YOKOGAWA

Co-innovating tomorrow™

Sense and non-sense of failure rates

Arjen de Koning and Ton Beems

Functional Safety Specialists

PS Congress 13th May 2026

Agenda

- **RTFM or just store “just in case”?**
- **Failure data IEC 61508 Ed.1 (1999) versus Ed. 2 (2010)**
- **Examples**
- **Proven in use / Prior use**
- **Examples**
- **Systematic Capability**
- **Examples**

Disclaimer: in this presentation we have used examples of existing safety manuals and certificates, we did our best to anonymize company names and persons but could not hide everything. It is not our intent to harm or insult companies or persons in any way.
We are human beings, human beings make mistakes, we cannot avoid this and we have to accept it. Therefore FSM: reduce or avoid (systematic) failures.

RTFM or only store for: “just in case”?

- Safety equipment needs safety specific documentation: safety manuals
- Safety manuals belong to lifecycle documentation
- What is inside:
  - Classification type A or B (simple or complicated devices)
  - Failure data (λ_{SD}, λ_{SU}, λ_{DD} and λ_{DU})
  - Possible design / application constraints
  - Declaration of systematic safety integrity (later)
- Instead of filing with the rest of the documentation, give it a read through, you may discover some unexpected things…
- Question: who is reading every safety manual?

Failure modes and failure rates

Failure modes for a device are the different ways a device can fail and can be categorized as:

- **“safe” failure mode means the device can reach safe state or is forced to the safe state**
- **“dangerous” failure mode means the device cannot reach safe state anymore**

The Failure Rate says something about the frequency of a failure mode of a component or a device. Industrial databases of failure rates per component are available for example: Siemens, TelCordia, MIL handbook etc.

Failure rate units differ per database:

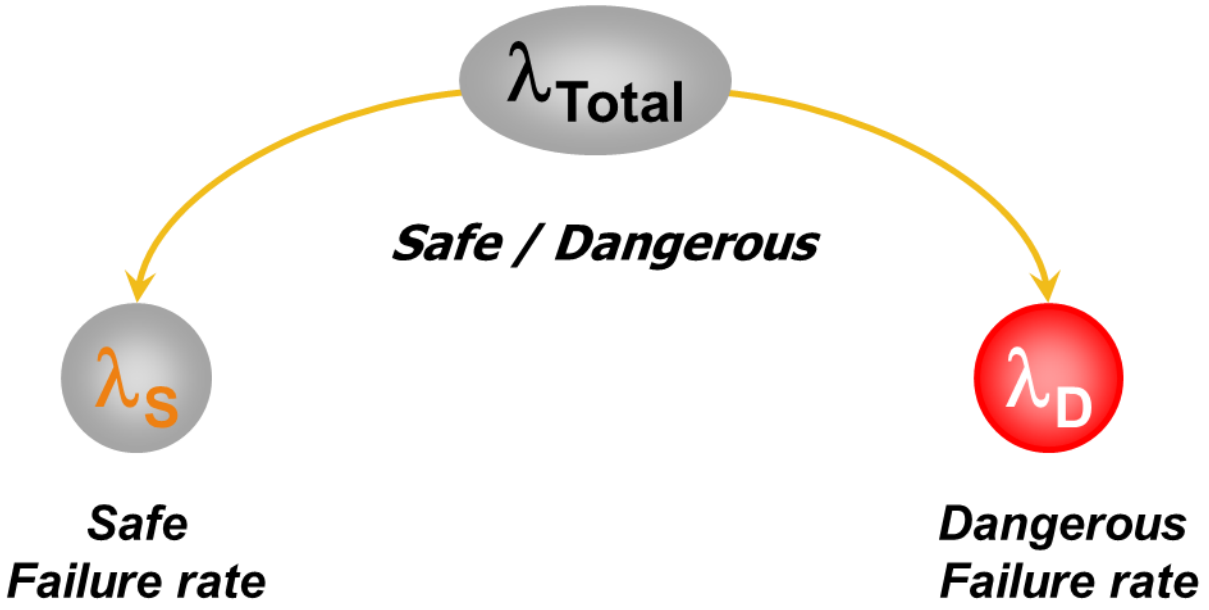
- **per year, per million hours, per billion hours (FIT), years (MTBF)**

FMEA

By analysing the failure modes of each component, the effect of such failure on the device can be determined. The overall effect can be that the device enters either in the safe or in the dangerous mode.

