excellence in dependable automation

exida.com
excellence in dependable automation

IEC 61508 Maintenance – Status

- ✓ IEC 61508 Maintenance Projekt ist aus dem zulässigen Zeitrahmen gelaufen
  - Viele Baustellen
    auch durch neue Mitglieder (Frankreich, USA, IEC 61511 Team)
  - Bestehende Anforderungen, die tiefgehenden sicherheitstechnische Kenntnisse erfordern, werden in Frage gestellt.
- ✓ IEC 61508 Maintenance Projekt muss auf State 0 zurückgesetzt werden
- ✓ IEC muss ein neues Maintenance Projekt bewilligen
- ✓ Die bisherigen Arbeiten sollen in das neu aufzulegende Maintenance Projekt übergehen

exida.com
excellence in dependable automation

IEC 61508-1 / -2 Baustellen

- ✓ Anwendbarkeit nicht nur auf komplette Sicherheits-funktionen sondern auch auf Subsysteme / Geräte
  - Definition Subsystem
  - SIL capability
- ✓ Systematisierung der Tabellen und Integration in die Hauptteile
- ✓ ASICs
- ✓ Additional requirements for data communications
- ✓ Betriebsbewährtheit

exida.com
excellence in dependable automation

IEC 61508-3 Baustellen

- Relativ wenig Änderungen bis jetzt
  - Systematisierung der Tabellen und Integration in die Hauptteile
  - Data-driven Software-Design (Rail, Air-traffic control)
- Zu erwarten
  - Objekt-Orientierung
  - Tools
  - Security

exida.com
excellence in dependable automation

IEC 61508 Nebenbaustellen

- ✓ Tochterstandards
  - IEC 61511 „Functional safety – Safety instrumented systems for the process industry sector “
  - IEC 62061 „Safety of machinery – Functional safety of electrical, electronic and programmable control systems”
  - Draft IEC 61326-3 “Electrical equipment for measurement, control and laboratory use – EMC requirements
    Part 3 - Immunity requirements for equipment performing or intended to perform safety functions (functional safety) in industrial applications”
  - Draft IEC 61784-3 “Digital data communications for measurement and control – Part 3: Profiles for functional safe communications in industrial networks”
  - Und viele mehr: Nukleartechnik, Explosionsschutz, Gassensorik

exida.com
excellence in dependable automation

IEC 61508 Maintenance

- ✓ Neue Begriffe
  - Target failure measure ersetzt durch
    - Risk Reduction Factor – statt Probability of Failure on Demand
    - Hazard rate – statt Probability of dangerous failure per hour
  - Risk reduction factor = Factor by which a demand mode safety function reduces the estimated frequency of the harmful event.
  - Hazard rate = Dangerous failure rate of the combination of the EUC/EUC control system together with the (P)ES.
  - Demand mode: where the safety function is only performed intermittently on demand in order to transfer the EUC into a specified safe state.
  - Continuous mode: where the safety function retains the EUC in a safe state as part of normal operation.

exida.com
excellence in dependable automation

IEC 61508 Maintenance

- ✓ Präzisierung
  - If the rate of dangerous failure of the EUC control system is claimed as being lower than 10^{-5} dangerous failures per hour then the EUC control system shall be considered to be a safety-related system subject to the requirements of this standard.
  - Competence of persons – jetzt normativ

exida.com
excellence in dependable automation

IEC 61508 Maintenance – Subsystem

- ✓ Neue Möglichkeiten
  - Nicht nur die gesamte Sicherheitsfunktion kann SIL compliant sein, sondern auch Teilsysteme (Subsystem / Element) → **SIL Capability**
  - **Subsystem** = any entity of the top-level architectural design of a safety-related system where a failure of the subsystem results in failure of a safety function. (IEC 62061)
  - Element = part of a subsystem comprising a single component or any group of components that performs one or more element safety functions.
  - **Safety Manual** = a document that provides all the information relating to the functional safety properties of an element that is required to ensure that the complete system meets the requirements of IEC 61508.
  - The **Safety Justification** shall document the basis for the information contained in the Safety Manual.

exida.com
excellence in dependable automation

IEC 61508 Maintenance – SIL Capability

- ✓ Neue Möglichkeiten
  - **SIL Capability** = a measure (expressed on a scale of 1 to 4) of the confidence that an element safety function will not fail due to relevant systematic failure mechanisms when the element is applied in accordance with the instructions specified in the element safety manual.
  - **Safety Criticality** (Categories) = the potential of an encapsulated component (or module or subsystem) whose deviation from its specified functionality creates an unsafe situation of the safety-related system.

