

***Modification in
IEC 61508:2010 standard and
their influence on the process safety?***

***György Baradits PhD., SIL4S
Árpád Pozsgai, ProCoPlan***

Major changes	Relevant to the process safety
Management of functional safety	Yes
Terminology	Yes
Modes of operation	Yes
Architectural constraints	Yes
Systematic safety integrity	Partly Yes
Systematic Capability introduced (SC1..SC4)	Partly Yes
Security (Cyber-Security)	Yes (but not mandatory)
E/E/PE system design requirements specification	No (only for manufactures)
Digital communications	No (only for manufactures)
ASICS & integrated circuits	No (only for manufactures)
Safety manual for compliant items	Yes
Software design	No (only for manufactures)
Competence	Yes

Definition	Comment
application	Existed, but not in the old "Definition and abbreviation"
application data	Existed, but not in the old "Definition and abbreviation"
application software	Existed, but not in the old "Definition and abbreviation"
average probability of dangerous failure on demand	Based on IEC 61511, PFD_{avg}
process safety time	Existed, but not in the old "Definition and abbreviation"
proven in use	Existed, but not in the old "Definition and abbreviation"
safe failure fraction	Existed, but not in the old "Definition and abbreviation", see IEC 61511
probability of dangerous failure on demand	Replace probability of failure on demand, PFD

Definition	Comment
probability of dangerous failure on demand	Replace "probability of failure on demand", PFD
probability of dangerous failure per hour	Replace "probability of failure per hour", PFH
other risk reduction measure	Replace "other technology safety-related system"
system software	Existed, but not in the old "Definition and abbreviation"
element	Old one: module
compliant item safety manual	New, based on IEC 61511 Safety Manual
configuration baseline	New, "configuration management"?)
configuration data	New, "configuration management"?)

Definition	Comment
soft-error	New, IEC 61508:2010-4
software on-line support tool	New, IEC 61508:2010-4
subsystem	New, IEC 61508:2010-4
systematic capability	New, IEC 61508:2010-4
target risk	New, IEC 61508:2010-4
element safety function	New, IEC 61508:2010-4
harmful event	New, IEC 61508:2010-4
no effect failure	New, IEC 61508:2010-4

Definition	Comment
no part failure	New, IEC 61508:2010-2
overall safety function	New, IEC 61508:2010-4
pre-existing software	New, IEC 61508:2010-4
application specific integrated circuit, ASIC	New, IEC 61508:2010-4

- Extended scope from safety function to safety function performed by device (subsystem like logic solver, field devices)
- New terms:
 - Overall safety function (IEC 61508:2010-1)
 - Element safety function (IEC 61508:2010-2)
 - Compliant items, systematic capability (IEC 61508:2010-1)
 - Safety manual for compliant items (IEC 61508:2010-1)
 - Safety justification, connected to proven in use (IEC 61508:2010-2)
- **Mathematic more profound terms**
 - Average probability of **dangerous** failure on demand – PFD (IEC 61508:2010-1)
 - Average frequency of **dangerous** failure – PFH (IEC 61508:2010-1)
- **Terms in IEC 61508 and IEC 61511 is now the same (modes and failure rates)**

