TECHNISCHE UNIVERSITÄT WIEN

TTTech

Dependable Computer Systems

Part 4: Certification – Processes and Standards

Contents

- Generic Characteristics
- Example: TTTech´s Software Development
- Example: Traceability in the Development of an Ethernet Switch
- Certificates
- Standards
  - Safety Integrity Levels (SIL)
  - Automotive SIL (ASIL)
  - Design Assurance Levels (DAL)
- The Safety Case

Generic Characteristics of Development Processes for Dependable Systems

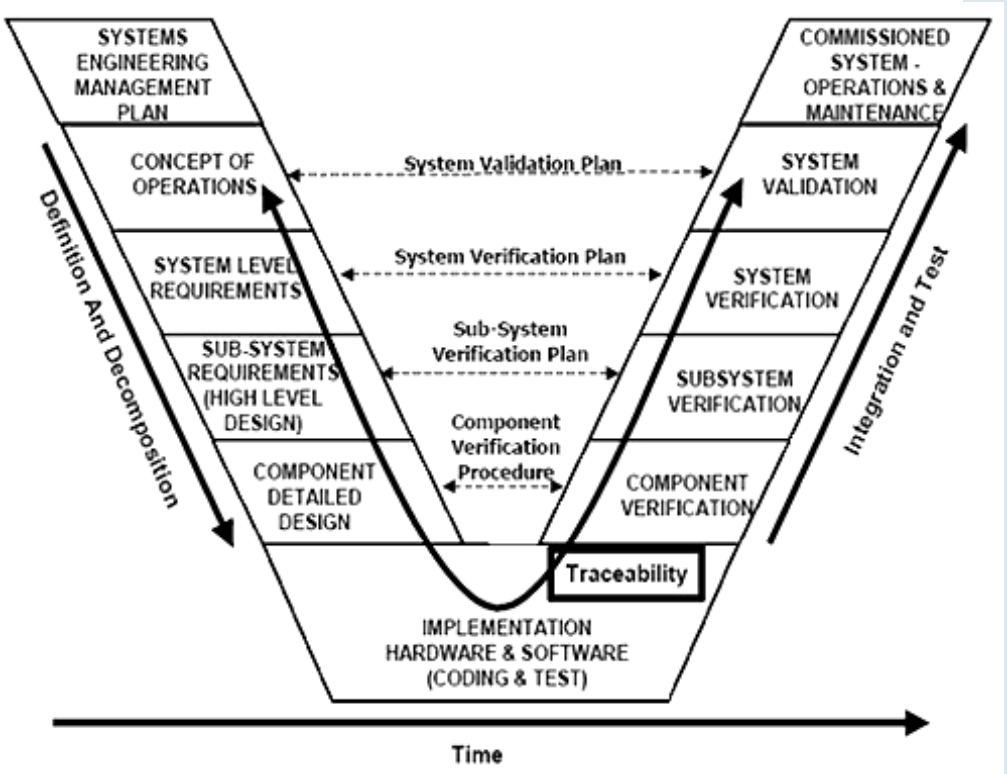
Objectives of Development Processes

- The aim of development processes is to minimize the likelihood of development faults, i.e., faults that occur during the creation of the system (HW, SW, etc.)

- For example: since the introduction of the DO-178B standard “Software Considerations in Airborne Systems and Equipment Certification” in the 1990s, not a single lethal incident has occurred that would trace back to a software development fault.

Typical activities in such development processes

- Requirements Capturing
- High-Level Requirements Document
- Low-Level Requirements Document
- Conceptual Design Document
- Detailed Design (i.e., implem-entation)
- Verification and Validation
- Peer review and auditing
- Key property of the documents: traceability



