ISO26262 AND IEC61508 FUNCTIONAL SAFETY OVERVIEW

KAVYA PRABHA DIVAKARLA
SYSTEM ENGINEER
AUTOMOTIVE MICROCONTROLLER AND PROCESSORS

AMF-AUT-T2713 | JUNE 2017

SECURE CONNECTIONS
FOR A SMARTER WORLD

AGENDA

1. Functional Safety Introduction
2. IEC 61508, ISO 26262 Introduction
3. Safety Integrity Levels
4. Hardware
5. Software
6. Tools
7. Customer Documents
8. What’s next

01.

Functional Safety

An Introduction to Functional Safety

NXP

What is functional Safety?

- ISO 26262 Definition:
  - Absence of unacceptable risk due to hazards caused by mal-functional behavior of electrical and/or electronic systems and the interactions of these systems

- IEC 61508 Definition:
  - Safety is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.
  - Functional Safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

What is relevant to NXP is that for the first time these standards call out requirements for electronic components

Functional Safety Basic Concepts

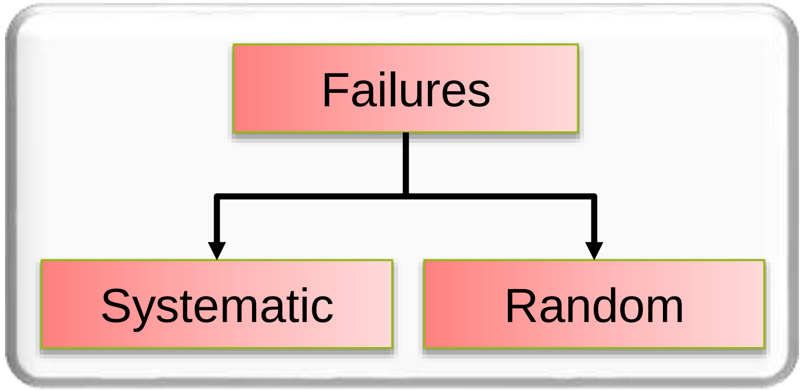
- All systems will have some inherent, quantifiable failure rate. It is not possible to develop a system with zero failure rate.
- For each application, there is some tolerable failure rate which does not lead to unacceptable risk.
- Acceptable failure rates vary per application, based on the potential for direct or indirect physical injury in the event of system malfunction.
- The hazards and risks of applications can be analyzed and assigned categories based on the level of acceptable risk. These categories are known as *Safety Integrity Levels*, or *SILs*.

Terms & Definitions

- **Fault**
  - Operational issue in a system which may lead to a failure
- **Failure**
  - Result of a fault which leads to an inability to execute safety critical functionality
- **Fault Tolerance**
  - Ability to continue safe operation after a fault
- **Fail Safe System:**
  - System where a fault which may lead to failures is detected and the system is put into a safe state such that faults may not propagate to other systems
- **Fail Functional/Operational System**
  - System where a fault which may lead to failures is detected and the system can continue operation without loss of safety function
- **Reliability**
  - Ability to execute operations in system without failure (*generally independent of consideration for a safety function*)
- **Availability**
  - Amount of time in which a safety function is available divided by total system operation time. Systems with high reliability and fail functional systems tend to have higher availability than fail safe systems
- **Security**
  - Ability to detect, resist, or prevent tampering with product functionality
- **Dependability**
  - Availability + Reliability + Safety + Security + Maintainability

Safety Failures and their causes

Failures in a functional safety system can be broadly classified into two categories: Systematic and Random failures



- Systematic Failures
  - Result from a failure in design or manufacturing
  - Often a result of failure to follow best practices
  - Occurrence of systematic failures can be reduced through continual and rigorous process improvement and robust analysis of any new technology

- Random Failures
  - Result from random defects or soft errors inherent to process or usage condition
  - Rate of random faults cannot generally be reduced; focus must be on the detection and handling of random faults to prevent application failure

Note: *Software failures are considered to be systematic*

Implementing Functional Safety is about

How products are developed:

- Addresses the aspect of Systematic Failures
  - Result from a failure in design or manufacturing
  - Relevant to Hardware and Software
  - Occurrence of failures can be reduced through continual and rigorous process improvement

Products that detect and handle faults:

- Addresses the aspect of Random Failures
  - Inclusion of mechanisms to detect and handle random defects inherent to process or usage condition
  - Relevant to Hardware only
  - Supported by FMEDA*, Dependency and Fault Tree Analysis and communicated as FIT*

- FMEDA – Failure Mode Effects and Diagnostic Analysis
- FIT – Failure in Time

Functional Safety is not

- Security
- Reliability
- Quality

Functional Safety Standards

Standard	Targeted End Equipment Applications
IEC 61508	Electrical, Electronic, Programmable Electronic Systems
ISO 26262	Road Vehicles (except Mopeds) up to 3500Kg*
EN 50129	Railway Signaling
ISO 22201	Elevator / Escalator
IEC 61511	Process Industry (Chemical, Oil Refining etc.)
IEC 61800	Adjustable speed AC motor drive
IEC 62061	Industry Machinery (electronics)
ISO 13849	Industry Machinery
IEC 60730	Automatic Controls for Household use

* Weight restriction will be removed in 2nd edition

02.

IEC 61508, ISO 26262 Introduction

Introduction to the standards and key concepts

IEC 61508 – Functional Safety of Electrical, Electronic, and Programmable Electronic (E/E/PE) Systems

- Basic Safety Publication
- 1st edition in 1998, updated to 2nd edition in 2010.
- Performance based targets for both systematic and random failure management
- Covers safety management, system/HW design, SW design, production, and operation of safety critical E/E/PE systems

Scope of IEC 61508

- IEC 61508 has specific requirements for E/E/PE systems and SW
  - In 1st edition, there is no recognition of HW beyond system level.
  - In 2nd edition, HW component requirements are introduced for “ASICs”

- IEC 61508 definition of ASIC is not 100% clear. It can be interpreted to cover a number of products:
  - Custom ICs designed for a specific safety system
  - Semi-custom ICs designed for a type of safety system
  - FPGA, PLD, and CPLD devices

- A HW component compliant to IEC 61508 is called a “compliant item”

- For easy application to the largest market, new HW components should be developed as IEC 61508 compliant items.