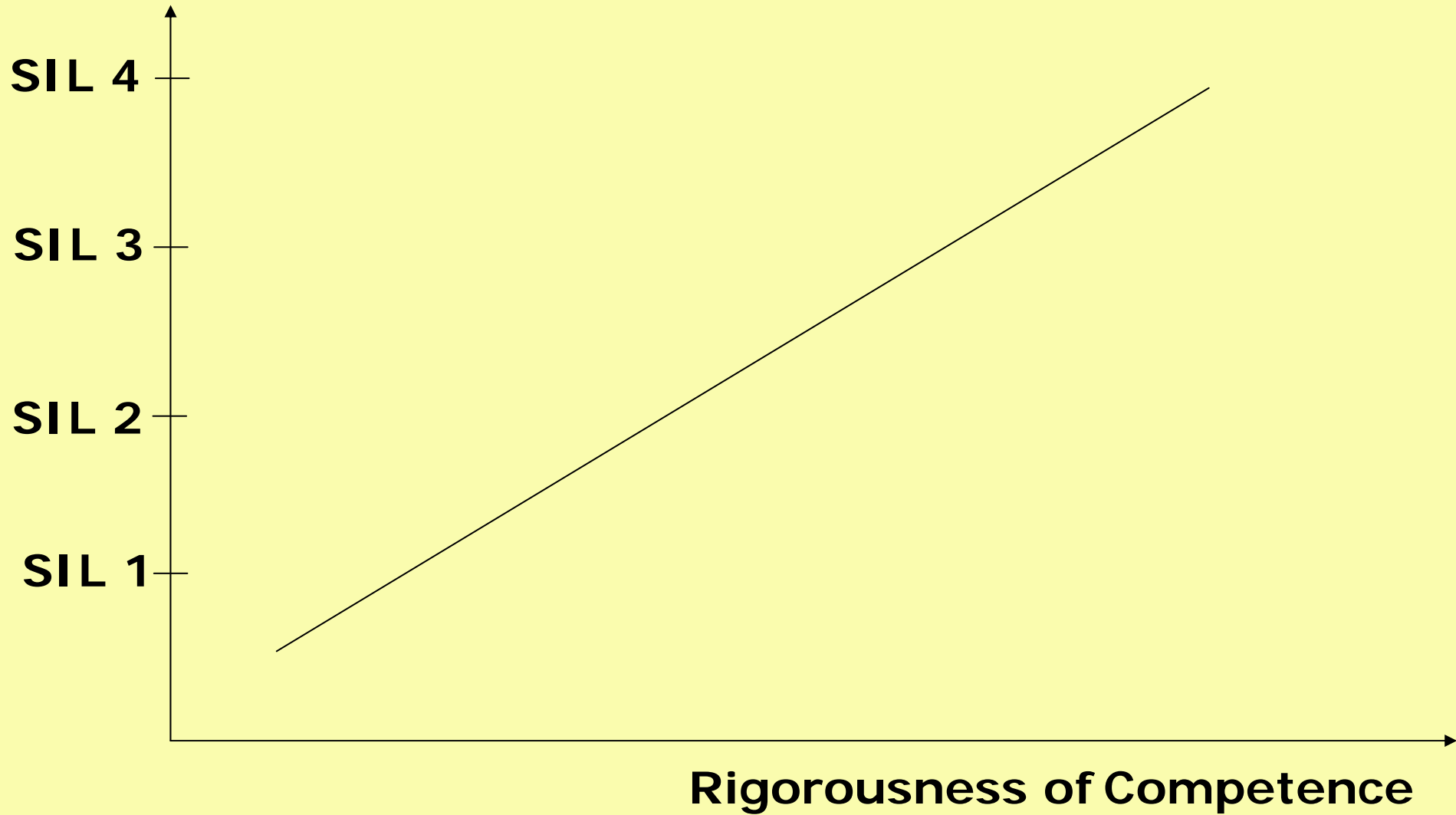
- **Now normative, previously was informative**
- **Objectives:**
 - *To specify the **responsibilities** in the management of functional safety*
 - *To specify the **activities** to be carried out by those with responsibilities in the management of functional safety*
- **Requirements:**
 - ***Appointment** of one or more persons of an organization with responsibilities*
 - ***Identification of all persons** responsible for any activities relevant to the achievement of functional safety*
 - *All persons responsible for any activities relevant to the achievement of functional safety shall be **competent** for the duties they have to perform.*

■ In Company level shall decide about

- *The responsibilities of the persons*
- *The level of supervision required*
- *More rigorous shall be the specification of competence according to the potential consequences in the event of failure of the Safety-Related Systems or SIL of Safety Related System (SIS in 61511 standard)*
- *The greater the consequences, the more rigorous shall be the specification of competence*
- *The higher the safety integrity levels, the more rigorous shall be the specification of competence*
- *The newer or more untried these are, the more rigorous shall be the specification of competence*
- *The type of competence appropriate to the circumstances (for example qualifications, experience, relevant training)*
- *Relevance of qualifications, engineering-, safety engineering knowledge, knowledge of the legal and safety regulatory*