Adding up all component failure rates with a safe effect results in the safe failure rate of the device: λ_S

Adding up all component failure rates with a dangerous effect results in the dangerous failure rate of the device: λ_D



FMEA = Failure Modes and Effects Analysis

FMEDA

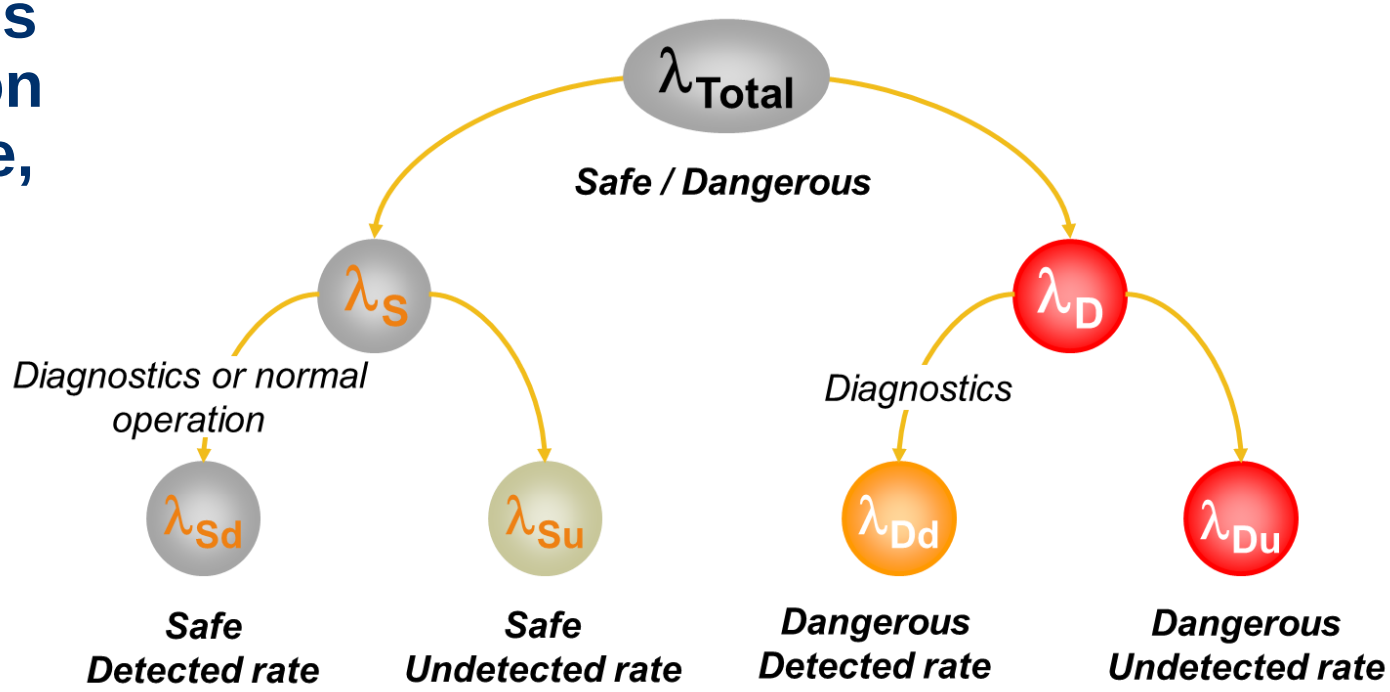
Many devices have internal diagnostics. When diagnostics is applied, failures in a device or system can be revealed. Diagnostics means a periodical/continuous automatic test

When failures are detected various actions can be taken depending on the severity of the detected failure, for example:

- **an alarm can be initiated**
- **the system can be shut down**

Now you can do an FMEDA

FMEDA = Failure Modes, Effects and Diagnostic Analysis



Failure Rates for safety calculations

These three don't really bother you :

they are detected (so you will repair them) or undetected, but safe anyway.

Of course they are not useless: these are used in the calculation of the Availability and the Safe Failure Fraction.

This one really bothers you :

it will make that the SIF cannot perform the (safety) action.

It is the only one that goes into the PFD_{AVG} calculation.

