High and Continuous Mode SIFs: SIL Assessment

1. Introduction

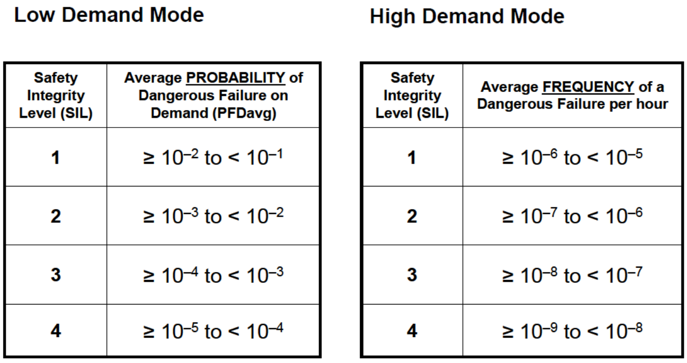
Demand on a protective function is an event scenario resulting from a failure in the process, equipment or control function that require specified safety action to be taken by the protective (safety) function. ‘Demand mode’ classification describes a safety system in terms of the frequency of demand or how often the system is activated. This means the likelihood or frequency at which safety system is required to act in order to avert a hazardous event. Safety instrumented functions (SIFs) are classified as low demand, high demand and continuous demand mode functions. Why this classification is important for safety systems? Risk based implementation of safety systems relies on design of the safety system on the basis of the safety integrity level of the SIF. SIL of a safety function is a measure of its reliability. The reliability evaluations and the SIL definitions are different for the three modes of demand. Here is a discussion how the demand interval impacts the SIL definition and the process of SIL selection.

2. Understanding system reliability or safety integrity level

Safety integrity of a system is its reliability over a time period of interest, which is usually measured as an average value over the system test period. Reliability is often specified as the average probability of failure, which is less abstract and measurable. Safety systems are assumed to be periodically tested to maintain its performance reliability at a required high value or to limit its failure probability at a low value. Demand on this system initiates activation of the system to avert an imminent hazard scenario. When a demand interval is larger than the system test interval, the periodic testing contributes to the reliability or safety integrity of the system and average failure probability is a correct measure of system safety integrity or reliability. These are called low demand functions. When the demand interval is shorter than the proof test interval, benefit of testing cannot be attributed to the system reliability. Here a time average of failure probability cannot be a measure, instantaneous reliability or failure rate (failure/hour) need to be considered. These are called high demand systems. Continuous mode functions are specific high demand functions where a constant demand is always present for the safety system or safety function.

Hence there are two sets of definitions for safety integrity level in functional safety standards, one for low demand safety functions and the other covers both high and continuous demand safety functions.

Reference IEC 61511/61508 Tables for Safety Integrity Levels.



Low Demand Mode

Safety Integrity Level (SIL)	Average PROBABILITY of Dangerous Failure on Demand (PFDavg)
1	$\geq 10^{-2}$ to $< 10^{-1}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
4	$\geq 10^{-5}$ to $< 10^{-4}$

High Demand Mode

Safety Integrity Level (SIL)	Average FREQUENCY of a Dangerous Failure per hour
1	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-9}$ to $< 10^{-8}$

More accurate definitions for low demand, high demand and continuous demand modes follow.

3. Definitions of demand on safety functions as per IEC 61508/ 61511

Safety instrumented functions in the process industry are predominantly low demand functions. These are emergency shutdown functions in other words, which comes in to action as safeguards whenever a failure in the equipment, operator error or a failure in the continuous control (basic process control system) occurs. Low demand functions typically have a demand rate lesser than once a year. Demand interval for low demand functions shall be higher than twice the test interval, as per definition. High demand functions have a demand rate greater than once a year. Also if the demand interval is shorter than half the proof test interval, it is considered as high demand. Continuous safety functions are high demand functions with a continuous frequency of activation of the SIF, which means that a failure of SIS itself causes a hazardous event.

The definitions as given in IEC 61508 and IEC 61511 standards for Low demand, high demand and continuous demand functions are:-

	IEC61508:2010	IEC61511:Ed.2
Low Demand	where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or	Mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year
High Demand	where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year	mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demand is greater than one per year
Continuous Demand	where the safety function retains the EUC in a safe state as part of normal operation	mode of operation where the SIF retains the process in a safe state as part of normal operation

IEC 61511 Ed.1 standard had a deviant definition, which combined high demand and continuous safety functions, considering that both the functions behave the same way in terms of demand frequency and the SIL assignment for both functional shall be similar. Edition 2 of IEC 61511 however retains the distinct definitions and identifies ‘high’ and ‘continuous’ demand functions separately similar to that in IEC 61508 standard.

Low demand functions are usually activated when a continuous process control function fails.

Summarising from the above, characteristics of Low demand functions are

>> Demand interval greater than one year;

>> Demand interval is larger than twice the proof test interval;

>> SIF failure alone will not lead to a hazardous event.

High demand functions are also activated when there is a failure in a basic control or regulatory functionality, however these are characterised by

>> Demand interval less than a year;

>> Demand interval is closer to or less than the proof test interval;

>> SIF failure alone will not lead to a hazardous event.

Continuous safety functions are acting upon a safety demand in a continuous manner, by establishing a safe state each time there is an operational deviation. These can be called continuous control safety functions.

>>Continuous demand on safety system;

>> SIF failure alone can lead to a hazardous event.

