 10^{-6}$ failures per hour

$\lambda^{DD} = 0 * 10^{-6}$ failures per hour

$\lambda^{DU} = 3.6 * 10^{-6}$ failures per hour

(NOTE: the terms detected and undetected refer to failures diagnosed by automatic diagnostics not those detected by the overt false trip of the SIF.)

Solenoid Valve:

$\lambda^{SD} = 0 * 10^{-6}$ failures per hour

$\lambda^{SU} = 1.8 * 10^{-6}$ failures per hour

$\lambda^{DD} = 0 * 10^{-6}$ failures per hour

$\lambda^{DU} = 1.2 * 10^{-6}$ failures per hour

(NOTE: the terms detected and undetected refer to failures diagnosed by automatic diagnostics not those detected by the overt false trip of the SIF.)

According to the architecture limits of IEC 61508, Route 1_H to what SIL does this SIF design qualify?

Answer: The sensor element consists of one switch, Type A. It has HFT of 0 since one dangerous failure will fail the SIF. The SFF is 40% ($2.4*10^{-6}$ / ($2.4 * 10^{-6} + 3.6 * 10^{-6}$)). According to Table A.1, the sensor element qualifies for SIL 1.

The final element subsystem consists of one solenoid valve, Type A. It has a HFT of 0. The SFF is 60% ($1.8 * 10^{-6}$/($1.8 * 10^{-6} + 1.2 * 10^{-6}$)). According to Table A.1, the final element qualifies for SIL 2. The overall design is qualified to SIL 1 since the lowest SIL level element (sensor element) is the limiting factor. Note how this result differs from that of Example 1 based on Route 2_H.

EXAMPLE A.2

Two microcomputer based transmitters have been chosen for a SIF sensor element design. The logic solver is programmed to trip if either transmitter indicates a dangerous condition (1oo2). The manufacturer's data sheet for the transmitter lists the SFF as 78.4%. To what SIL level is this sensor element design qualified per IEC 61508, Route 1_H HFT requirements?

Answer: The sensor devices are of Type B. The sensor design has a HFT of 1 since one transmitter can fail dangerously and the SIF can still perform the safety function. The SFF is between 60% and 90%, therefore the sensor element design qualifies for SIL 2. Note how this result differs from that of Example 2 based on Route 2_H.

Recall that the reasoning behind adding architectural constraints in the first place was the concern that some analysts would produce unrealistically low (optimistic) failure rates leading to optimistic values for PFDavg and unsafe designs. Architectural constraints were a defense against unrealistically low failure rates. Now note that the Route 1_H method ultimately relies on failure rates to determine minimum HFT requirements. Thus this method potentially suffers from the same concerns that were raised about PFDavg.