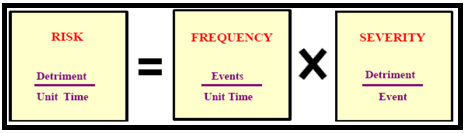
Safety Integrated Level ( SIL ) Verification

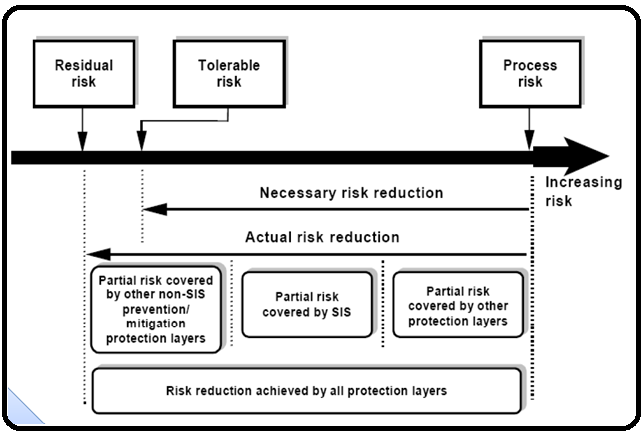
General Definition

What is risk?

A Risk is the amount of harm that can be expected to occur during a given time period

due to specific harm event.





Safety related system consists of:

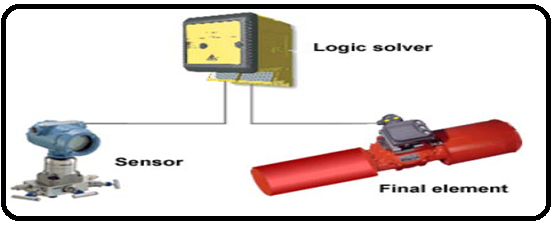
* Mechanical protection system
* Passive protection system
* Basic process control system
* Alarms
* Safety instrumented system (SIS)

What is SIS?

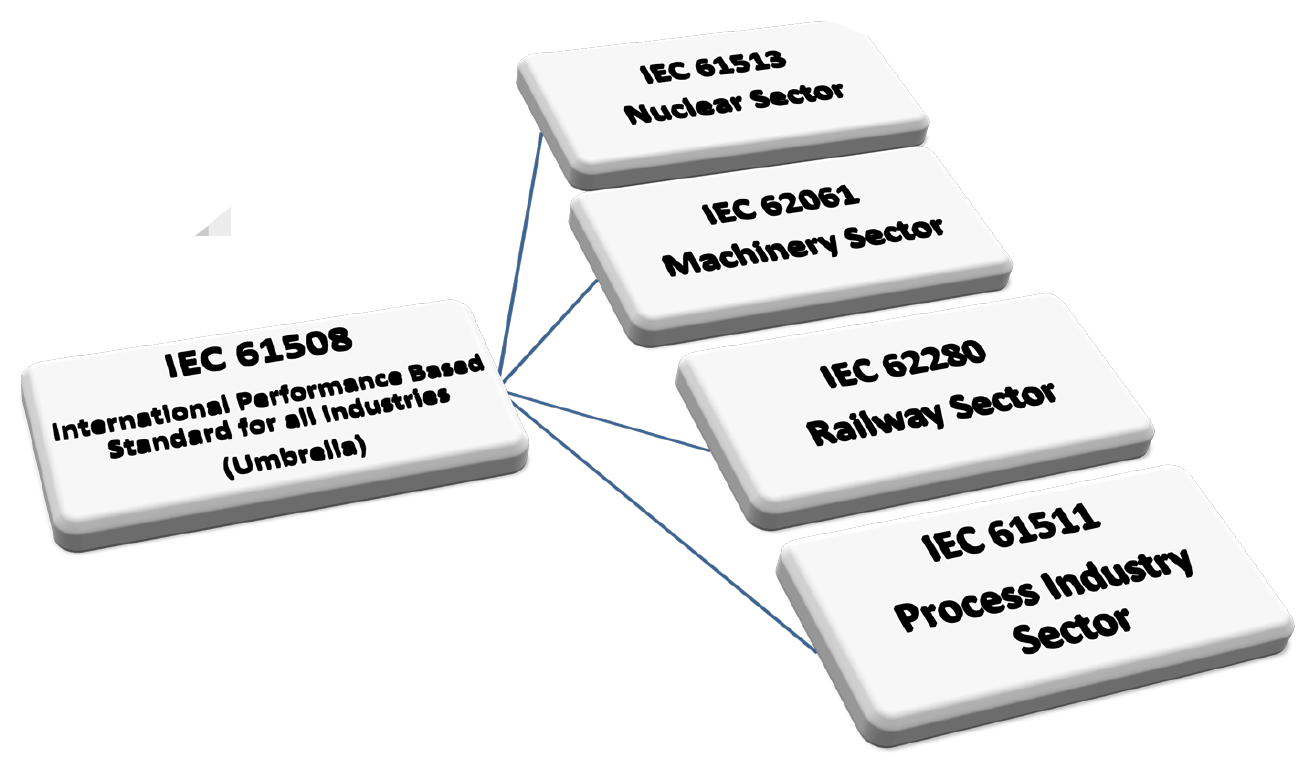
A relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).

Notes

1. The function of SIS is called SIF. More than one SIF could be allocated to a SIS.
2. A SIS consists of a sensor, logic solver and final element.



1. The ability of a SIS is to carry out the actions necessary to achieve a safe state in process.
2. Standards: IEC-60508 for general industry and IEC-60511 for oil and gas industry.