4. SIL level for high demand or continuous functions

Methods to assess SIL levels for low demand functions are clearly identified in the standards and well established, example LOPA technique. Techniques for assessing SIL levels for high demand and continuous safety functions are not discussed in the standards.

Why an event tree or LOPA cannot be used for High demand functions?

Frequency calculation used for LOPA has a limitation when the demand frequency gets higher.

LOPA equation for mitigated frequency Fmitigated, considering a simple scenario having a single Independent Protection Layer (IPL) is

Fmitigated = Finitiating * IPL PFD

This holds good for all low demand scenarios, i.e. for all initiating event frequencies (Finitiating) <1 per year. PFD is the probability of failure on demand of the IPL

When the demand frequency is 1 in a year

Fmitigated = 1 * IPL PFD

This means that mitigated event frequency is the same as the IPL failure probability. So far the equation holds good. When the event frequency is higher, say 2 per year

Fmitigated = 2 * IPL PFD

This means that the mitigated frequency is higher than the IPL PFD which is incorrect as the IPL limits the occurrence of the hazardous event to the probability of its own failure and a higher probability of an undesired event is not possible, irrespective of the demand rate.

Hence usual LOPA equations cannot be applied to high demand or continuous demand safety functions.

5. Assessment of integrity level for a High Demand SIF

SIL assessment shall carefully evaluate the scenarios when the demand rate is higher than once per year. Study requires a more detailed analysis of event propagation and the action of the existing protection layers than that required for LOPA. First evaluate the initiating event and demand frequency and then the protection layers. If the SIF is the first layer of protection, then the SIF shall be evaluated like a high demand function, however if there is another IPL and activation of that IPL is chronologically ahead of the SIF when the scenario propagation is evaluated, then the high demand is seen and mitigated by the first IPL. Here the LOPA model is still valid, however the frequency calculation needs some adjustments as the demand encountered by the SIF is only the failure frequency of the first IPL. The equation for SIL calculation shall be as below.

Example: Figure 1

Fmitigated = Finitiating * IPL1PFD * IPL2 PFD

When the demand frequency 'Finitiating' is >1 demand rate calculation will be incorrect as seen earlier. Demand on the SIF (IPL2) will be the actual failure rate of IPL1. Hence demand on SIF remains still < 1, i.e. the failure rate of IPL1, assuming the PFD of IPL1 < 1.

Fmitigated = IPL1 failure rate * IPL2PFD

When SIF is the only IPL, or is the first IPL to activate when there is a demand initiated, this is an actual high demand SIF and the SIL level is determined as below.

Example:

Scenario considered is a flare knock out drum pressure protection function. Vapour recovery line is provided connected from the flare knock out drum and a vapour recovery compressor further sends out the compressed gases to a downstream section of the plant. A specific demand scenario is unplanned or spurious shutdown of the downstream section or the vapour recovery compressor trip. This was estimated as 5 times a year. The vessel is provided with a pressure high high shutdown function and a PSV which is fully sized to mitigate the high pressure scenario due to downstream blockage. There is no pressure control provided for the knock out drum.

Due to any of the demand scenarios, the pressure starts rising and the high high pressure protection function opens a diverter valve to flare line.

Frequency equation is as below.

Finitiating = 5/ year

Fmitigated = 5 * IPL1PFD * IPL2 PFD

= 5 * SIF PFD * PSV PFD

Since the demand rate is >1, above equation will be incorrect; as this implies that the demand frequency on the second IPL is higher than the PFD of the first IPL. Hence the equation can be re-written as below:

Fmitigated = SIF (failure frequency) * IPL2 PFD

To assess the SIL required for the SIF we have to use the SIL definition table for high demand functions from IEC 61508/61511.

Residual (gap) Frequency = Ftolerable frequency / Fmitigated

$$= F_{tolerable} \text{ frequency} / IPL2_{PFD}$$

If Tolerable frequency is 1E-06, and PFD of IPL2 is 0.1

Residual (gap) frequency, which is the dangerous failure frequency of the SIF shall be

$$= 1.E\text{-}06 / 0.1$$

$$= 1.0E\text{-}05$$

As per the IEC 61511 Table for high demand SIL, this frequency corresponds to a SIL level of SIL-1.

6. Assessment of integrity level for a Continuous safety function

For a continuous demand function, the demand rate is much higher. SIL assessment for continuous safety function shall be exactly same as the method described above for high demand SIFs, as it can be seen that the initial demand rate has no impact on the assessment, as the failure frequency of the IPL shall decide the risk reduction requirement, irrespective of the initial demand frequency. However continuous safety functions are very rare in the process industry as most of the process deviations or demands are met by a control function.

7. Summary

It is important to correctly assess the demand mode of a safety function. If a high demand scenarios is wrongly assessed as a low demand SIF the resulting SIL requirement will be higher which will lead to improper implementation and maintenance requirements.

Lower the demand on the safety function, easier to achieve the high reliability requirements and also better maintainability. For low demand systems internal diagnostics and proof tests can be utilised to maintain the system highly reliable and available throughout the lifecycle. For high demand SIFs proof test intervals cannot ensure required reliability. If diagnostic intervals are short enough, diagnostic credit can be considered for system reliability. Standard requires a two order of magnitude higher frequency for diagnostic tests to be able to account them as reliable means to detect and take corrective action for the dangerous faults. For continuous mode safety functions both proof tests and diagnostic tests cannot be considered as improving the system reliability.

Higher demand systems may be carefully reviewed for lowering the demand frequency by improving the design eg., by adding an intermediate layer of protection or by decreasing the demand frequency itself.