Education Institute for

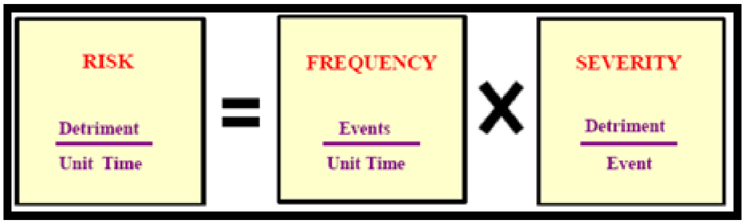
Equipment & Process Design

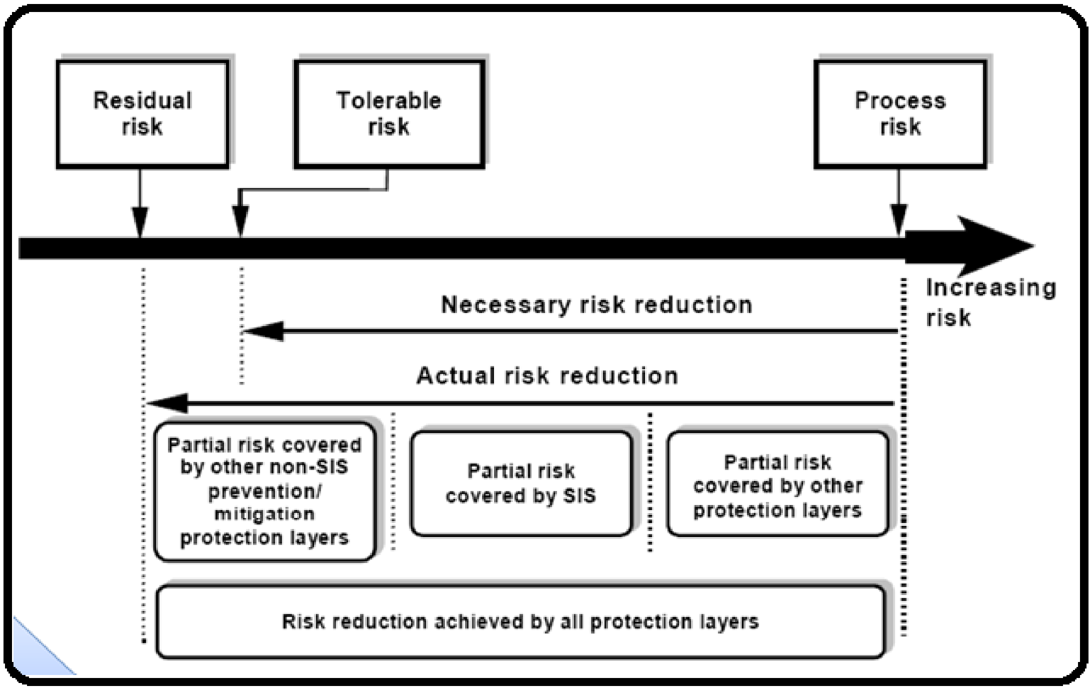
Safety Integrated Level (SIL) Verification

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.




Residual risk
Tolerable risk
Process risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other non-SIS prevention/ mitigation protection layers
Partial risk covered by SIS
Partial risk covered by other protection layers
Risk reduction achieved by all protection layers

Safety related system consists of:

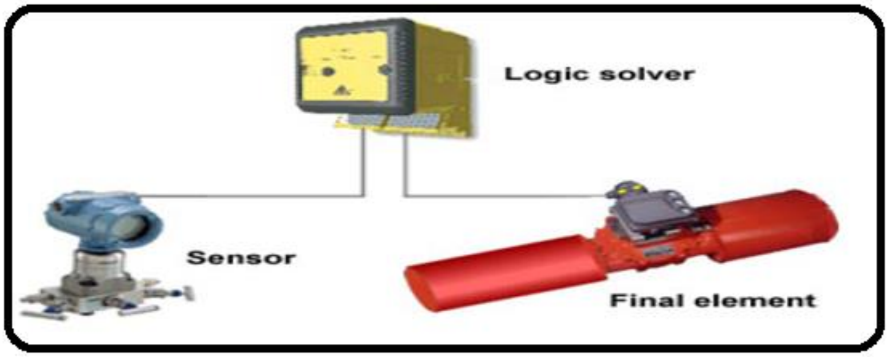
- Mechanical protection system
- Passive protection system
- Basic process control system
- Alarms
- Safety instrumented system (SIS)

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).

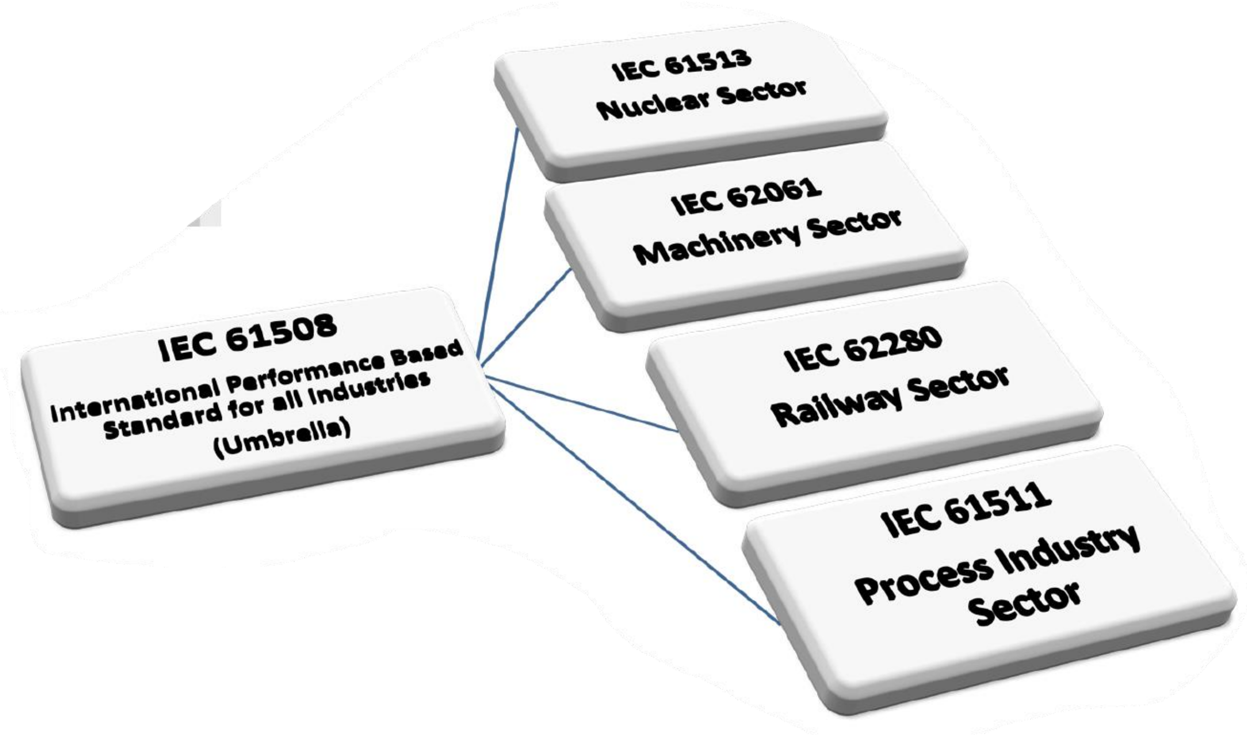
Notes

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.