IEC-61508:

Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems

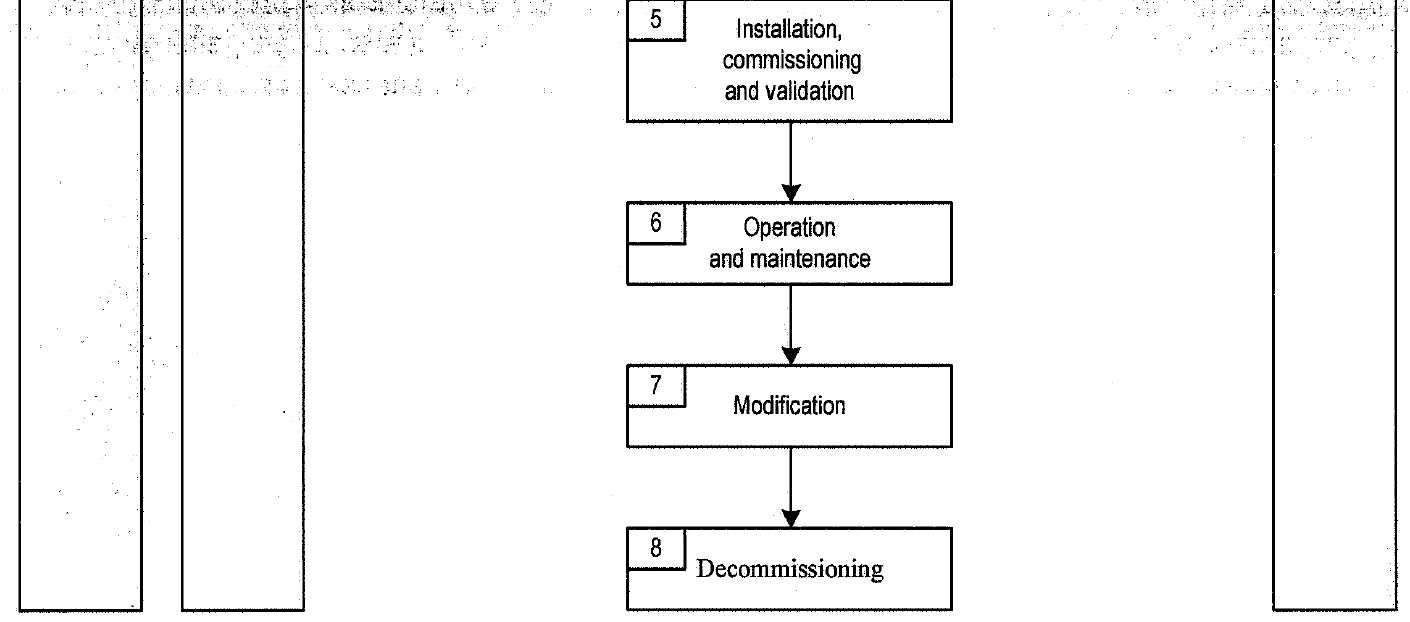
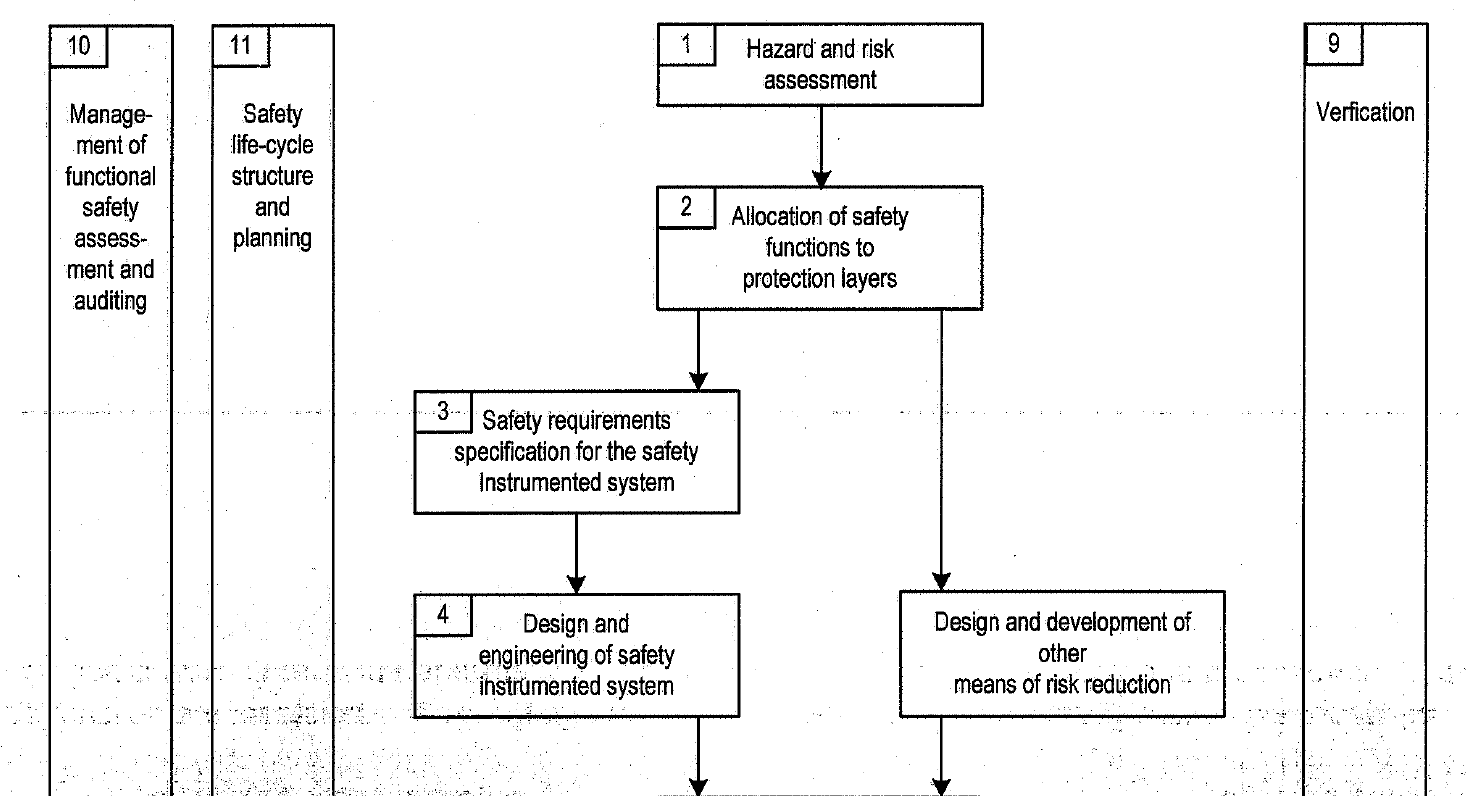
IEC-61511:

Functional safety –safety instrumented systems for the process industry sector

ANSI ISA-84.00.01:

Application of Safety Instrumented Systems for the Process Industries





Stages of SIL Study

1.Target SIL Evaluation

What SIL should be allocated for the SIF?