exida.com
excellence in dependable automation

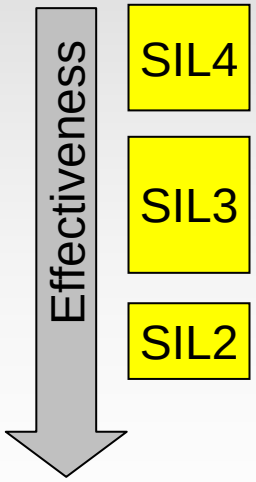
IEC 61508 – Safety Criticality

- ✓ Safety Criticality
  - The potential of an encapsulated entity to create an unsafe situation of the safety-related system.
  - C3: Safety Critical = the criticality of an entity, where a single deviation from the specified function(s) may cause an unsafe situation.
  - C2: Safety Relevant = the criticality of an entity, where a single deviation from the specified function(s) cannot cause an unsafe situation, but the combination with a second failure of another component may cause an unsafe situation.
  - C1: Interference Free = the criticality of an entity, which does not implement safety critical or safety relevant functions, but has read-only interfaces with entities of such criticality.

exida.com
excellence in dependable automation

Independence: Pre-requisite for SCA

- Software components shall have clearly restricted functionality and interface
- The timely interference of the software functions is monitored by the logical and timely program flow monitoring as required by IEC 61508-2.



- Software components run on separate H/W
- Software components run in separate, H/W protected memory segments, communicating by message passing only
- Software components are encapsulated
  (supported by the programming language (Modula, ADA, Java, C# and demonstrated by the Linker Xref listings)
- If none of these apply, then the highest Criticality is inherited

exida.com
excellence in dependable automation

Safety Criticality Analysis

Safety Criticality: Objective

identify areas where additional effort increases safety integrity most

- Safety functions
- Safety support functions
- Not-safety functions

Technical requirements:
- Safety Measures
- Independence

Verification requirements:
- Failure Analysis
- Testing
- Support Impact Analysis

exida.com
excellence in dependable automation

IEC 61508 – Safety Criticality

SIL Capabilty of the component		Criticality of the component		
		C1	**C2**	**C3**
SIL of the safety function or safety-related system	**SIL1**	Demonstrate sufficient independence	Meet applicable **SIL1** requirements	Meet applicable **SIL1** requirements
	SIL2	Demonstrate sufficient independence	Meet applicable **SIL1** Requirements	Meet applicable **SIL2** Requirements
	SIL3	Demonstrate sufficient independence	Meet applicable **SIL2** Requirements	Meet applicable **SIL3** Requirements
	SIL4	Demonstrate sufficient independence	Meet applicable **SIL3** Requirements	Meet applicable **SIL4** requirements

exida.com
excellence in dependable automation

IEC 61508 Maintenance - Tabellen

- ✓ Tabellen sind jetzt im Hauptteil von -2 und -3, den Kapiteln zugeordnet - Beispiel

7.2 E/E/PES Design requirements specification

Table NEW 2 – Properties of the System (or Software, or Hardware) Safety Requirements Specification for systematic integrity

Properties required for systematic integrity. See IEC 61508-4.		Evidence required to demonstrate SIL			
		1	2	3	4
1.1	Completeness with respect to the safety needs			TO	TO
1.2	Correctness with respect to the safety needs	T	T	T TO	T TO TR*
1.3	Freedom from intrinsic specification faults	T	T	TO	TO TR*
1.4	Avoidance (where practicable) of what is not related to the safety of the EUC			T	TO
1.5	Sufficient independence of components to avoid common cause failures on the system level		T	TO	TO TR**
1.6	Documentation of the safety requirements: clear, unambiguous	T	T	T	T

TR*: when reasonably achievable.
TR**: this by itself is sufficient evidence.

exida.com
excellence in dependable automation

IEC 61508 Maintenance - Tabellen

- ✓ Neue Begriffe – Properties
  - Completeness, Correctness, Consistency
  - Freedom of intrinsic faults
  - Independence to avoid CC failures
  - Avoidance of what is not related to safety
  - Clear, unambiguous, documentation – trustworthy, credible
  - Testability, repeatable
  - Predictable, Defensive, Modifiable design
  - Assessable

exida.com
excellence in dependable automation

IEC 61508 Maintenance - Tabellen

- ✓ Neue Begriffe – Evidence
  - **Technical evidence** (T) without or with limited objective acceptance criteria, e.g., black-box testing based on judgement, field trials.
  - **Technical evidence with objective acceptance criteria** (TO) that can give a high level of confidence that the required property is achieved; e.g., test / analysis coverage measures.
  - **Technical evidence and rigorous reasoning** (TR) including objective, systematic evidence that the required property is achieved, e.g. formal proof, demonstrated adherence to architectural constraints that guarantee the property.
  - **Functional Safety Management-based** evidence
  - (Independent) **Expert Judgement** (IEJ) that the property is achieved is based on expert experience. The reviews and inspections are performed by technically independent, competent, informed individuals having sufficient means and time.