http://www.mitre.org/sites/default/files/images/selc-te-vv-fig2.gif

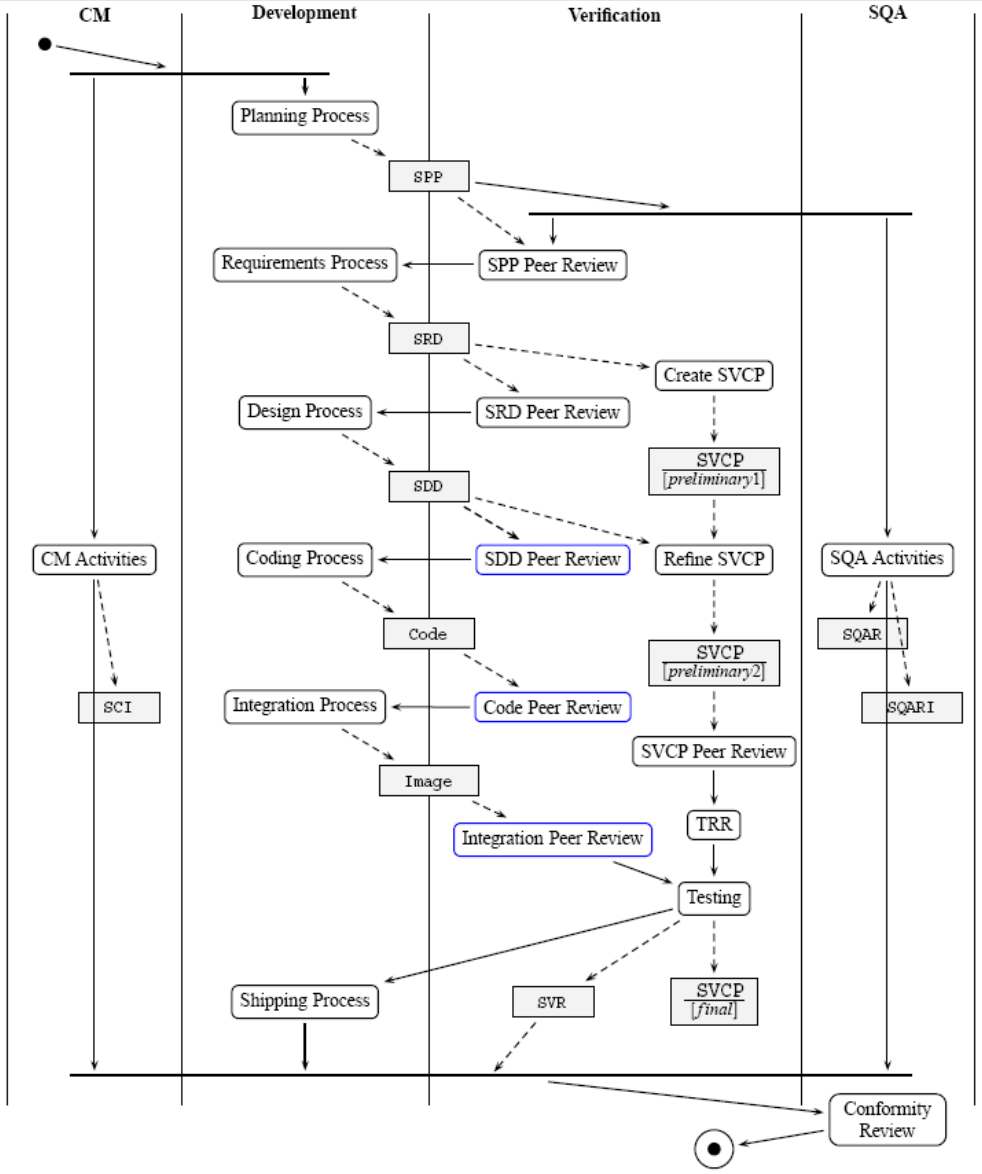
Verification and Validation

- Verification is the process to check whether a product satisfies its requirements.
- Validation is the process to check if the product satisfies its purpose.

- Why is verification different from validation?

  → Sometimes, a product's purpose is not fully described by its requirements.