3. The ability of a SIS is to carry out the actions necessary to achieve a safe state in process.

4. Standards: IEC-60508 for general industry and IEC-60511 for oil and gas industry.

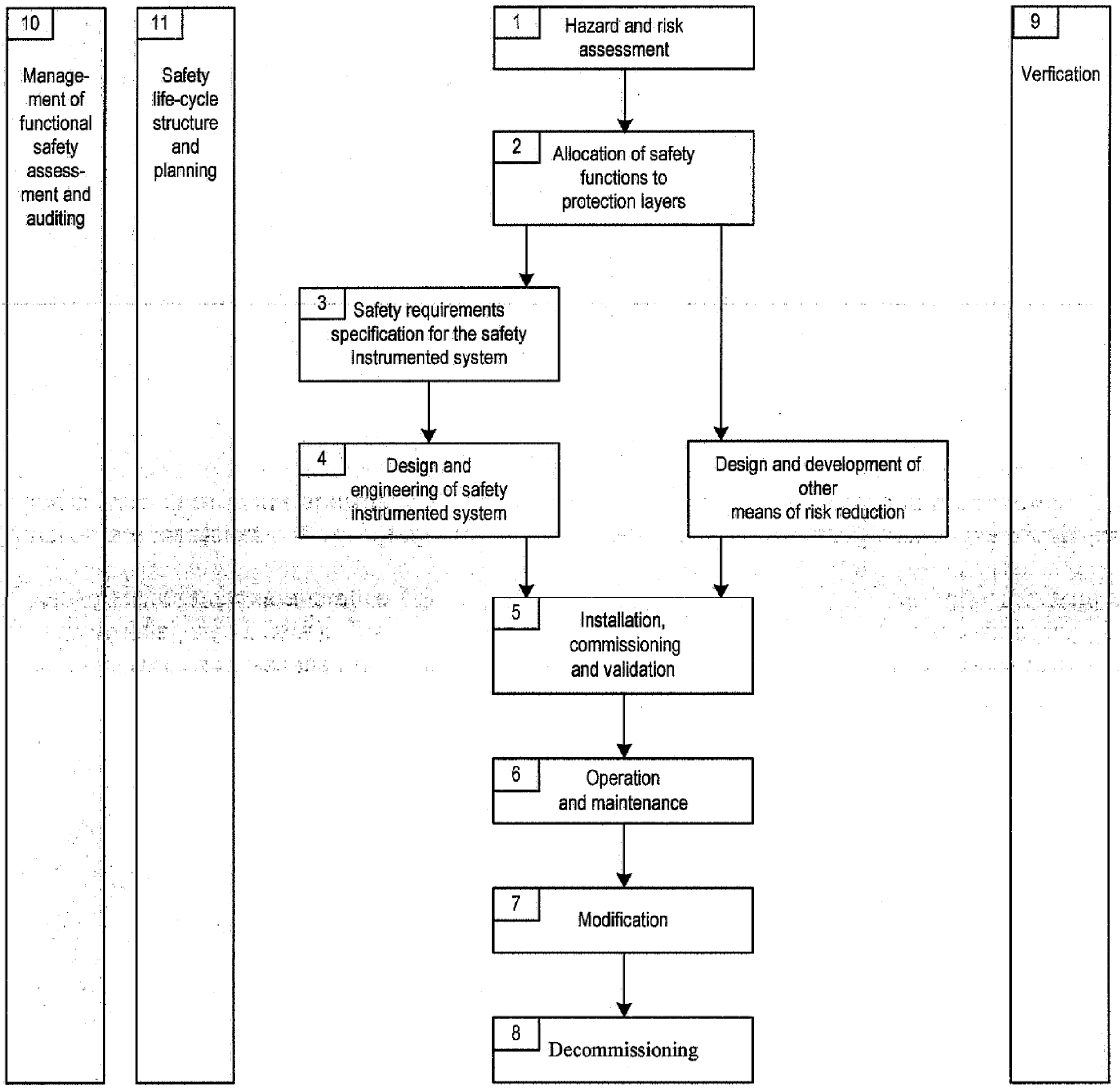


IEC-61508:
Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems

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

Lifecycle from IEC 61511


10
Manage-ment of functional safety assess-ment and auditing
11
Safety life-cycle structure and planning
1
Hazard and risk assessment
2
Allocation of safety functions to protection layers
3
Safety requirements specification for the safety Instrumented system
4
Design and engineering of safety instrumented system
Design and development of other means of risk reduction
5
Installation, commissioning and validation
6
Operation and maintenance
7
Modification
8
Decommissioning
9
Verfication

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?

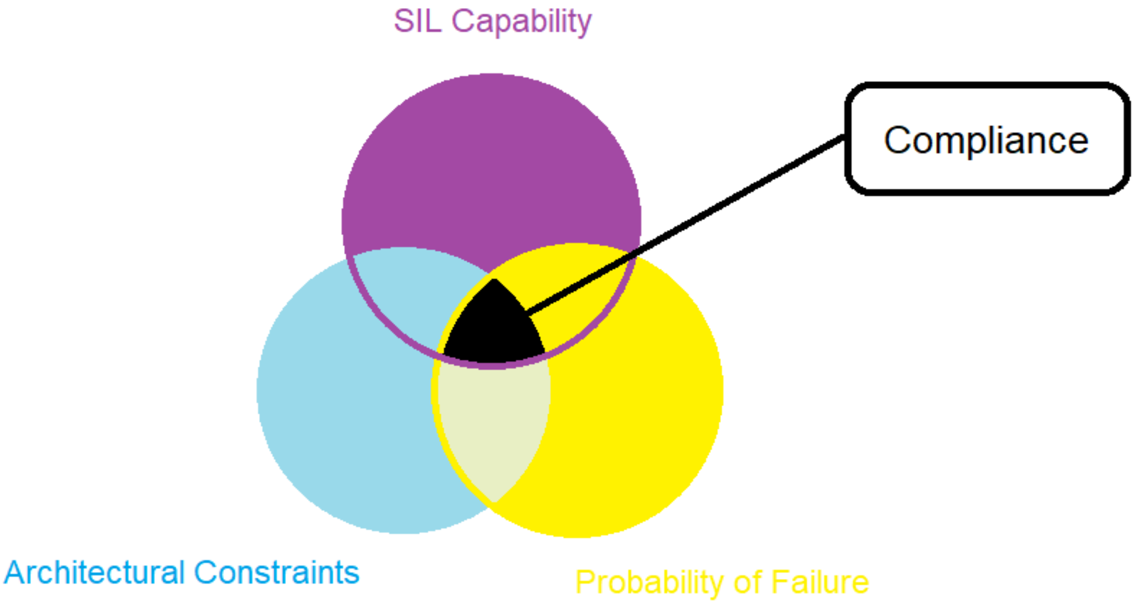
SIL Verification Procedure

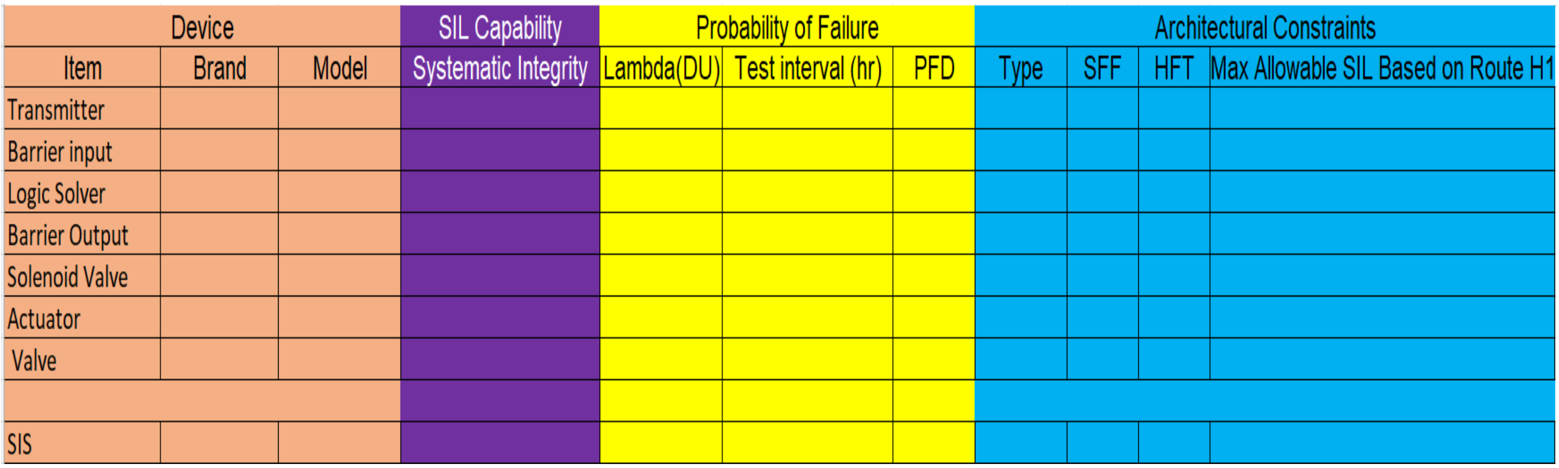
In order to verify the selected SIL in a loop, 3 components should be taken into account.

A. SIL capability stated in the certificate

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

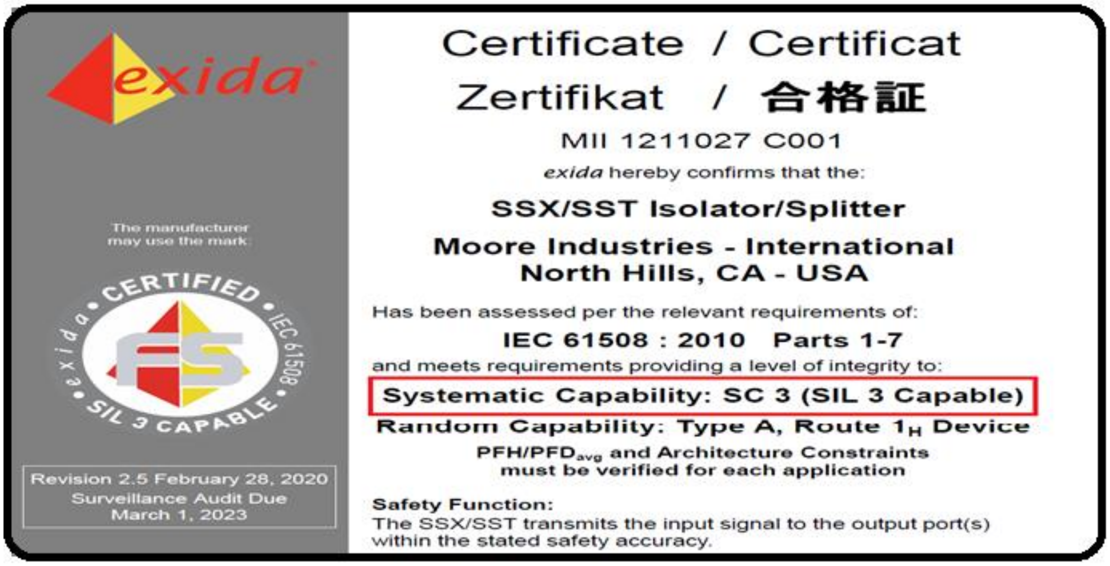
C. Check architectural constrains by checking first rout.