exida.com
excellence in dependable automation

Neue Tabellen - SW

IEC 61508-2 /-3

Table NEW 2 – Properties of the System (or Software, or Hardware) Safety Requirements Specification for systematic integrity

Properties required for systematic integrity. See IEC 61508-4.		Evidence required to demonstrate SIL			
		1	2	3	4
1.1	Completeness with respect to the safety needs			TO	TO
1.2	Correctness with respect to the safety needs	T	T	T TO	T TO TR*
1.3	Freedom from intrinsic specification faults	T	T	TO	TO TR*
1.4	Avoidance (where practicable) of what is not related to the safety of the EUC			T	
1.5	Sufficient independence of components to avoid common cause failures on the system level		T	TO	
1.6	Documentation of the safety requirements: clear, unambiguous	T	T	T	

TR*: when reasonably achievable.
TR**: this by itself is sufficient evidence.

Table NEW 2A – Properties of the System (or Software, or Hardware) Safety Requirements Specification for systematic integrity

Properties required for systematic integrity. See IEC 61508-4 for definitions.		Evidence type	Overall approach to achieving evidence. See Table B below.
1.1	Completeness with respect to the safety needs	FSM	1, 2, 3, 4
		T/TO/TR	6
		EJ/IEJ	12
1.2	Correctness with respect to the safety needs	FSM	1, 3
		T/TO/TR	T: 6, 9, 10 TO: 10 TR: 11
		EJ/IEJ	12
1.3	Freedom from intrinsic specification faults	FSM	1, 5
		T/TO/TR	T / TO: 10 TR: 11
		EJ/IEJ	12
1.4	Avoidance (where practicable) of what is not related to the safety of the EUC	FSM	1, 2, 3
		T/TO/TR	7, 8
		EJ/IEJ	12
1.5	Sufficient independence of components to avoid common cause failures on the system level	FSM	1, 2, 5
		T/TO/TR	T: 13, 16 TO: 14, 16, 17 TR: 15, 16
		EJ/IEJ	12

Table NEW 2B – Overall approach to achieving evidence

6	Forward traceability, from the parts of the input documents that put safety needs (see 2) on the item being specified, to the corresponding Safety Requirements Specification statements. (TO if coverage targets are defined, justified and met.)
13	Demonstration of sufficient independence of components to avoid common cause failures on the system level: a structured approach.
14	Demonstration of sufficient independence of components to avoid common cause failures on the system level: a mathematical approach.
15	Demonstration of sufficient independence of components to avoid common cause failures on the system level: hardware separation of differing criticalities.
16	Demonstration of sufficient independence of components to avoid common cause failures on the system level: purposeful software design for independence.

IEC 61508-6 /-7 – Technical Report

exida.com
excellence in dependable automation

Neue Tabellen - HW

XA.1 Definition of Properties of Hardware Fault Control

Property	Definition	Requirements	SIL 1	SIL 2	SIL 3	SIL 4
Effectiveness with respect to dangerous failures of the safety-related system	Property of the run-time test and monitoring measures to detect component failures which may result in dangerous behaviour of the safety-related system. *Note. The safety functions and the safe and unsafe system behaviour are usually specified in the Safety Requirements Specification.*	P2-7.4.3.1	FSM + T	FSM + TOC	FSM + TOC + iEJ	FSM + TRR + iEJ
Completeness with respect to safety-related components	Property of the run-time test and monitoring measures to cover all components of the safety-related system whose failure which may result in dangerous behaviour of the safety-related system. *Note. The safety functions and the safe and unsafe system behaviour are usually specified in the Safety Requirements Specification.*	P2-7.4.7.3	FSM	FSM + TOC or FSM + T + iEJ	FSM + TOC + iEJ	FSM + TOC + iEJ
Correctness with respect to the safety-related response of the safety-related system	Property of the run-time test and monitoring measures to react to potentially dangerous component failures such that they do not result in dangerous behaviour of the safety-related system. *Note. The safe state for the safety-related system is usually specified in the Safety Requirements Specification.*	P2-7.4.3.2.5 P2-7.4.6	FSM + T	FSM + TOC	FSM + TOC + iEJ	FSM + TRR
Timeliness with respect to the safety-related response of the safety-related system	Property of the run-time test and monitoring measures to detect potentially dangerous component failures in time such that they do not result in dangerous behaviour of the safety-related system. *Note. The time constraints for the safety-related system are usually*	P2-7.4.3.2.3 P2-7.4.3.2.4 P2-7.4.3.2.5	FSM	FSM + TOC	FSM + TOC + iEJ	FSM + TRR