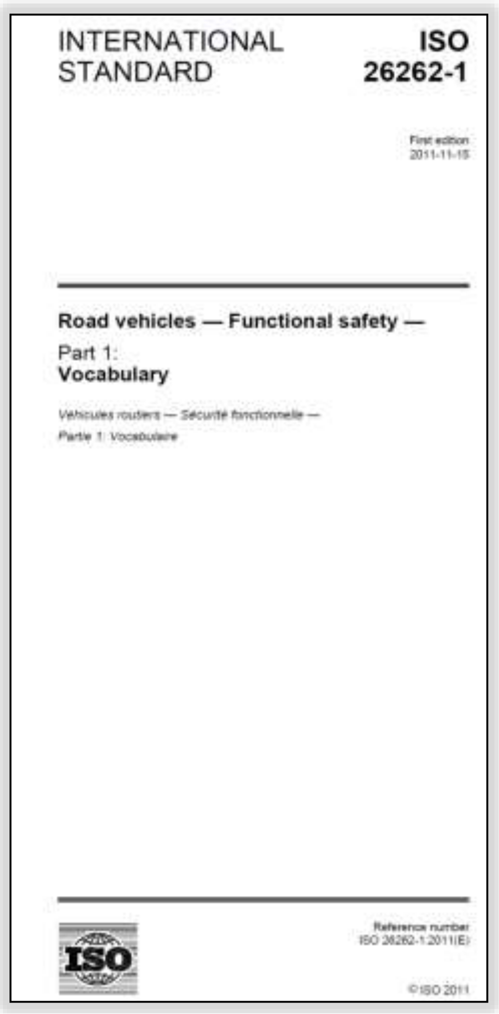
IEC 61508 Reading recommendation

	0	1	2	3	4	5	6	7
Marketing/Sales	●	❍	❍	❍	●	❍	❍	❍
Field Applications and Systems Engineering	●	●	●	●	●	❍	❍	❍
Engineering Management	●	●	❍	❍	●	❍	❍	❍
HW Developers	●	❍	●	❍	●	❍	●	●
SW Developers	●	❍	❍	●	●	❍	●	●
Quality Engineering	●	●	❍	❍	●	●	❍	❍
Safety Engineering	●	●	●	●	●	●	●	●

● = recommended; ❍ = optional

- part 0, Technical Report: Functional Safety and IEC 61508
- part 1, General Requirements
- part 2, Requirements for E/E/PE Systems
- part 3, Software Requirements
- part 4, Definitions and Abbreviations
- part 5, Examples of Methods for the determination of Safety Integrity Levels
- part 6, Guidelines on the Application of IEC 61508-2 and IEC 61508-3
- part 7, Overview of Techniques and Measures

ISO 26262 – Functional Safety of Road Vehicles


INTERNATIONAL STANDARD

ISO 26262-1

First edition
2011-11-15

Road vehicles — Functional safety —

Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

Reference number
ISO 26262-1:2011(E)

©ISO 2011

- Vertical standard, performance based.
- First edition published in 2011.
- Follows similar structure to IEC 61508, but totally replaces instead of augmenting.
- Separates system design from hardware component design. As a result, most components used require compliance.
- 2nd edition available in draft

ISO 26262 Reading recommendation

	1	2	3	4	5	6	7	8	9	10
Marketing/Sales	●	❍	❍	❍	❍	❍	❍	❍	❍	●
Field Applications and Systems Engineering	●	❍	●	●	●	●	❍	❍	❍	●
Engineering Management	●	●	❍	❍	❍	❍	❍	❍	❍	●
HW Developers	●	❍	●	●	●	❍	❍	●	●	●
SW Developers	●	❍	●	●	❍	●	❍	●	●	●
Quality Engineering	●	●	❍	❍	❍	❍	●	❍	❍	●
Safety Engineering	●	●	●	●	●	●	●	●	●	●

- part 1, Vocabulary
- part 2, Management of functional safety
- part 3, Concept phase
- part 4, Product development: system level
- part 5, Product development: HW level
- part 6, Product development: SW level
- part 7, Production and operation
- part 8, Supporting processes
- part 9, Safety analyses
- part 10, Guideline
- Part 11, Semiconductor Guideline*
- Part 12, Adaptation for Motor cycles*