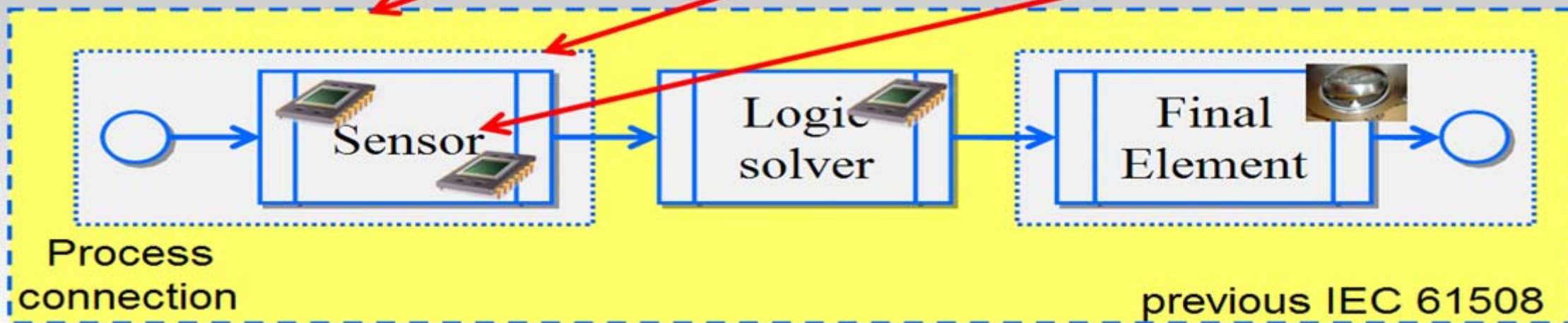
- **Competences shall be**
 - *Specified and*
 - *procedures shall be developed and documented...that persons shall have the appropriate competence (i.e. training, technical knowledge, experience and **qualifications**) relevant to the specific duties that they have to perform (for example TÜV FSE or CFSE is required to do any work on a SIS in any life cycle phase)*
- **Knowledge of**
 - *Given technology*
 - *Given profession (instrument, technology, electric etc..)*
 - *Knowledge of Safe Engineering*
 - *Relevant standards (IEC 61508:2010, IEC 61511)*
 - *Relevant local law and rules (SEVESO II Directives etc...)*
 - *Relevant company guidelines (in MOL FSQM)*

SIL value
Consequences
Novelty level



- Element, subsystem, element safety function, overall safety function

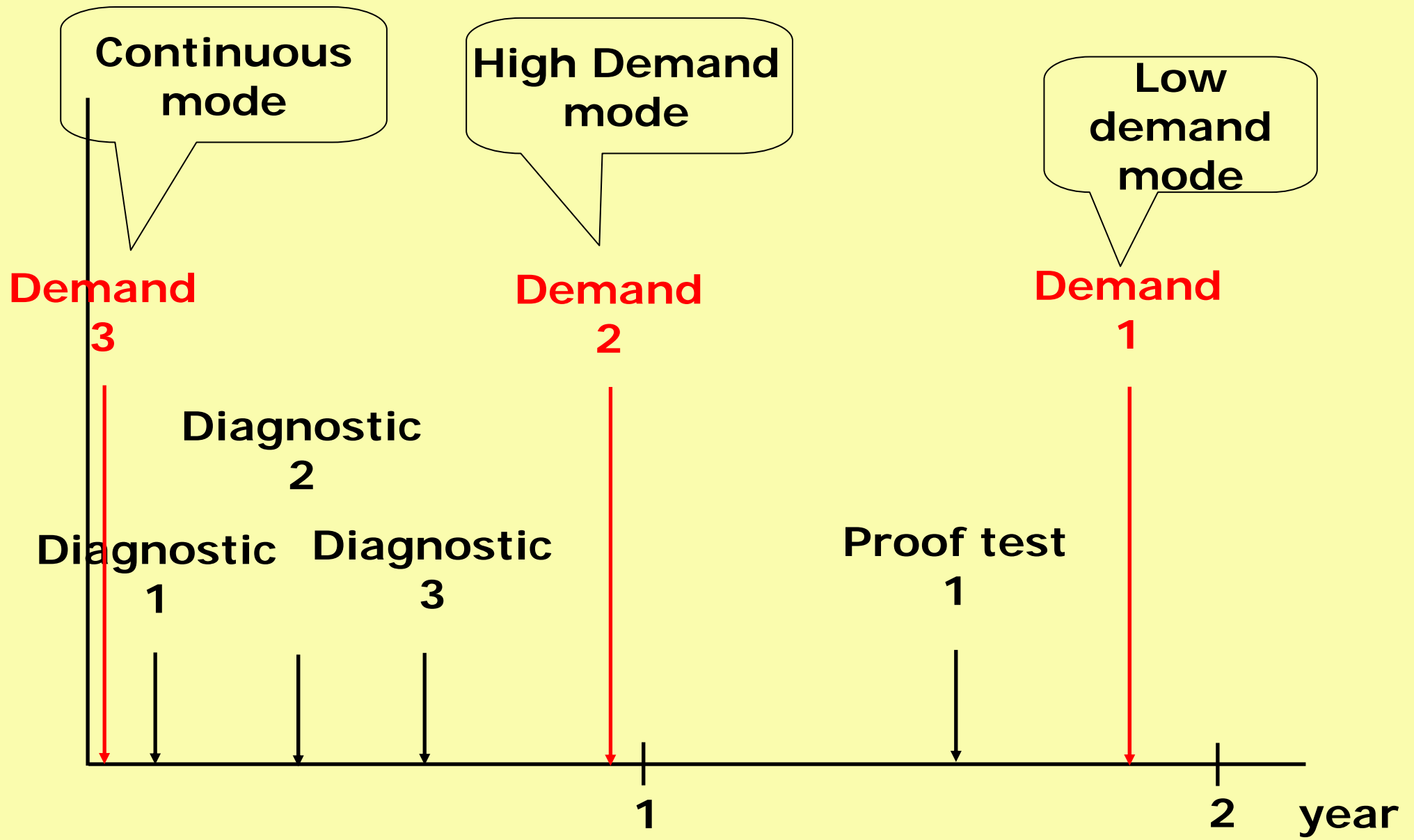
Scope Levels: System, Subsystem, Element