Example: TTTech´s Software Development



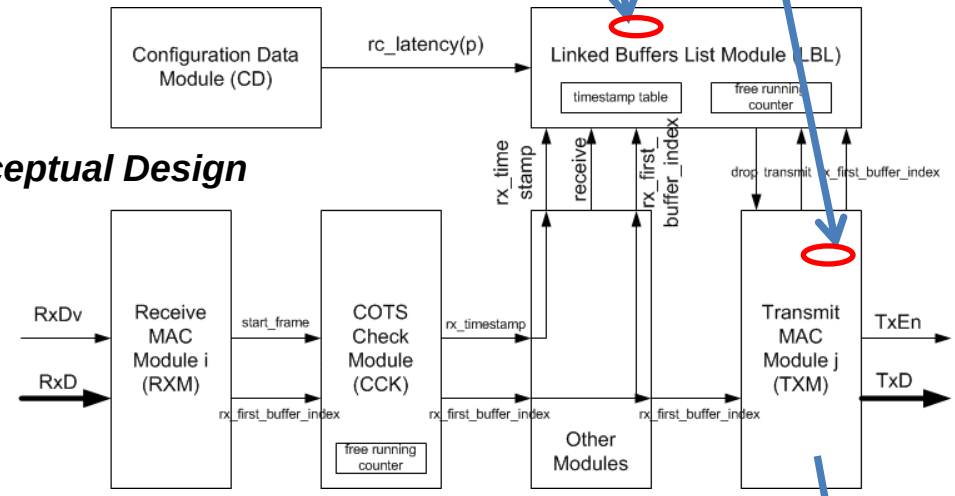
- The flowchart to the left shows how software processes are implemented at TTTech.
- Each development process creates an artifact as output (documents or code).
- *Software Verification Cases and Procedures (SVCP)* are developed in parallel to the refinement steps of the development process.
- All development, planning and verification artifacts are *peer reviewed* prior to release.
- The Testing Process creates the *Software Verification Results (SVR)* as objective evidence for the correct implementation of all high- and low-level requirements.
- SQAR, SW Quality Assurance Record
- SQARI, SW Quality Assurance Record Index

Example: Traceability in the Development of an Ethernet Switch

Requirement

1737 **VLU-4650** The switch shall drop the frames policed at switch ingress, as critical traffic in accordance with
1738 DCH-2052 and dispatched as rate constrained traffic that reside in the switch more than a statically config-
1739 urable amount of time (*rc_latency* parameter defined on a per output port basis described by MNI-3724).
1740 ***Guidance:*** *When a CT frame was dropped because of age violation, the diagnosis counter rcframe_age_err*
1741 *is incremented by 1, according to DCI-2745*

Conceptual Design



Implementation

```
if R.tdma_frame >= SERDES_PORTS_NO then
   V.age_time       := ONE_SECOND;                          --\ReqRef{VLU-4650}
 else
   V.age_time       := cdi.age_time(stdvec_to_int(R.tdma_frame));   --\ReqRef{VLU-4650}
 end if;

elsif R.start_tdma_buffer_d = '1' then
   V.tdma_frame     := ismi.tdma_frame;                     --\ReqRef{VLU-4650}

   if ctci.valid = '1' and R.one_time = '1' then
      V.ramo_lbl_to_link_ram_addr      := ctci.tail_index;  --\ReqRef{MNI-3660},
```

Test

```
[PURPOSE]
This test case checks if the switch ip drops incoming RC
frames that ageded out inside the IP.\\

[AUTHOR]
AST

[RESULT]
PASS

[REQUIREMENTS]
\ReqRef{MNI-3700}
\ReqRef{VLU-4650}
\ReqRef{DCI-2745}

[PRECONDITIONS]

\footnotesize
\begin{verbatim}

The test assumes the following configuration is loaded:
General Parameters Table:
 - static cots routing          := 1
                                := 0
                                := 0xDEADBEEF
                                := 0xFFFFFFFF
                                := 500 (4us) - has the resolut
                                s
```

Certificates

What is being certified?

- Product
  - a regulatory body approves that a product has certain characteristics.
  - e.g., type certificate of an airplane
- Company
  - a regulatory body approves that a given company follows given standards.
  - e.g., ISO 9001

Certificates Examples

- Type Certificate (Aerospace):
  - is issued to signify the airworthiness of an aircraft manufacturing design,
  - is issued by a regulating body (e.g., FAA, EASA).

- Automotive Equivalent?

