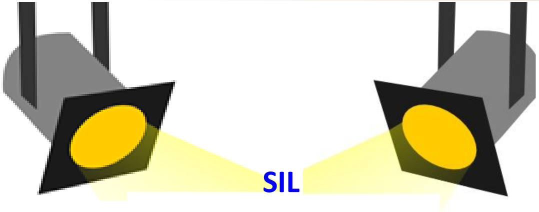
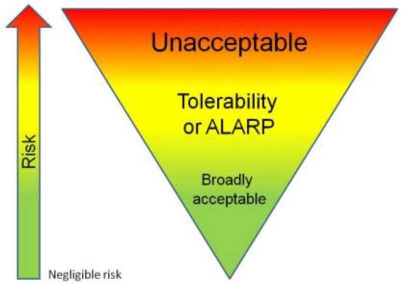


What is Safety Integrity Level (SIL) ?

SIL means how we measure the performance of safety functions carried out by safety instrumented system (SIS) OR The amount of risk reduction that an SIS can provide. The SIL is the key design parameter **specifying the amount of risk reduction that the safety equipment is required to achieve** for a particular function in question. If an SIL is not selected, the equipment cannot be properly designed because only the action is specified, not the integrity. Best equipment design requires two types of specifications : a specification of **what the equipment does** and a specification of **how well the equipment performs that function**. The safety integrity level addresses this second specification by indicating the minimum probability that the equipment will successfully do what it is designed to do when it is called upon to do it. Safety integrity levels (SILs) are categories based on the probability of failure on demand (PFD) for a particular safety instrumented function (SIF).
SIL requirement is reviewed based on Which is critical system ? How repaired or maintained ? and How built ?

SAFETY INTEGRITY LEVEL (SIL)	LOW DEMAND MODE OF OPERATION (Probability of failure to perform its designed function on demand)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Probability of one dangerous failure per hour)
4	>= 10^{-5} up to < 10^{-4}	>= 10^{-9} up to < 10^{-8} h^{-1}
3	>= 10^{-4} up to < 10^{-3}	>= 10^{-8} up to < 10^{-7} h^{-1}
2	>= 10^{-3} up to < 10^{-2}	>= 10^{-7} up to < 10^{-6} h^{-1}
1	>= 10^{-2} up to < 10^{-1}	>= 10^{-6} up to < 10^{-5} h^{-1}
	PFD	PFH
	Probability of Failure on Demand	Probability of Failure per Hour

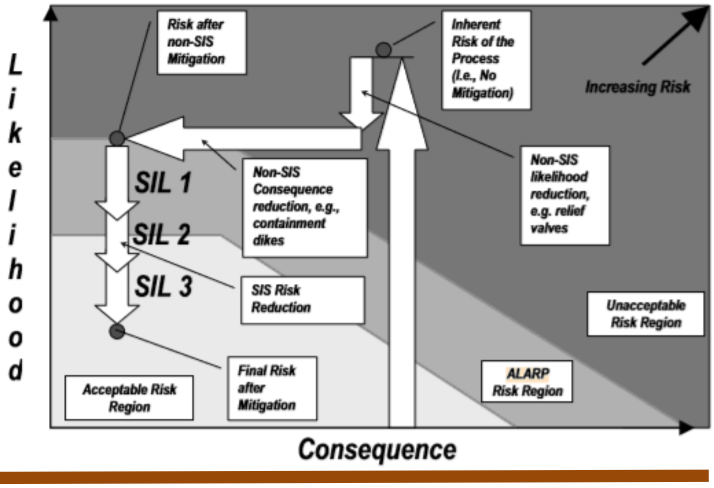


Risk & the need for Company's Safety Target :

- There is no such thing as zero risk. This is because **no physical item has a zero failure rate, no human being makes zero errors and no piece of software design can foresee every possibility.** Therefore defining and accepting a tolerable risk for any activity prevails.