Device			SIL Capability	Probability of Failure			Architectural Constraints			
Item	Brand	Model	Systematic Integrity	Lambda(DU)	Test interval (hr)	PFD	Type	SFF	HFT	Max Allowable SIL Based on Route H1
Transmitter										
Barrier input										
Logic Solver										
Barrier Output										
Solenoid Valve										
Actuator										
Valve										
SIS										

1.SIL capability stated in the certificate


exida
CERTIFIED • IEC 61508 • SIL 3 CAPABLE • exida
FS

The manufacturer may use the mark:

Revision 2.5 February 28, 2020
Surveillance Audit Due
March 1, 2023

Certificate / Certificat
Zertifikat / 合格証

MII 1211027 C001

exida hereby confirms that the:

SSX/SST Isolator/Splitter

Moore Industries - International
North Hills, CA - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

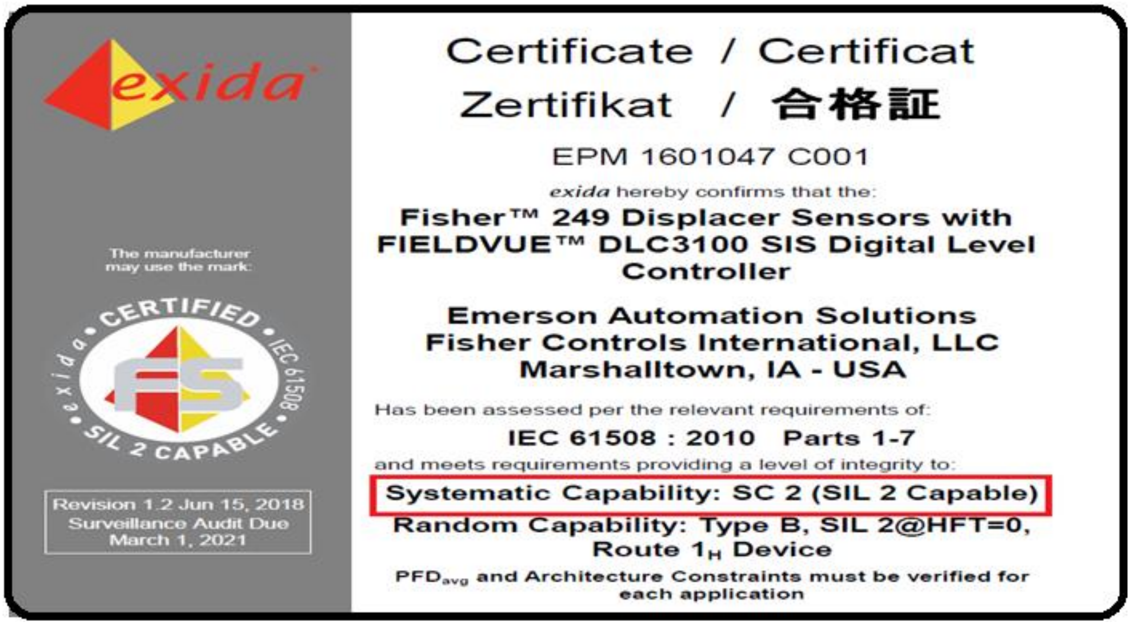
and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 1_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
The SSX/SST transmits the input signal to the output port(s) within the stated safety accuracy.


exida
CERTIFIED • IEC 61508 • SIL 2 CAPABLE • exida
FS

The manufacturer may use the mark:

Revision 1.2 Jun 15, 2018
Surveillance Audit Due
March 1, 2021

Certificate / Certificat
Zertifikat / 合格証

EPM 1601047 C001

exida hereby confirms that the:

Fisher™ 249 Displacer Sensors with FIELDVUE™ DLC3100 SIS Digital Level Controller

Emerson Automation Solutions
Fisher Controls International, LLC
Marshalltown, IA - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B, SIL 2@HFT=0, Route 1_H Device

PFD_{avg} and Architecture Constraints must be verified for each application

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

Primary Definitions:

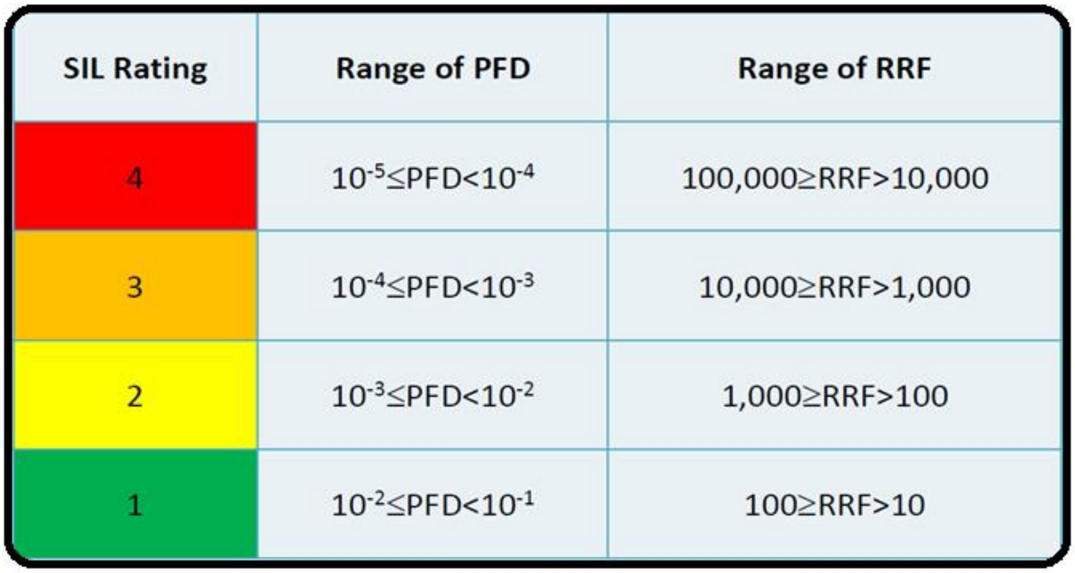
Failure Frequency:
The probability that a system fails during a specified period of time.

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.

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\lambda^{DU} \times \frac{\mathrm{TI}}{2}\right]$$

Test intervals (TI) (directly affects PFD)



SIL Rating	Range of PFD	Range of RRF
4	$10^{-5} \leq PFD < 10^{-4}$	100,000≥RRF>10,000
3	$10^{-4} \leq PFD < 10^{-3}$	10,000≥RRF>1,000
2	$10^{-3} \leq PFD < 10^{-2}$	1,000≥RRF>100
1	$10^{-2} \leq PFD < 10^{-1}$	100≥RRF>10

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)

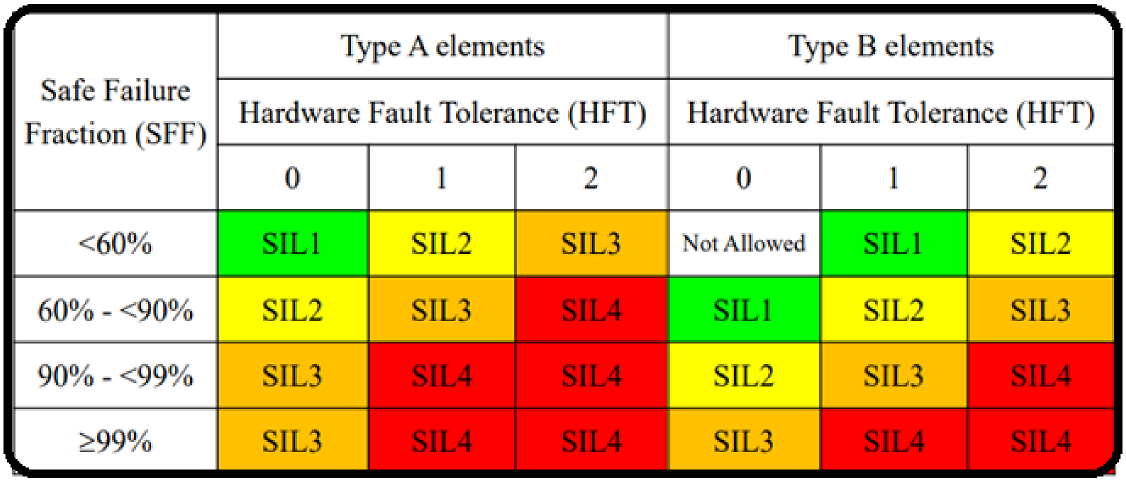
Safe/Detected: λ^{SD}
Safe/Undetected: λ^{SU}
Dangerous/Detected: λ^{DD}
Dangerous/Undetected: λ^{DU}

$$SFF = (Ysd + Ysu + Ydd)/ (Ysd + Ysu + Ydd+ Ydu)$$

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.

