MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

SIL – SAFETY INTEGRITY LEVEL

CLARIFYING MYTHS AND TRUTHS ABOUT SIL CERTIFICATION

Technical Center of Excellence
Webinar

23 Feb 2022

Webinar agenda

Subjects we will discuss

Why is SIL certification important?

- What is functional safety
- Functional safety standards

What does it mean? What does it imply?

- Certification process
- What means "SIL Certified"

How to interpret SIL certificates and major safety indicators

- Functional Safety jargon
- How to read a SIL certificate

Myths and Truths

- Some common myths and truths
- Q&A

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

WHY IS SIL CERTIFICATION IMPORTANT?

WHAT IS FUNCTIONAL SAFETY

SIL Certification

What is functional safety?

SIL Certification

What is functional safety?

To what risk am I exposed?

SIL Certification

What is functional safety?

To what risk am I exposed?

Height?

SIL Certification

What is functional safety?

To what risk am I exposed?

Height?

Landing zone?

5 seconds? 15 minutes?
Every day?

SIL Certification

What is functional safety?

To what risk am I exposed?

Height?

Landing zone?

5 seconds? 15 minutes?
Every day?

RISK

SIL Certification

What is functional safety?

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the gear well designed?
Well manufactured?

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the gear well designed?
Well manufactured?

Is there a defect?
Is it scratching on a rock?

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the gear well designed?
Well manufactured?

Is there a defect?
Is it scratching on a rock?

Am I using it properly?
Is it appropriated for my case?

SIL Certification

What is functional safety?

Risk reduction measures effectiveness

Risk reduction effectiveness?

Was the gear well designed?
Well manufactured?

Is there a defect?
Is it scratching on a rock?

Am I using it properly?
Is it appropriated for my case?

SIL Certification

What is functional safety?

To what risk am I exposed?

Height?

5 seconds? 15 minutes? Every day?

Landing zone?

RISK

Am I using it properly?
Is it appropriated for my case?

Risk reduction effectiveness?

Was the gear well designed?
Well manufactured?

Is there a defect?
Is it scratching on a rock?

Am I using it properly?
Is it appropriated for my case?

Risk reduction measures effectiveness

RISK REDUCTION FACTOR

Functional Safety

Why SIL certification is important?

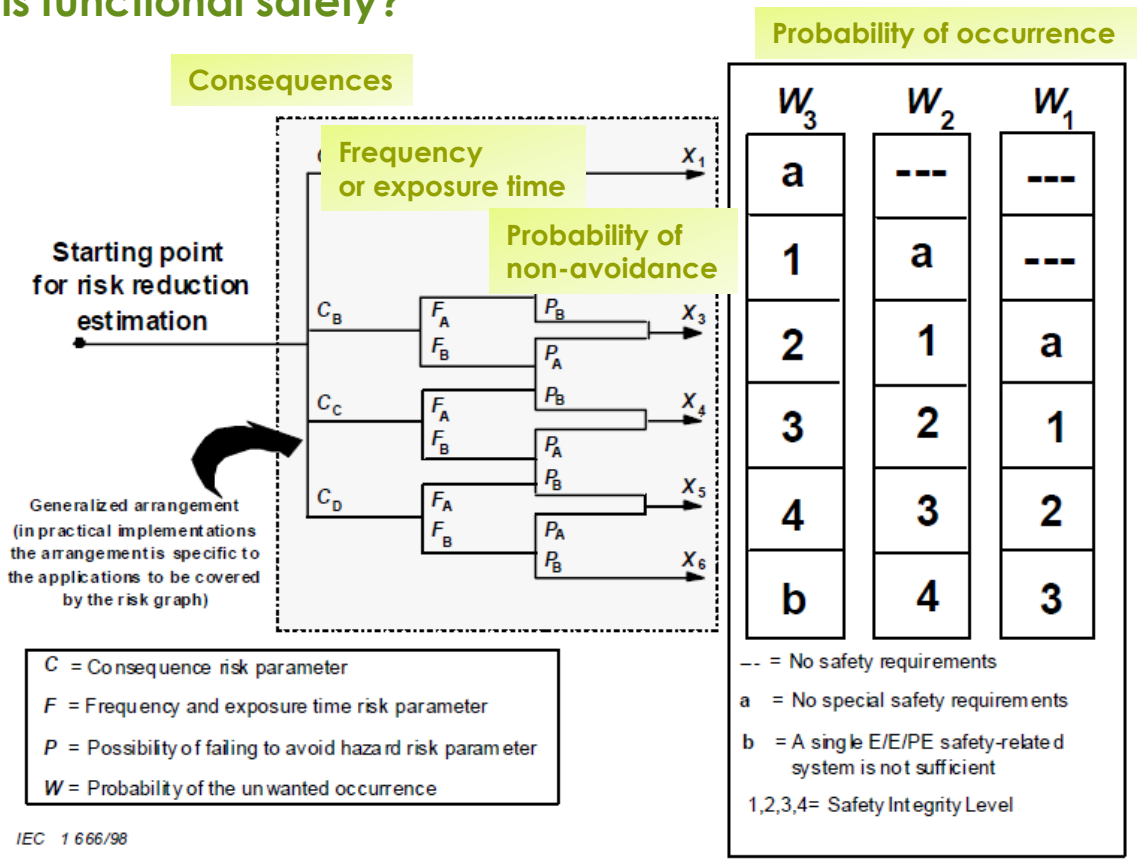
To what risk am I exposed?

Risks and hazards

SIL Certification

What is functional safety?

To what risk am I exposed?



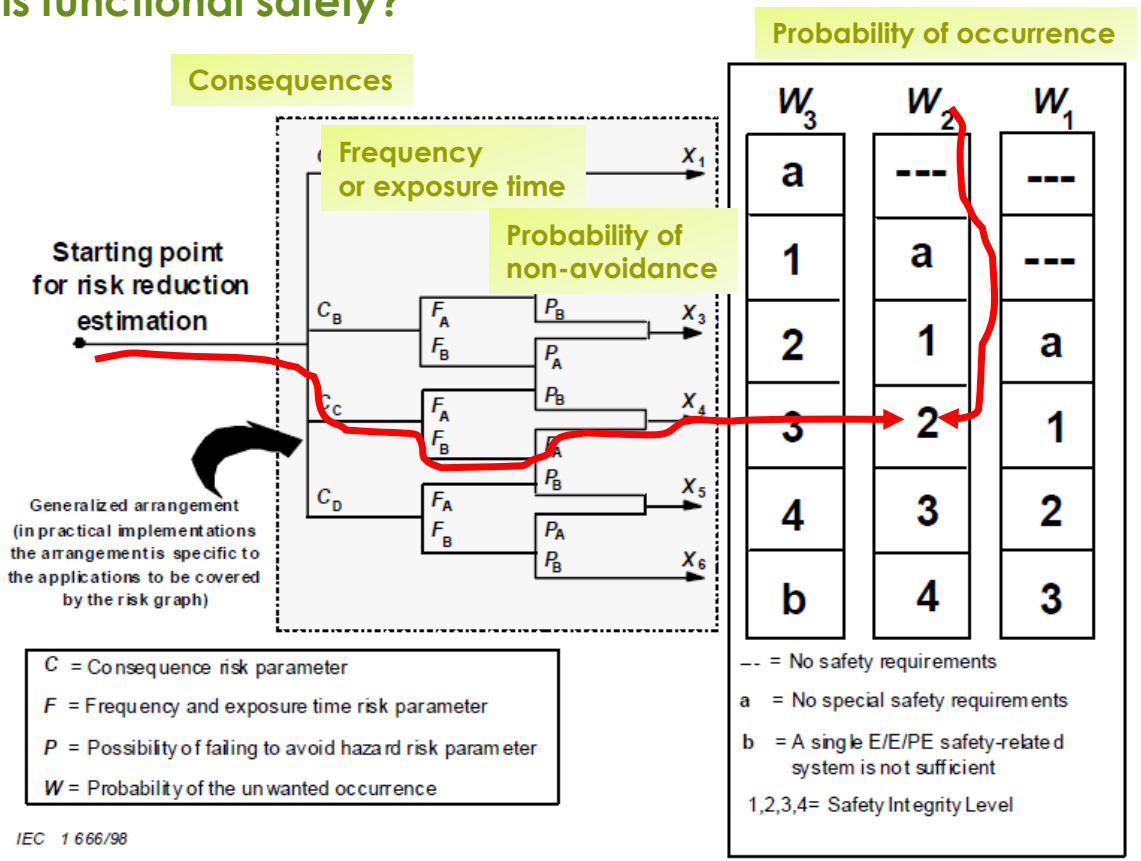
Evaluation of risk

MEGGITT

SIL Certification

What is functional safety?

To what risk am I exposed?



Evaluation of risk

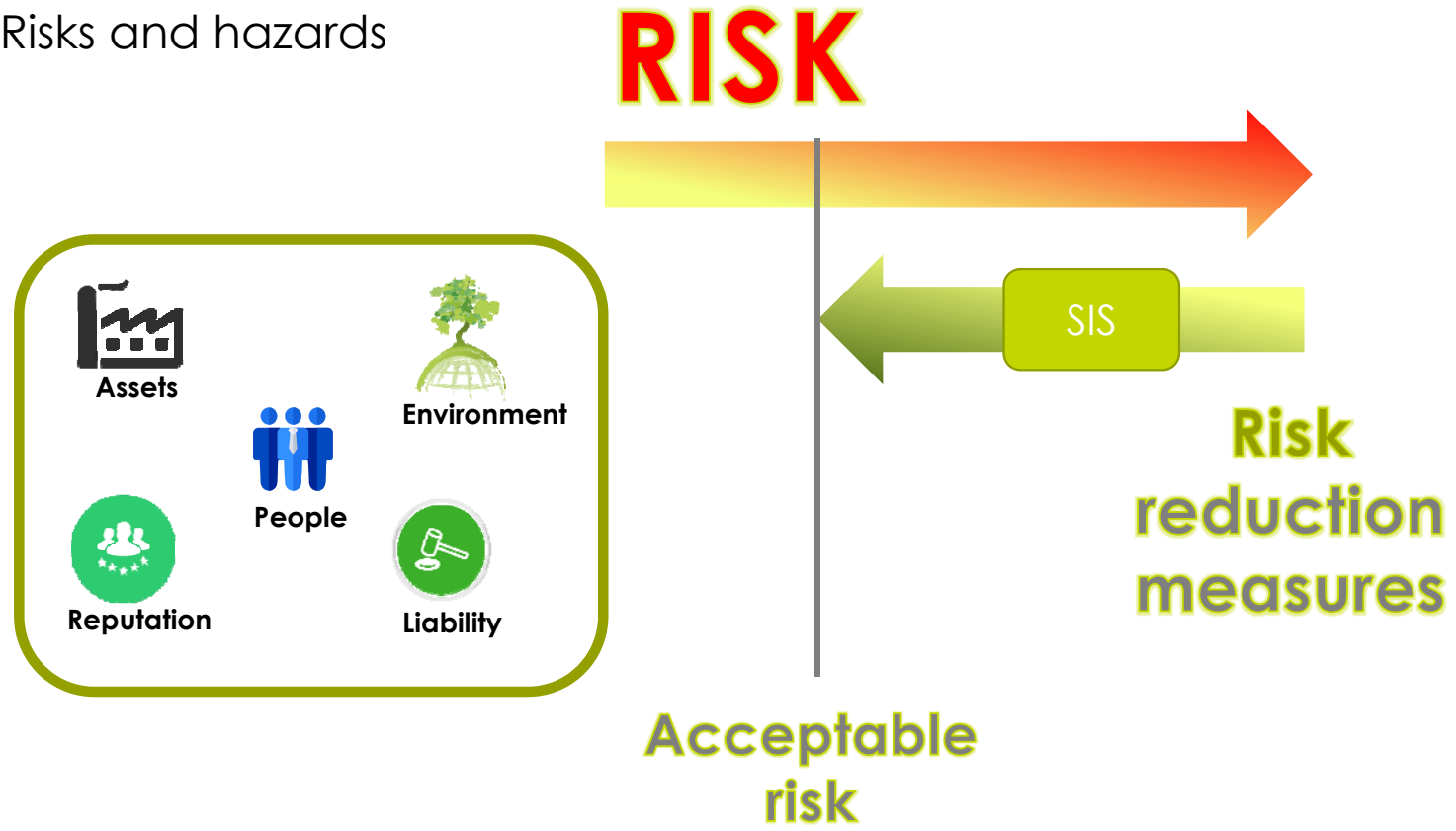
MEGGITT

Functional Safety

Why SIL certification is important?