Safe Failure Fraction

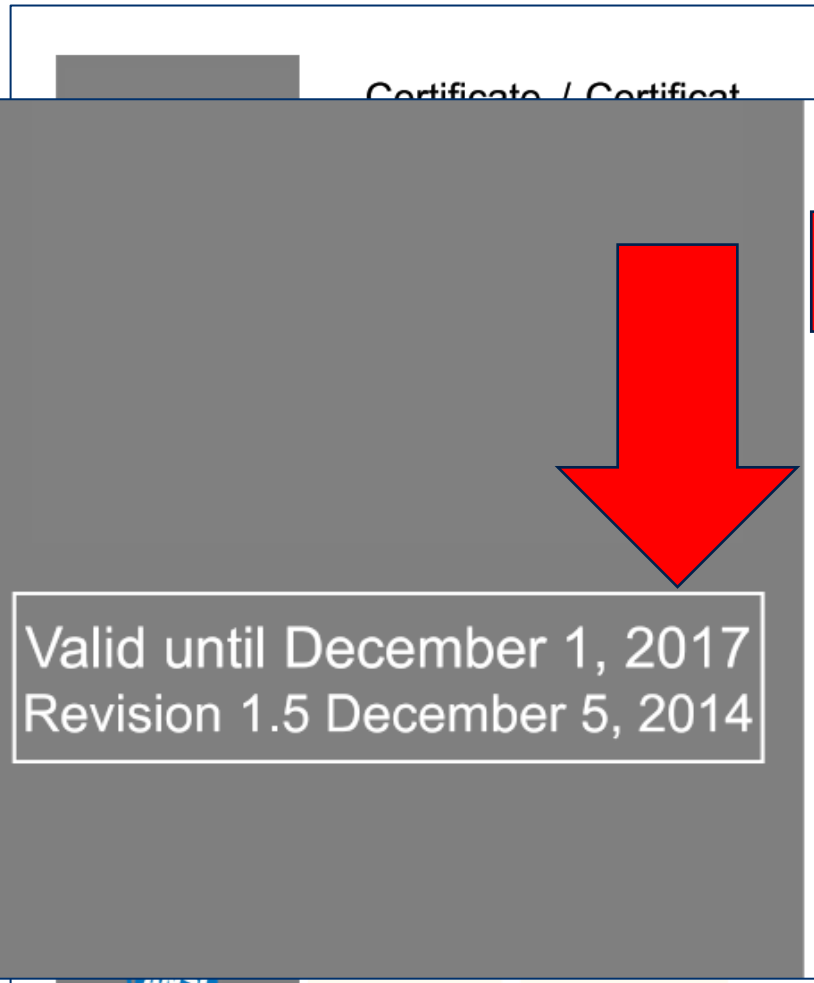
$$SFF = \frac{(\lambda_S + \lambda_{DD})}{(\lambda_S + \lambda_{DD} + \lambda_{DU})}$$

IEC61508 Edition 1 (1999) ➔ Safety Manuals started including in λ_{SU} not only "safe undetected" failures but also "No effect", "No part" etc.

If you increase λ_{SU} artificially: SFF will be close to 100%
Hence by adding components to a device SFF can increase

IEC61508 Edition 2 (2010) ➔ a component that is $\lambda_{No\ Part}$ or has $\lambda_{No\ Effect}$ on the SIF can not be part of SFF calculation anymore

Example 1: what do we see?



Has been assessed per the relevant requirements of:

IEC 61508 : 2000 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

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

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

Example 2a: what do we see?

This is to certify that the

A90RL Ball Valve

manufactured by

SRi Engineering
279-305 Bd Danielle Casanova
BP. 316
13309
MARSEILLE
FRANCE

has been assessed by with reference to the
CASS methodologies and found to meet the requirements of

IEC 61508-2:2010

The Product and its associated data contained herein can be considered for use in the design of safety functions up to and including

SIL 2* **(without PVST)**
SIL 3* **(with PVST)**

when used in accordance with the scope and conditions of this certificate.

* The Product that has been certified is not implicit of the achieved Safety Integrity Level (SIL) of the safety related system

Certification Manager:

D Stubbings

Initial Certification: 13th July 2012
This certificate issued: 13th July 2012
Renewal date: 12th July 2017

This certificate may only be reproduced in its entirety, without any change.