2.SIL Verification

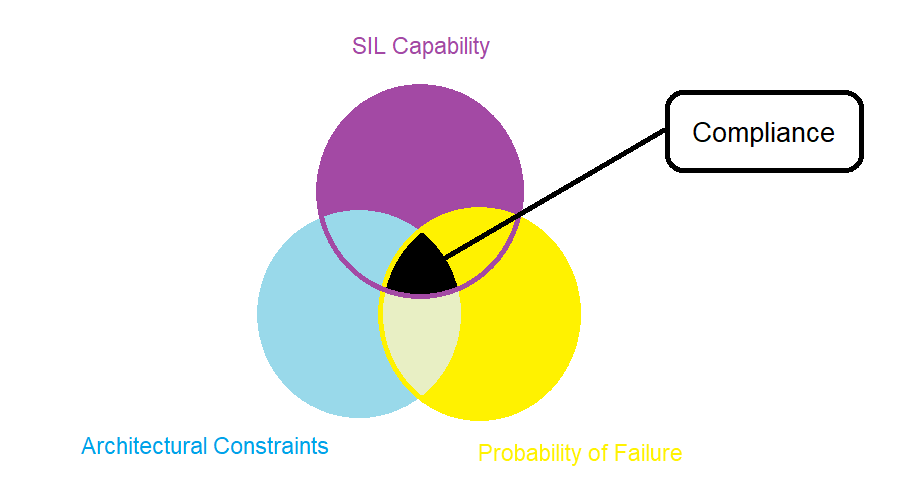
Does SIS fulfill Target SIL requirements?

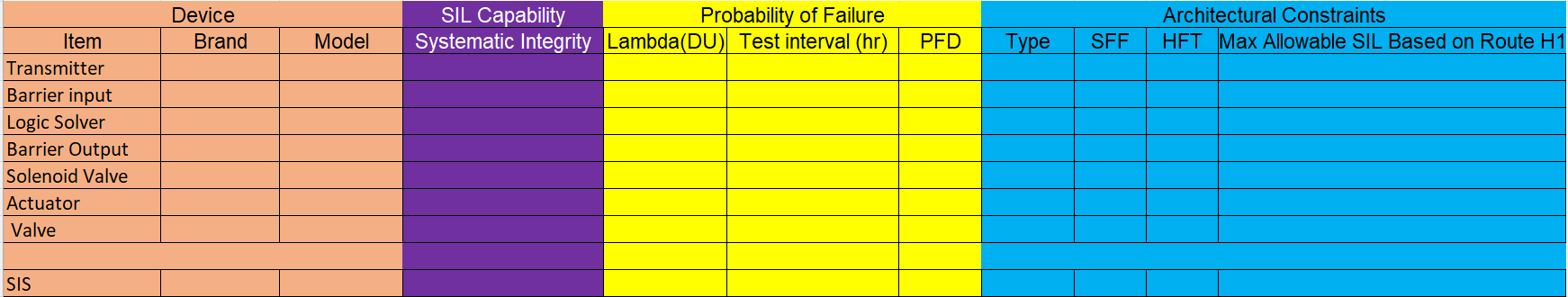
SIL Verification Procedure

In order to verify the selected SIL in a loop, 3 components should be taken into account.

A. SIL capability stated in the certificate

B. Calculate PFD for each and then sum them and find the corresponding SIL

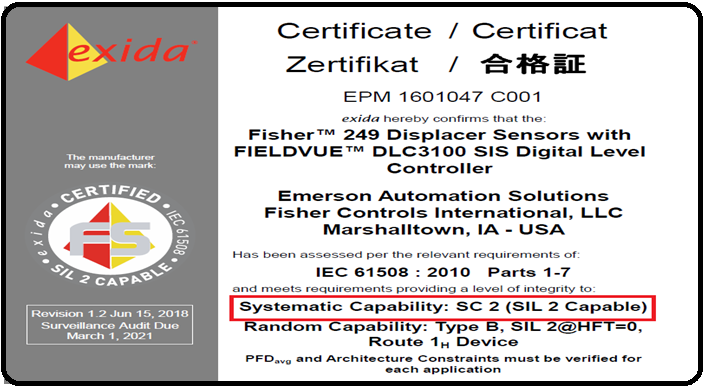
C. Check architectural constrains by checking first rout.



1.SIL capability stated in the certificate

---------------------------------------------------------------------------------------------------------------------





2.Calculate PFD for each and then sum them and find the corresponding SIL

Primary Definitions:

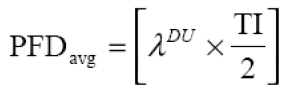
---------------------------------------------------------------------------------------------------------------------

Failure Frequency:

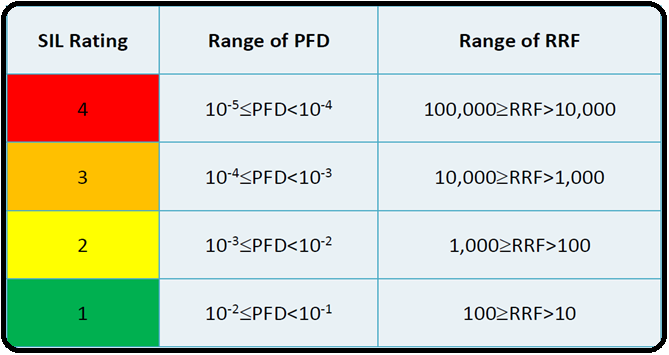
The probability that a system fails during a specified period of time.

Mean Time To Fail (MTTF)

Probability of Failure upon Demand (PFD) : equals to λ times TI divided by 2 if λ.TI<<1. It is assumed that after each time interval the equipment is as new as first day. Time interval is really important when regarding sil target.



Test intervals (TI) (directly affects PFD)



3.Check architectural constrains by checking first rout.