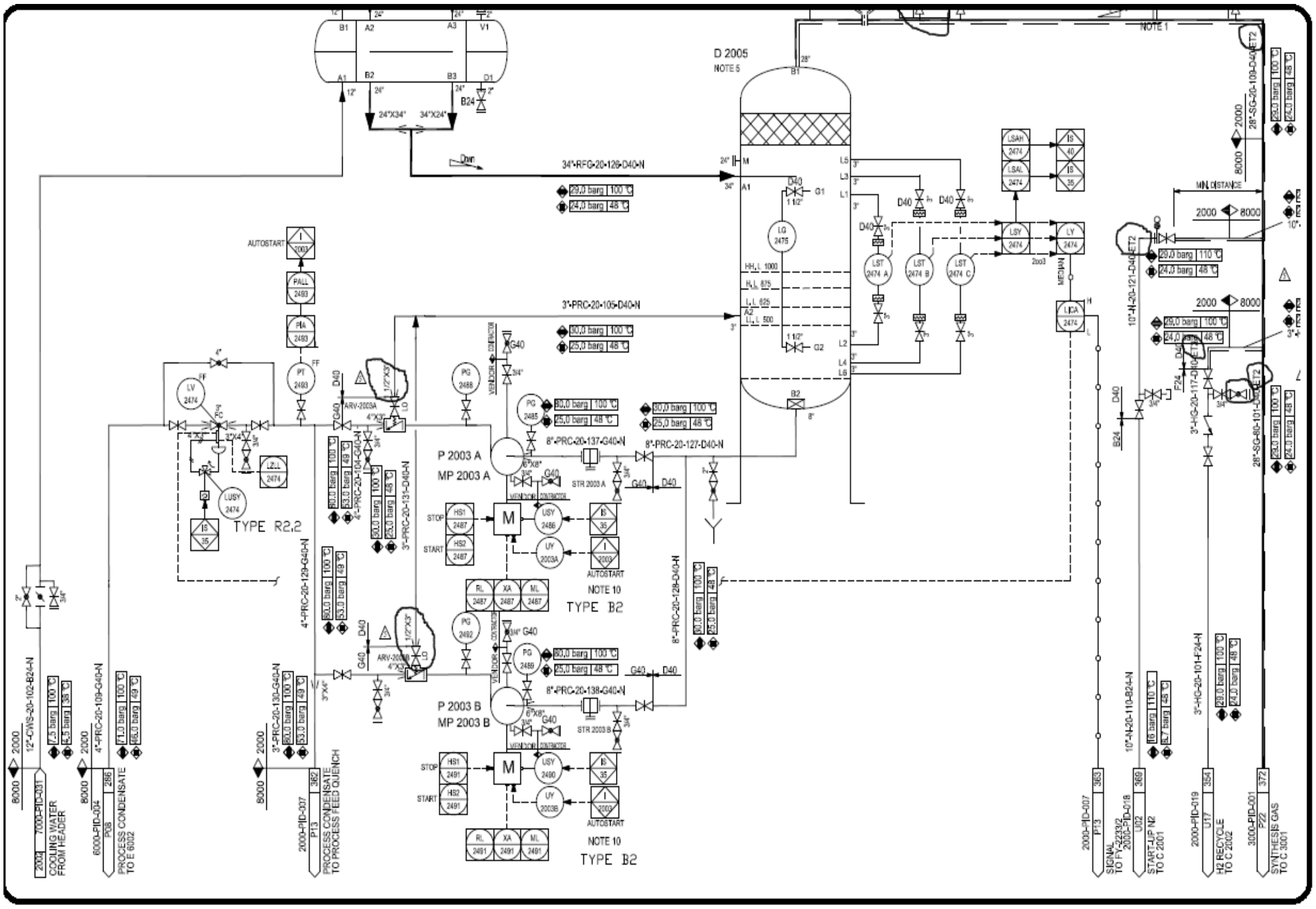
Subsystem type B: A subsystem shall be regarded as type B, if for the components required to achieve the safety function
the failure mode of at least one constituent component is not well defined; or
the behavior of the subsystem under fault conditions cannot be completely determined;
or there is insufficient 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.

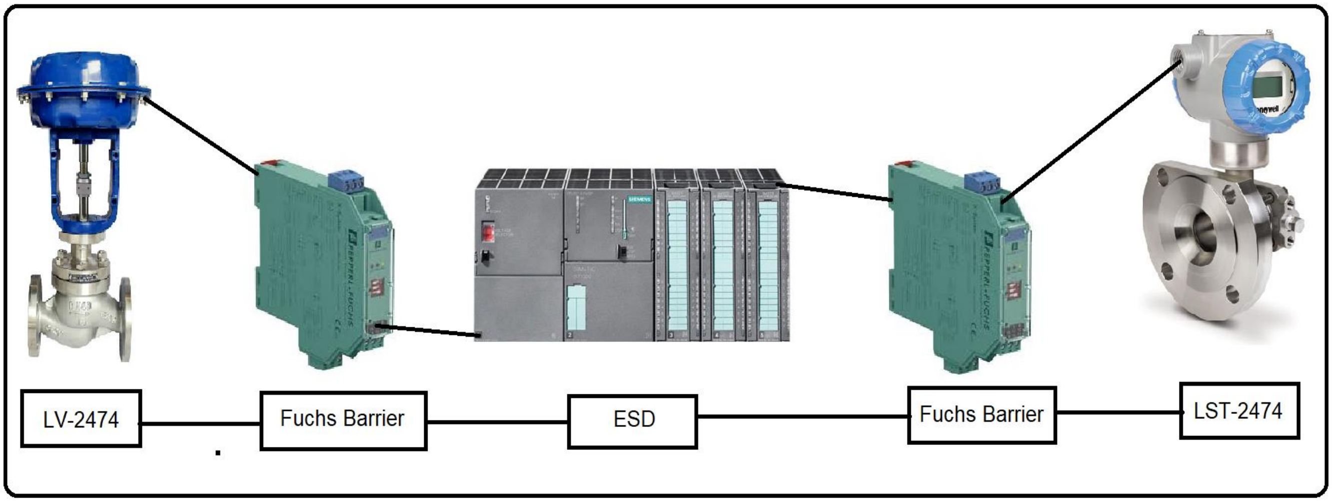
Architectural Constraints (Route 1H) (IEC 61508 part 2 –table 2)



Safe Failure Fraction (SFF)	Type A elements			Type B elements		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60% - <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% - <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

Real Case Example




LV-2474

Fuchs Barrier

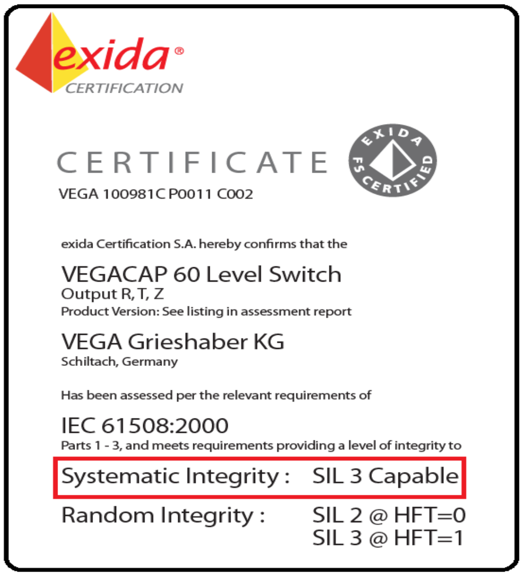
ESD

Fuchs Barrier

LST-2474

Calculation

1.SIL capability stated in the certificate



exida CERTIFICATION

CERTIFICATE

VEGA 100981C P0011 C002

exida Certification S.A. hereby confirms that the

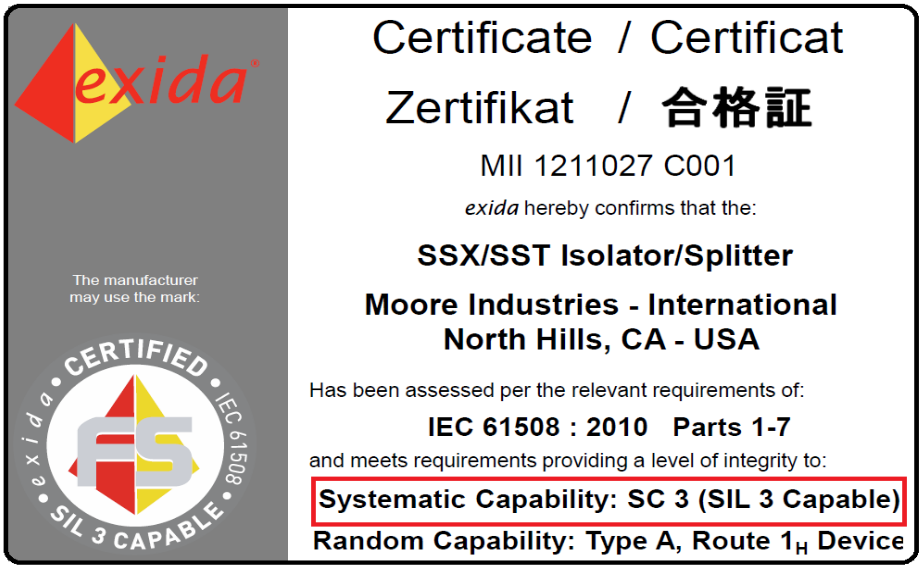
VEGACAP 60 Level Switch
Output R, T, Z
Product Version: See listing in assessment report