	Recommended methods	Type of evidence	Ref. to current tables	1	2	3	4	5	6	7
	7. Verifiability (Testability)									
	6. Freedom from Interference									
	5. Effectiveness with respect to Common Cause failures									
	4. Timeliness									
	3. Correctness									
	2. Completeness									
	1. Effectiveness									
1	Application of IEC 61508-2 tables 2 and 3 together with table A.1 *Note: Further guidance on the effectiveness of measures is given in IEC 61508-2 tables A.2 to A.15.*	TOC or TRR	P2-Table 2 P2-Table 3 P2-Table A.1	✓	✓					
1.1	Application of HFT >= 1	TRR	P2-Table 2 P2-Table 3	✓	✓	✓	✓		✓	✓
1.2	Application of HFT >= 1 using diverse hardware	TRR	P2-Table 2 P2-Table 3 P2-Table A.16	✓	✓	✓	✓	✓	✓	✓
1.3	Application of DC >= 90%	TOC	P2-Table 2 P2-Table 3 P2-Table A.1	✓	✓			✓		

exida.com
excellence in dependable automation

IEC 61508 Maintenance

- ✓ Neue Anforderungen - ASIC, FPGA, PLD

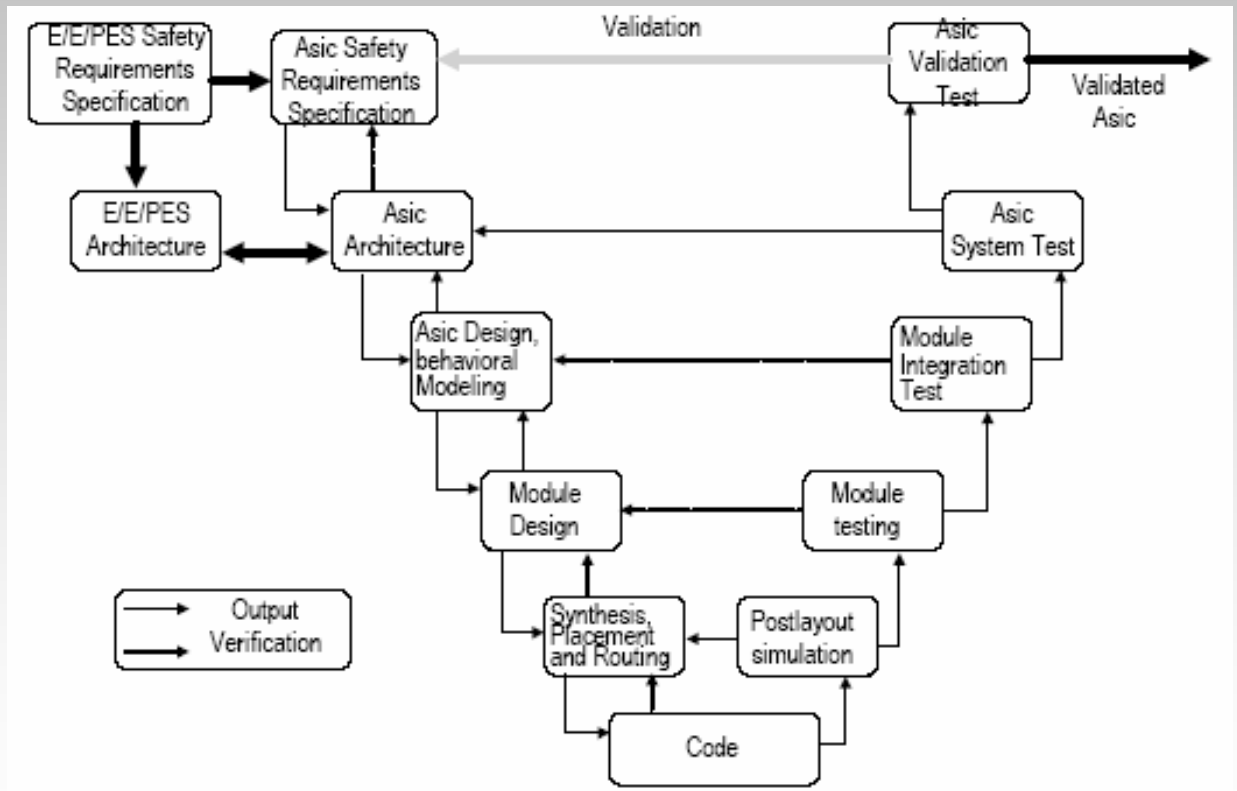