Primary Definition

---------------------------------------------------------------------------------------------------------------------

HFT (Hardware Fault Tolerance): maximum number of failures that can be tolerated in a SIS component

HFT for the following system:

|  |  |
| --- | --- |
| SYSTEM | HTF |
| 1001 | 0 |
| 1002 | 1 |
| 1003 | 2 |
| 2002 | 0 |
| 2003 | 1 |
| 2004 | 2 |

------------------------------------------------------------------------------------------------------------------------------------------

SFF (Safe Failure Fraction): fraction of safe failures.

SIF Failure Modes

Based on consequence

* Safe
* Dangerous

Based on diagnostic

* Detected (overt)
* Undetected (covert, hidden)

Safe/Detected: λSD

Safe/Undetected: λSU

Dangerous/Detected: λDD

Dangerous/Undetected: λDU

1. SFF = (Ysd + Ysu + Ydd)/ (Ysd + Ysu + Ydd+ Ydu)

---------------------------------------------------------------------------------------------------------------------

Subsystem type A**:** A subsystem can be regarded 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 under fault conditions can be completely 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.

Subsystem type B: A subsystem shall be regarded as type B, if for the components required to achieve the safety function

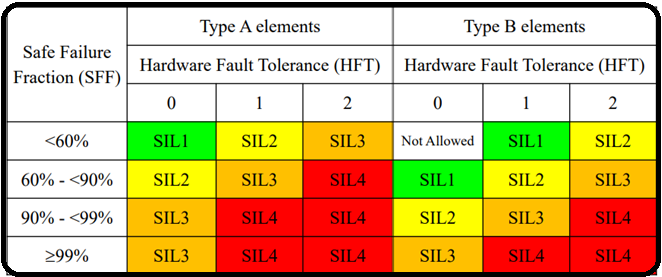
the failure mode of at least one constituent component is not well defined; or

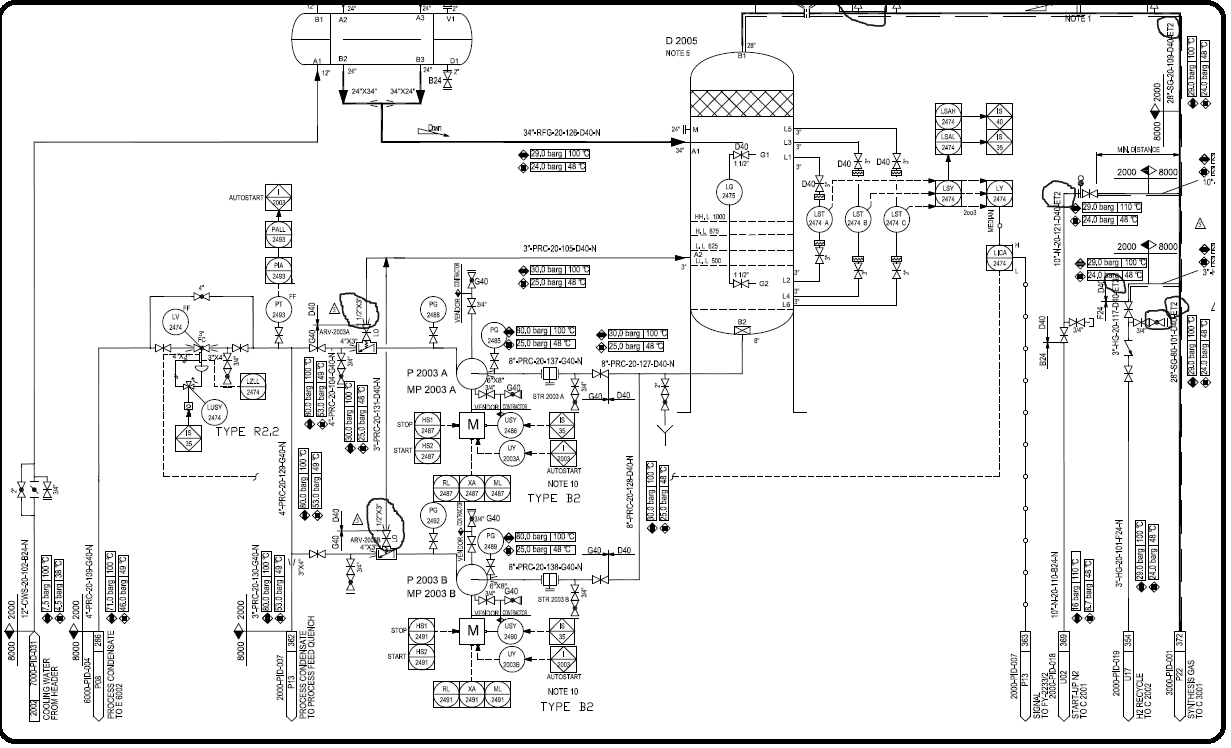
the behavior of the subsystem under fault conditions cannot be completely determined; or there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.

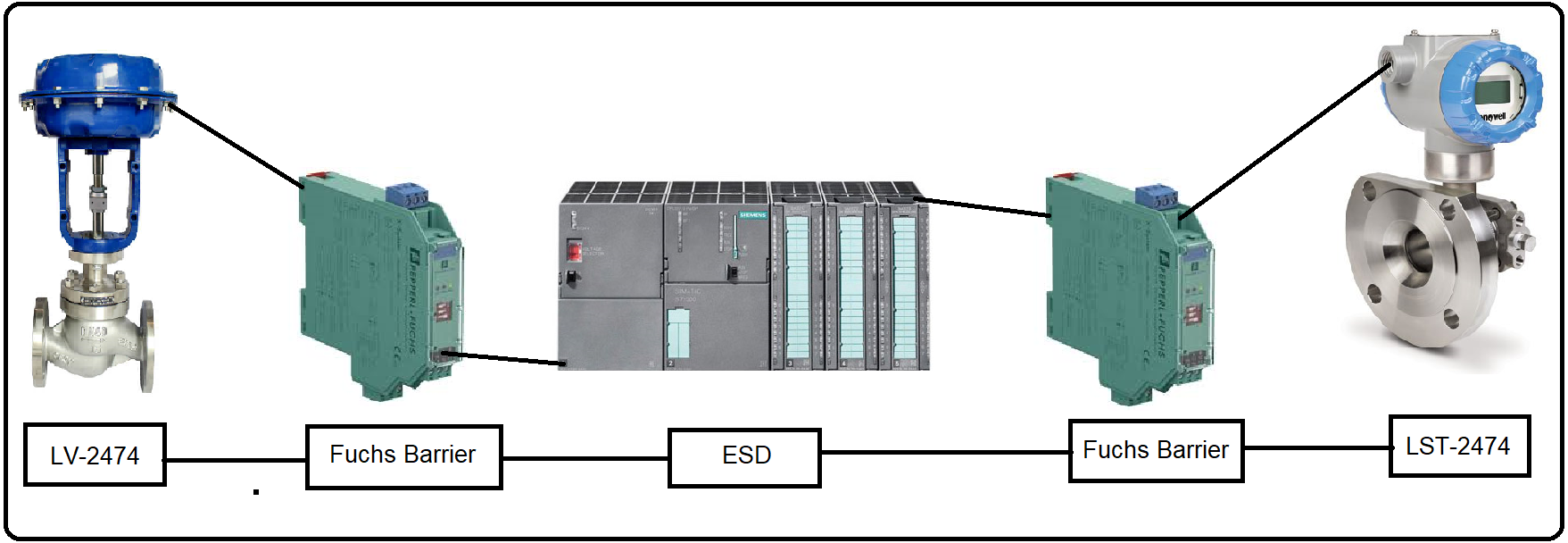
Simplifying, one can say that as long as programmable or highly integrated electronic components are used, a subsystem must be considered as type B.