Standards

Main Aspects of Development Processes

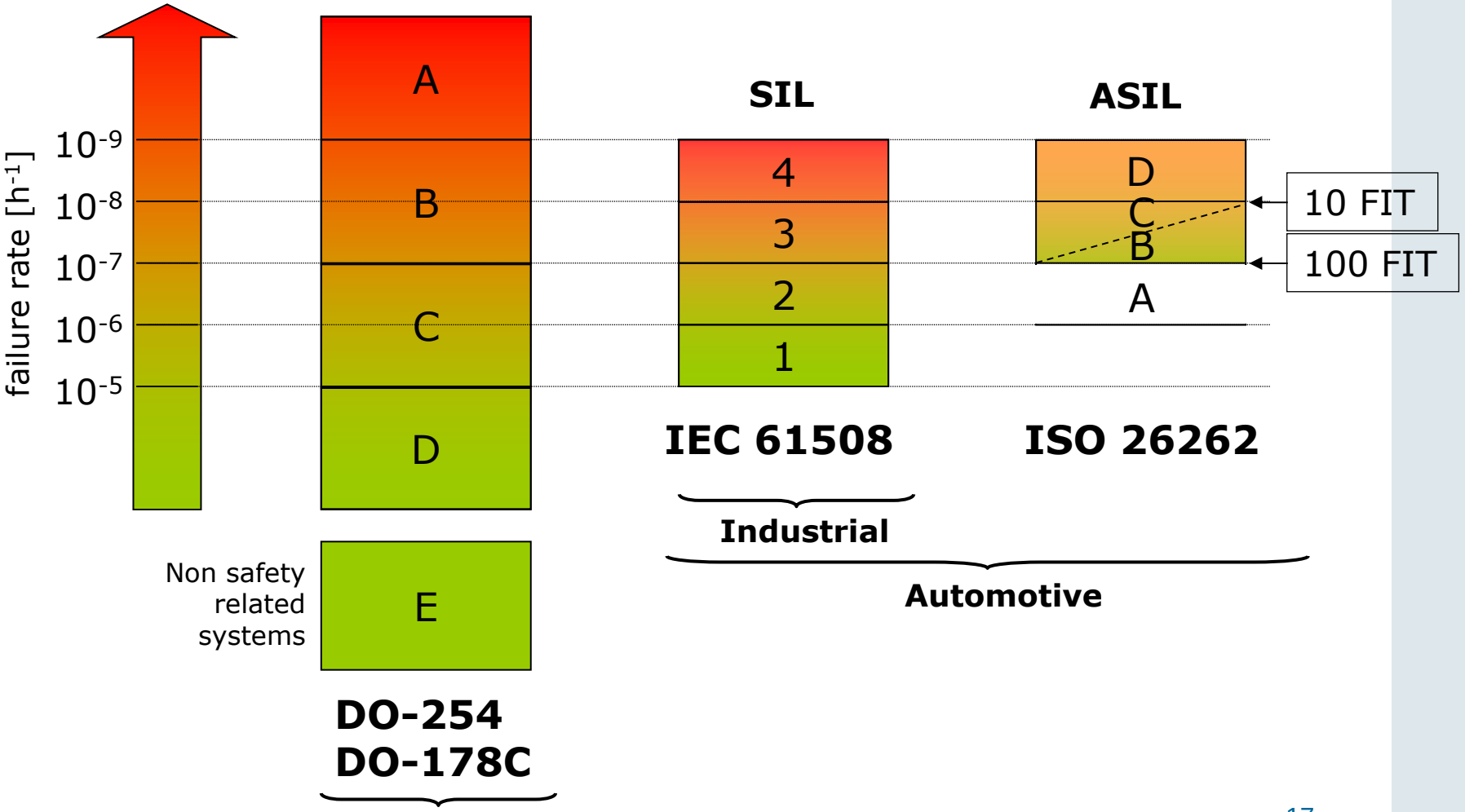
- Requirements on the development process in particular:
  - specification
  - design
  - verification
- Requirements on the safety management.

Example Standards

- IEC 61508 – “Functional Safety”
- ISO 26262 – “Road vehicles – Functional safety”
- ARP 4754 – “Certification Considerations for Highly-Integrated or Complex Aircraft Systems”
- DO 178B/C – “Software Considerations in Airborne Systems and Equipment Certification”