To what risk am I exposed?

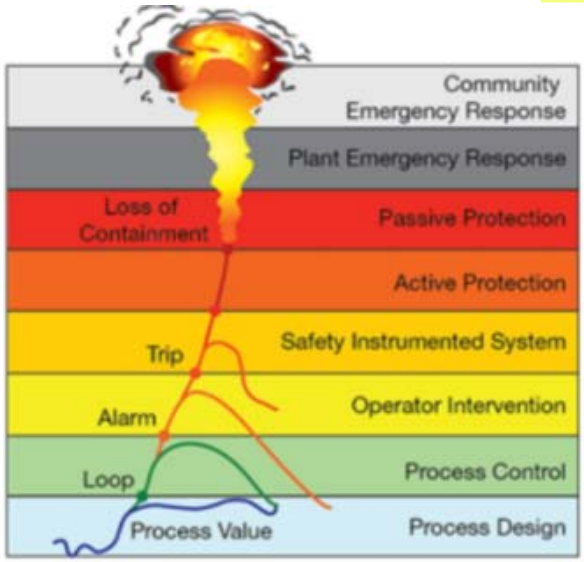
Risks and hazards

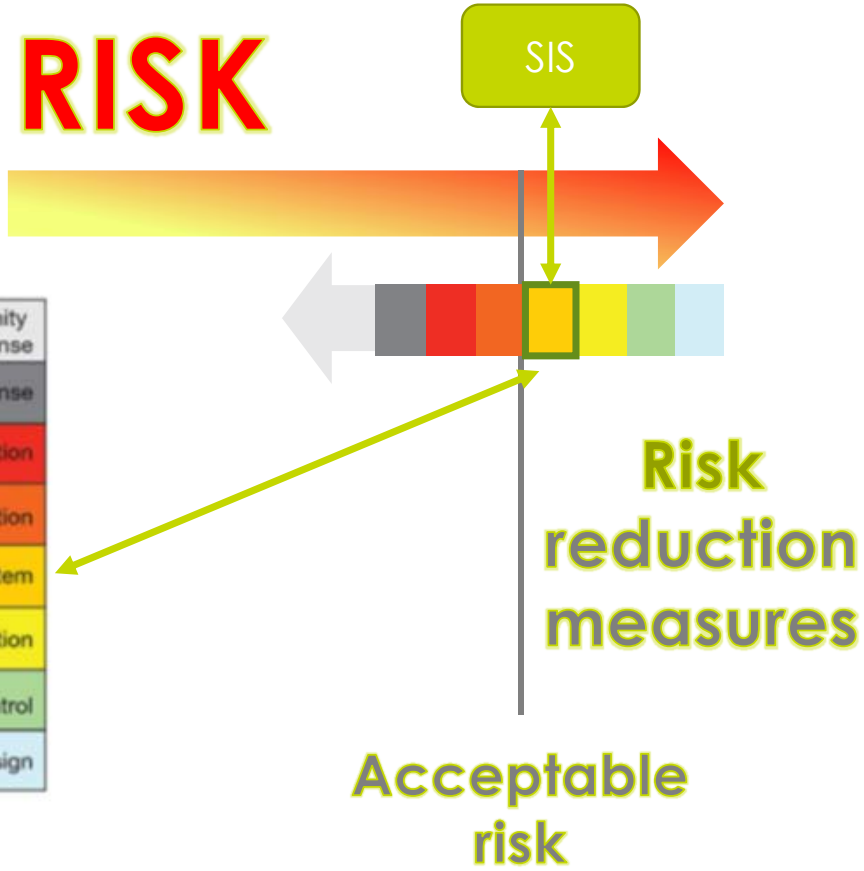


Functional Safety

Why SIL certification is important?

Risks and hazards





To what risk am I exposed?

SIL Certification

What is functional safety?

To what risk am I exposed?

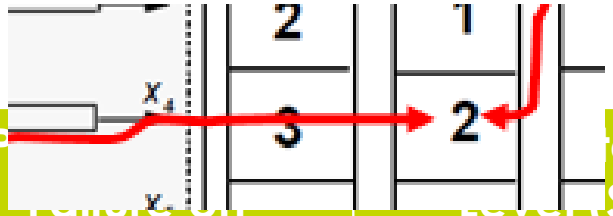
Risk Reduction Factor	Probability of Failure on Demand	Safety Integrity Level (SIL)
10 to 100	0.1 to 0.01	SIL 1
100 to 1'000	0.01 to 0.001	SIL 2
1'000 to 10'000	0.001 to 0.0001	SIL 3
10'000 to 100'000	0.0001 to 0.00001	SIL 4

Risk reduction vs Safety Integrity Level

SIL Certification

What is functional safety?

To what risk am I exposed?



Risk Reduction Factor	Probability of Failure on Demand	Safety Integrity Level (SIL)
10 to 100	0.1 to 0.01	SIL 1
100 to 1'000	0.01 to 0.001	SIL 2
1'000 to 10'000	0.001 to 0.0001	SIL 3
10'000 to 100'000	0.0001 to 0.00001	SIL 4

Risk reduction vs Safety Integrity Level

RISK REDUCTION EFFECTIVENESS

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the rope well designed?
Well manufactured?

Is there a defect in the rope?
Is it scratching on a rock?

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the rope well designed?
Well manufactured?

Systematic

Is there a defect in the rope?
Is it scratching on a rock?

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the rope well designed?
Well manufactured?

Systematic

Is there a defect in the rope?
Is it scratching on a rock?

Random

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the rope well designed?
Well manufactured?

Systematic Capability

Systematic

Probability of Failure

Is there a defect in the rope?
Is it scratching on a rock?

Random

SIL Certification

What is functional safety?

Risk reduction effectiveness?

Was the rope well designed?
Well manufactured?

Systematic Capability

Systematic

Is there a defect in the rope?
Is it scratching on a rock?

Probability of Failure

Random

Am I using it properly?
Is it appropriated for my case?

SIL Certification

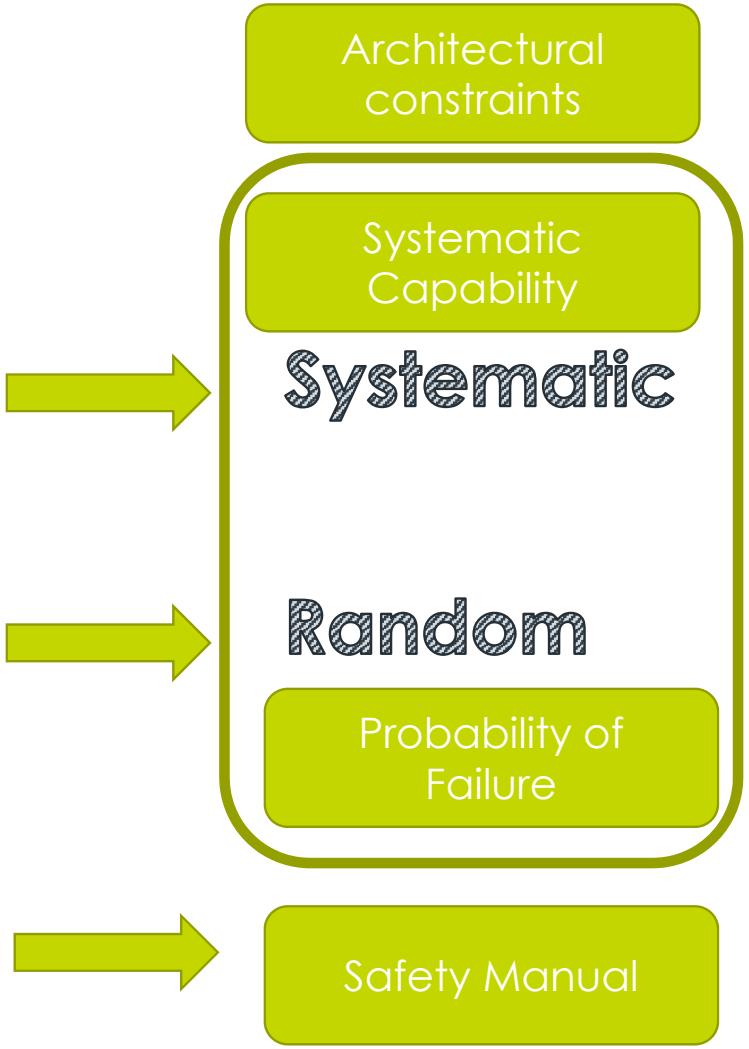
What is functional safety?

Risk reduction effectiveness?

Was the rope well designed?
Well manufactured?

Is there a defect in the rope?
Is it scratching on a rock?

Am I using it properly?
Is it appropriated for my case?



MEGGITT

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

FUNCTIONAL SAFETY

SIL Certification

What is functional safety?

RISK

To what risk am I exposed?

Height?

5 seconds? 15 minutes?
Every day?

Landing zone?

Risk reduction measures

Probability of failures?

Was the gear well designed?
Well manufactured?

Is there a defect?
Is it scratching on a rock?

The main goal of functional safety is to ensure that: **"…The safety function will be performed correctly or the system will fail in a predictable and safe manner. "**

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

WHY IS SIL CERTIFICATION IMPORTANT?

FUNCTIONAL SAFETY STANDARDS

SIL Certification

Functional Safety Standards

Requirements for suppliers of process control and instrumentation safety instruments

Ensures that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL)

Applicable for

- electrical
- electronic
- programmable electronic safety related systems

SIL Certification

Functional Safety Standards

Requirements for suppliers of process control and instrumentation safety instruments

IEC61508

Ensures that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL)