---------------------------------------------------------------------------------------------------------------------

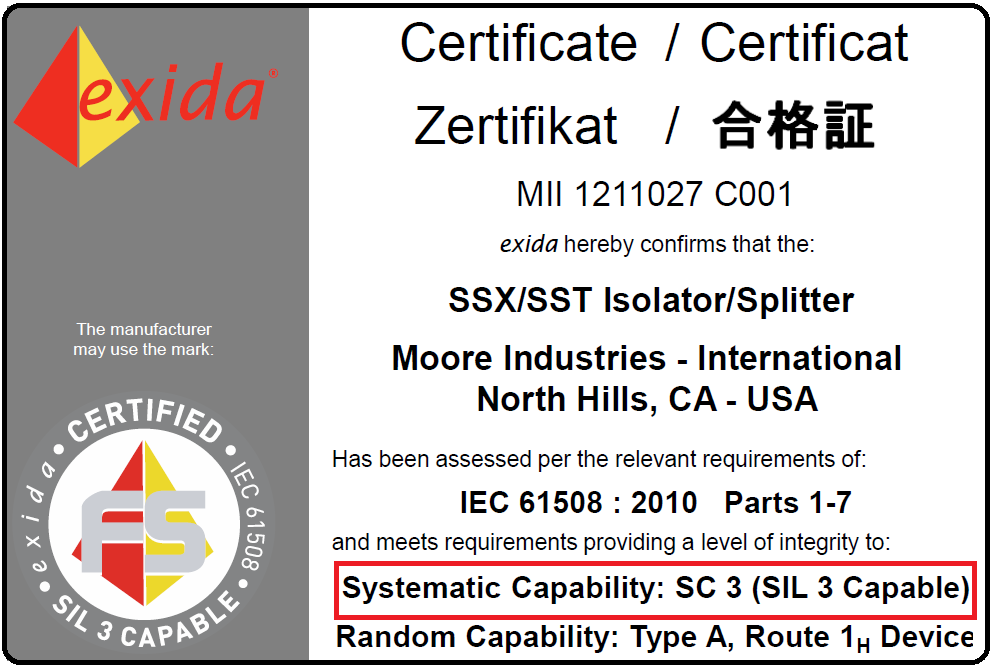
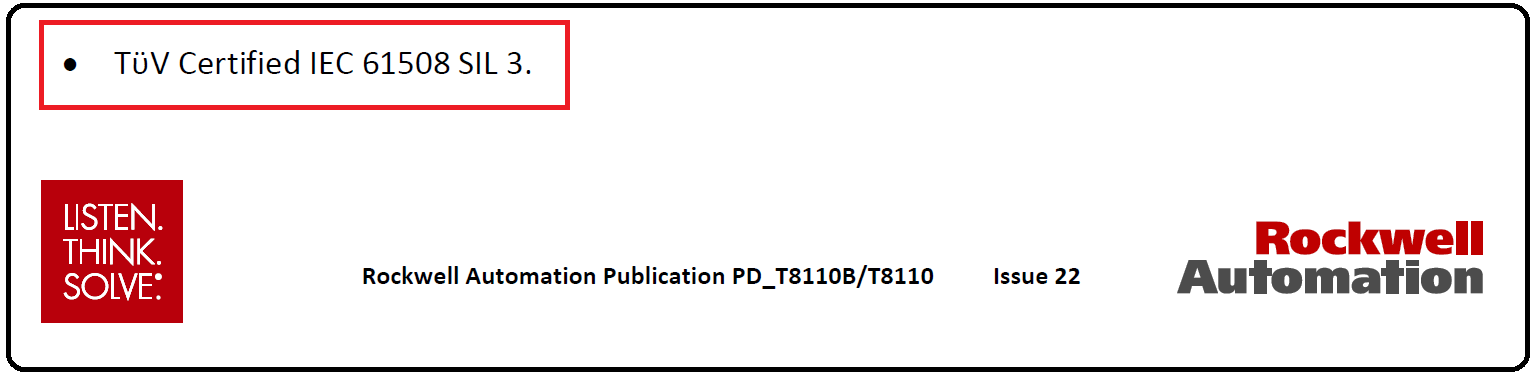
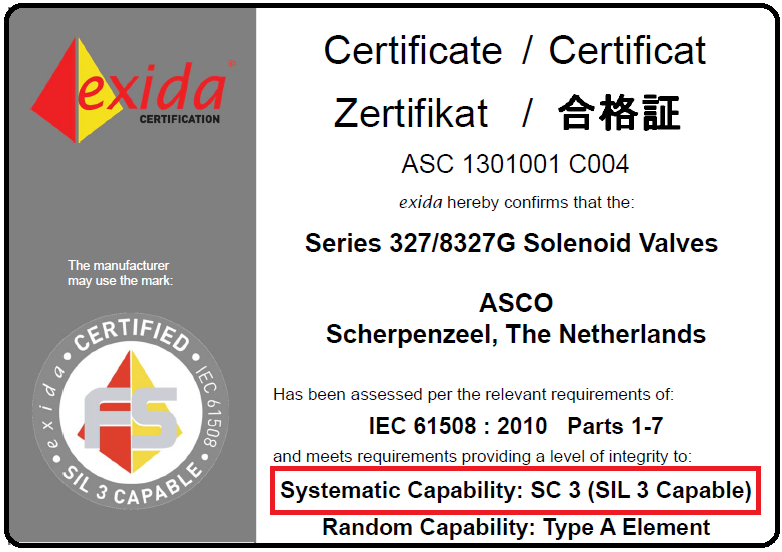
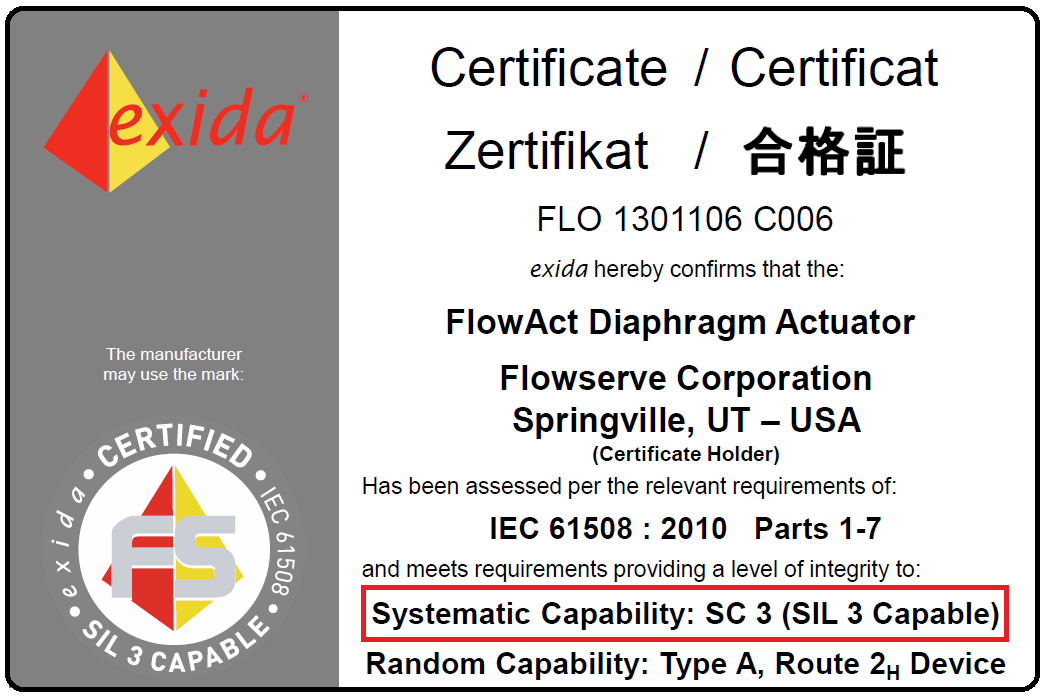
Architectural Constraints (Route 1H) (IEC 61508 part 2 –table 2)