Possible relation between safety standards

Multi-dimensional aspects needs to be considered here

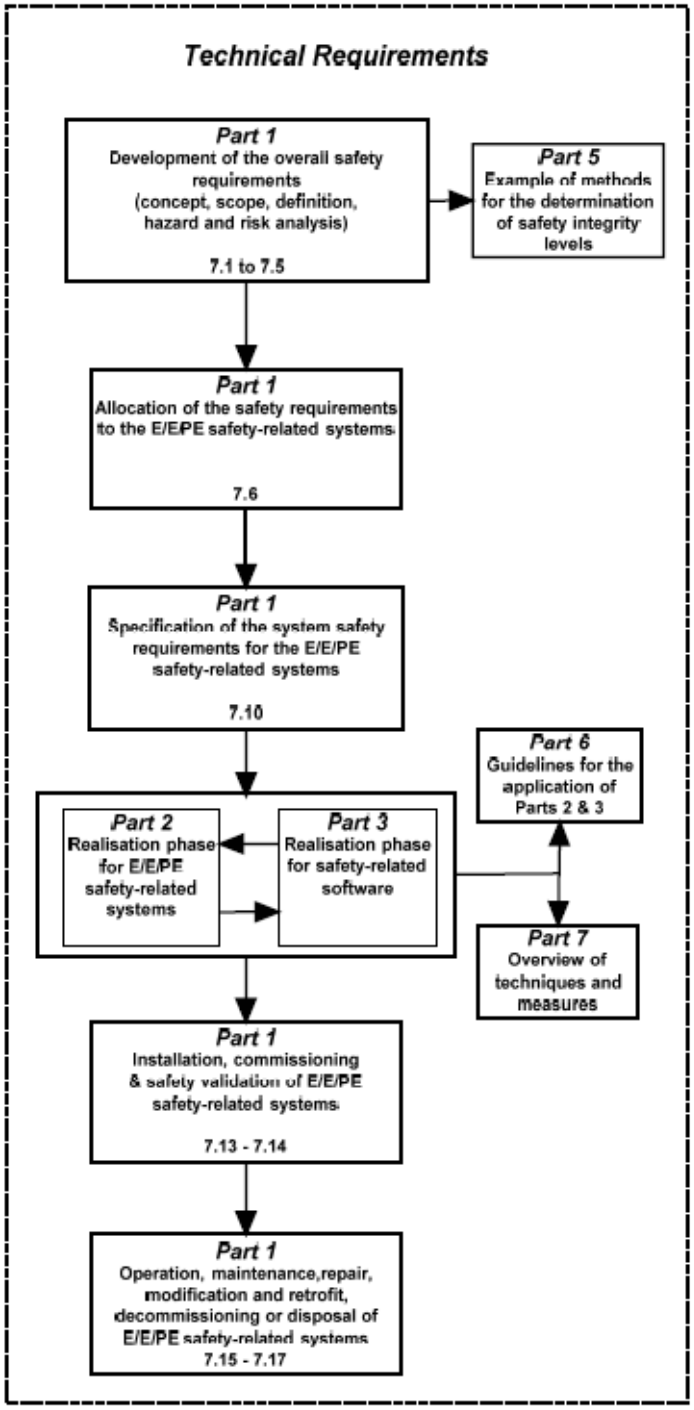


Terminology

- Certification-related standards have been developed in parallel to the academic work. Thus, the terminology as introduced by Avizienis et al. and used in this course, does not always apply.
- Certification-related standards introduce their individual terms and definitions.

Safety Life Cycle Considerations

- A complete framework for the safety life cycle consists of:
  - definition of different life cycle phases
  - specification of which activities to perform in each phase
  - specification of which inputs to provide to each of the activities
  - requirement on which results to achieve.
- Standards vary with respect to their framework completeness.
  - e.g., IEC 61508 defines a complete framew. (see next slide)
  - e.g., DO 178 defines only the results to be achieved