Applicable for

- electrical
- electronic
- programmable electronic safety related systems

SIL Certification

Functional Safety Standards

MEGGiTT

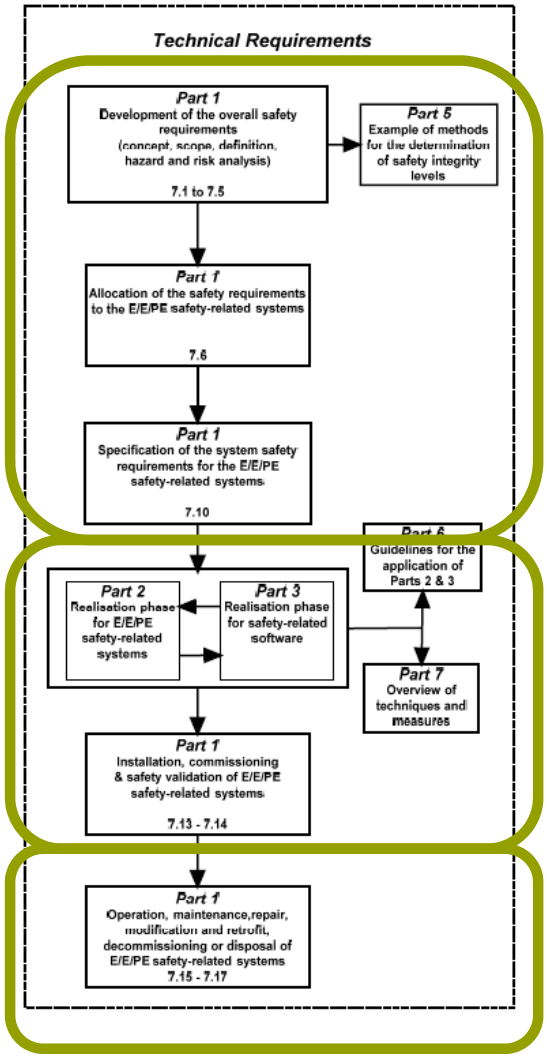
SIL Certification

IEC61508

Conceptualization and specification phases

Realization and validation phases

Operation, maintenance and decommissioning phases

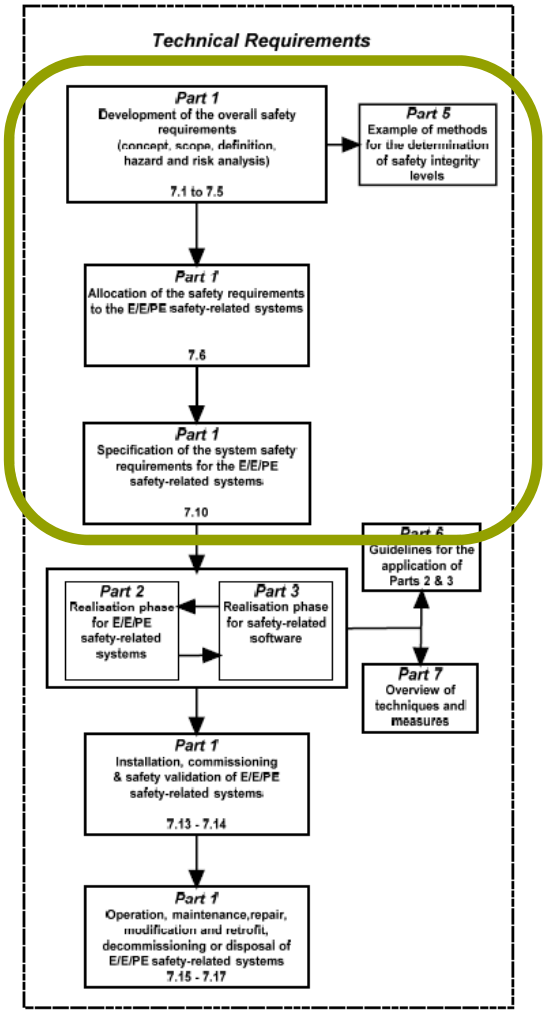


MEGGITT

SIL Certification

IEC61508

Conceptualization and specification phases

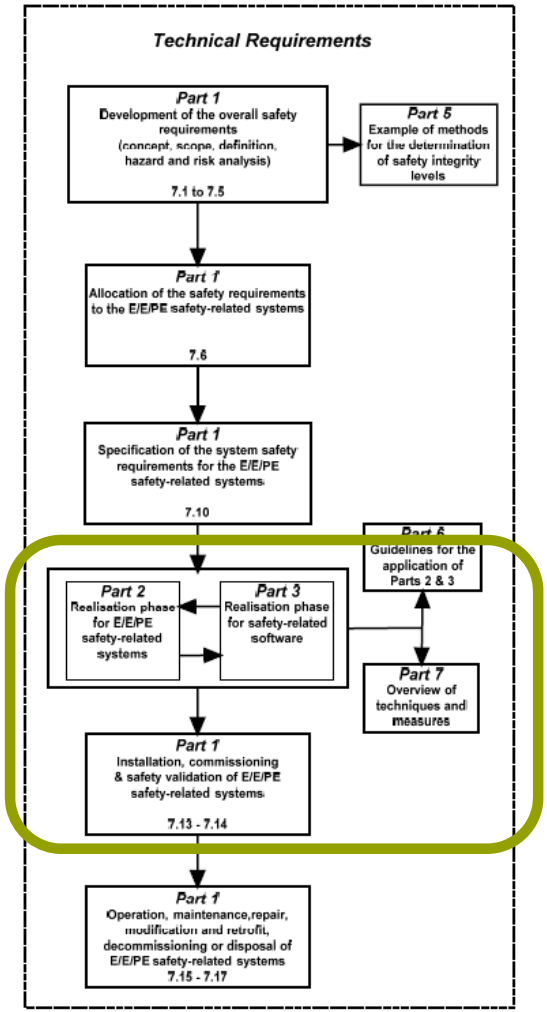


MEGGITT

SIL Certification

IEC61508

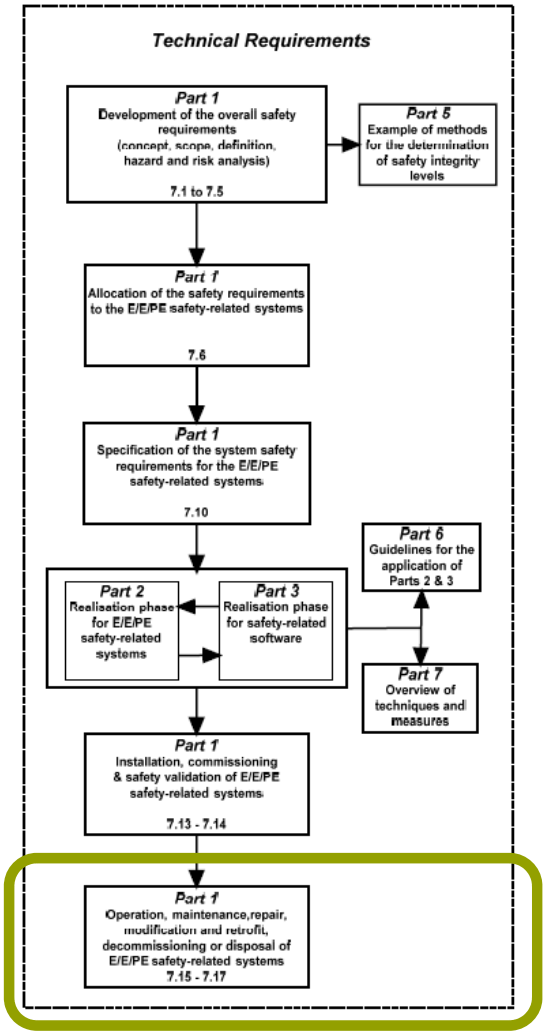
Realization and validation phases



MEGGITT

SIL Certification

IEC61508

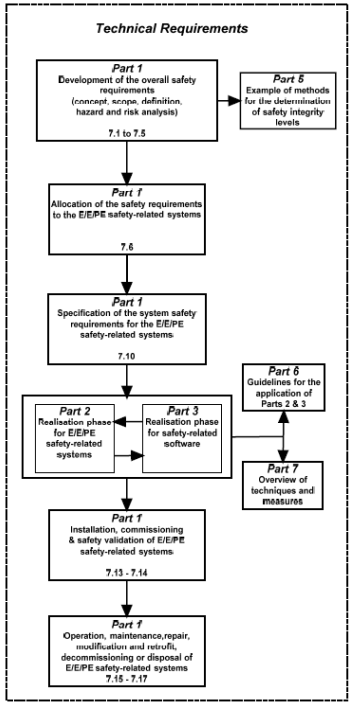


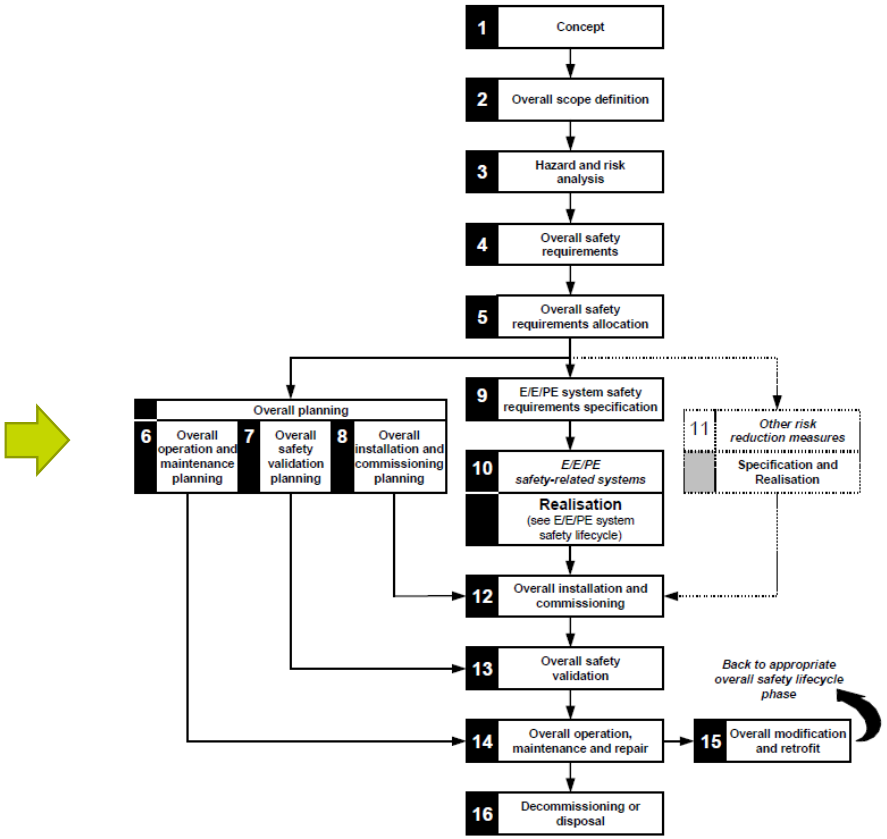
Operation, maintenance and decommissioning phases

MEGGITT

SIL Certification

IEC61508





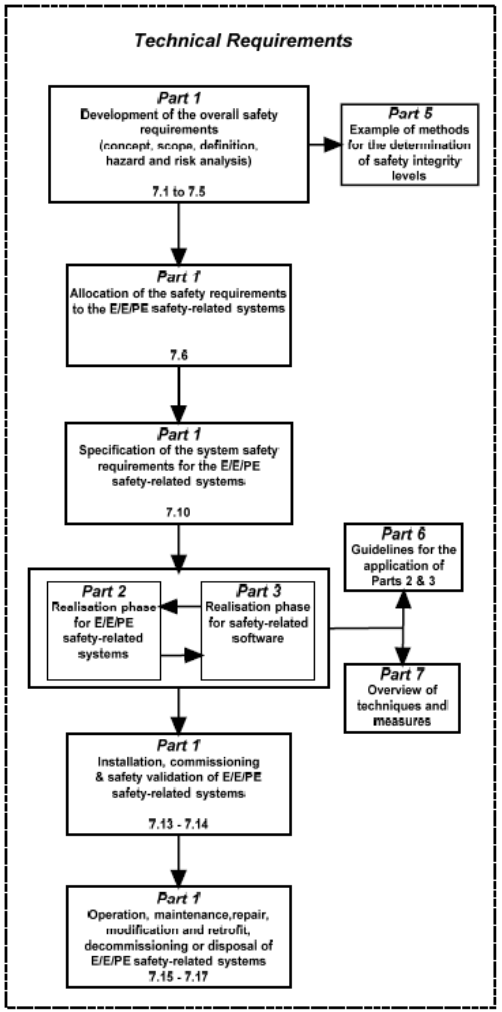
SIL Certification

IEC61508

Conceptualization and specification phases

Realization and validation phases

Operation, maintenance and decommissioning phases



MEGGiTT

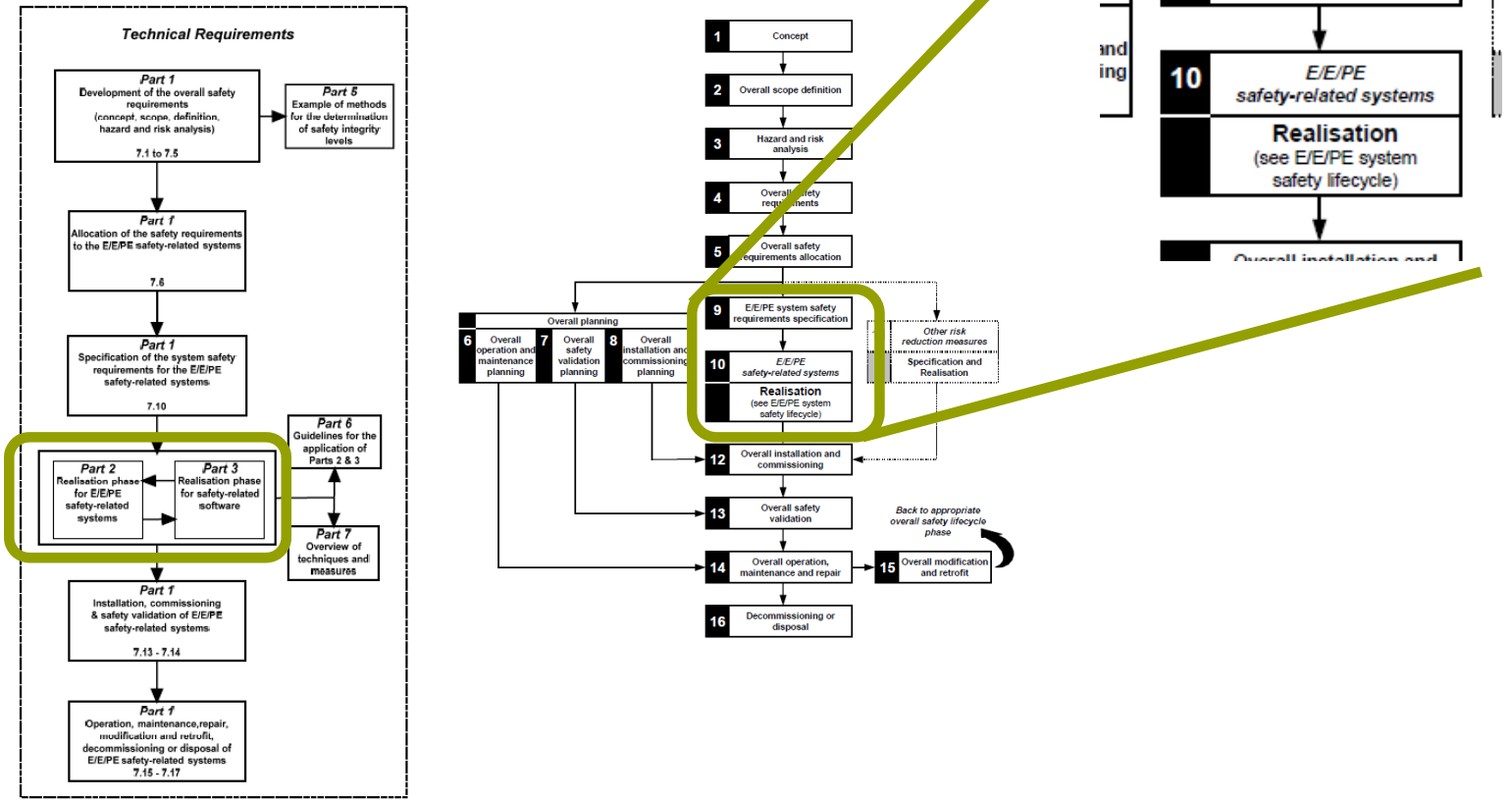
Enabling the Extraordinary
To Fly To Power To Live

WHAT DOES IT MEAN, WHAT IT IMPLIES?