VEGA Grieshaber KG
Schiltach, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000
Parts 1 - 3, and meets requirements providing a level of integrity to

Systematic Integrity :	SIL 3 Capable
Random Integrity :	SIL 2 @ HFT=0 SIL 3 @ HFT=1



exida

The manufacturer may use the mark:

Certificate / Certificat

Zertifikat / 合格証

MII 1211027 C001

exida hereby confirms that the:

SSX/SST Isolator/Splitter

**Moore Industries - International
North Hills, CA - USA**

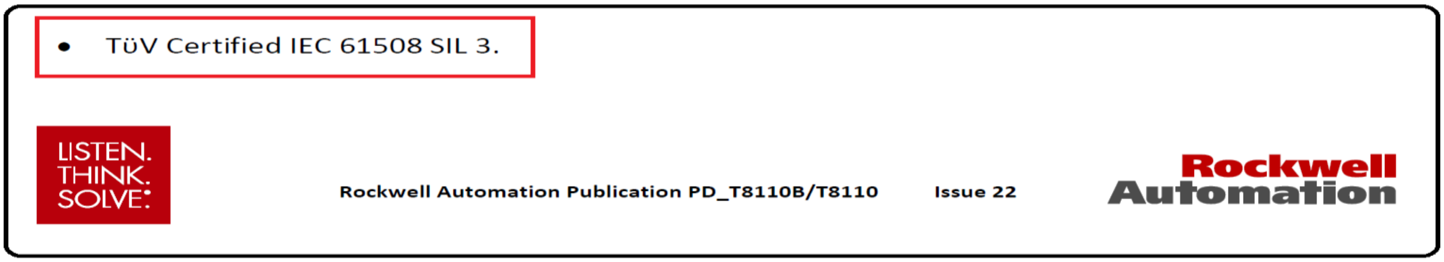
Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 1_H Device

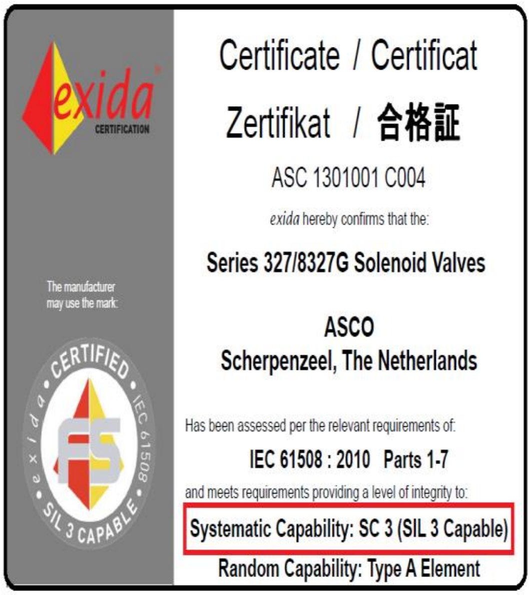


- TüV Certified IEC 61508 SIL 3.

LISTEN. THINK. SOLVE.

Rockwell Automation Publication PD_T8110B/T8110 Issue 22

Rockwell Automation



exida CERTIFICATION

The manufacturer may use the mark:

Certificate / Certificat

Zertifikat / 合格証

ASC 1301001 C004

exida hereby confirms that the:

Series 327/8327G Solenoid Valves

ASCO
Scherpenzeel, The Netherlands

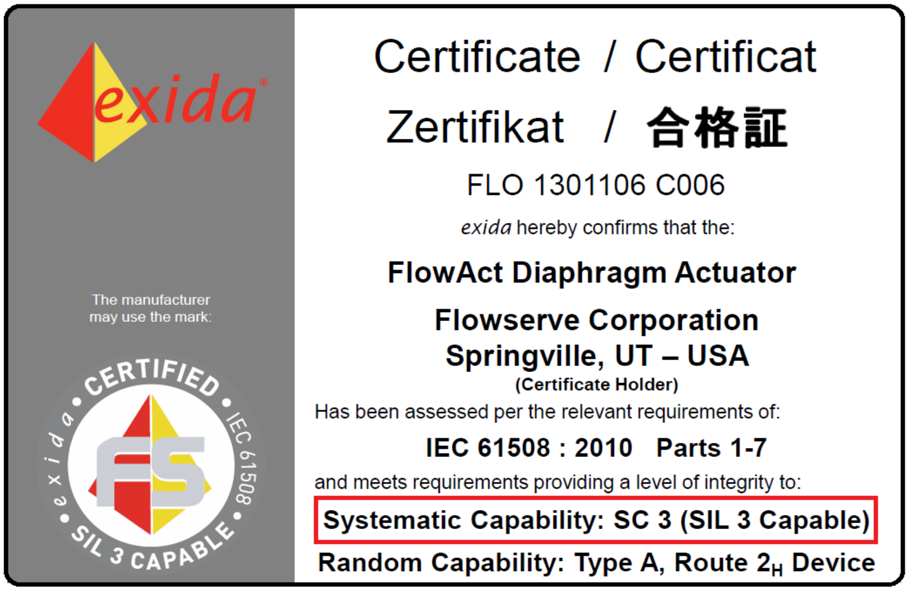
Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A Element



exida

The manufacturer may use the mark:

Certificate / Certificat

Zertifikat / 合格証

FLO 1301106 C006

exida hereby confirms that the:

FlowAct Diaphragm Actuator

**Flowserve Corporation
Springville, UT – USA
(Certificate Holder)**

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

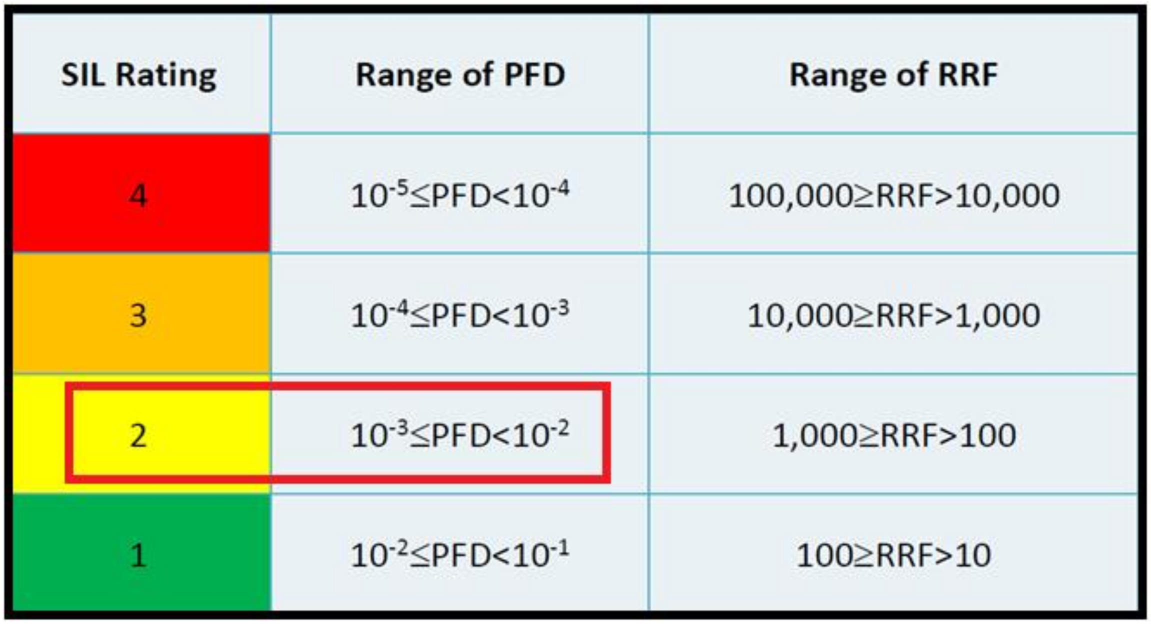
and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