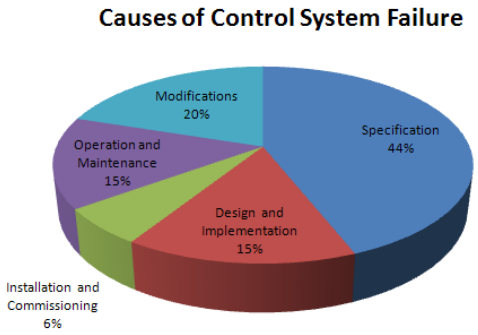
As Low As Reasonably Practicable (ALARP):

- The philosophy of dealing with risks that fall between an upper and lower extreme. The upper extreme is where the risk is so great that it is refused altogether, while the lower extreme is where the risk is, or has been made, so small as to be insignificant. This philosophy considers both the **costs and benefits of risk reduction** to make the risk "as low as reasonably practicable."
- The three levels of risk are "Unacceptable" where the risk should not be undertaken at all, the "ALARP" region where practical risk reduction is required, and the "Broadly Acceptable" region where the risk is already acceptable and no further reduction needs to be considered.


Likelihood
Risk after non-SIS Mitigation
Inherent Risk of the Process (I.e., No Mitigation)
Increasing Risk
SIL 1
SIL 2
SIL 3
Non-SIS Consequence reduction, e.g., containment dikes
Non-SIS likelihood reduction, e.g. relief valves
SIS Risk Reduction
Unacceptable Risk Region
Final Risk after Mitigation
ALARP Risk Region
Acceptable Risk Region
Consequence

Functional Safety :

Functional safety involves identifying specific hazardous failures which lead to serious consequences (e.g. Death) and then establishing maximum tolerable frequency targets for each mode of failure. It is part of the overall safety of the system or piece of equipment that depends on the system or equipment which is operating correctly based on its inputs (incorporating safe operation of human error, Hardware failure and surrounding conditions).



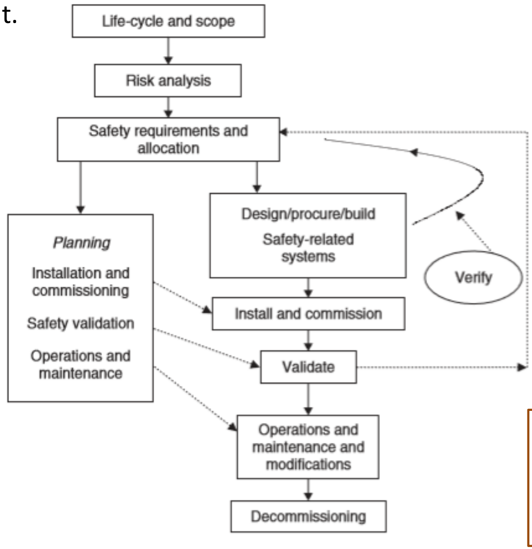
From this figure it is very clear major system failures are because of **specifications (44 %).**

Assessment of SIL:

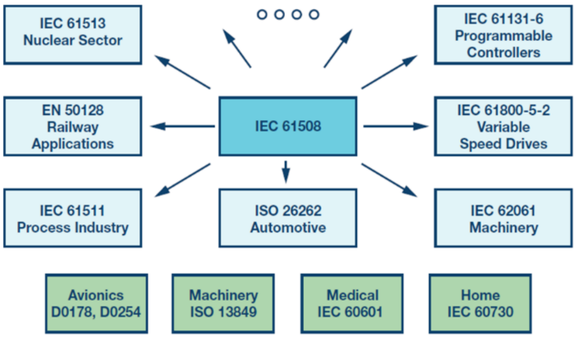
SIL	Assessed by
4	Independent organisation
3	Independent department
2	Independent person
1	Independent person

Life Cycle Approach & Standards :

The various life-cycle activities and defences against systematic failures, necessary to achieve functional safety, occur at different stages in the design and operating life of any equipment.



IEC 61508 is the base standard and referred in case where no functional safety standard exists. For process industry IEC 61511 is important.



Safe State : The state of the equipment under control (EUC) when there is **freedom from unacceptable risk.**

Safety Instrumented Function (SIF) : A function with a specified safety integrity level, which is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event. **5 Basic properties are Sense, Logic, Actuate, Timing and Safety Integrity.**

Safety Instrumented System (SIS) : A set of sensors, logic solvers, and actuators designed to carry out one or more safety instrumented functions.

Safety Integrity Level (SIL) : Discrete level (one out of a possible four) for specifying the probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all of the stated conditions within a stated period of time. **Safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.**

Safety Requirements Specification (SRS) : Specification containing all of the requirements of the safety functions that have to be performed by the safety related systems.

Hazard Identification, Hazard Analysis and Determining required Risk Reduction are important steps for SIL Selection.

All previous Newsletters are available in download section of our website (www.nexapsm.com).