CERTIFICATION PROCESS

SIL Certification

IEC61508



MEGGITT

SIL Certification

IEC61508

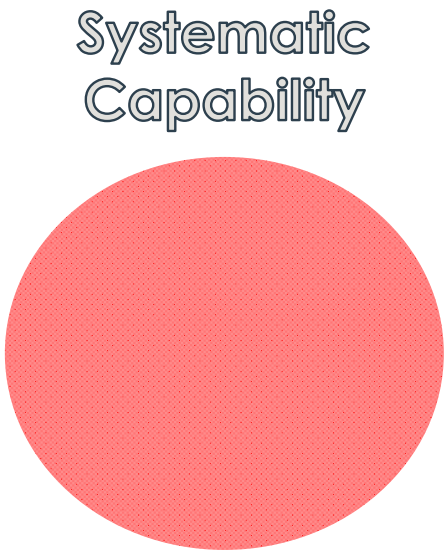
What is SIL…?

Risk Reduction Factor	Probability of Failure on Demand	Safety Integrity Level (SIL)
1o to 100	0.1 to 0.01	**SIL 1**
100 to 1'000	0.01 to 0.001	**SIL 2**
1'000 to 10'000	0.001 to 0.0001	**SIL 3**
10'000 to 100'000	0.0001 to 0.00001	**SIL 4**

SIL Certification

IEC61508

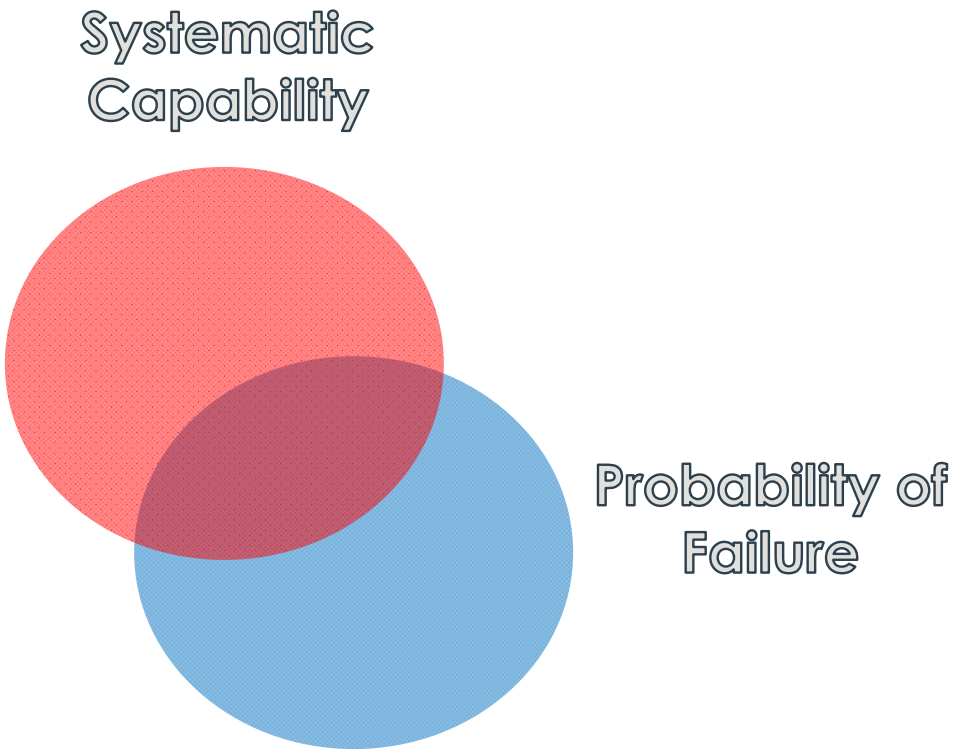
What is SIL…?



SIL Certification

IEC61508

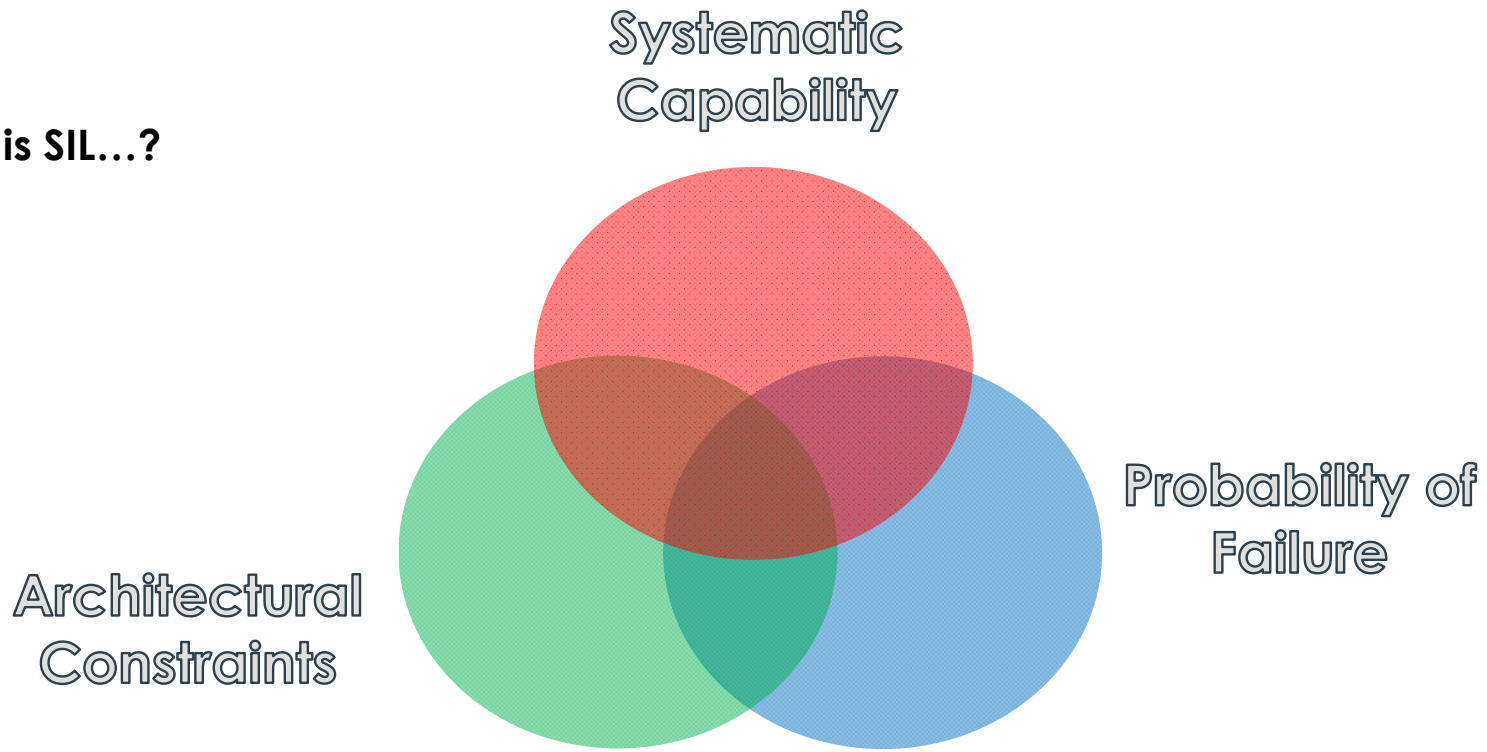
What is SIL…?



SIL Certification

IEC61508

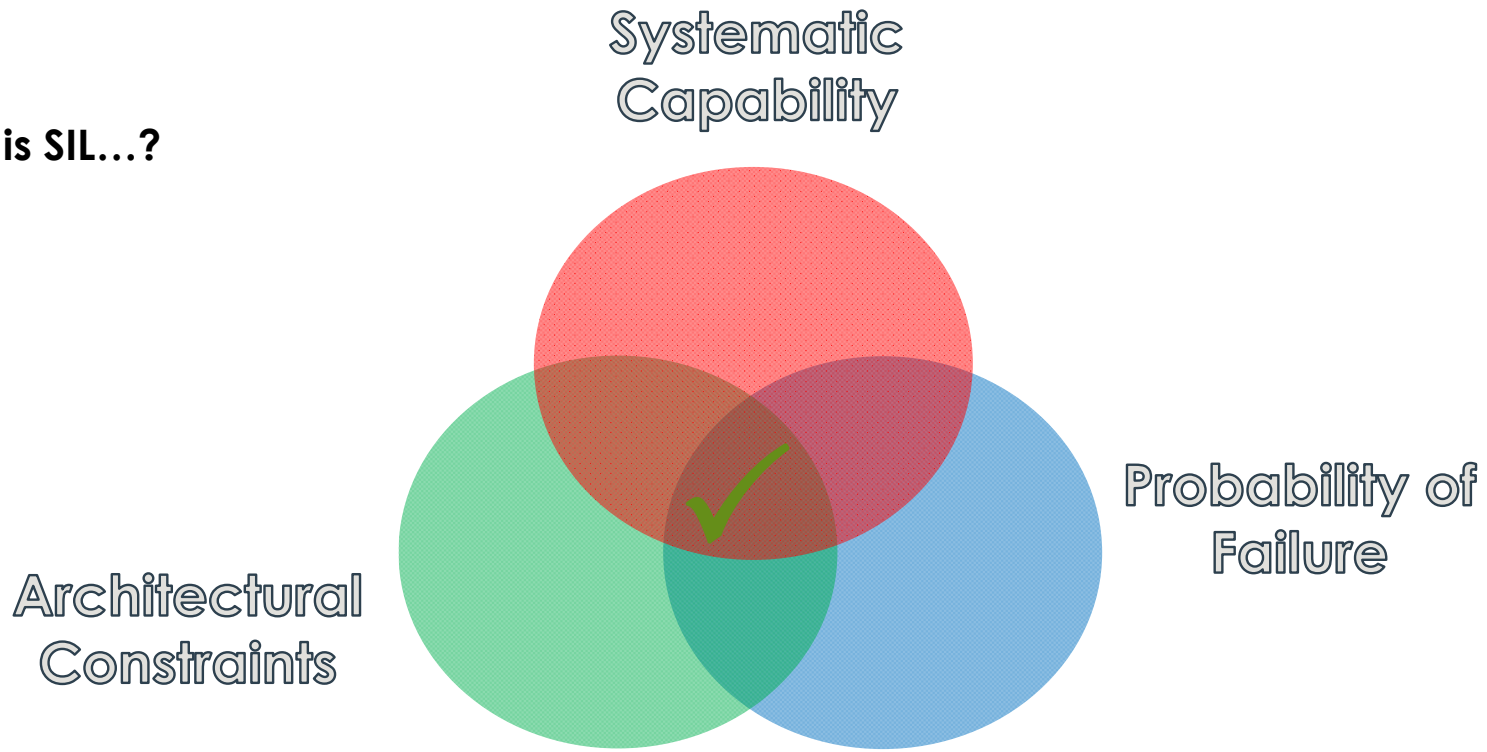
What is SIL…?