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

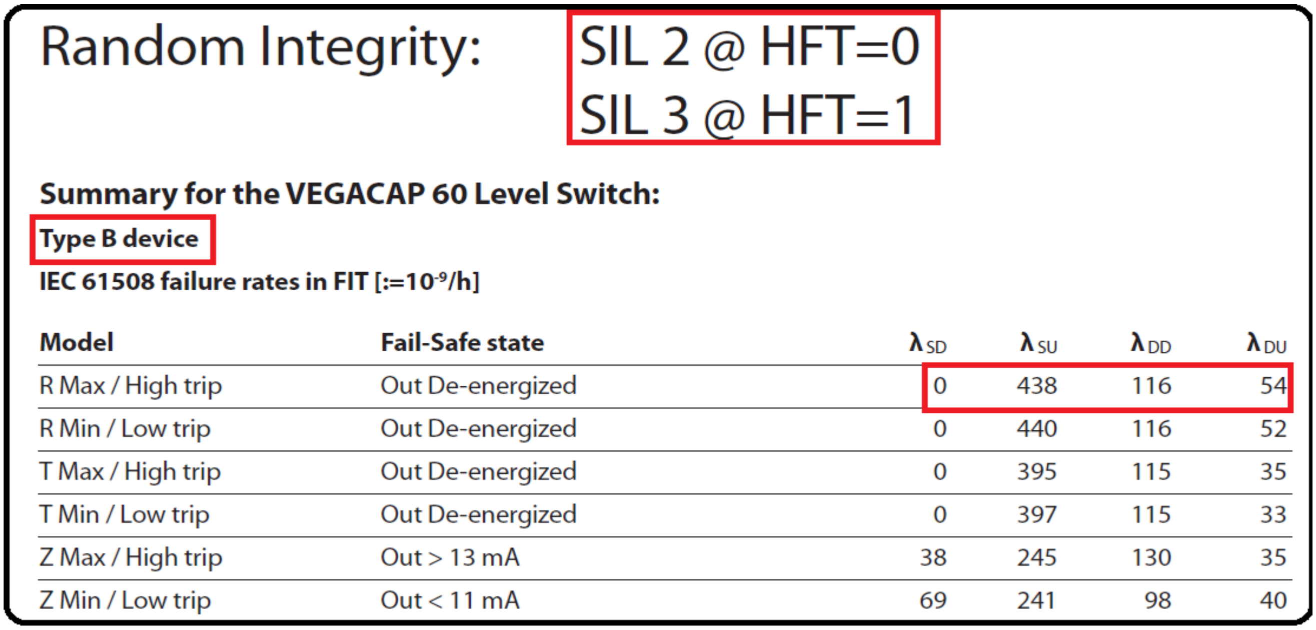
Device	λ	TI	PFD	PFD
Level Transmitter	5.4E-08	8760	$\lambda^3. TI^3 /4$	2.65E-11
Barrier input	5.30E-08	8760	λ. TI /2	2.32E-04
Logic Solver	3.012E-09	8760	λ. TI /2	1.32E-04
Barrier Output	5.30E-08	8760	λ. TI /2	2.32E-04
Solenoid Valve	1.88E-07	8760	λ. TI /2	8.23E-04
Actuator	1.56E-07	8760	λ. TI /2	6.83E-04
Globe Valve	8.16E-07	8760	λ. TI /2	3.57E-03
				5.68E-03



SIL Rating	Range of PFD	Range of RRF
4	$10^{-5} \leq PFD < 10^{-4}$	100,000≥RRF>10,000
3	$10^{-4} \leq PFD < 10^{-3}$	10,000≥RRF>1,000
2	$10^{-3} \leq PFD < 10^{-2}$	1,000≥RRF>100
1	$10^{-2} \leq PFD < 10^{-1}$	100≥RRF>10

3.Check architectural constrains by checking first rout.

1. Level Transmitter



Random Integrity: SIL 2 @ HFT=0

SIL 3 @ HFT=1

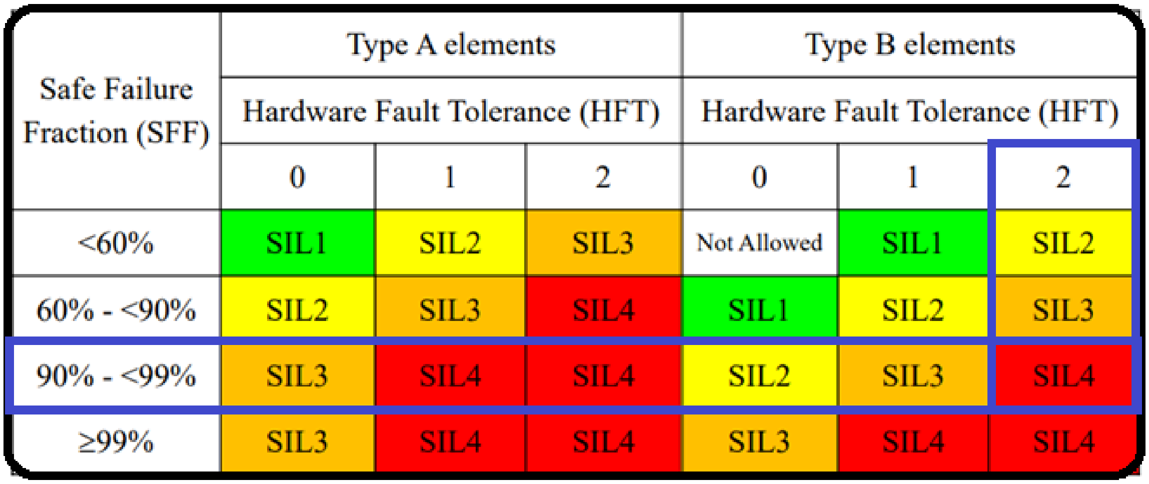
Summary for the VEGACAP 60 Level Switch:

Type B device

IEC 61508 failure rates in FIT [:=10^{-9}/h]

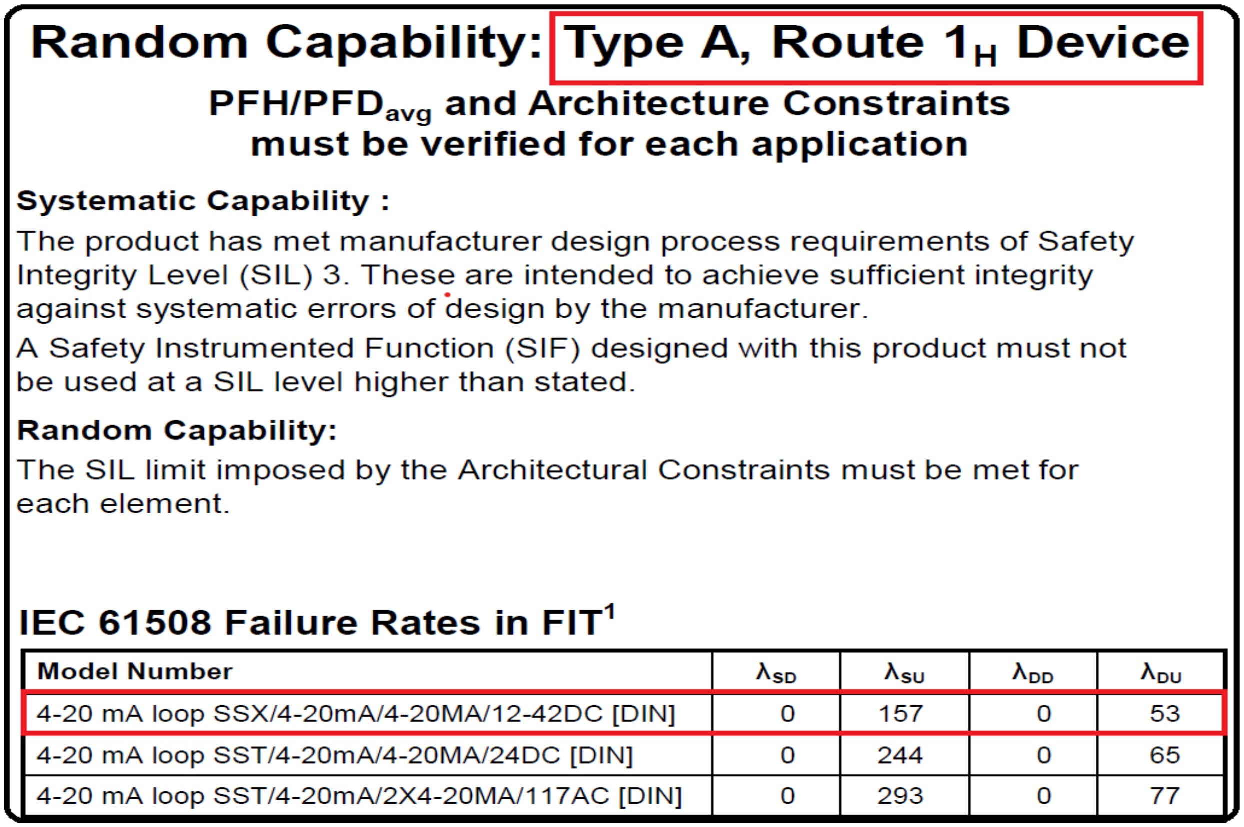
Model	Fail-Safe state	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
R Max / High trip	Out De-energized	0	438	116	54
R Min / Low trip	Out De-energized	0	440	116	52
T Max / High trip	Out De-energized	0	395	115	35
T Min / Low trip	Out De-energized	0	397	115	33
Z Max / High trip	Out > 13 mA	38	245	130	35
Z Min / Low trip	Out < 11 mA	69	241	98	40