Other Requirements

Part 4
Definitions & abbreviations

Part 1
Documentation Clause 5 & Annex A

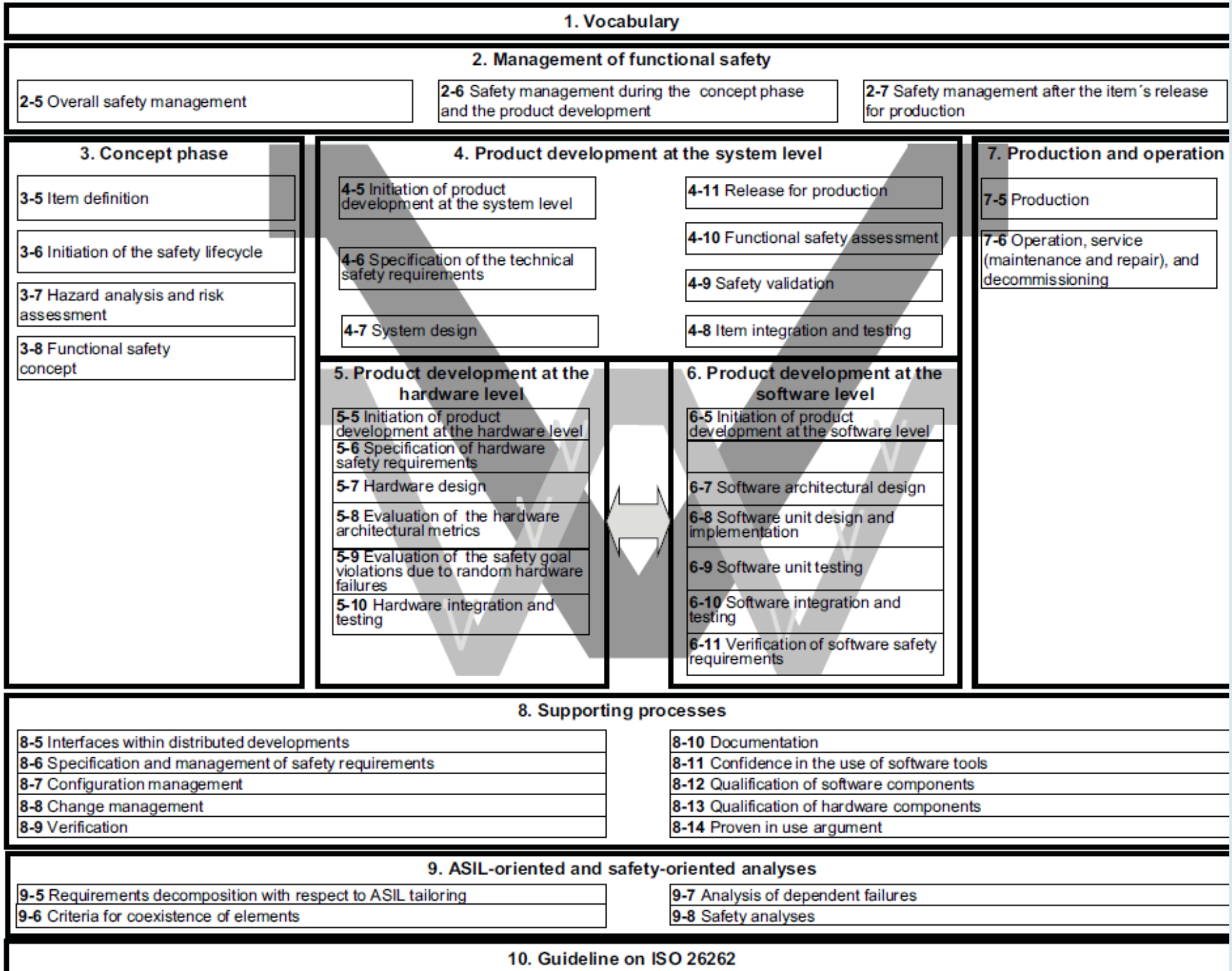
Part 1
Management of functional safety Clause 6

Part 1
Functional safety assessment Clause 8

We will discuss later how some of these parts tie into each other.

SW/HW Development Life Cycle

- Standards also vary in imposing requirements on the SW/HW development life cycle.
  - e.g., IEC 61508 does not require any particular SW development process
  - e.g., ISO 26262 defines a V-Model as a reference software development process (see next slide).


1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

Safety Integrity Levels

Safety Integrity Levels (IEC 61508)

- **3.5.1 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 for the EUC [Equipment Under Control], in respect of a specific hazardous event (see 3.4.1 and 3.4.2)
- **3.5.4 safety integrity:**
  - probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time
- **3.5.8 safety integrity level SIL:**
  - discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Safety Integrity Levels (IEC 61508) cont.

Is the result of a risk assessment (IEC 61508 – part 5).

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 $< 10^{-5}$

Safety Integrity Levels (IEC 61508) cont.

mode of operation: way in which a safety function operates, which may be either

- 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; or
- 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; or
- continuous mode: where the safety function retains the EUC in a safe state as part of normal operation

Safety Integrity Levels (IEC 61508) cont.

average probability of dangerous failure on demand (PFD_{avg}):

- mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

average frequency of a dangerous failure per hour (PFH)

- average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time

Safety Integrity Levels (IEC 61508) cont.