- **Did the design change?**
- **Without PVST your λ_{DD} is to be added to λ_{DU} , you cannot improve λ_{DU} with your PVST coverage factor!**
- **SIL4 also implies SC4 (see later!)**
- **Forget SIL3 for single valves, with only a few exceptions**

This is to certify that the

A90RL Ball Valves

manufactured by

Sud Robinetterie Industrie
279-305 boulevard Danielle Casanova
13014 Marseille
FRANCE

has been assessed by with reference to the
CASS methodologies and found to meet the requirements of

IEC 61508-2:2010

as an element/subsystem suitable for use in safety related systems performing safety functions up to and including

SIL 3* **(without PVST)**
SIL 4* **(with PVST)**

when used in accordance with the scope and conditions of this certificate.

* This certificate does not waive the need for further functional safety verification to establish the achieved Safety Integrity Level (SIL) of the safety-related system.

Certification Manager:

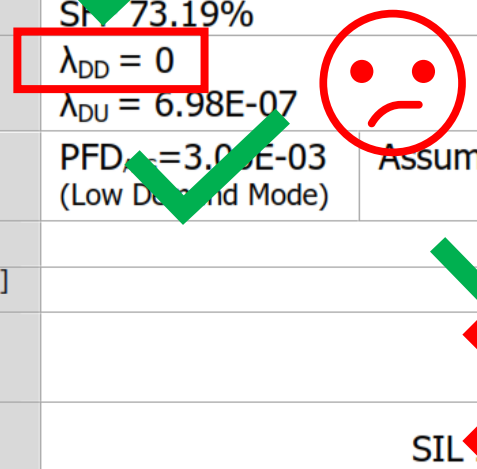
James Lynskey

Initial Certification: 14/06/2021
This certificate issued: 01/07/2021
Renewal date: 02/11/2026

Example 2b: what do we see?

Product description and scope of certification

Product Identification: A90RL Series Ball Valve			
SAFETY FUNCTION: 'To ensure the Normally Open Valve Closes in response to Actuation'			
Architectural constraints:	Type A HFT=0; (1oo1) SFF=73.19%		SIL2
Random hardware failures:	λ_{DD} = 0 λ_{DU} = 6.98E-07	λ_{SD} = 0 λ_{SU} = 1.91E-06	
Probability of failure on demand:	PFD$_{avg}$=3.05E-03 (Low Demand Mode)	Assuming: - PTI = 8760[4] MTTR = 8Hrs[4]	SIL2
Hardware safety integrity compliance[1]	Route 1_H		
Systematic safety integrity compliance[1]	Route 1_S		
Systematic Capability[2]	SC 2		
Overall SIL-capability achieved[3]	SIL 2 (Low Demand)		



If a device is suitable for SIL3 (with partial stroke testing), then the manufacturer shall have an FSM system in place with SC3

(will come back)

Safety manual 2012, page 2

Example 2c: what do we see?

Product description and scope of certification

Table1: Summary of assessment for the A90RL Ball Valves in HFT=0 configurations.

Parameter name	Symbol	1oo1 HFT=0 PTI = 6 month	1oo1 HFT=0 PTI = 1 year	2oo2 HFT=0 PTI = 6 month	2oo2 HFT=0 PTI = 1 year
Hardware Fault Tolerance	HFT	0	0	0	0
Proof Test Interval	T	4380 (6 Month)	8760 (1 year)	4380 (6 month)	8760 (1 year)
Mean Time To Repair	MTTR	3	3	3	3
Type A/B	Type A	Type A	Type A	Type A	Type A
Dangerous undiagnosed failures	λ_{DU}	6.47E-10	6.47E-10	6.47E-10	6.47E-10
PFD_{AVG}	PFD_{AVG}	1.42E-5	2.83E-5	4.25E-5	8.50E-5
SIL capability (Low demand mode)		SIL 3	SIL 3	SIL 3	SIL 3

Table 2: Summary of assessment for the A90RL Ball Valves in HFT=1 configurations.