SFF = (438 + 116) / (438 + 116 +54) = 91.11%



Safe Failure Fraction (SFF)	Type A elements			Type B elements		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60% - <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% - <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

2.Barrier Input / Output



Random Capability: Type A, Route 1_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Systematic Capability :

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

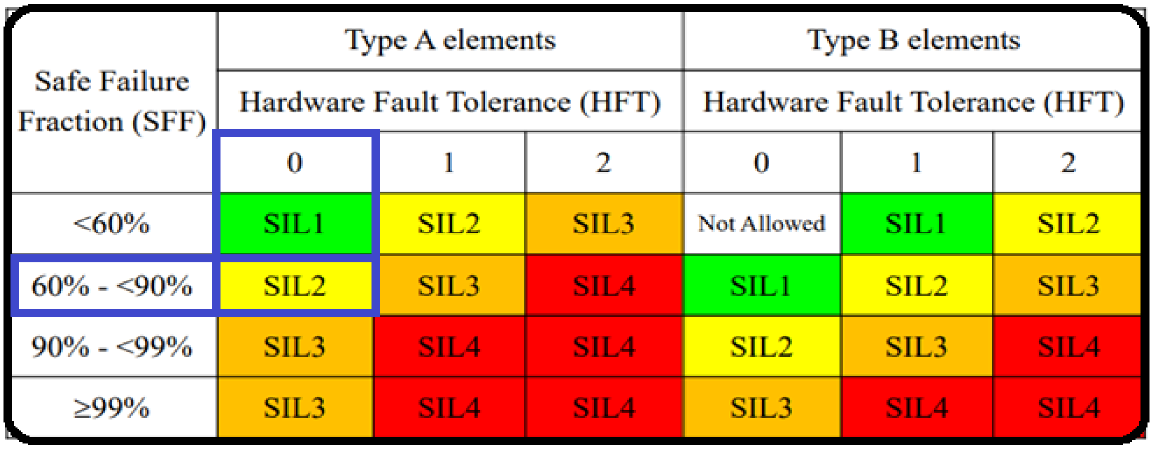
Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

IEC 61508 Failure Rates in FIT[1]

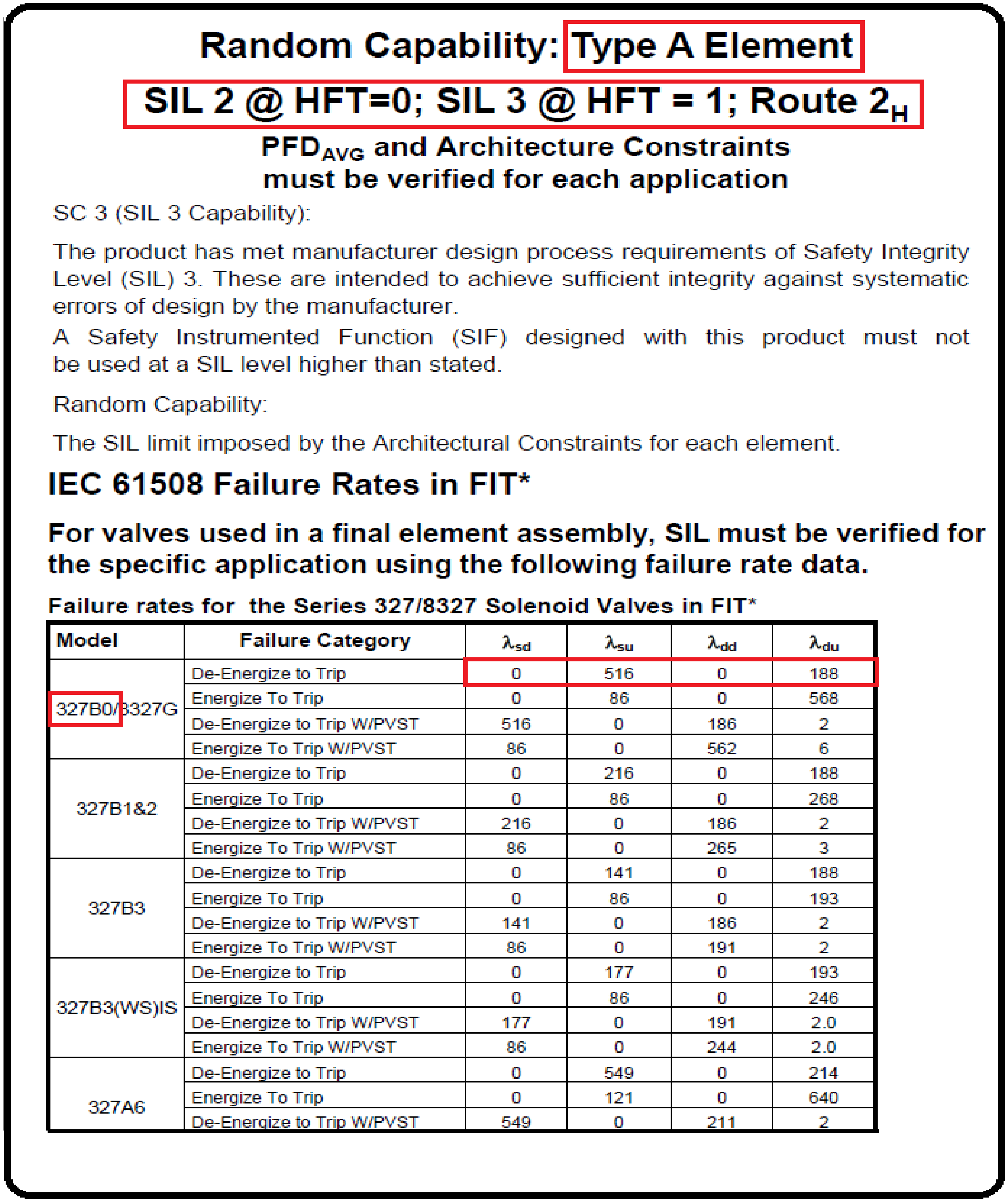
Model Number	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
4-20 mA loop SSX/4-20mA/4-20MA/12-42DC [DIN]	0	157	0	53
4-20 mA loop SST/4-20mA/4-20MA/24DC [DIN]	0	244	0	65
4-20 mA loop SST/4-20mA/2X4-20MA/117AC [DIN]	0	293	0	77

$$\boxed{SFF = 157 / (157 + 53) = 74.7\%}$$



Safe Failure Fraction (SFF)	Type A elements			Type B elements		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60% - <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% - <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

3.Selonoid Valve



Random Capability: Type A Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFD_{AVG} and Architecture Constraints must be verified for each application

SC 3 (SIL 3 Capability):

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints for each element.

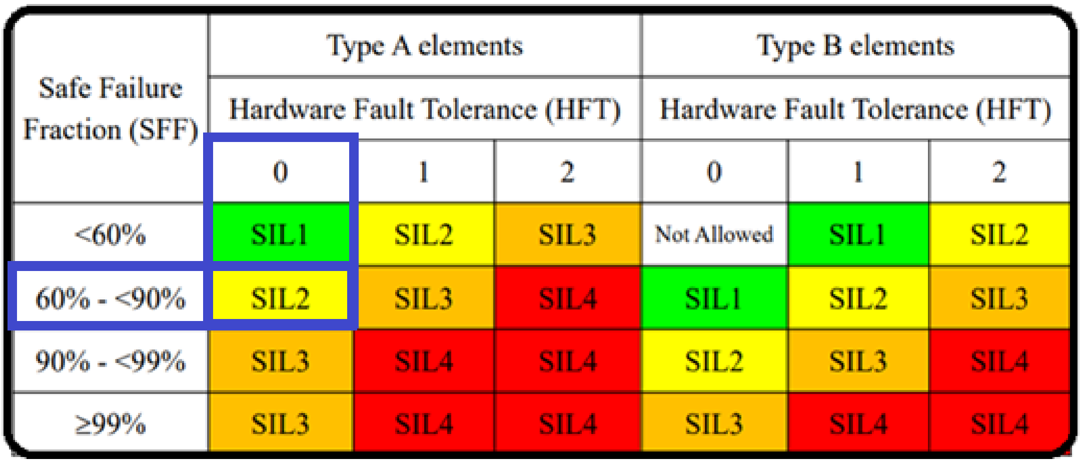
IEC 61508 Failure Rates in FIT*

For valves used in a final element assembly, SIL must be verified for the specific application using the following failure rate data.