SIL Certification

IEC61508

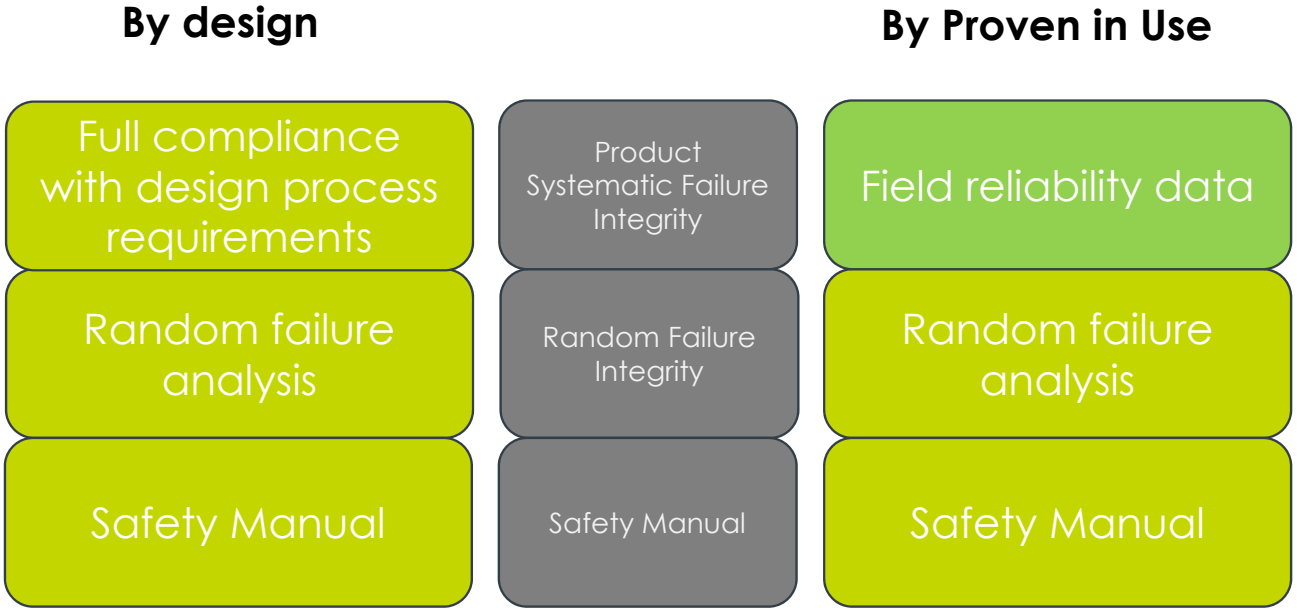
What is SIL…?



SIL Certification

IEC61508

SIL certification process for E/E/PE Safety-related systems



SIL Certification

IEC61508

SIL certification process for E/E/PE Safety related systems

Certification artifacts:

- **FMEDA**
- **FIT**
- **Sw HAZOP**
- **Functional Safety Mng Plan**
- **Safety Requirements Specification**
- **Verification test plan**
- **Validation test plan**
- **Tool classification**
- **Sw coding guidelines**
- **Safety Manual**
- **… and many others…**

SIL Certification

IEC61508

SIL certification process for E/E/PE Safety related systems

Minimum level of independence	SIL1	SIL2	SIL3	SIL4
Independent person				
Independent department				
Independent external organization				

Accepted

Accepted under conditions

Not accepted

SIL Certification

IEC61508

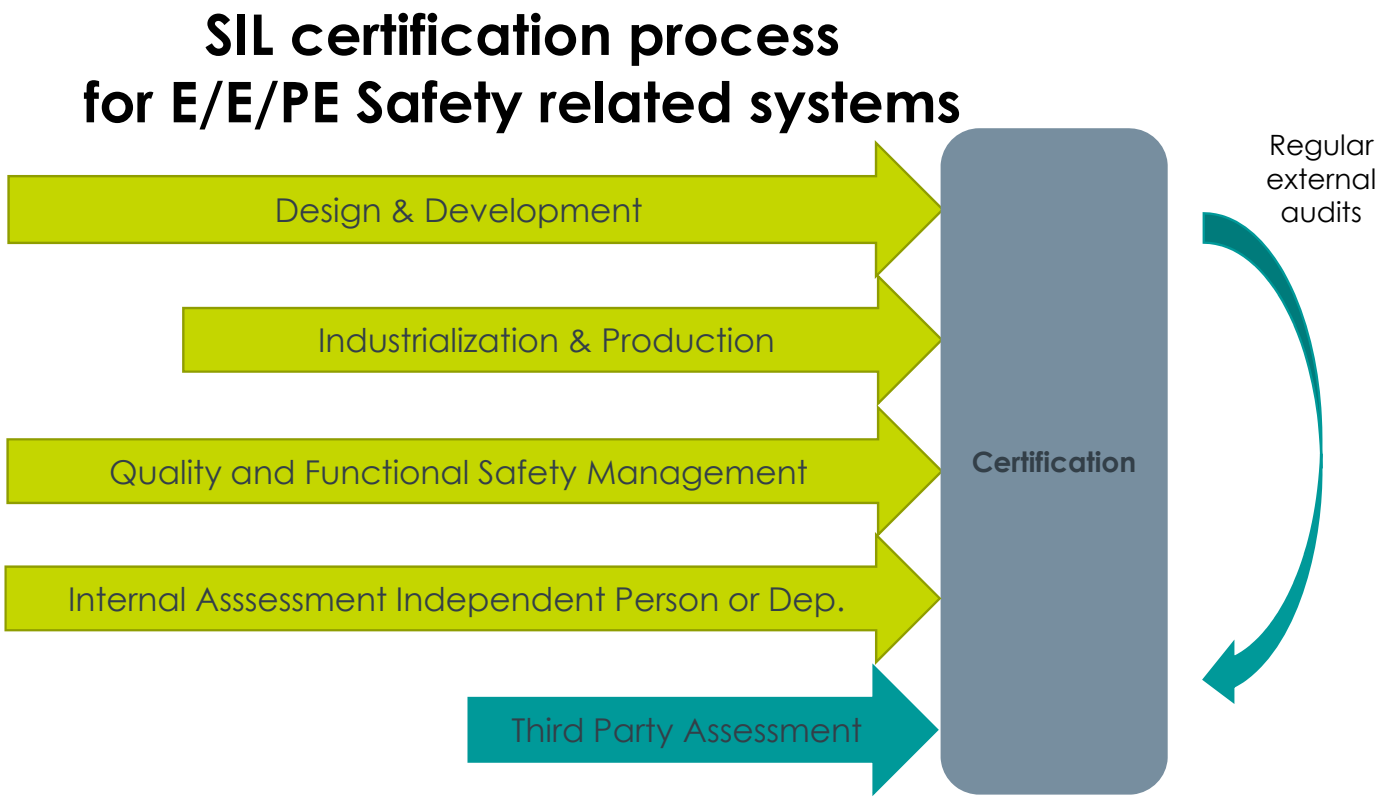
SIL certification process for E/E/PE Safety related systems

Minimum level of independence	SIL1	SIL2	SIL3	SIL4
Independent person				
Independent department				
Independent external organization				

- Accepted
- Accepted under conditions
- Not accepted

SIL Certification

IEC61508



MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

SIL CERTIFICATION PROCESS

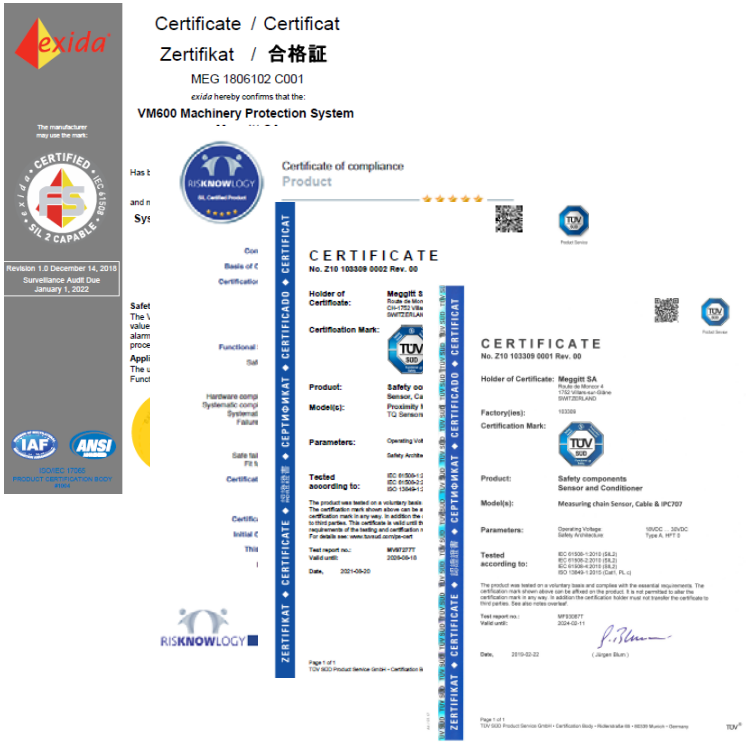
WHAT DOES IT MEAN TO BE CERTIFIED

SIL Certification

Functional Safety Standards

Credibility of safety properties

- Systematic fault avoidance
- Random fault avoidance
- Application context



"…The safety function will be performed correctly or the system will fail in a predictable and safe manner. "

MEGGITT

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

HOW TO INTERPRET A SIL CERTIFICATE

FUNCTIONAL SAFETY TERMS & ABBREVIATIONS

IEC61508

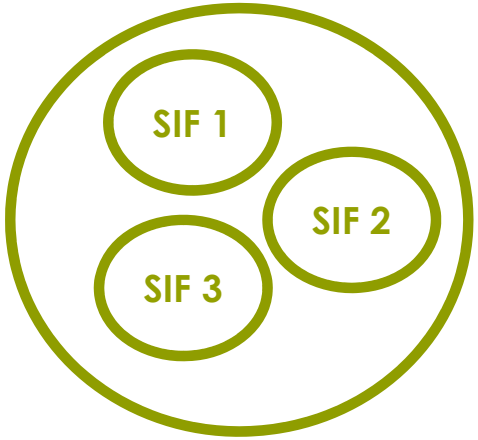
Terminology and basic definitions

SIL Certification

Functional Safety Terms and Abbreviations

SIS: Safety Instrumented System is a combination of sensors, controllers and actuators to execute one or more SIF.

SIF: Safety Instrumentated Function is a set of equipment used to reduce the risk to a specific hazard.



SIL Certification

Functional Safety Terms and Abbreviations

SIS: Safety Instrumented System is a combination of sensors, controllers and actuators to execute one or more SIF.

SIF: Safety Instrumentated Function is a set of equipment used to reduce the risk to a specific hazard.

Safety function: function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state.

Safe-state: a state where the hazard is removed.

SIL Certification

Functional Safety Terms and Abbreviations

SIS: Safety Instrumented System is a combination of sensors, controllers and actuators to execute one or more SIF.

SIF: Safety Instrumentated Function is a set of equipment used to reduce the risk to a specific hazard.

Safety function: function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state.

Safe-state: a state where the hazard is removed.

Example:

Safety function: *Read measured values from transducer inputs, compare them to alarm set points and generate a trip relay output.*

Safe-state: *tripped relay output.*

SIL Certification

Functional Safety Terms and Abbreviations

Safety function: function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state.

Safe-state: a state where the hazard is removed.

Example:

Safety function: *Read measured values from transducer inputs, compare them to alarm set points and generate a trip relay output.*

Safe-state: *tripped relay output.*

The safety function detects a problem and triggers the safe-state.

There is a mal-function detected in the safety system itself that, by default, will trigger the safe-state.

SIL Certification

Functional Safety Terms and Abbreviations

STR: Spurious Trip Rate

The safety function detects a problem and triggers the safe-state.

There is a mal-function detected in the safety system itself that, by default, will trigger the safe-state.

Example:

Safety function: *Read measured values from transducer inputs, compare them to alarm set points and generate a trip relay output.*

Safe-state: *tripped relay output.*

SIL Certification

Functional Safety Terms and Abbreviations

SIL: discrete relative levels (SIL1 to SIL4) of risk-reduction provided by a safety function, corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and 1 the lowest.