* New to 2nd edition

● = recommended; ❍ = optional

Scope of ISO 26262

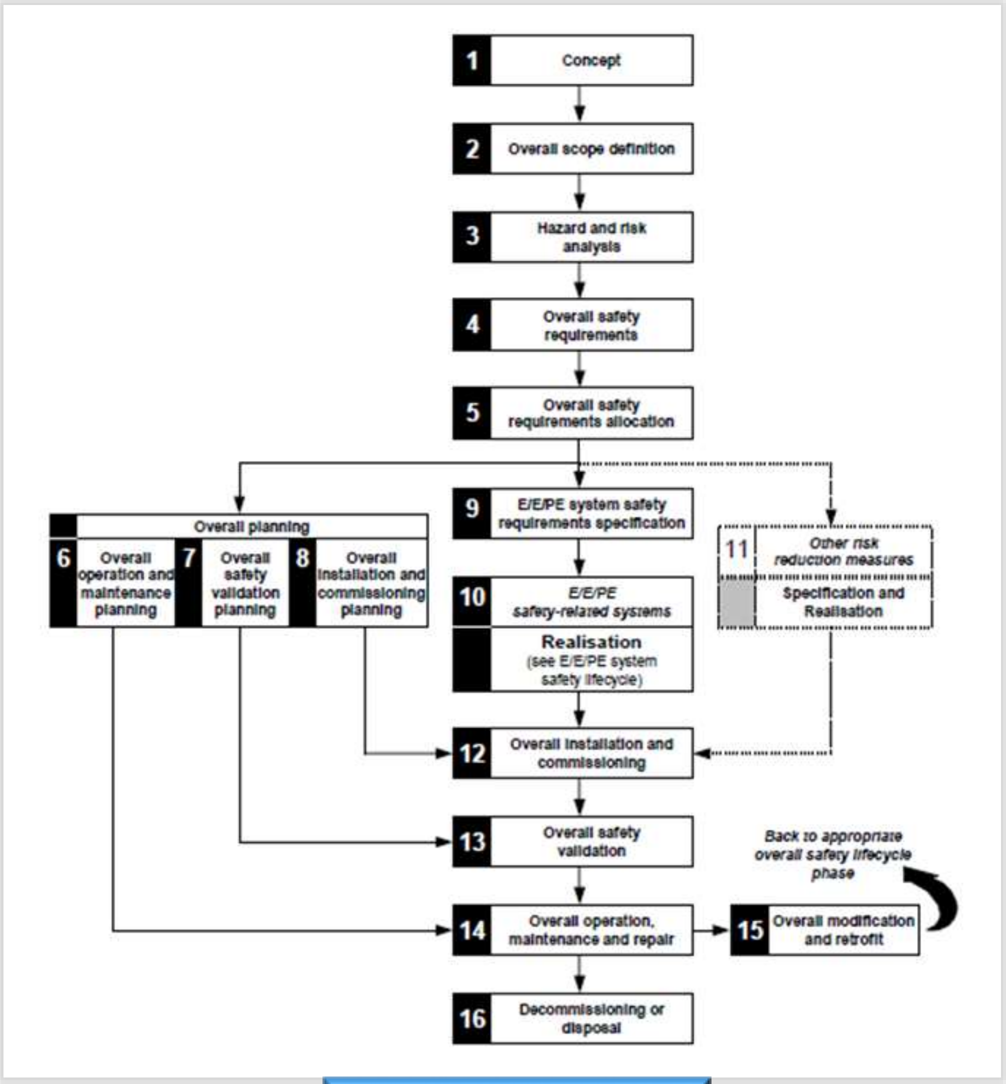
- ISO 26262 addresses
  - Safety-related systems including one or more E/E systems installed in series production road vehicles (except Mopeds) with a maximum gross weight up to 3500 Kg*.
- ISO 26262 does not address
  - unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities

For Vehicles (and their components) released for production prior to the publication date of ISO 26262:

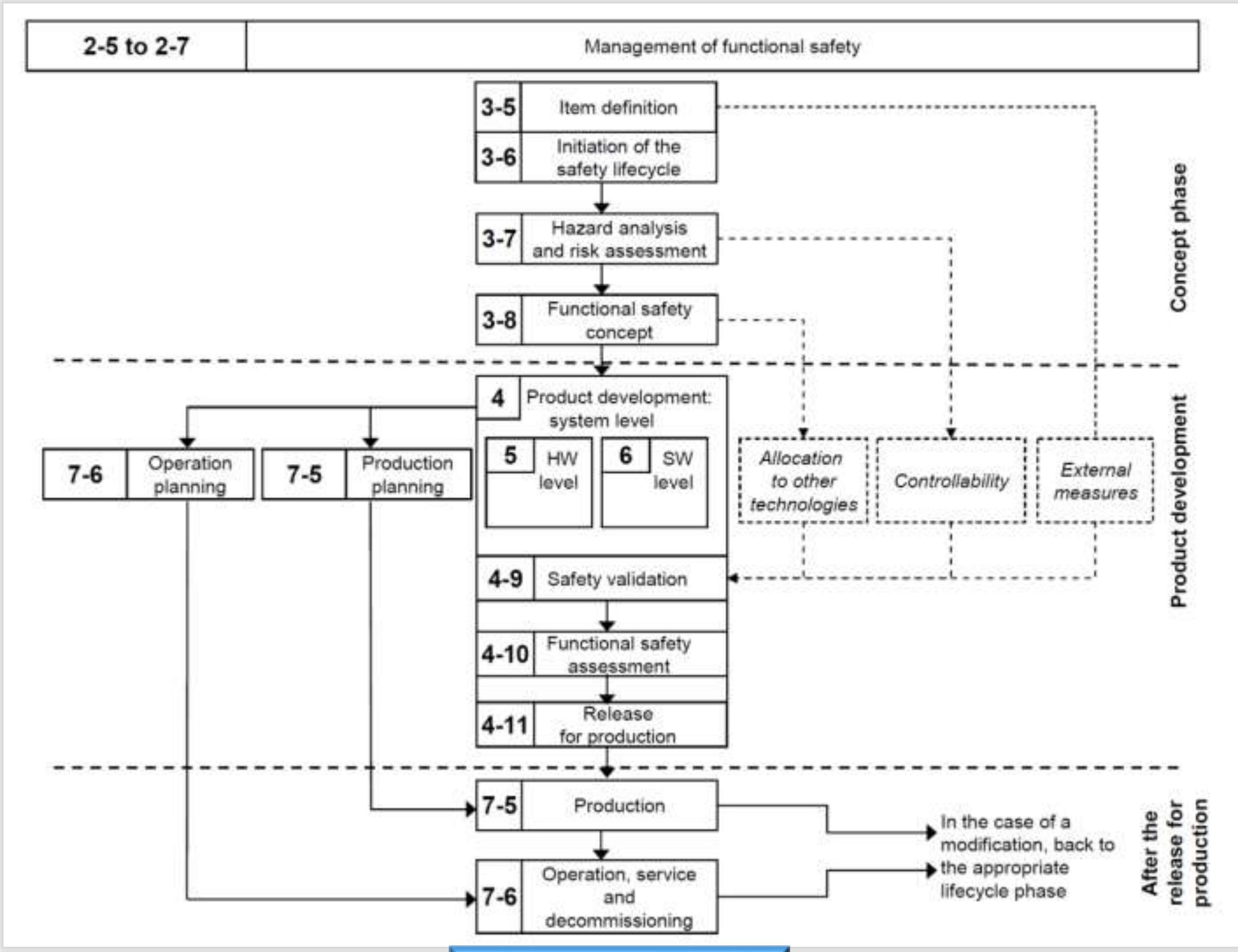
- **Proven in use concept** allows continued use of existing systems, sub-systems and components only if no changes are made to the implementation