Parameter name	Symbol	1oo2 HFT=1 PTI = 6 month	1oo2 HFT=1 PTI = 1 year	2oo3 HFT=1 PTI = 6 month	2oo3 HFT=1 PTI = 1 year
Hardware Fault Tolerance	HFT	1	1	1	1
Proof Test Interval	T	4380 (6 Month)	8760 (1 year)	4380 (6 month)	8760 (1 year)
Mean Time To Repair	MTTR	3	3	3	3
Type A/B	Type A	Type A	Type A	Type A	Type A
Dangerous undiagnosed failures		6.47E-11	6.47E-11	1.29E-10	1.29E-10
PFD_{AVG}	PFD_{AVG}	1.42E-6	2.83E-6	2.83E-6	5.67E-6
SIL capability (Low demand mode)		SIL 4	SIL 4	SIL 3	SIL 3

Safety manual 2021, page 2

- Where did PVST go??
- $PFD_{1oo1} = ½ \lambda_{DU} \times t = 2.83e^{-6}$
- λ_{DU} and PFD_{AVG} improved a factor 10^3 compared with 2012
- HFT=1 λ_{DU} and PFD_{AVG} improve factor 10^4 compared with 2012
- PFD_{AVG} in SIL 5 bandwidth?
- $PFD_{1oo2} = (\lambda_{DU}^2 \times t^2)/3 = 1.07e^{-11}$
- PFD_{2oo3} = not possible
- MTTR = 3 hrs

So, in case of detected fault, process stopped, valve removed, repaired, replaced, retested in 3 hours?

Example 3: what do we see?

CERTIFICATE

Engineering For The Future

DECLARATION OF CONFORMITY

This is to certify that the Solenoid Valve 24102 is meeting the requirement of SIL - LEVEL 2 as per guidelines of EN- 61508.

PFD value of the valve is < 9 x 10-5 at confidence interval of 90%.

The SFF according to Table A-1, IEC 61508-2 is Greater or Equal to 0.82.

Signature of the Manufacturer

Manager - Quality

INDIA

- **Date ?? ➔ IEC 61508 Ed1 or Ed 2?**
- **PFD < 9e-5 ➔ SIL4?? @ prooftest interval?**
- **Confidence interval??**
- **Type A or type B device ??**
- **SFF according table A.1 IEC 61508 part 2**

Table A.1 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction

Component	See table(s)	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Electromechanical devices	A.2	Does not energize or de-energize Welded contacts	Does not energize or de-energize Individual contacts welded	Does not energize or de-energize Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent) No positive opening (for position switches this failure is not assumed if they are built and tested according to IEC 60947-5-1, or equivalent)

Example 4: what do we see?

Useful Lifetime

A time of usage of more than 5 years (+ 1.5 years of storage) can only be favoured under responsibility of the operator, consideration of specific external conditions (securing of required quality of media, max. temperature, time of impact), and adequate test cycles. Please consider the references in the Safety Manual according test intervals and procedures as well as maintenance in respect with the useful lifetime , including the possibility of longer periods of use.

Translation:

- **After 5 years (or 6.5 incl. storage) it is not our responsibility anymore**
- **We recommend replacement every 5 years…**

HFT assessment – 3 routes

1. **IEC 61508 Route 1H** based on SFF
2. **IEC 61508 Route 2H** based on field experience (proven in use)
3. **IEC 61511** based on field experience (prior use)

IEC 61508 Route 1H (SFF based)

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Table 3 — Hardware safety integrity: architectural constraints on type B safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

Type A: simple devices **Type B: complicated devices**

Based on field experience

IEC 61508 Route 2H (proven in use)

IEC 61511 (prior use)

SIL		Minimum Hardware Fault Tolerance (see clause 7.4.4.3)
1	any mode	0
2	low demand mode	0
2	high demand or continuous mode	1
3	any mode	1
4	any mode	2

IEC 61508 - failure data must be:

- based on feedback from field operation in a similar application and environment
- collected in accordance with international standards
- evaluated and judged by expert

IEC 61511 – failure data formulated slightly different:

- also based on similar operating environments.

Who can really claim proven in use / prior use ?

Who has the overview of:

- the total number of the (same) devices
- same application, same environment
- maintenance records, failure records
- all this for many years

The End User!

Do manufacturers know:

- where their hardware eventually is installed (Arctic vs. Dessert)
- how correct maintenance is done
- if replacement is done without their knowing
- all this for many years

NO!!!

Example - Valves: market is flooded with 2H certificates

Why are they successful?

- if it looks official enough, people believe everything…
- from “trustworthy” companies
- people do not read the certificates anymore…

Safety Certificate page 1

exida

The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 3 CAPABLE

Revision 2.0 June 30, 2016
Surveillance Audit Due
April 1, 2019

Certificate / Certificat
Zertifikat / 合格証

ASC 1301001 C005

exida hereby confirms that the:

Series 551 and 553 Pilot Operated Inline Spool Valves

ASCO Numatics
Lucé, France

Have 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

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

Safety Function:
The Valve will move to the designed safe position when de-energized within the specified safety time.