Systematic Capability: measure (SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function.

SIL Certification

Functional Safety Terms and Abbreviations

Low demand mode: is where the frequency of demands for operation made on a safety-related system is no greater than one per year.

High demand mode: is where the frequency of demands for operation made on a safety-related system is greater than one per year.

Continuous mode: is where the function retains the safe-state as part of normal operation.

SIL Certification

Functional Safety Terms and Abbreviations

HFT: Hardware fault tolerance

MooN (e.g. 1oo2, 2oo2): M out of N channel voting architecture.

Type A: a simple element, with well know failure modes, behavior and dependable failure data.

Type B: a complex element, where failure modes are not well defined and there is no dependable failure data.

SIL Certification

Functional Safety Terms and Abbreviations

Route 1_H: architectural constraints based on hardware fault tolerance and safe failure fraction concepts.

Route 2_H: architectural constraints based on component reliability data from field feedback, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

Route 1_S: systematic integrity requirements for the avoidance (prevention) and requirements for the control of systematic faults.

Route 2_S: systematic integrity evidence that the equipment is 'proven in use' (PIU)

Route 3_S: systematic integrity evidence for pre-existing software elements.

SIL Certification

Functional Safety Terms and Abbreviations

Failure Rate (λ): failures per unit of time (typically measured in FIT (10^{-9} Failures In Time).

λS: Safe failures

λDD: Dangerous Detected failures

λDU: Dangerous Undetected failures

SFF: Safe Failure Fraction (ratio between λS+λDD and λDU.

PFD/PFH: Probability of failure by demand (low demand mode) OR per by hour (high demand mode).

SIL Certification

Functional Safety Terms and Abbreviations

Failure Rate (λ): failures per unit of time (typically measured in FIT (10^{-9} Failures In Time).

λS: Safe failures

λDD: Dangerous Detected failures

λDU: Dangerous Undetected failures

SFF: Safe Failure Fraction (ratio between λS+λDD and λDU.

PFD/PFH: Probability of failure by demand (low demand mode) OR per by hour (high demand mode).

SIL Certification

Functional Safety Terms and Abbreviations

Failure Rate (λ): failures per unit of time (typically measured in FIT (10^{-9} Failures In Time).

λS: Safe failures

λDD: Dangerous Detected failures

λDU: Dangerous Undetected failures

SFF: Safe Failure Fraction (ratio between λS+λDD and λDU.

PFD/PFH: Probability of failure by demand (low demand mode) OR per by hour (high demand mode).

SIL Certification

Functional Safety Terms and Abbreviations

PTC: Proof test coverage is a measure of how many undetected dangerous failures are detected by the proof test.

PTI: Proof test interval is the maximum time that the safety system can be used without testing.

PFDavg: mean unavailability of an E/E/PE safety-related system to perform the specified safety function when a demand occurs.

λDU: Dangerous Undetected failures

SIL Certification

Functional Safety Terms and Abbreviations

From: Endress+Hauser white paper

SIL Certification

Functional Safety Terms and Abbreviations

From: Endress+Hauser white paper

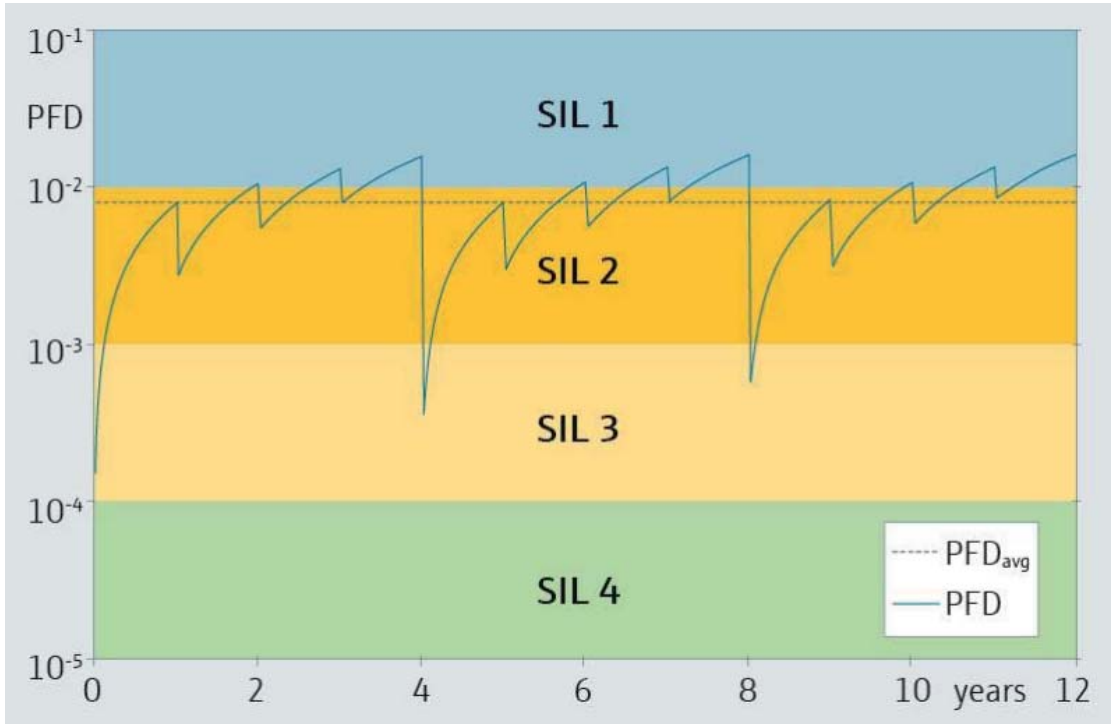
SIL Certification

Functional Safety Terms and Abbreviations

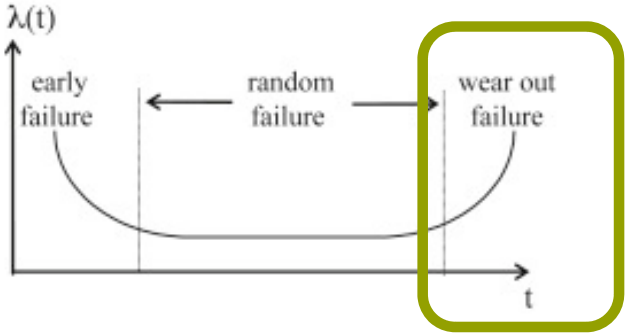
From: Endress+Hauser white paper

SIL Certification

Functional Safety Terms and Abbreviations



From: Endress+Hauser white paper



MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

HOW TO INTERPRET A SIL CERTIFICATE

HOW TO READ A SIL CERTIFICATE

SIL Certification

How to read a SIL certificate

ISO/IEC 17065:2012
Conformity assessment —
Requirements for bodies certifying products, processes and services

And many others….

A conformity certificate must, in general, contain:

- the name and address of the certification body
- the date certification is granted
- the name and address of the client
- the scope of certification (the product(s), process(es) or service(s) for which the certification is granted, the applicable certification scheme, and the standard(s) and other normative document(s), including their date of publication, to which it is judged that the product(s), process(es) or service(s) comply)
- the term or expiry date of certification, if certification expires after an established period
- any other information required by the certification scheme
- the signature or other defined authorization of the person(s) of the certification body assigned such responsibility.

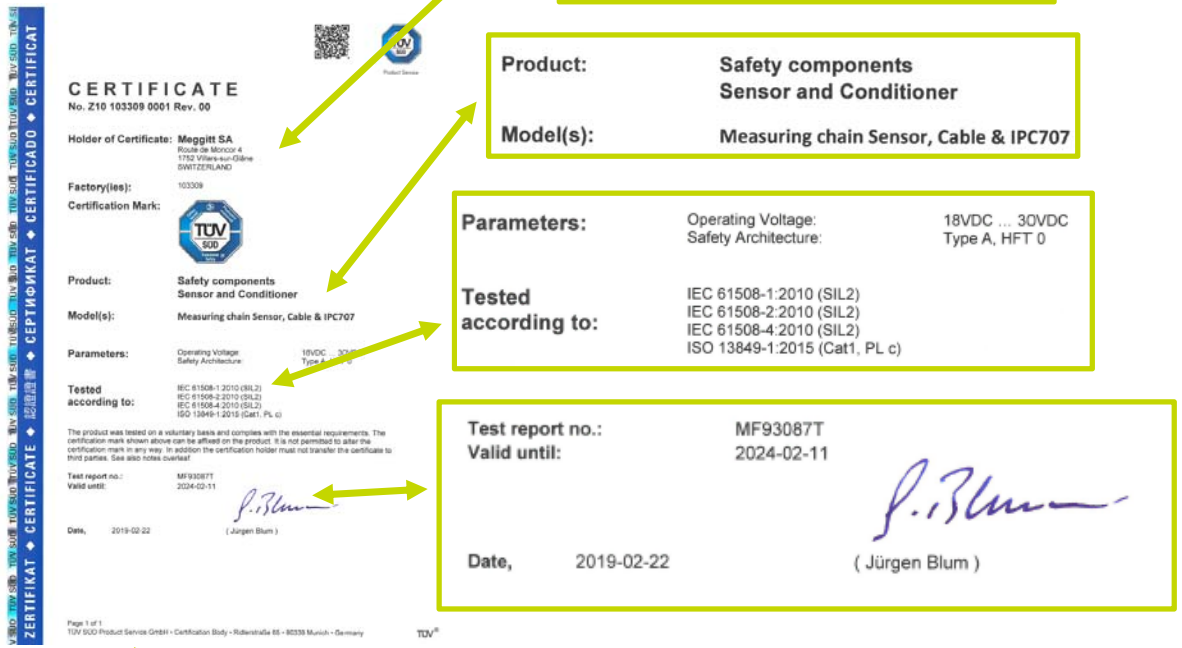
MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

CERTIFICATE EXAMPLE 1

SIL Certification

How to read a SIL certificate



CERTIFICATE
No. Z10 103309 0001 Rev. 00

Holder of Certificate: Meggitt SA
Route de Moncor 4
1752 Villars-sur-Glâne
SWITZERLAND

Factory(ies): 103309

Certification Mark:

Product: Safety components
Sensor and Conditioner

Model(s): Measuring chain Sensor, Cable & IPC707

Parameters: Operating Voltage: 18VDC ... 30VDC
Safety Architecture: Type A, HFT 0

Tested according to:
IEC 61508-1:2010 (SIL2)
IEC 61508-2:2010 (SIL2)
IEC 61508-4:2010 (SIL2)
ISO 13849-1:2015 (Cat1, PL c)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf

Test report no.: MF93087T
Valid until: 2024-02-11

Date, 2019-02-22 (Jürgen Blum)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

ZERTIFIKAT ◆ CERTIFICATE ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

SIL Certification

How to read a SIL certificate

3.3 Safety properties(s)

Table 3-1 lists the other important safety properties for an IPC707 measurement chain.

Safety property	Description / Value
SIL level (IEC 61508)	SIL 2
Systematic capability (IEC 61508)	2
PL and Cat levels (ISO 13849)	PL c and Cat 1. See also 3.5 ISO 13849-1 performance level.
Modes of operations	Low Demand mode or Continuous mode
Type of subsystem	Type A
Hardware fault tolerance (HFT)	0
Dangerous-detected failures (λ_{DD})	2261 failure rate (FIT). Note: For dangerous-detected failures (λ_{DD}), the IPC707 output is defined.
Dangerous-undetected failures (λ_{DU})	70 failure rate (FIT). Note: For dangerous-undetected failures (λ_{DU}), the IPC707 output is undefined, that is, other current or voltage values.
Safe-detected failures (λ_{SD}) and safe-undetected failures (λ_{SU})	0 failure rate (FIT). Note: The IPC707 has neither safe-detected (λ_{SD}) nor safe-undetected (λ_{SU}) failures, that is, there is no safe state.
Safe failure fraction (SFF) for Type A subsystem	97 % (calculated value). SIL 2 requires ≥60 % is for a Type A device with HFT = 0.
Process safety time (PST)	<5 ms in Low Demand mode. <500 ms in Continuous mode. Note: This is the time required for an IPC707 signal conditioner with diagnostics to update the nominal value of the diagnostic component (DC) of the output signal, with the minimum configurable low-pass (LP) filter of 200 Hz.
Allocation of SIL budget	PFDavg <20 % of the SIL 2 budget for a PTI ≤5 years. PFH <20 % of the SIL 2 budget at 7.02 × 10^{-8} FIT. Note: For an IPC707 measurement chain (that is, IPC707-compatible sensor, IPC707-compatible cabling and IPC707 signal conditioner with diagnostics).
Safety accuracy	Sensitivity: ±10 %. High-pass (HP) filter cutoff frequency: −75 to +100 % from 1 to 110 Hz. Low-pass (LP) filter cutoff frequency: −40 % to +100 % from 0.2 to 20 kHz. Noise: ≤1 % of full scale deflection (measurement component (AC)).