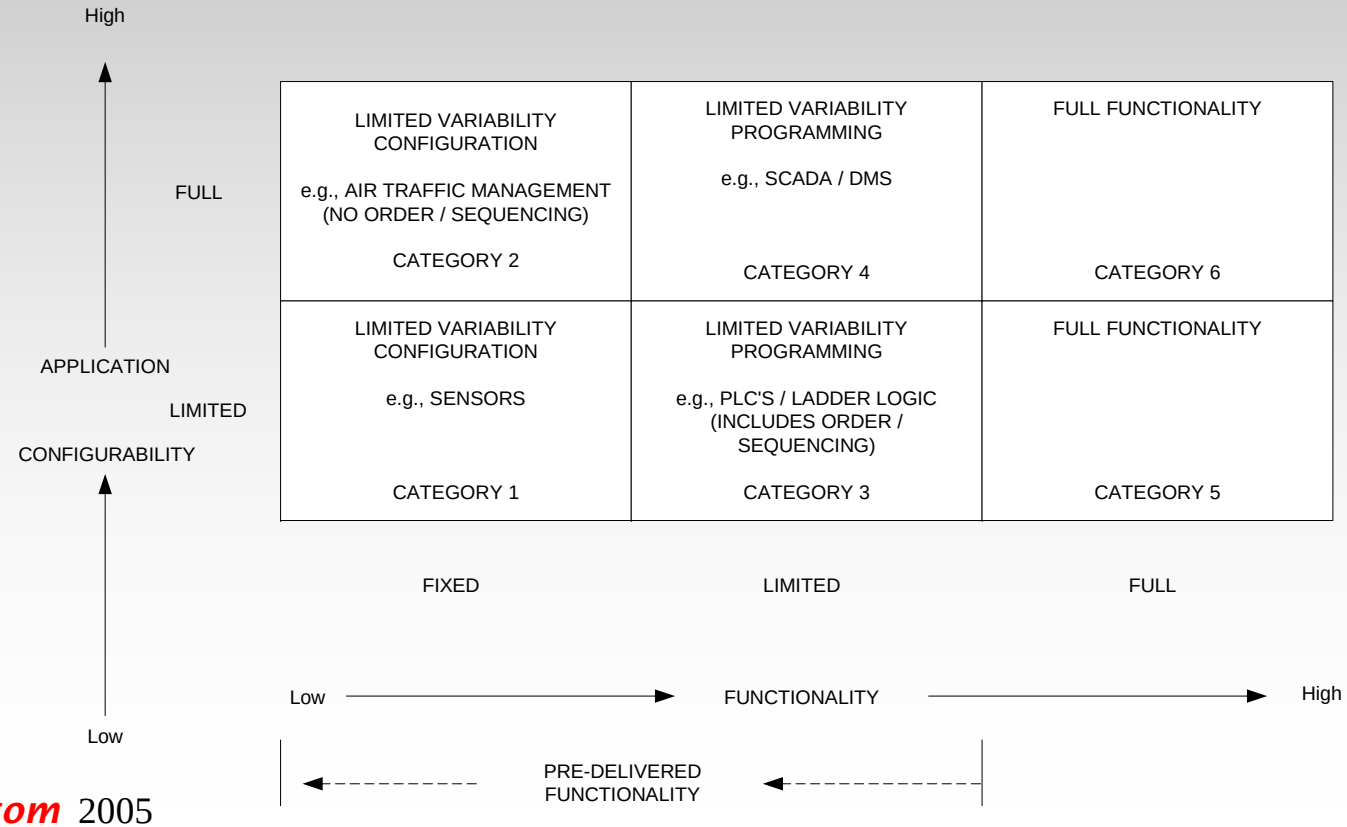


Figure 3 – ASIC development lifecycle (the V-Model)

exida.com
excellence in dependable automation

IEC 61508 Maintenance

- ✓ Neue Anforderungen – Data driven Systems
  - Systemverhalten bestimmt durch Konfiguration (Full / Limited Application configurability)



exida.com
excellence in dependable automation

IEC 61508 Maintenance

- ✓ Neue Anforderungen – Data driven systems
  - The configuration language does not allow the programmer to alter the function of the product. Instead configuration is constrained to creation of extensive static data parameters to enable the product to be matched to its external interfaces.
  - In addition the degree of rigour in demonstrating the safety integrity should include but not be limited to the following:
    - Automation tools for creation of data;
    - Consistency checking;
    - Rules checking.

excellence in dependable automation