* Weight restriction will be removed in 2nd edition

Safety Lifecycle



IEC 61508



ISO 26262

ISO 26262 Key Differences from IEC 61508

- ISO 26262 aligns with auto industry use cases and definition of acceptable risk

- IEC 61508 concept of safety function is replaced with ISO 26262 safety goals.
  - Safety function concept was based on the idea of defining a system under control and then "bolting-on" risk reduction measures
  - Safety goal concept requires that risk reduction be part of the initial control system design

- Typical IEC 61508 systems are installed and then validated in place. ISO 26262 systems must be validated before release to market.

- ISO 26262 standard clearly defines work products for each requirement. This makes determination of compliance easier but limits flexibility of development system definition.

- ISO 26262 has hazard and risk analysis, failure rates and metrics adapted for Automotive use cases.

03.

Safety Integrity Levels

Classification of functional safety products

Determining ISO 26262 ASIL Level

- To determine the ASIL level of a system a Risk Assessment must be performed for all Hazards identified.
- Risk is comprised of three components: **Severity, Exposure & Controllability**

S = Severity

Class	Description
S0	No injuries
S1	Light and moderate injuries
S2	Severe and life-threatening injuries (survival probable)
S3	Life-threatening injuries (survival uncertain), fatal injuries

C = Controllability

Class	Description
C0	Controllable in general
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

E = Exposure

Class	Description
E0	Incredible
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

ASIL Determination Table

Risk = Severity x (Exposure * Controllability)

		Controllability		
Severity	Exposure	C1 Simply	C2 Normal	C3 Difficult
S1 Light and moderate injuries	E1 Very Low	QM	QM	QM
	E2 Low	QM	QM	QM
	E3 Medium	QM	QM	ASIL A
	E4 High	QM	ASIL A	ASIL B
S2 Severe and life-threatening injuries (survival probable)	E1 Very Low	QM	QM	QM
	E2 Low	QM	QM	ASIL A
	E3 Medium	QM	ASIL A	ASIL B
	E4 High	ASIL A	ASIL B	ASIL C
S3 Life-threatening injuries (survival uncertain), fatal injuries	E1 Very Low	QM	QM	ASIL A
	E2 Low	QM	ASIL A	ASIL B
	E3 Medium	ASIL A	ASIL B	ASIL C
	E4 High	ASIL B	ASIL C	ASIL D

Automotive Application Safety levels (e.g.)

Subsystem	ASIL Safety Level
ADAS – Vision/Radar	B-D
Airbags	D
Alternator	C-D
Body Control Module	A-B
Brake System (ABS, ESC, Boost)	A-D+
Collision Warning -	A-B
Cruise Control	A-D
Drowsiness Monitor	A-B
E-Call / Telematics	A-B
Fuel Pump	B
Engine Oil Pump	B
Electric Mirrors	A-B
Electrochromatic Mirrors	A-B
Engine Control	B-D
Lighting	A-B
Night Vision	A-B
Power Door, Liftgate, Roof, Trunk	A-B
Rain Sense Wipers	A-B
Steering (EPS)	D-D+
Throttle Control	A-D
Tire Pressure Warning	A-B
Transmission	B-D
Transmission Oil Pump	B-C
Window Lift	A-B

- Many applications that don’t have strict safety requirements today may have them in the future.
- For example, **SAE** is providing guidelines for determining ASILs. Applying these guidelines will mean that auto apps that haven’t been “safety” to-date could be held subject to ISO26262.
- Carmakers who require conformance will open a market window for safety-capable suppliers like NXP.

Safety – ISO26262 Decomposition

Achieve an ASIL level with QM products

Decomposition is more relevant at the system level vs. component level

- It is possible to achieve an ASIL level by developing a subsystem of multiple components which achieves the ASIL level as a whole.
- Decomposition redundantly assigns the same safety requirement to two independent and diverse elements.

ASIL B = ASIL A + ASIL A

ASIL B = ASIL B + QM

- Enables the use of lower rated ASIL or QM products (from a systematic integrity point of view).
- Key Point: Decomposition makes it possible to use components that achieve lower ASIL independently.

Way to achieve Fault Metrics
- IO must be handled / checked by ASIL product
- Decision must be made / checked by ASIL product
- QM product must be TS-16949

IEC 61508 Terminology for Safety Systems

- **Low demand mode** safety functions are required to operate at low frequencies, typically once or so per year.

- **High demand mode** safety functions are required to operate at high frequencies, typically many times per hour

- **Continuous demand mode** safety functions operate continuously.

- **Hardware Fault Tolerance (HFT)** is the number of faults that can occur without failure of the safety function. HFT>0 requires redundancy.

- **Safe Failure Fraction (SFF)** is the ratio of safe and dangerous (but detected) failures in a system safety function to the total failure rate

Determining IEC 61508 SIL

Likelihood	Definition	Range (failures/year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

- **Class I**: Unacceptable in any circumstance
- **Class II**: Undesirable, tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
- **Class III**: Tolerable if the cost of risk reduction would exceed the improvement
- **Class IV**: Acceptable as it stands, though it may need to be monitored

SIL Requirements

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

- Low demand functions have less stringent requirements on PFD_{avg} to achieve a specific SIL.
- High demand and continuous demand functions have more stringent requirements on PFH to achieve a specific SIL.
- Process and machinery applications mix low and high demand functions.
- Transportation applications are typically high demand.