Notes
Failure rate calculations and analysis were performed with a long-term ambient temperature of 80 °C (176 °F).
For IPC707 with diagnostics, output values are defined in Table 2-1 and 7.7.1 Defining the alarm levels.

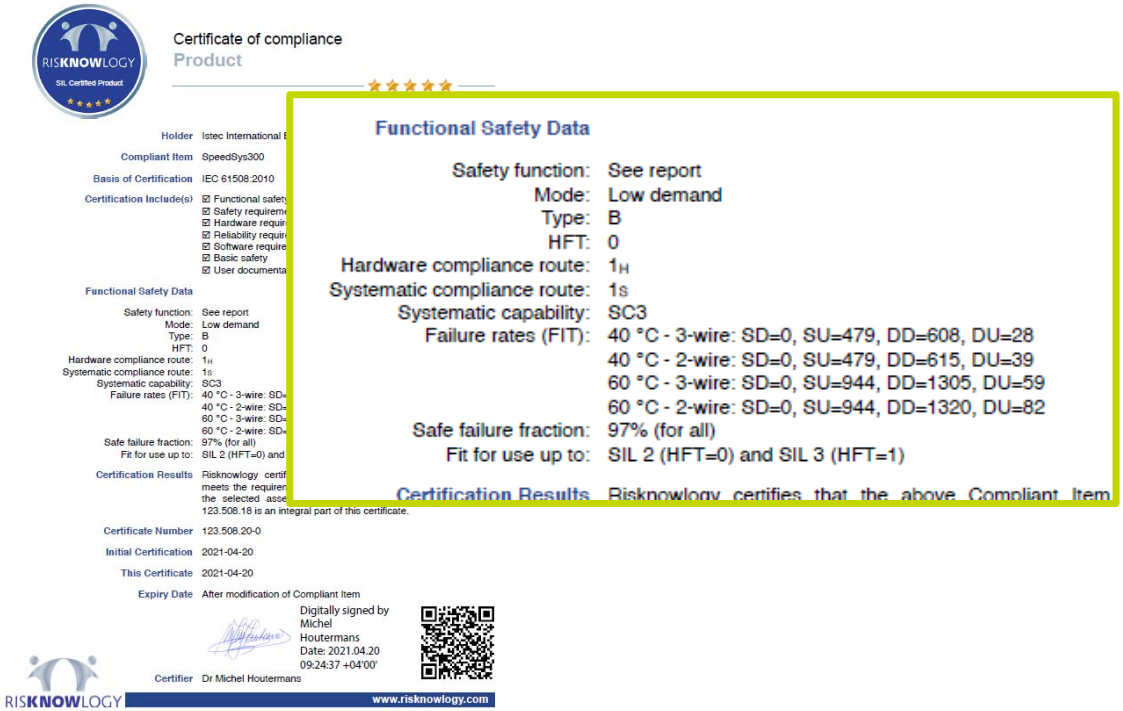
MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

CERTIFICATE EXAMPLE 2

SIL Certification

How to read a SIL certificate



Certificate of compliance

Product

Holder Istec International E

Compliant Item SpeedSys300

Basis of Certification IEC 61508:2010

Certification Include(s) ☑ Functional safety ☑ Safety requirem ☑ Hardware requir ☑ Reliability requir ☑ Software require ☑ Basic safety ☑ User documenta

Functional Safety Data

Safety function: See report
Mode: Low demand
Type: B
HFT: 0
Hardware compliance route: 1_H
Systematic compliance route: 1_S
Systematic capability: SC3
Failure rates (FIT): 40 °C - 3-wire: SD=
40 °C - 2-wire: SD=
60 °C - 3-wire: SD=
60 °C - 2-wire: SD=
Safe failure fraction: 97% (for all)
Fit for use up to: SIL 2 (HFT=0) and

Certification Results Risknowlogy certif meets the requiren the selected asse 123.508.18 is an integral part of this certificate.

Certificate Number 123.508.20-0

Initial Certification 2021-04-20

This Certificate 2021-04-20

Expiry Date After modification of Compliant Item

Digitally signed by Michel Houtermans
Date: 2021.04.20 09:24:37 +04'00'

Certifier Dr Michel Houtermans

RISKNOWLOGY www.risknowlogy.com

Functional Safety Data

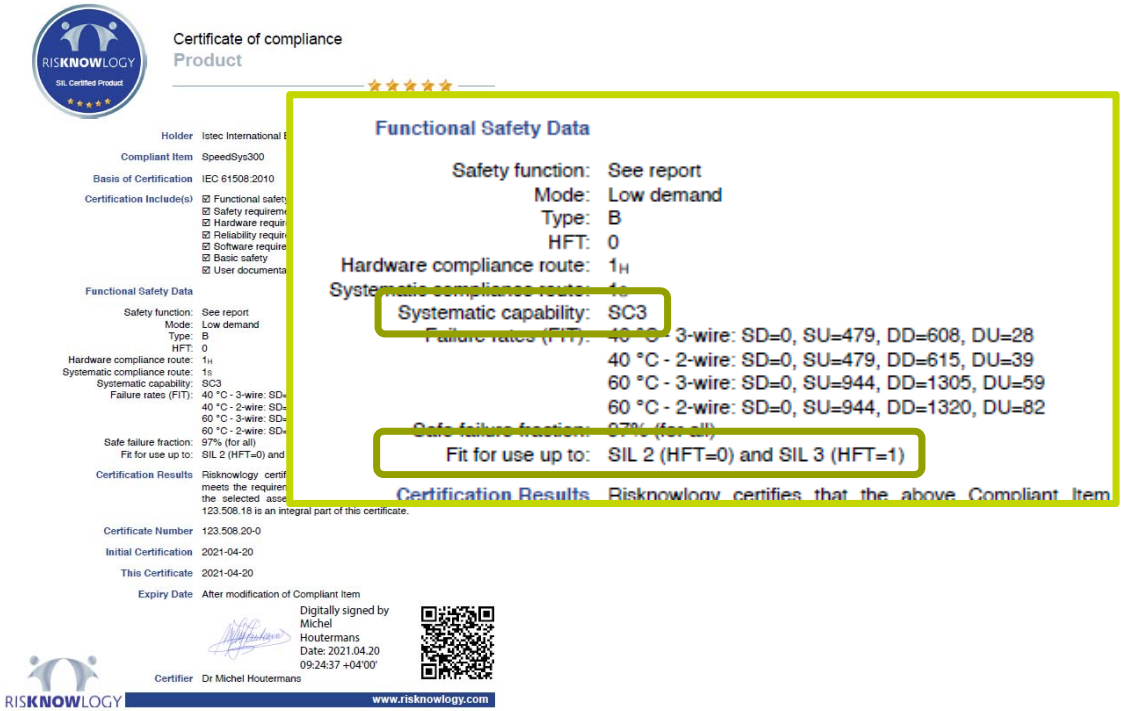
Safety function:	See report
Mode:	Low demand
Type:	B
HFT:	0
Hardware compliance route:	1_H
Systematic compliance route:	1_S
Systematic capability:	SC3
Failure rates (FIT):	40 °C - 3-wire: SD=0, SU=479, DD=608, DU=28
	40 °C - 2-wire: SD=0, SU=479, DD=615, DU=39
	60 °C - 3-wire: SD=0, SU=944, DD=1305, DU=59
	60 °C - 2-wire: SD=0, SU=944, DD=1320, DU=82
Safe failure fraction:	97% (for all)
Fit for use up to:	SIL 2 (HFT=0) and SIL 3 (HFT=1)

Certification Results Risknowlogy certifies that the above Compliant Item

MEGGITT

SIL Certification

How to read a SIL certificate



Certificate of compliance

Product

Holder Istec International

Compliant Item SpeedSys300

Basis of Certification IEC 61508:2010

Certification Include(s) ☑ Functional safety ☑ Safety requirem ☑ Hardware requir ☑ Reliability requir ☑ Software require ☑ Basic safety ☑ User documenta

Functional Safety Data

Safety function: See report
Mode: Low demand
Type: B
HFT: 0
Hardware compliance route: 1_H
Systematic compliance route: 1_S
Systematic capability: SC3
Failure rates (FIT): 40 °C - 3-wire: SD=0, SU=479, DD=608, DU=28
40 °C - 2-wire: SD=0, SU=479, DD=615, DU=39
60 °C - 3-wire: SD=0, SU=944, DD=1305, DU=59
60 °C - 2-wire: SD=0, SU=944, DD=1320, DU=82
Safe failure fraction: 97% (for all)
Fit for use up to: SIL 2 (HFT=0) and SIL 3 (HFT=1)

Certification Results Risknowlogy certifies that the above Compliant Item meets the requirements of the selected assessment scheme. 123.508.18 is an integral part of this certificate.

Certificate Number 123.508.20-0

Initial Certification 2021-04-20

This Certificate 2021-04-20

Expiry Date After modification of Compliant Item

Digitally signed by Michel Houtermans
Date: 2021.04.20 09:24:37 +04'00'

Certifier Dr Michel Houtermans

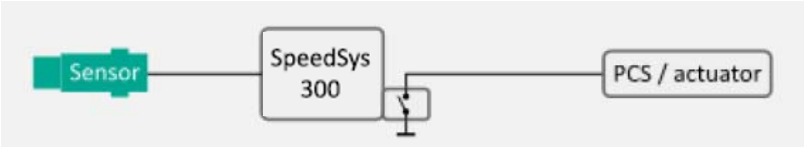
RISKNOWLOGY www.risknowlogy.com

MEGGITT

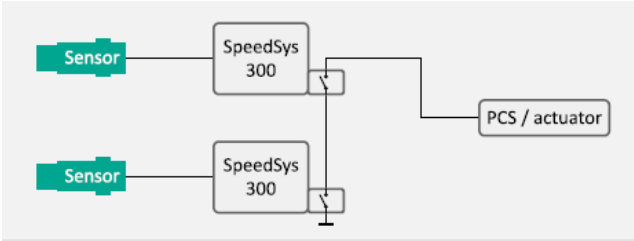
SIL Certification

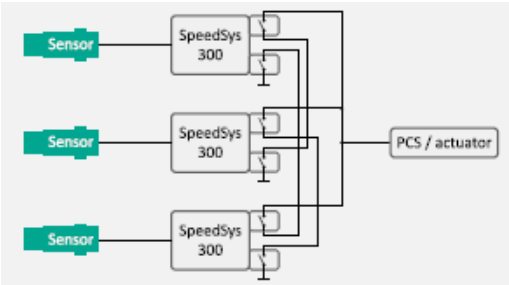
How to read a SIL certificate

SIL2, HFT 0



SIL3, HFT 1





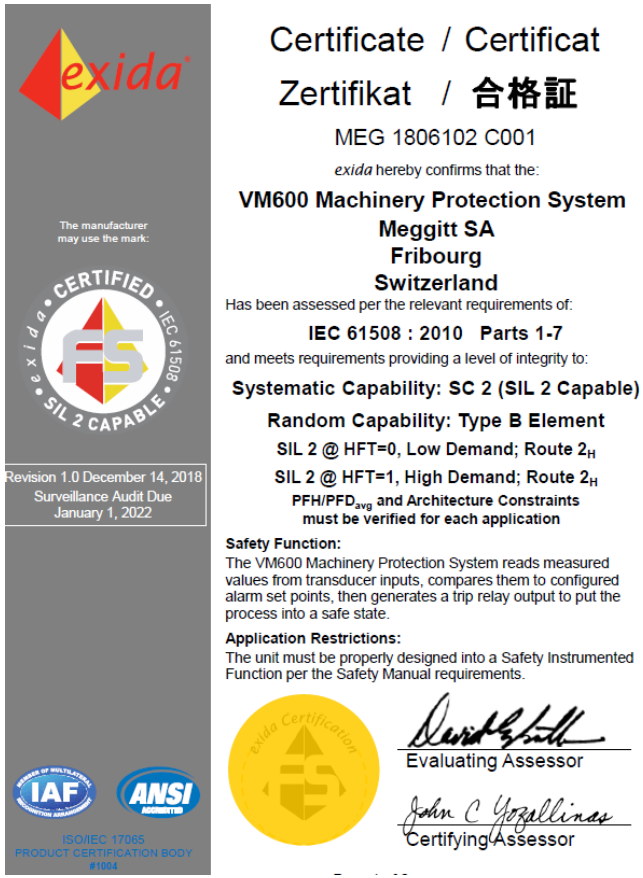
MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