Real Case Example

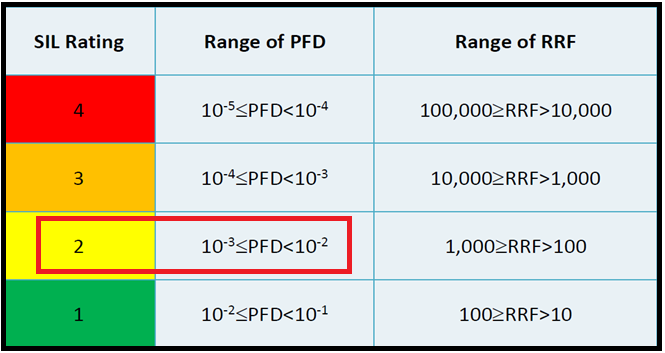


Calculation

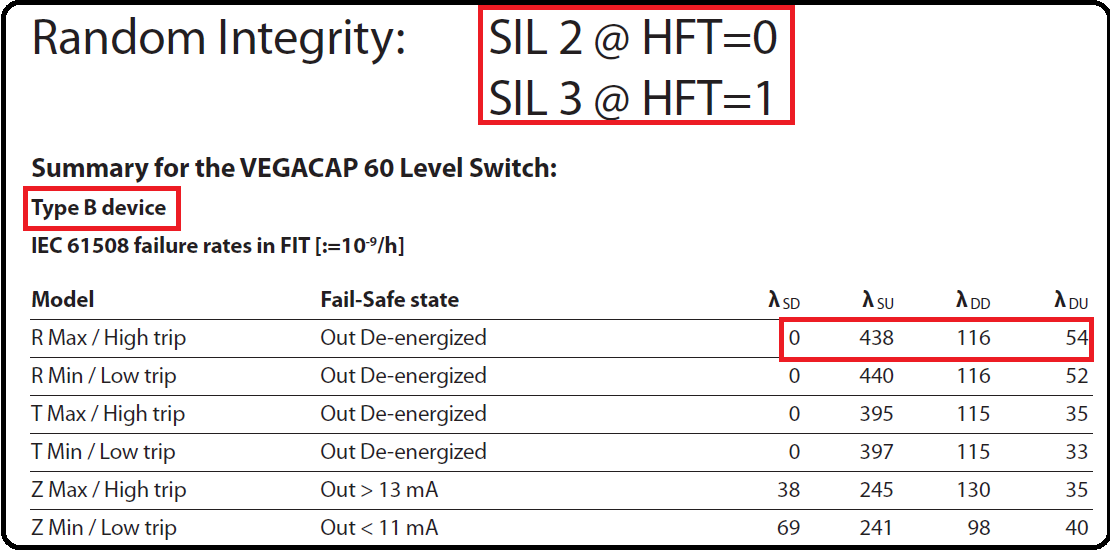
1.SIL capability stated in the certificate

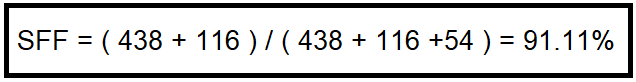
2.Calculate PFD for each and then sum them and find the corresponding SIL