Determination of SIL based on HFT and SFF

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

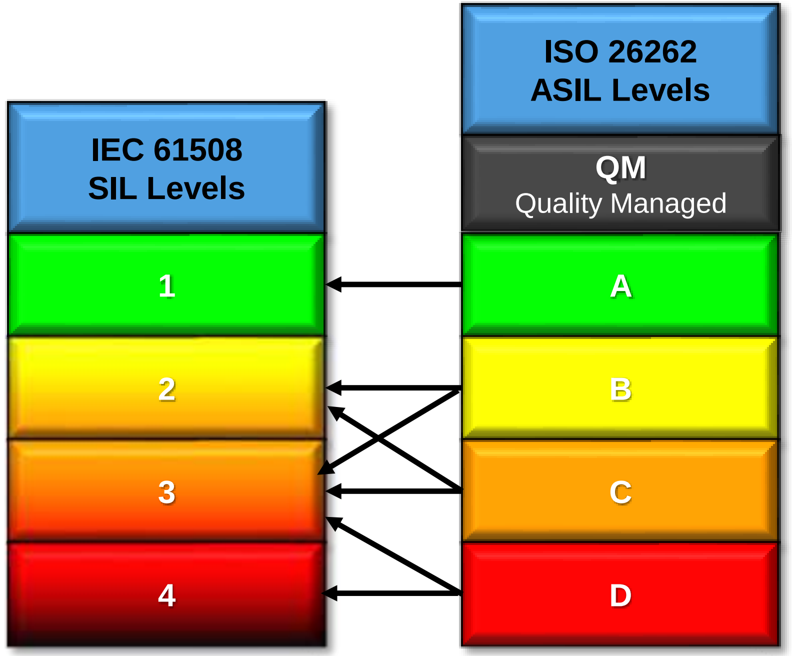
Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

- **Type A** products are simple products in which all failure modes are known
- **Type B** products are complex products in which all failure modes are not known (e.g. semiconductor).
- **Hardware Fault Tolerance (HFT)** is the number of faults that can occur without failure of the safety function. HFT>0 requires redundancy.
- **Safe Failure Fraction** (SFF) is defined as the ratio of safe and dangerous (but detected) failures in a system safety function to the total failure rate
- SFF is calculated at element (component) or system level for a safety function. It should not be applied for sub-elements.

ISO 26262 vs IEC 61508 Safety Integrity Levels

- ISO 26262 was developed to meet automotive industry specific needs as replacement for IEC 61508.
- IEC 61508 defines 4 safety integrity levels (SIL1,2,3,4)
- ISO26262 defines a Quality Managed level in addition to 4 safety integrity levels (ASIL A,B,C,D)
- There is no direct correlation between IEC61508 SIL and ISO 26262 ASIL levels



04.

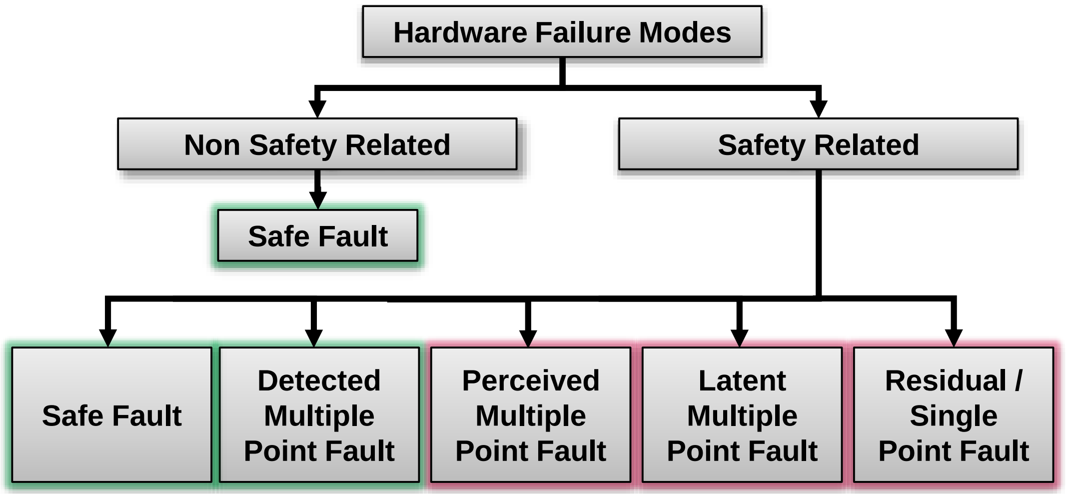
Hardware

Expectations established on hardware development and products

ISO 26262 Failure Rates

Failure Rate λ

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}$$



λ_{SPF} – Single Point Faults
λ_{RF} – Residual Faults
λ_{MPFDP} – Detected/Perceived Multi Point Faults
λ_{MPFL} – Latent Multi Point Faults
λ_{MPF} – $\lambda_{MPFDP} + \lambda_{MPFL}$ = Multi Point Faults*
λ_{S} – Safe Faults

* **multiple-point fault** is an individual fault that, in combination with other independent faults, leads to a multiple-point failure

ISO 26262 Fault Metrics

Minimize single point and residual faults.

- ✓ Detected and handled by system within system safety response time.

$$single\ point\ fault\ metric = 1 - \frac{\sum(\lambda_{SPF} + \lambda_{RF})}{\sum \lambda} = \frac{\sum(\lambda_{MPF} + \lambda_{S})}{\sum \lambda}$$

Metric	ASIL B	ASIL C	ASIL D
Single point fault metric	≥ 90%	≥ 97%	≥ 99%

Minimize latent multi point faults.