CERTIFICATE EXAMPLE 3

SIL Certification

How to read a SIL certificate



exida

The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 2 CAPABLE

Revision 1.0 December 14, 2018
Surveillance Audit Due
January 1, 2022

IAF ANSI

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

MEG 1806102 C001

exida hereby confirms that the:

VM600 Machinery Protection System
Meggitt SA
Fribourg
Switzerland

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 Element

SIL 2 @ HFT=0, Low Demand; Route 2_H

SIL 2 @ HFT=1, High Demand; Route 2_H

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

Safety Function:
The VM600 Machinery Protection System reads measured values from transducer inputs, compares them to configured alarm set points, then generates a trip relay output to put the process into a safe state.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

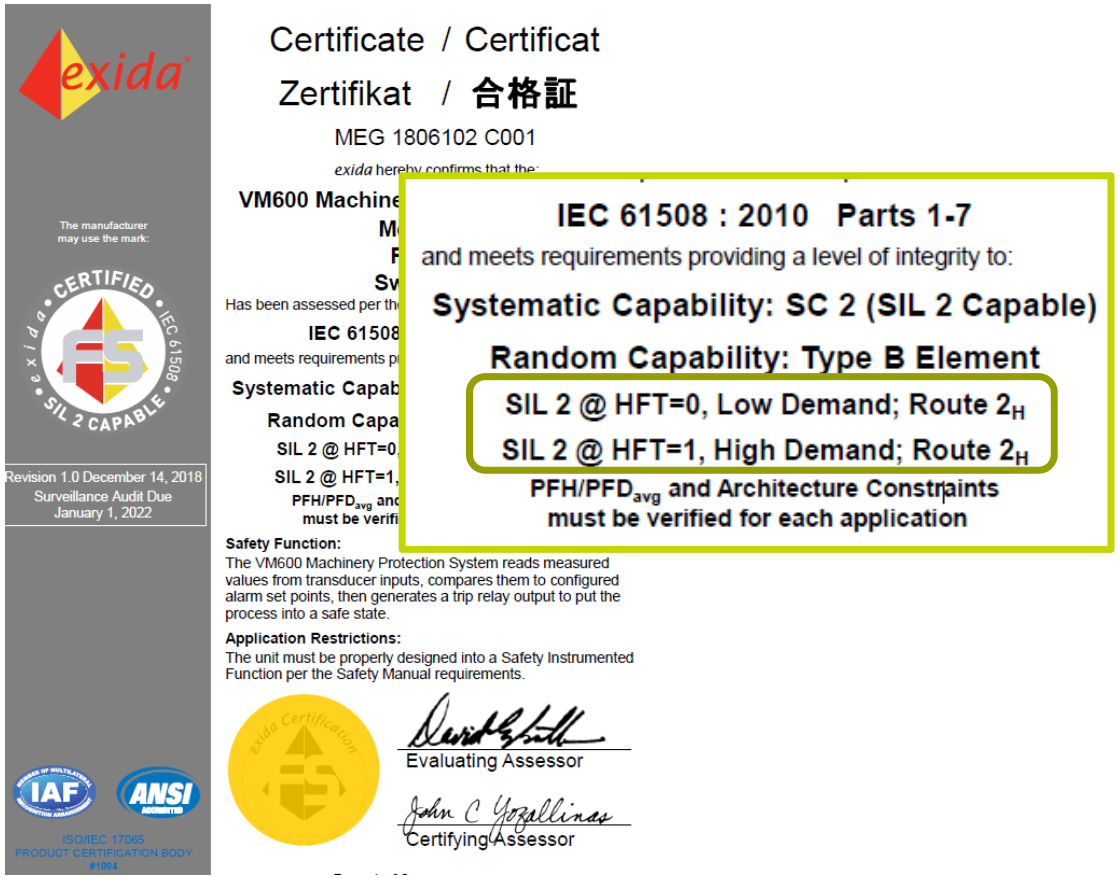
exida Certification

Evaluating Assessor

Certifying Assessor

SIL Certification

How to read a SIL certificate



exida

The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 2 CAPABLE

Revision 1.0 December 14, 2018
Surveillance Audit Due
January 1, 2022

IAF ANSI

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

MEG 1806102 C001

exida hereby confirms that the:

VM600 Machine
M
P
Sv

Has been assessed per th

IEC 61508

and meets requirements p

Systematic Capab

Random Capa

SIL 2 @ HFT=0

SIL 2 @ HFT=1

PFH/PFD$_{avg}$ and
must be verifi

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 Element

SIL 2 @ HFT=0, Low Demand; Route 2$_H$

SIL 2 @ HFT=1, High Demand; Route 2$_H$

PFH/PFD$_{avg}$ and Architecture Constraints must be verified for each application

Safety Function:

The VM600 Machinery Protection System reads measured values from transducer inputs, compares them to configured alarm set points, then generates a trip relay output to put the process into a safe state.

Application Restrictions:

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

exida Certification

Evaluating Assessor

Certifying Assessor

MEGGiTT

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

MYTHS AND TRUTHS

OPEN DISCUSSION ON COMMON MYTHS AND TRUTHS

SIL Certification

Myths and Truths

Common questions, myths and truths about functional safety

SIL Certification

Myths and Truths

True or False	True	?	No	
It is just a paper			***X***	It is much more than a paper. It is sound verification of all safety relevant aspects, covering the entire safety life-cycle. Functional Safety certification implies a significant amount of work and commitment.
It just requires more documentation			***X***	It requires as well specific design and implementation measures, testing, tools, analysis, etc that are dedicated to safety. Documents are just evidences of the activities performed.
A SIL product is always better than an non-SIL one			***X***	Not necessarily. A SIL product shall be used WHEN it is needed. Due to increased safety measures and techniques, a SIL product may have lower availability and/or higher cost.

SIL Certification

Myths and Truths

True or False	True	?	No	Notes
"Proven in use" is better than "by design"… or vice-versa			***X***	The functional safety standard gives similar attention to both methods. It is the set of safety properties that matters at the end.
Proof testing is just a test to see if my safety system is working well.			***X***	No. It is a test designed to cover undetected dangerous failures.
SIL x is a property of an element or device			***X***	No. SIL should be interpreted as the capability to implement safety functions up to SIL x.
It is only a design feature			***X***	No, it goes beyond the design itself.
Systematic Capability is a limiting factor	***X***			Yes. All three barriers are limiting factors: Systematic Capability, Probability of Failure and Architectural Constraints

SIL Certification

Myths and Truths

True or False	True	?	No	Notes
A longer proof test interval, means a better safety system		***X***		Not necessarily. It can also mean that you have a more "complicated" proof test procedure or that you have a high diagnostic coverage, therefore higher Spurious Trip Rate. To understand the quality of a safety system you need to look into all the different safety properties.
Safety and reliability are the same thing			***X***	No. For example, a system producing many spurious trips is still safe, but not reliable. On the other hand, a system with low diagnostics can be reliable, but less safe.
HFT means redundancy			***X***	No. For example a 2oo4 architecture (HFT of 2) has a redundancy of 3.

MEGGiTT

SIL Certification

Myths and Truths

True or False	True	?	No	Notes
In a safety measurement chain, I can simple replace one element by another similar element from a different model or vendor, as long as it has the same SIL level		X		You must ensure that all safety properties still fit in your SIF or SIS. For example, you must check that your probability of failure (SIL budget) is still OK. SIL is a RANGE of values.
I can increase my SIL via redundancy		X		Not always. First, this is limited by the SC level. SIL level can be as high as the minimum SC level in the chain. The SC level can be increased by 1 if diverse redundant systems are used in a dual channel architecture.

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

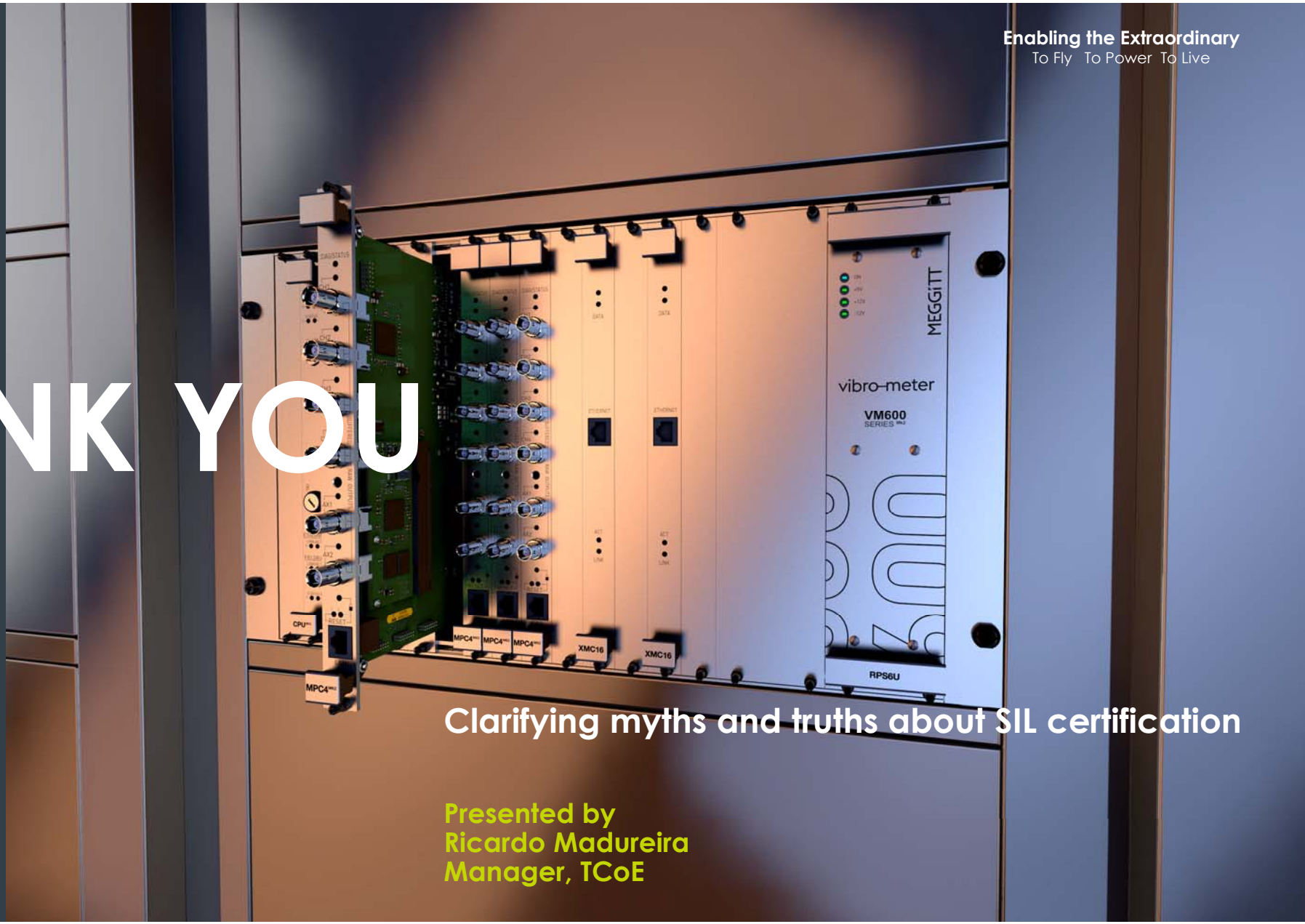
Q&A

Technical Center of Excellence
Webinar

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

THANK YOU



Clarifying myths and truths about SIL certification

Presented by
Ricardo Madureira
Manager, TCoE

Disclaimer

Business legal entity, Business address

Legal entity registration information as appropriate

Information contained in this document may be subject to export control regulations of the United Kingdom, European Union, United States or other national jurisdictions, including the US International Traffic in Arms Regulations and/or Export Administration Regulations.

Each recipient of this document is responsible for ensuring that transfer or use of any information contained herein complies with all relevant Export Control Regulations.