Johnson Controls
Functional Safety - SIL2

Why Functional Safety

On July 10, 1976, an accident occurred in a chemical factory in a small town called Seveso in northern Italy. As a result of this accident, high toxic dioxin (TCDD) was rapidly released into the environment. The environment and people have suffered great harm as this substance enters the air. The main reason for this boiler is uncontrolled high heating and subsequent high pressure damage to the safety devices.
The lack of an automatic cooling system of the reactor and the absence of experienced chemical workers in the field and at the factory are also important reasons when an accident occurs.
The only pleasing situation in this accident was that the leaked toxic gas was not at very high levels.
Following the Seveso accident, various directives and regulations were made to protect people and the environment. In the eighties, as a result of the Seveso experience, the European community began to implement regulations that would lead to drastic changes through various sanctions on dangerous areas.

And as a result of all these studies, important standards such as IEC 61508 and IEC 61511 have emerged. Risk definition has been made with these standards and regulations have been made in this direction.

Functional Safety

Freedom from unacceptable risk of physical injury or of damage to the health of people

Risk management typically uses the ALARP (as low as reasonably practicable) principle to define tolerable risk.

For example Fire Detection System

Detection of smoke/heat/CO by Detectors and activate a fire suppression system

Standards associated with Functional Safety

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety related systems (SRS)

- **IEC 61511** Safety instrumented systems for the process industry sector
- **IEC 61513** Nuclear industry
- **IEC 62061** Safety of machinery

Safety-Related System - SRS

A safety-related system (SRS) provides functions which significantly reduce the risk of a hazard, and in combination with other risk reduction measures, reduces the overall risk to a tolerable level

Process instruments are components of a SRS.

This comprises the significant components of a complete safety-relevant process unit:

- Sense
- Logic
- Actuate

All units together constitute an SRS

Safety Instrumented Functions (SIF)

A SIF is made of 5 elements – Sense, Logic, Actuate, Timing, SIL (SLATS)

Sense
On activation of the call point

Logic & Actuate
The fire alarm panel will activate the relevant evacuate output group

Timing
Immediately sounding the evacuate sounder

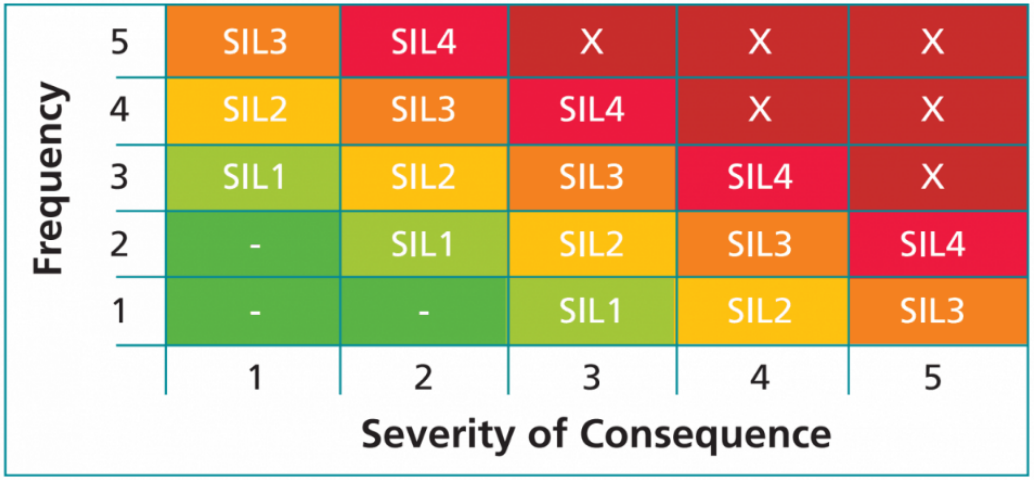
SIL
The Safety Integrity Level of this Safety Instrumented Function is SIL2

Single complete system/loop (SIF)

Sub-System | Sub-System | Sub-System

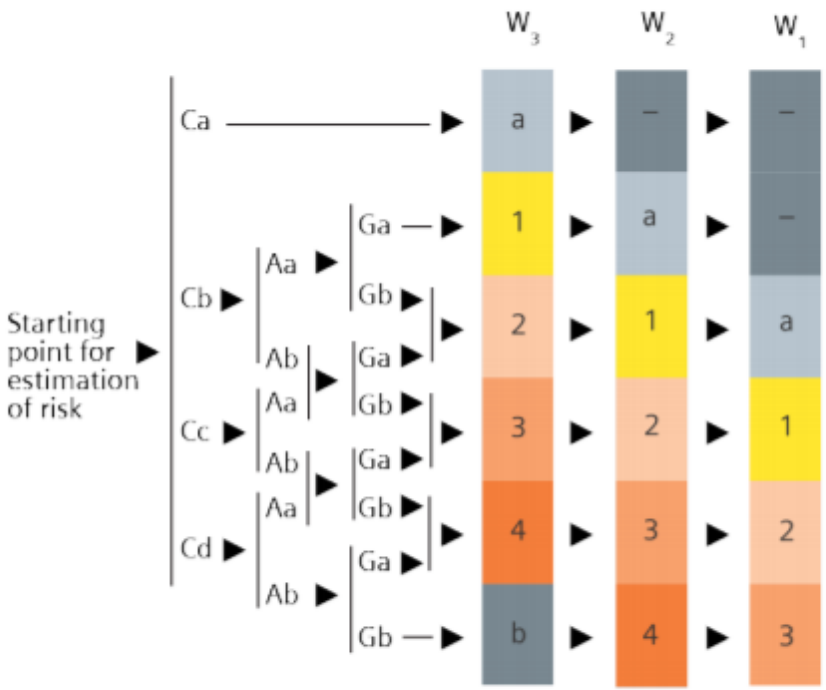
Determination of SIL

- Different risks originate from plants or plant components
- As the risk increases, the safety-related system (SRS) also increase.
- The standards IEC 61508 and IEC 61511 defines four different SIL's
- **SIL Level is a function of hazard frequency and hazard severity. Hazards that can occur more frequently or that have more severe consequences will have higher SIL Levels.**