- System
 - Subsystems (serial and/or parallel)
 - Elements (serial and/or parallel)
- Compliant Item introduced relevant to IEC 61508:2010

- **According IEC 61508:2010, Volume 4, 3.5.16.**
 - *Low demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year*
 - *High demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year*
 - *Continuous mode: where the safety function retains the EUC in a safe state as part of normal operation*

Demand mode 61511	Continuous mode 61511	
Low demand 61508:2000	High Demand 61508:2000	Continuous 61508:2000
Use PFD _{avg} table	Use PFH table	Use PFH table
Take credit for proof testing	No credit for proof testing	No credit for proof testing
Take credit for automatic diagnostic	Take credit for automatic diagnostic	No credit for automatic diagnostic



- **Compliant item:** is any item (e.g. an element) on which a claim is being made with respect the clauses of IEC 61508:2010
- **Element Safety function of a Compliant Item**
 - *Part of the safety function implemented by an element*
- **Systematic Capability**
 - *Measure: SC 1 to SC 4, the systematic safety integrity of an element meets the requirements of specified SIL, when it meets the safety manual of the element*
- **Safety Manual of a Compliant Item**
 - *Provides all information required to meet the requirement of IEC 61508:2010*

- The evidence required in order to demonstrate that a SIS function meets its target SIL (i.e. the SIL Achievement exercise) is far more than a quantitative exercise, based solely on target failure measure. Architectural Constraints and Systematic Capability must also be taken into account.
- **safety integrity = hardware safety integrity + systematic safety integrity**
 - *Architectural Constraints: as the requirements for hardware safety integrity*
 - *Systematic Capability (SC1..SC4): as the requirements for systematic safety integrity*
- **Eg.: Having 'Systematic Capability X', which means, "the product element meets the requirements ... which is achieved by following a SIL X compliant development process."**

- Hardware compliance routes:
- In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level):
 - *Route 1H: based on hardware fault tolerance (HFT) and safe failure fraction (SFF) concepts; or (as in the previous release!!!)*
 - *Route 2H: based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels (proven in use and responsibility customer)*

- **Route 1H:** Maximum allowable SIL for a safety function carried out by type B safety related system