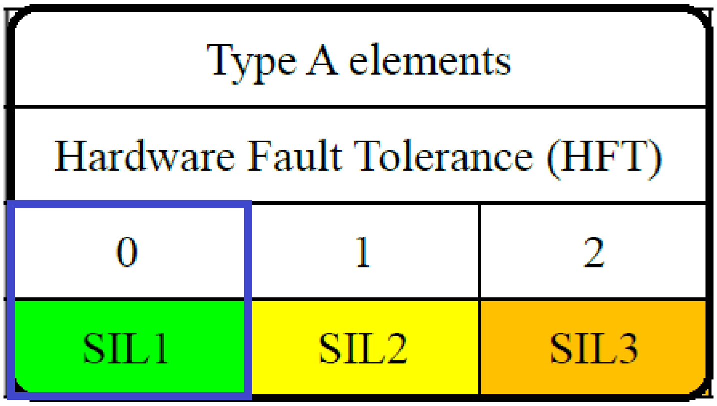
Failure rates for the Series 327/8327 Solenoid Valves in FIT*

Model	Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}
327B0/8327G	De-Energize to Trip	0	516	0	188
	Energize To Trip	0	86	0	568
	De-Energize to Trip W/PVST	516	0	186	2
	Energize To Trip W/PVST	86	0	562	6
327B1&2	De-Energize to Trip	0	216	0	188
	Energize To Trip	0	86	0	268
	De-Energize to Trip W/PVST	216	0	186	2
	Energize To Trip W/PVST	86	0	265	3
327B3	De-Energize to Trip	0	141	0	188
	Energize To Trip	0	86	0	193
	De-Energize to Trip W/PVST	141	0	186	2
	Energize To Trip W/PVST	86	0	191	2
327B3(WS)IS	De-Energize to Trip	0	177	0	193
	Energize To Trip	0	86	0	246
	De-Energize to Trip W/PVST	177	0	191	2.0
	Energize To Trip W/PVST	86	0	244	2.0
327A6	De-Energize to Trip	0	549	0	214
	Energize To Trip	0	121	0	640
	De-Energize to Trip W/PVST	549	0	211	2

$$\boxed{\text{SFF} = 516 / (516 + 188) = 73.29\%}$$

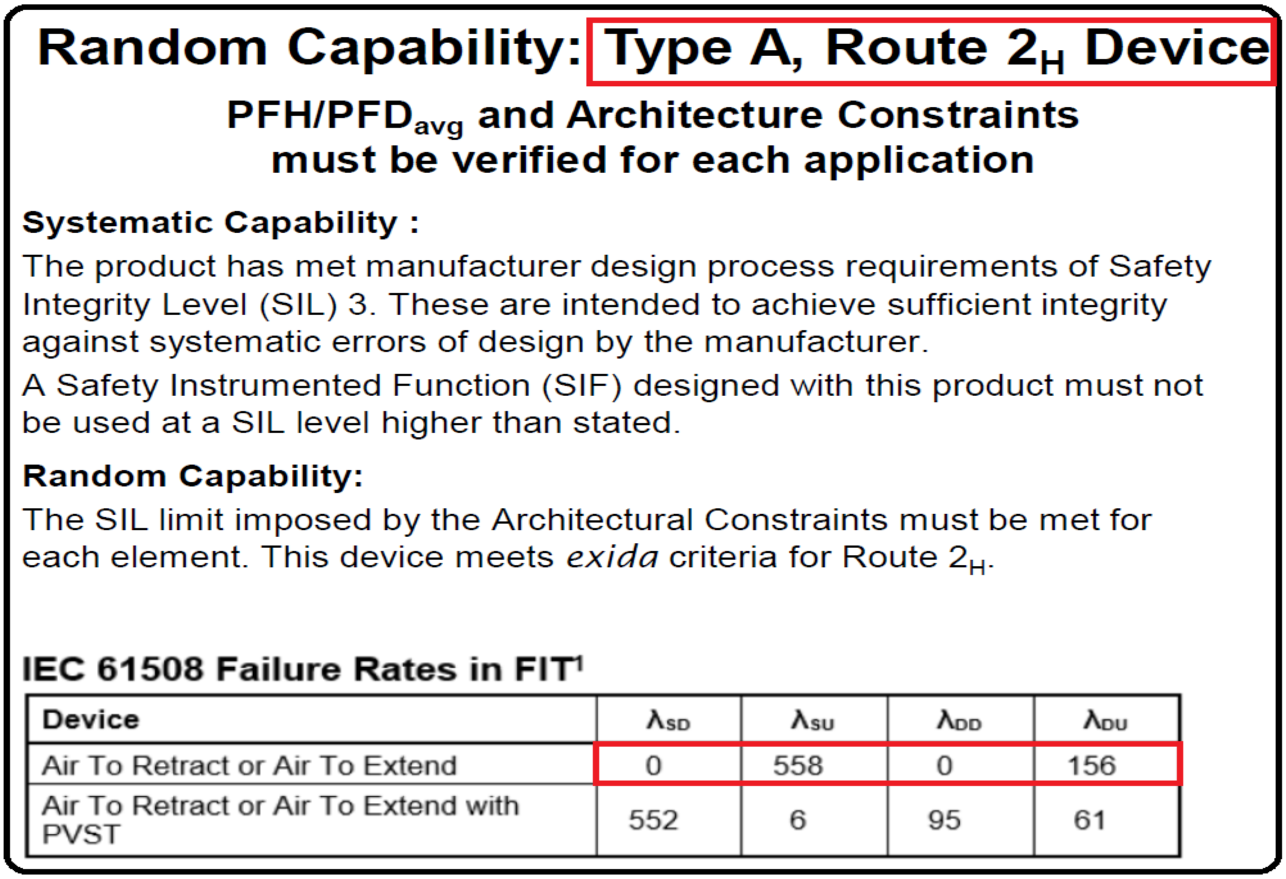


Safe Failure Fraction (SFF)	Type A elements			Type B elements		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60% - <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% - <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4



Type A elements		
Hardware Fault Tolerance (HFT)		
0	1	2
SIL1	SIL2	SIL3

4.Actuator



Random Capability: Type A, Route 2_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Systematic Capability :

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

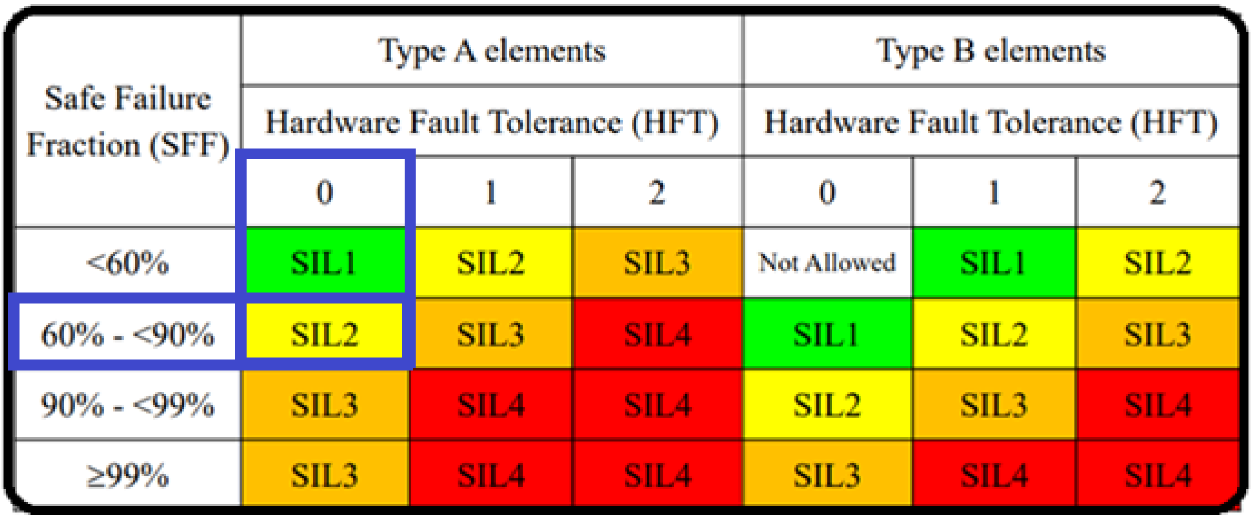
Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

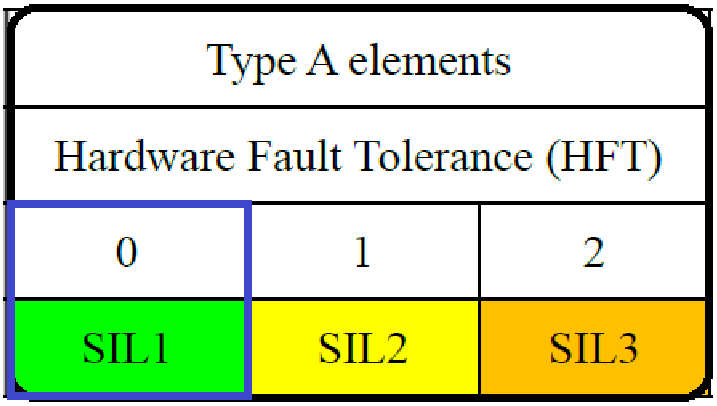
IEC 61508 Failure Rates in FIT[1]

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Air To Retract or Air To Extend	0	558	0	156
Air To Retract or Air To Extend with PVST	552	6	95	61

SFF = 558 / (558 + 156) = 78.15%



Safe Failure Fraction (SFF)	Type A elements			Type B elements		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60% - <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% - <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4



Type A elements		
Hardware Fault Tolerance (HFT)		
0	1	2
SIL1	SIL2	SIL3

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