Determination of SIL

Determination of SIL according to the "qualitative method":



a: no special safety requirements
b: a single SIS is sufficient
1,2,3,4: safety integritiy level (SIL)

Extent of damage	
Ca	Light injury of a person, small environmental damage
Cb	Severe injury or death of a person
Cc	Death of several persons
Cd	Death of very many persons
Duration of stay of a person in the damaged area	
Aa	Seldom to frequent
Ab	Frequent to permanent
Aversion of danger	
Ga	Possible under certain conditions
Gb	Hardly possible
Probability of occurence	
W1	Verly low
W2	Low
W3	Relatively high

SIL Probabililty

SIL Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> %99.99	%0.001 to %0.01	100000 to 10000
SIL 3	%99.9 to %99.99	%0.01 to %0.1	1000 to 1000
SIL 2	%99 to %99.9	%0.1 to %1	100 to 100
SIL 1	90% to %99	%1 to %10	10 to 10

Category	Typical SIL	Consequence upon failure
Catastrophic	4	Loss of multiple lives
Critical	3	Loss of a single life
Marginal	2	Major injuries to one or more persons
Negligible	1	Minor injuries at worst or material damage only
No consequence	0	No damages, except user dissatisfaction

Why is it important to be SIL2 compliant

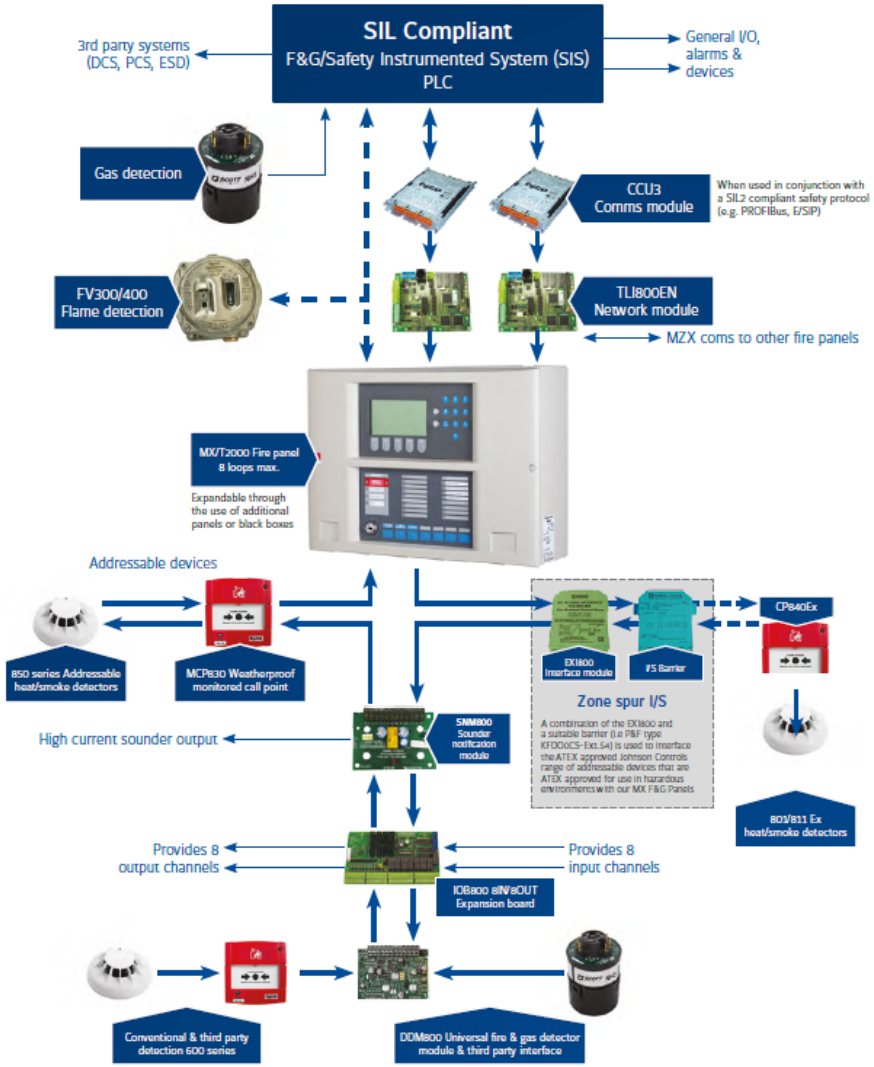
Certification

The International Electrotechnical Commission's (IEC) standard IEC 61508 defines SIL using requirements grouped into two broad categories:

- Hardware safety integrity
- Systematic safety integrity

Device /system must meet requirements for both cat. to achieve a given SIL.

The SIL2 rated complete solution



What does SIL2 mean to a fire system

Each element of a SIL rated safety function must have a calculated probability of failure on demand. All sub components are included in the safety calculation.

Evidence of these safety calculations in the form of a Safety Analysis Report (SAR) is critical in proving functional safety compliance.

Independent certification body (e.g. are TUV, ESC, EXIDA,SIRA).