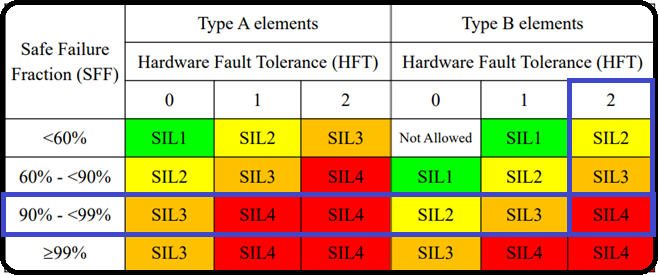
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | λ | TI | PFD | PFD |
| Level Transmitter | 5.4E-08 | 8760 | λ3. TI3 /4 | 2.65E-11 |
| Barrier input | 5.30E-08 | 8760 | λ. TI /2 | 2.32E-04 |
| Logic Solver | 3.012E-09 | 8760 | λ. TI /2 | 1.32E-04 |
| Barrier Output | 5.30E-08 | 8760 | λ. TI /2 | 2.32E-04 |
| Solenoid Valve | 1.88E-07 | 8760 | λ. TI /2 | 8.23E-04 |
| Actuator | 1.56E-07 | 8760 | λ. TI /2 | 6.83E-04 |
| Globe Valve | 8.16E-07 | 8760 | λ. TI /2 | 3.57E-03 |
|  |  |  |  | 5.68E-03 |



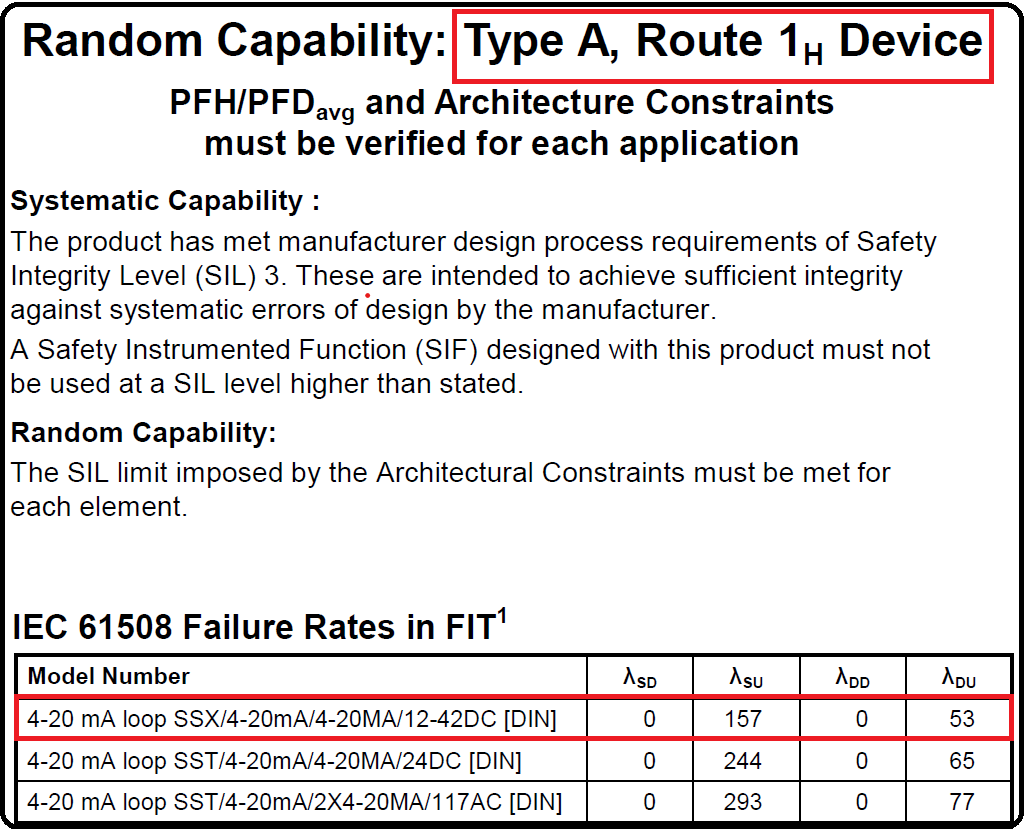
3.Check architectural constrains by checking first rout.

