Device Selection Process for Your SIF

To determine whether an approved device can meet the required SIF for use in a SIL, there are three factors which must be assessed to arrive at a final device SIL Capability:

- **Probability of Failure on Demand (PFDoD)**
- **Architectural Constraint (Silac)**
- **Systematic Capability (Silsc)**

### Information to determine these SIL capabilities can be found in the IEC 61508 approved device's safety certificate and FMEDA report.

Upon assessing these three factors the device’s SIL Capability for a SIF is based on the lowest of the Silac, Silsc or PFDoD. For example, if Silac and PFDoD achieve SIL 3 but the Silsc is SIL 2 then the device can only be applied in SILs up to SIL 2.

### Device SIL Capability

![Silac and Silsc Diagram](Image)

- **Silac** - **Architectural Constraint**
  - **Silsc** - **Systematic Capability**

#### SILsf - Probability of Failure on Demand

The PFDoD (PFH for high demand applications) is calculated for each instrument (or set of instruments for redundant architecture) based on the architecture, dangerous failure rate and proof test interval. The sum of PFDoD (PFH) for all instruments in the SIL limits the maximum permissible SIL.

#### PFD/PFH Requirements for Safety Instrumented Functions

<table>
<thead>
<tr>
<th>SIL</th>
<th>Average Probability of Failure on Demand (PFDoD)</th>
<th>Resistance Factor (RFR)</th>
<th>Average Frequency of a Dangerous Failure per Hour (PFH)</th>
<th>Resistance Factor (RFR)</th>
<th>Average Frequency of a Dangerous Failure per Hour (PFH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>0.1-1.0</td>
<td>10-100</td>
<td>0.000001-0.0000001</td>
<td>100,000-1,000,000</td>
<td></td>
</tr>
<tr>
<td>SIL 3</td>
<td>0.000001-0.0000001</td>
<td>1,000-10,000-100,000</td>
<td>0.0000001-0.000000001</td>
<td>1,000,000-10,000,000</td>
<td></td>
</tr>
<tr>
<td>SIL 4</td>
<td>0.0000001-0.000000001</td>
<td>10,000-100,000</td>
<td>0.0000000001-0.0000000001</td>
<td>10,000,000-100,000,000</td>
<td></td>
</tr>
</tbody>
</table>

#### Device SIL Capability

- **Silac** - **Architectural Constraint**
- **Silsc** - **Systematic Capability**

The SIL is limited by the instrument device type (A or B). Safe Failure Function (SFF) and Hardware Fault Tolerance (HFT) in the SIL.

#### Safety Failure Function (SFF)

The use of the average failure rate for any dangerous detected failure and safe plus false failure.

<table>
<thead>
<tr>
<th>SFF Type</th>
<th>Probability of Failure (PF)</th>
<th>Probability of False Failure (PFH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type A</td>
<td>≤ 0.01</td>
<td>≤ 0.01</td>
</tr>
<tr>
<td>Type B</td>
<td>≤ 0.001</td>
<td>≤ 0.001</td>
</tr>
<tr>
<td>Type C</td>
<td>≤ 0.0001</td>
<td>≤ 0.0001</td>
</tr>
</tbody>
</table>

#### SILsf - Systematic Capability

This is defined on the Certificate as the Systematic Capability or Systematic Integrity level. This corresponds directly to the device’s maximum SIL capability.

### Device Selection via Proven In Use

When instrument do not have SIL capabilities are defined via Proven In Use as follows. The proven-in-use data must be verified that the Proven In Use data is drawn from similar applications and environmental conditions.

#### Determining what SIL (Safety Integrity Level) each SIF (Safety Instrumented Function) Needs

<table>
<thead>
<tr>
<th>SIL</th>
<th>SILac</th>
<th>SILsc</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>SIL 1</td>
<td>SIL 1</td>
</tr>
<tr>
<td>SIL 2</td>
<td>SIL 2</td>
<td>SIL 2</td>
</tr>
<tr>
<td>SIL 3</td>
<td>SIL 3</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SIL 4</td>
<td>SIL 4</td>
<td>SIL 4</td>
</tr>
</tbody>
</table>

#### Beta Factor (β)

- The percent of the failures that are associated to common cause failures modes.
- The factor by which the SIL capacity is reduced due to the presence of common cause failures.
- The Beta Factor is a function of the reliability of individual components of the system and is a measure of the system's inherent risk.

#### Overall Risk Reduction Strategy

- The overall risk reduction strategy is the product of the SIL capacity and the Beta Factor (β).
- The Beta Factor should be considered as a measure of the inherent risk of the system. It is typically defined as the ratio of the average failure rate with common cause failures to the average failure rate without common cause failures.
- The Beta Factor is used to determine the SIL capacity of a system. The SIL capacity is the minimum SIL level that is required to achieve the overall risk reduction strategy. The SIL capacity is determined by dividing the overall risk reduction strategy by the Beta Factor.

### Additional Resources

- [IEC 61508 - Functional Safety](https://www.iec.ch/functionalsafety/)
- [Further Reading on Safety Instrumented Systems](http://www.isa.org/moree/)
- [Moore Industries Worldwide](http://www.moore.com/safetysystems/)

### Functional Safety - A to Z Glossary

- **Architectural Constraints (Silac)** - Limitations imposed on the components and architecture selected for implementation of a safety instrumented function (SIF). Architectural constraints are determined through an analysis of the environment and system requirements.
- **Beta Factor (β)** - The percent of the failures that are associated to common cause failures modes.
- **Common Cause Failures (CCF)** - Failures that occur when two or more components fail simultaneously due to a single event. CCFs are typically caused by system-level events such as power failures or hardware failures.
- **Device SIL Capability** - The lowest SIL capability that a device can achieve.
- **Device Selection via Proven In Use (Silpd)** - A method of selecting devices for safety-critical applications based on proven performance in similar systems.
- **Hazard and Operability Study (HAZOP)** - A structured technique used to identify and analyze potential hazards in a system.
- **Hardware Fault Tolerance (HFT)** - A method of designing safety-critical systems to ensure that the system can continue to operate properly even in the event of a hardware failure.
- **ISGS** - Industry Safety Group System.
- **MTBF** - Mean Time Between Failures.
- **PFDAVG** - Probability of Dangerous Failure per Hour (PFH) averaged over the lifetime of the system.

### Further Reading on Safety Instrumented Systems

- **IEC** - International Electrotechnical Commission
- **ISA** - Instrumentation, Systems, and Automatics Society of America

---

**Demand Moore Reliability**

Ask your local sales representative for a full 24x2 36 poster