Example - Valves: market is flooded with 2H certificates

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

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

Systematic Capability :

These products have 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 these products 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.

Safety Certificate page 2

Google

Key Exida Criteria for Proven in Use

- **Operational History:** Extensive field data demonstrating the device has been used successfully in similar environments and applications.
- **Field Data Accuracy:** A documented and maintained quality system for collecting field return data to ensure data accuracy.
- **Failure Analysis:** A rigorous assessment to prove the absence of systematic faults, including a review of revision history.
- **Data Sufficiency:** Sufficient operating hours must be documented to support the required safety integrity level.
- **IEC 61508 Requirements:** The evidence must demonstrate that the device complies with the requirements of IEC 61508, or specifically 7.4.4.1.1 for user-driven prior use, to be considered for use in a safety-instrumented system. exida +3

This is 114155 years…

Route 2H Focus

- **Exida often uses a 2H approach**, requiring over 1,000,000,000 unit operating hours in field failure data for all components.
- The device should typically have a diagnostic coverage (for dangerous failures) of 60% or more, particularly for Type B components.
- No new technology (i.e., components lacking extensive field history) should be present. exida +1

Do you read the small letters?

So not the IEC 61508 Ed2 criteria but some "home-made" requirements instead…

And the people that do read and understand the IEC standards feel like fighting windmills

Systematic Safety Integrity – Systematic Capability

Three basic requirements have to be fulfilled in order to claim any SIL:

1. **PFD_{AVG} of the SIF shall be within the target SIL bandwidth.**
2. **Hardware fault tolerance (HFT) for the target SIL to be justified.**

Hardware safety integrity

3. **Systematic Capability shall comply with the requirements for the target SIL**

Systematic safety integrity

SC is a measure of the quality of the (manufacturer's) organization and its Functional Safety Management system. It is expressed as SC1 to SC4 and must correspond with the (highest) target SIL.

Who shall prove Systematic Capability?

Systematic Capability is determined by the applied Functional Safety Management (FSM) in an FSM system for:

1. **The manufacturers of all bought-in devices in the (pipe to pipe) SIF:**

   Declaration of manufacturer is needed (or from certification body).

2. **For all parties involved in the safety life cycle (End User, EPC, SIS integrator etc.) .**

Systematic Capability is determined by the applied FSM:

- **Have an FSM system in place which is regularly audited by someone with the correct independence. The higher the required SIL level, the more independence is required (independent department/organization).**
- **Audit report to draw a conclusion on the achieved systematic safety integrity (SC).**

Example - Systematic Capability understood?

12. SYSTEMATIC CAPABILITY

The systematic capability of the device is 3.

This systematic capability is guaranteed only if the user:

- Use the device according to the instructions for use and to the present Manual.
- Use the device in the appropriate environment (limitation of use).

3.6 Systematic integrity

Systematic integrity requirements according IEC 61508 up to and including Safety Integrety level (SIL) 3 are fulfilled. These requirements include adequate integrity against systematic errors in the product design, and controlling systematic failures in the selection and manufacturing process. Series 5000, 6000, 7000, 9000 flanged ball valves must not be used in safety integrity functions with higher than the stated SIL level without a proven in use statement or, in some cases, redundant designs.

With this knowledge, can you tell me?

My Japanese colleague designed a new transmitter and asks me what to do to make it a SIL transmitter.

What will be my 3 answers?

1. **Do an FMEDA. (for the λ_{SD} λ_{SU} λ_{DD} and λ_{DU} ➔ PFD_{AVG} and SFF**
2. **Setup an FSM system for your design and manufacturing organization to prove SC.**

Then it becomes very silent…

3. **Or, talk to your colleagues who designed the EJX transmitter, they have already done it…**

YOKOGAWA

Any questions ?

Co-innovating tomorrow™

Want to know more?

- **Visit us on our stand**
- **Come to our Safety event in Amersfoort on 24th June**

YOKOGAWA

Co-innovating tomorrow™

TON
BEEMS

DAVE
VAN DEN HAM

ARJEN
DE KÖNING

CLAUDY
DE GROOTE

JOIN US

Safety inspiration in-depth session

June 24 2026, 09:30-13:00, Amersfoort