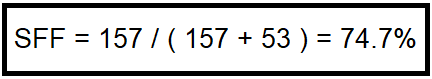
1. Level Transmitter

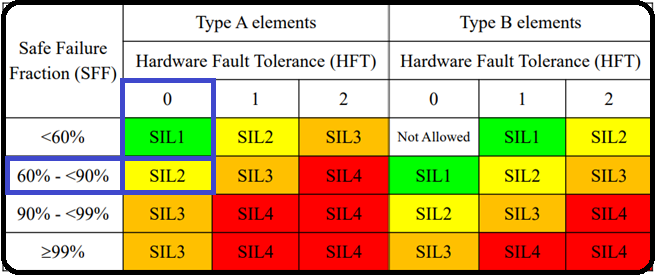


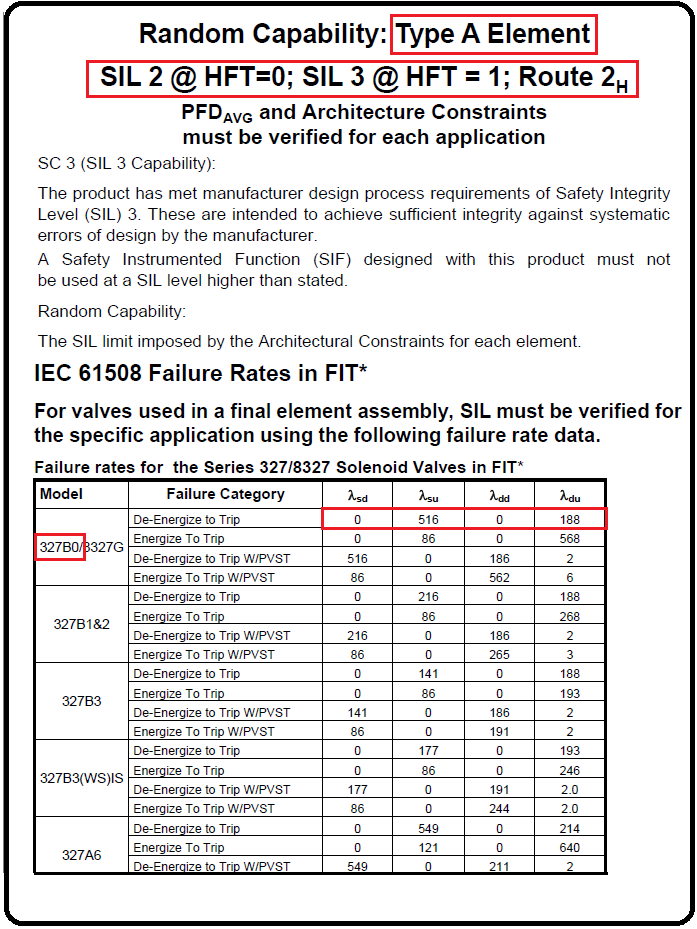


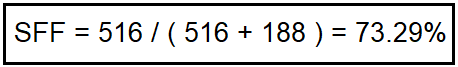
2.Barrier Input / Output

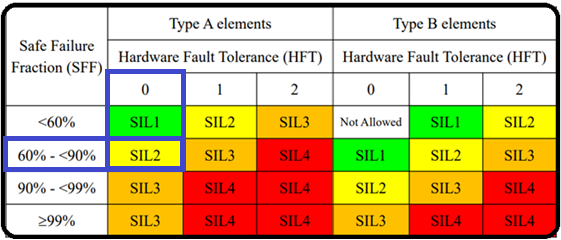


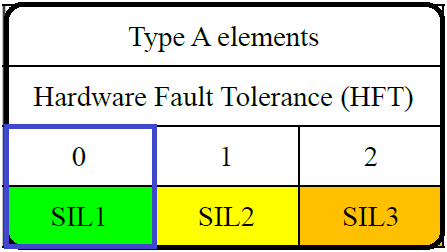


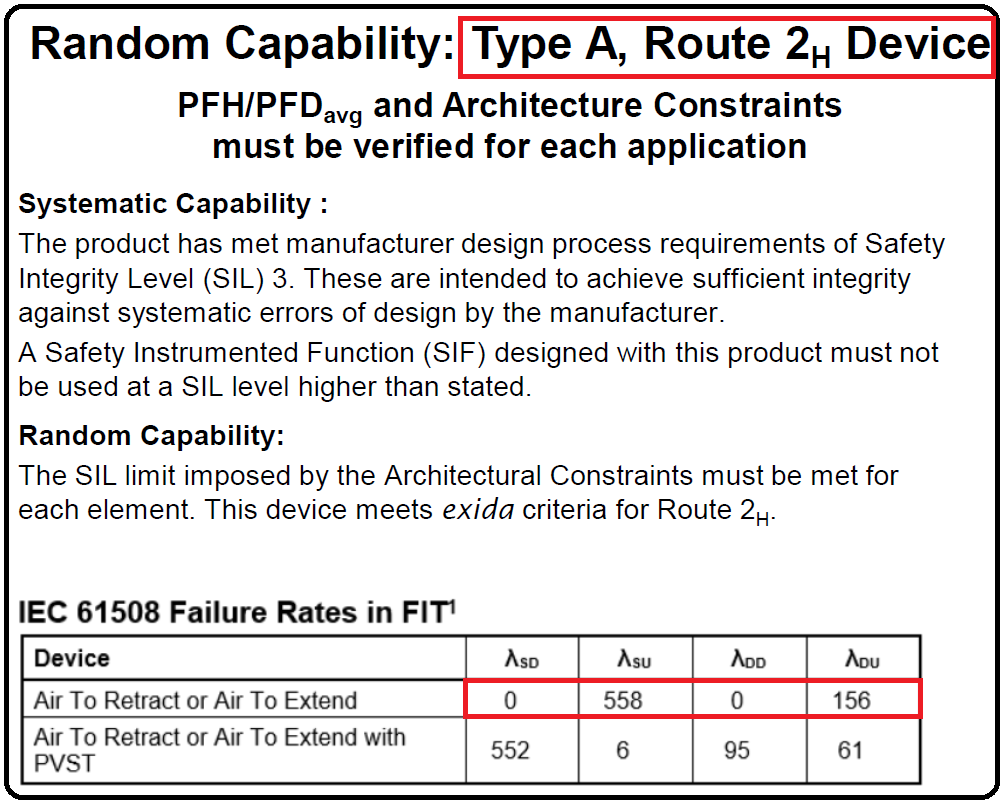


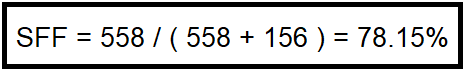
3.Selonoid Valve

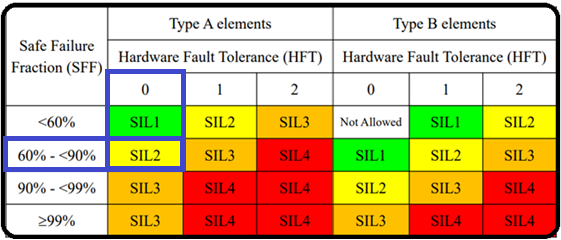


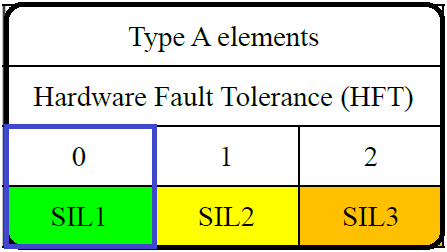




4.Actuator







Results

|  |  |
| --- | --- |
| SIL Capability | SIL 3 |
| Probability of Failure | SIL2 |
| Architectural Constraints | SIL1 |
| Verified SIL | SIL1 |

References and Software

Failure Rate Data

* OREDA -SINTEF
* PERD -CCPS
* TECDOC & EIREDA–IAEA
* SERH -Exida
* GS EP EXP 405 TOTAL
* www.sael-online.com

Software

* exSILentiaby exida, www.exida.com
* SILSolverby SIS-Tech, www.sis-tech.com
* SILCoreby ACM (Canada), www.silcore.com
* AEShieldby AE Solutions, www.aesolns.com