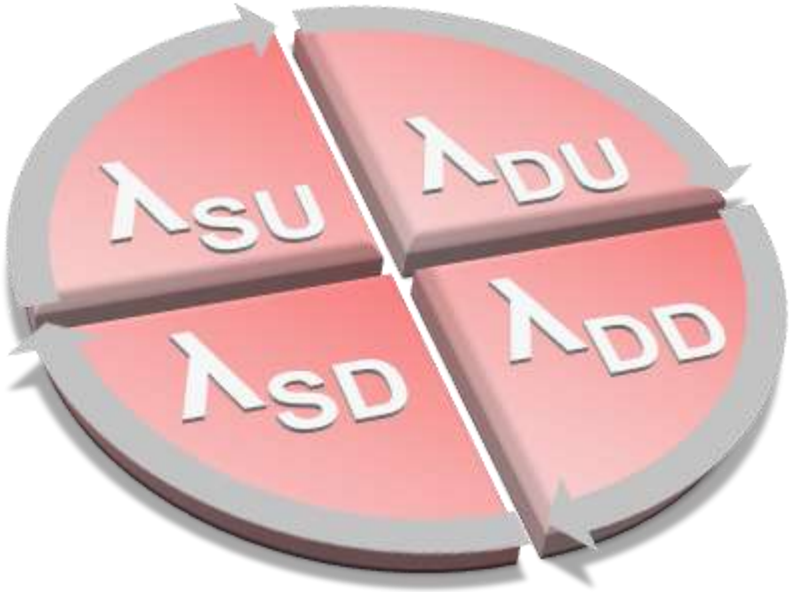
- ✓ Detected and handled within hours through test algorithms.

$$latent\ fault\ metric = 1 - \frac{\sum(\lambda_{MPFL})}{\sum(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum(\lambda_{MPFDP} + \lambda_{S})}{\sum(\lambda - \lambda_{SPF} - \lambda_{RF})}$$

Metric	ASIL B	ASIL C	ASIL D
Latent fault metric	≥ 60%	≥ 80%	≥ 90%

IEC 61508 Failure Rates

Failure Rate λ



- λ_S – Safe failure rate
  - **No impact** on safety function
  - **λ_{SD} –** Safe detected failure rate
  - **λ_{SU} –** Safe undetected failure rate

- λ_D – Dangerous failure rate
  - **Impact** on safety function
  - **λ_{DD} –** Dangerous detected failure rate
  - **λ_{DU} –** Dangerous undetected failure rate

$$\lambda = \lambda_S + \lambda_D = (\lambda_{SD} + \lambda_{SU}) + (\lambda_{DD} + \lambda_{DU})$$

FIT = Failures In Time = 1 failure in 10^9 device hours

IEC 61508 Safe Failure Fraction & SIL Determination

Safe Failure Fraction (SFF) = $1 - \frac{\lambda_{DU}}{\lambda}$

High Demand System

Hardware Fault Tolerance = 0 (single channel)
1 Fault may lead to loss of safety function.
EX: 1oo1, 1oo1D, 2oo2…

Hardware Fault Tolerance = 1 (redundant)
2 or more faults needed to loss of safety function.
2oo3, 4oo5…

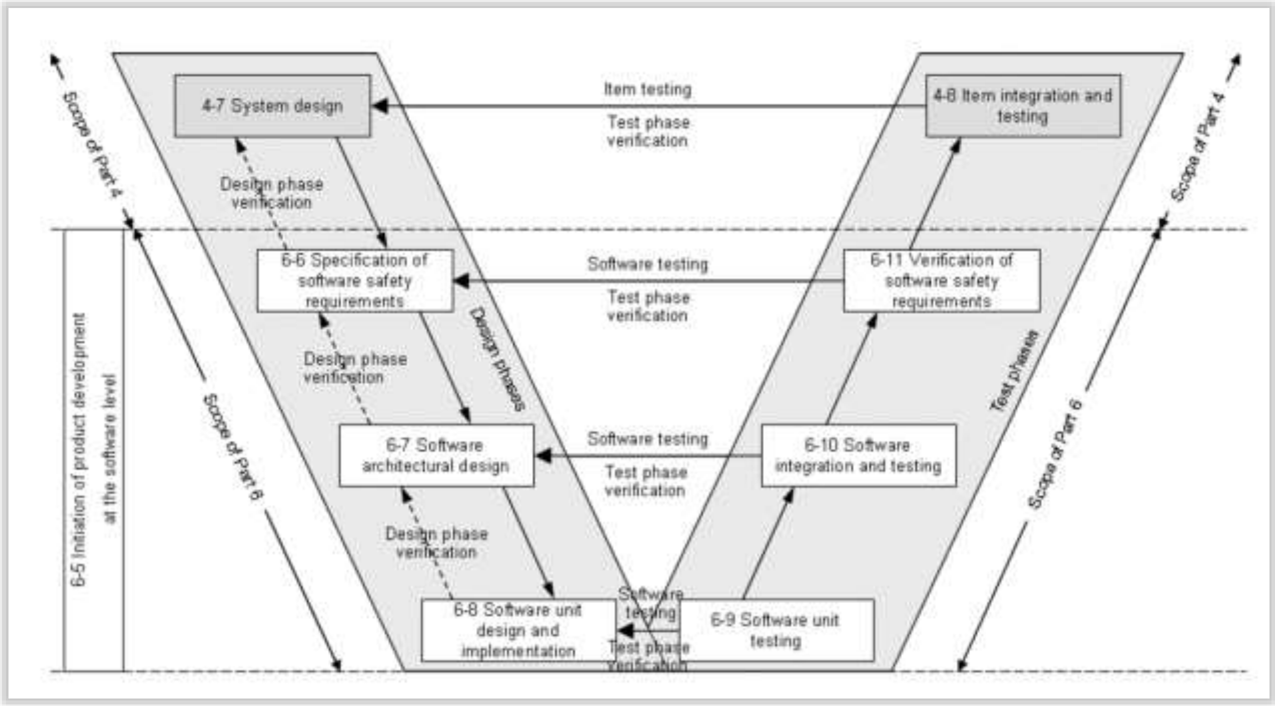
Safe Failure Fraction (High Demand System)	Hardware Fault Tolerance	
	HFT = 0	HFT = 1
0 … < 60%	-	SIL1
60% … < 90%	SIL1	SIL2
90% … < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL4

05.