Safe failure fraction (SFF)	HFT=0	HFT=1	HFT=2
$SFF < 60\%$	-	SIL1	SIL2
$60\% \leq SFF < 90\%$	SIL1	SIL2	SIL3
$90\% \leq SFF < 99\%$	SIL2	SIL3	SIL4
$99\% \leq SFF$	SIL3	SIL4	SIL4
see Route 2H	SIL1-SIL2	SIL3	SIL4

- **The alternative approach to Safe Failure Fraction and only for Type B**
- **Reliability data used shall be:**
 - *based on field feedback*
 - *based on data collected in accordance with international standards (e.g., IEC 60300-3-2 or ISO 14224:);*

SIL	HFT	Type of element	Diagnostic Coverage	Comment
SIL4	2	Type B	DC > = 60%	Low Demand
SIL3	1	Type B	DC > = 60%	Low Demand
SIL2	1	Type B	DC > = 60%	High Demand and Continuous
SIL2	0	Type B	DC > = 60%	Low Demand
SIL1	0	Type B	DC > = 60%	

- **Safety integrity = hardware safety integrity + systematic safety integrity**
- **Systematic safety integrity: part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure.**
- **There are three possible Routes to compliance which are:**
 - *Route 1S: Requirements for the avoidance (prevention) and requirements for the control of systematic faults. This covers both hardware and software.*
 - *Route 2S: Evidence that the equipment is "proven in use" (PIU). This covers both hardware and software (new!).*
 - *Route 3S: For pre-existing software elements only. This covers only software.*
 - *(Note: "S" as Systematic)*

- **Systematic Capability (SC1..SC4):** as the requirements for systematic safety integrity is addressing two major issues:
 - *Avoidance or control of systematic failures caused by hardware design, environmental stress and operational failure*
 - *Avoidance of systematic failures during software development*
- **Systematic Capability is introduced and is defined as** "...a measure (expressed on a scale of 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..."
- **A Systematic Capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.**

- Security is addressed but in an informative way (NOT MANDATORY!).
- Malevolent and unauthorised actions have to be addressed during the *hazard and risk analysis*.
- If a security threat is seen as being reasonably foreseeable, then a security threats analysis should be carried out and if security threats have been identified then a vulnerability analysis should be undertaken in order to specify security requirements
- For guidance on security risks analysis, see IEC 62443 series: Industrial communication networks – Network and system security

- The E/E/PE requirements specification in Edition 1 of IEC 61508 comprised a single specification (i.e. a single step process). IEC 61508:2010 comprises two specifications (i.e. a two step process) namely:
 - *Step 1: Develop the E/E/PE system Safety Requirements Specification (SRS)*
 - *Note: obligation of user (and system designer) where, SRS = safety functions requirements specification + system safety integrity requirements specification*
 - *Step 2: Develop the E/E/PE system design requirements specification (in IEC 61508-2, see the box 9 of safety life cycle). NEW sub-phase of E/E/PE system safety lifecycle (in realisation phase), including ASICs & software.*
 - *Note: Obligation of product designer (manufacturing of subsystems and elements)*

- Only for manufacturing of subsystems and elements!!
- Requirements for application specific integrated circuits (ASICs) are now included, namely:
 - *An appropriate group of techniques and measures shall be used that are essential to prevent the introduction of faults during the design and development of ASICs;*
 - *Special architectural requirements for integrated circuits (ICs) with on-chip redundancy are given in a normative Annex*

- The purpose of the safety manual for compliant items is to document all the information, **including limitations**, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of the standard

- **Contents of Safety manual for compliant items (see: EN 61508-2:2010 Annex D):**
 - *Functional specification*
 - *Identification of the hardware and/or software configuration*
 - *Constraints on the use of the compliant item*
 - *Every failure mode with an estimated failure rate for the compliant item*
 - *Periodic proof test and/or maintenance requirements*
 - *Hardware fault tolerance*
 - *Classification as type A or type B*
 - *Systematic capability of the compliant item*
 - *Instructions or constraints relating to the application of the compliant item*
 - *Additional requirements relating to software compliant items*

- **Architectural constraints: Route methods**
- **Safety Function of element, device, subsystem (compliant items)**
- **Competence of persons**
- **Systematic capability**
- **SRS of element, device, subsystem**
- **Security of SIS**
- **Increasing the responsibility of the end user**

Thanks for the attention.