Software

Expectations established on software development and products

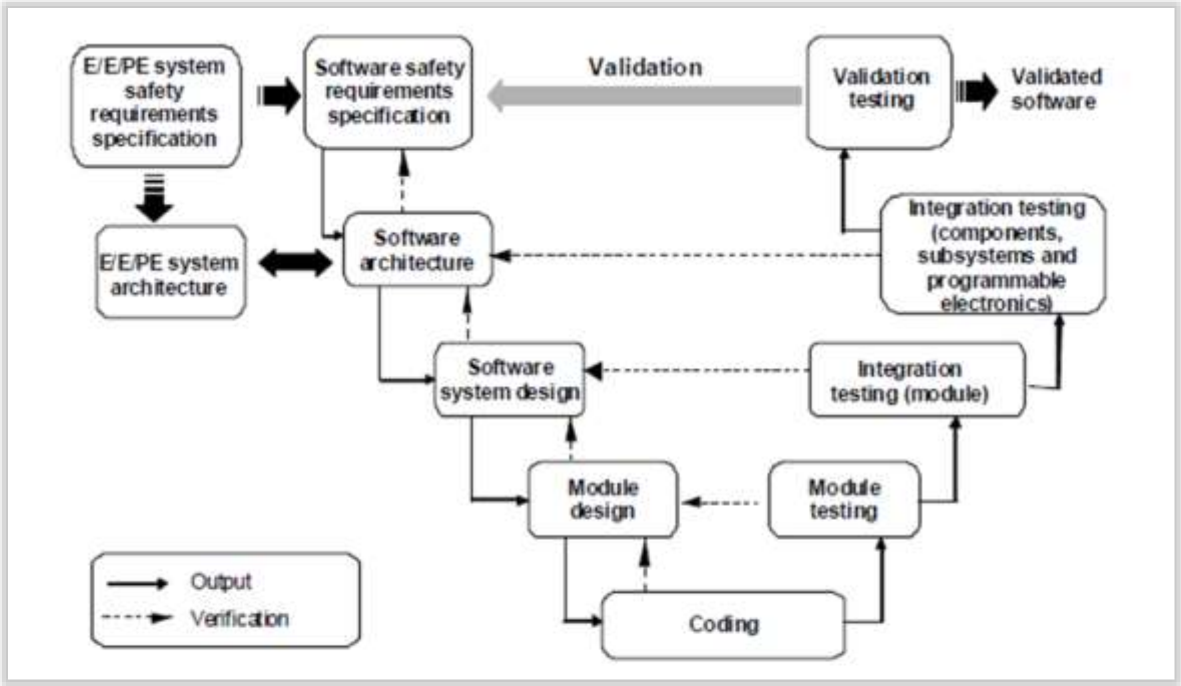
Software component development



ISO 26262

Software failures are considered to be systematic

IEC 61508



Coding guidelines and design principles

Topics		ASIL A	ASIL B	ASIL C	ASIL D
1a	Enforcement of low complexity[a]	++	++	++	++
1b	Use of language subsets[b]	++	++	++	++
1c	Enforcement of strong typing[c]	++	++	++	++
1d	Use of defensive implementation techniques	o	+	++	++
1e	Use of established design principles	+	+	+	++
1f	Use of unambiguous graphical representation	+	++	++	++
1g	Use of style guides	+	++	++	++
1h	Use of naming conventions	++	++	++	++

Methods		ASIL A	ASIL B	ASIL C	ASIL D
1a	Hierarchical structure of software components	++	++	++	++
1b	Restricted size of software components[a]	++	++	++	++
1c	Restricted size of interfaces[a]	+	+	+	+
1d	High cohesion within each software component[b]	+	++	++	++
1e	Restricted coupling between software components[a, b, c]	+	++	++	++
1f	Appropriate scheduling properties	++	++	++	++
1g	Restricted use of interrupts[a, d]	+	+	+	++

ISO 26262

IEC 61508

- O → Optional
- R → Recommended
- HR → Highly Recommended
- M → Mandatory

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Use of coding standard to reduce likelihood of errors	C.2.6.2	HR	HR	HR	HR
2	No dynamic objects	C.2.6.3	R	HR	HR	HR
3a	No dynamic variables	C.2.6.3	---	R	HR	HR
3b	Online checking of the installation of dynamic variables	C.2.6.4	---	R	HR	HR
4	Limited use of interrupts	C.2.6.5	R	R	HR	HR
5	Limited use of pointers	C.2.6.6	---	R	HR	HR
6	Limited use of recursion	C.2.6.7	---	R	HR	HR
7	No unstructured control flow in programs in higher level languages	C.2.6.2	R	HR	HR	HR
8	No automatic type conversion	C.2.6.2	R	HR	HR	HR

NOTE 1 Measures 2, 3a and 5. The use of dynamic objects (for example on the execution stack or on a heap) may impose requirements on both available memory and also execution time. Measures 2, 3a and 5 do not need to be applied if a compiler is used which ensures a) that sufficient memory for all dynamic variables and objects will be allocated before runtime, or which guarantees that in case of memory allocation error, a safe state is achieved; b) that response times meet the requirements.

NOTE 2 See Table C.11.

NOTE 3 The references (which are informative, not normative) "B.x.x.x", "C.x.x.x" in column 3 (Ref.) indicate detailed descriptions of techniques/measures given in Annexes B and C of IEC 61508-7.

* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. It is intended the only one of the alternate or equivalent techniques/measures should be satisfied. The choice of alternative technique should be justified in accordance with the properties, given in Annex C, desirable in the particular application.

Software error detection and handling

	Methods	ASIL			
		A	B	C	D
1a	Range checks of input and output data	++	++	++	++
1b	Plausibility check[a]	+	+	+	++
1c	Detection of data errors[b]	+	+	+	+
1d	External monitoring facility[c]	o	+	+	++
1e	Control flow monitoring	o	+	++	++
1f	Diverse software design	o	o	+	++

	Methods	ASIL			
		A	B	C	D
1a	Static recovery mechanism[a]	+	+	+	+
1b	Graceful degradation[b]	+	+	++	++
1c	Independent parallel redundancy[c]	o	o	+	++
1d	Correcting codes for data	+	+	+	+

ISO 26262

- O → Optional
- R → Recommended
- HR → Highly Recommended
- M → Mandatory

IEC 61508

	Technique/Measure *	Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Test case execution from cause consequence diagrams	B.6.6.2	---	---	R	R
2	Test case execution from model-based test case generation	C.5.27	R	R	HR	HR
3	Prototyping/animation	C.5.17	---	---	R	R
4	Equivalence classes and input partition testing, including boundary value analysis	C.5.7 C.5.4	R	HR	HR	HR
5	Process simulation	C.5.18	R	R	R	R

NOTE 1 The analysis for the test cases is at the software system level and is based on the specification only.

NOTE 2 The completeness of the simulation will depend upon the safety integrity level, complexity and application.

NOTE 3 See Table C.13.

NOTE 4 The references (which are informative, not normative) "B.x.x.x", "C.x.x.x" in column 3 (Ref.) indicate detailed descriptions of techniques/measures given in Annexes B and C of IEC 61508-7.

* Appropriate techniques/measures shall be selected according to the safety integrity level.

06.

Tools

Expectations established on software development tools

Tool Confidence Level

ISO 26262

- Part 8: 11. Confidence in the use of software tools
- 11.4.5: Evaluation of a software tool by analysis
  - **Determine Tool Impact (TI)**
    if a software tool can introduce or fail to detect errors in a safety-related
    - TI1: No impact
    - TI2: Impact
  - **Determine Tool Detection (TD) in usage of tool**
    - TD1: HIGH probability of detecting/preventing potential tool errors
    - TD2: MEDIUM probability of detecting/preventing potential tool errors
    - TD3: All other cases (LOW/unknown)
  - **Determine the Tool Confidence Level (TCL)**
- 11.4.6: Qualification of a software tool
  - TCL1: no qualification needed
  - TCL2,TCL3: qualification according to tables

		Tool error detection		
		TD1	TD2	TD3
Tool impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

Table 4 — Qualification of software tools classified TCL3

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance with a safety standard[a]	+	+	++	++

Requirements for Software Tools and Programming Languages

IEC 61508

Table A.3 – Software design and development – support tools and programming language

(See 7.4.4)

	Technique/Measure *	Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Suitable programming language	C.4.5	HR	HR	HR	HR
2	Strongly typed programming language	C.4.1	HR	HR	HR	HR
3	Language subset	C.4.2	---	---	HR	HR
4a	Certified tools and certified translators	C.4.3	R	HR	HR	HR
4b	Tools and translators: increased confidence from use	C.4.4	HR	HR	HR	HR

NOTE 1 See Table C.3.

NOTE 2 The references (which are informative, not normative) "B.x.x.x", "C.x.x.x" in column 3 (Ref.) indicate detailed descriptions of techniques/measures given in Annexes B and C of IEC 61508-7.

* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. It is intended the only one of the alternate or equivalent techniques/measures should be satisfied. The choice of alternative technique should be justified in accordance with the properties, given in Annex C, desirable in the particular application.

- O → Optional
- R → Recommended
- HR → Highly Recommended
- M → Mandatory

07.

Customer documents

Supporting documentation NXP provides to our customers to help in functional safety compliant development

NXP SafeAssure Products

To support the customer to build a safety system, the following deliverables are provided as standard for all ISO 26262 developed products.

- Public Information available via NXP Website
  - Quality Certificates
  - Safety Manual* (HW and SW)
  - Reference Manual
  - Data Sheet

- Confidential Information available under NDA
  - Safety Plan
  - ISO 26262 Safety Case (HW and SW)
  - Permanent Failure Rate data (Die & Package) - IEC/TR 62380 or SN29500
  - Transient Failure Rate data (Die) - JEDEC Standard JESD89
  - Safety Analysis (FMEDA*, DFA) & Report
  - SW FMEA and Test Reports
  - PPAP
  - Confirmation Measures Report (summary of all applicable confirmation measures)

* includes IEC 61508 relevant data

08.

What’s next

ISO 26262 is going through a revision that will be incorporated into the next revision ISO 26262:2018

ISO 26262:2018

- Overall the 2018 ISO 26262 is an incremental improvement
  - Very little new content towards fail operational / autonomous vehicles indicating not yet mature enough in industry to standardize
  - Minor references to address interaction of Safety & Security
- New content in current draft (ISO 26262:2016)
  - Scope now for series production road vehicles, except mopeds.
  - Specific content added for Trucks, Buses, Trailers, Semitrailers and motorcycles (although very minimal)
  - Part 11 guideline added for Semiconductors
  - Part 12 added for motorcycles (mapping of MSIL to ASIL)
  - Interaction between safety and security organizations mentioned (no specifics)
  - Method for dependent failure analysis provided in multiple examples
  - Guidance for fault tolerance

- Biggest impacts for NXP
  - Part 2 changes for confirmation measures
  - Part 8.13 changes for evaluation of hardware elements
  - Part 11 guideline for Semiconductors
- When do we implement 2018 content changes
  - 25% already implemented
  - 50% during BCaM7 (deploying in 2017)
  - 25% in 2018

SECURE CONNECTIONS
FOR A SMARTER WORLD