- *NOTE 3: Tables 2 and 3 relate the target failure measures, as allocated to a safety function carried out by an E/E/PE safety-related system, to the safety integrity level. It is accepted that it will not be possible to predict quantitatively the safety integrity of all aspects of E/E/PE safety-related systems. Qualitative techniques, measures and judgements will have to be made with respect to the precautions considered necessary to ensure that the target failure measures are achieved...*

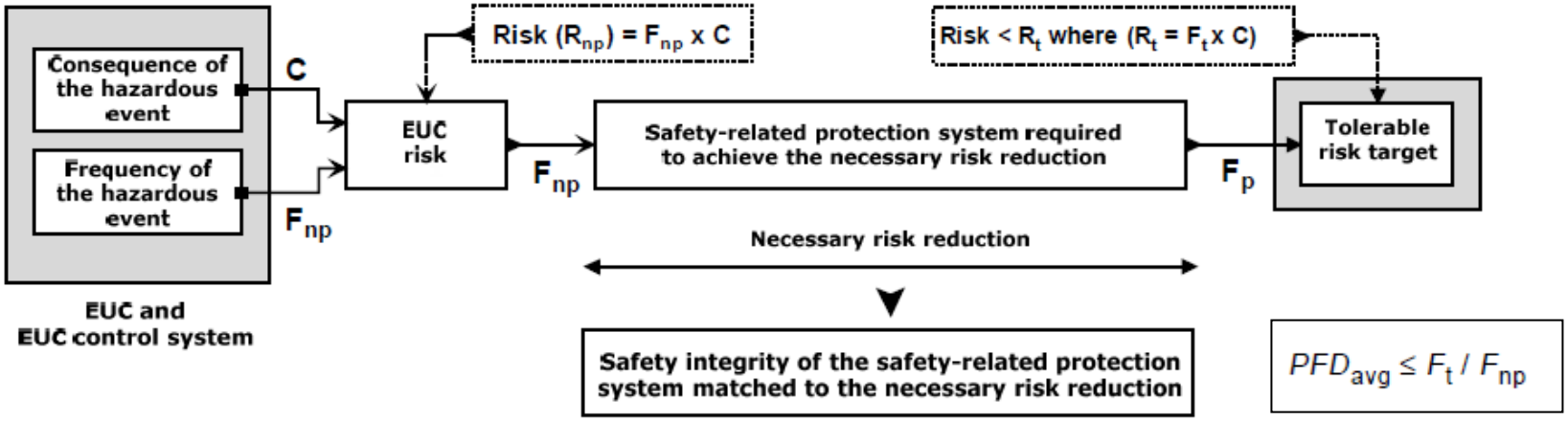
- *NOTE 4 For hardware safety integrity it is necessary to apply quantified reliability estimation techniques in order to assess whether the target safety integrity, as determined by the risk assessment, has been achieved, taking into account random hardware failures (see IEC 61508-2, 7.4.5).*

Safety Integrity Levels (IEC 61508) cont.

- Determination of the safety integrity of a safety function is non-trivial as it highly depends on expert knowledge in the application area.
- Various methods are informally presented in IEC to determine the safety integrity (and consequently also the SIL).
- Examples are: ALARP (as low as reasonable possible), and the quantitative method (IEC 61508 – part 5).

Safety Integrity Levels (IEC 61508) cont.

- Quantitative Risk Assessment Method



Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

F_{np} … demand rate demand rate on the safety-related protection system

F_p … risk frequency w protection

F_t … tolerable hazard frequency

Safety Integrity Levels (IEC 61508) cont.

Is the result of a risk assessment (IEC 61508 – part 5).

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 $< 10^{-5}$

Safety Integrity Levels (IEC 61508) cont.

- Once the SIL of a given safety function is determined, IEC 61508 (part 2, 3) defines particular requirements. IEC 61508 is product prescriptive, i.e., it requires that the end product implements specific features:

	Technique/Measure *	Ref.	SIL 1	SIL 2	SIL 3	SIL 4
	Architecture and design feature					
1	Fault detection	C.3.1	---	R	HR	HR
2	Error detecting codes	C.3.2	R	R	R	HR
3a	Failure assertion programming	C.3.3	R	R	R	HR
3b	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	C.3.4	---	R	R	----
3c	Diverse monitor techniques (with separation between the monitor computer and the monitored computer)	C.3.4	---	R	R	HR

IEC 61508 – part 7

Safety Integrity Levels (IEC 61508) cont.

- IEC 61508 part 7 gives an overview of techniques and measures, e.g. C.3.3 Failure assertion programming

C.3.3 Failure assertion programming

NOTE This technique/measure is referenced in Table A.17 of IEC 61508-2, and Tables A.2 and C.2 of IEC 61508-3.

Aim: To detect residual software design faults during execution of a program, in order to prevent safety critical failures of the system and to continue operation for high reliability.

Description: The assertion programming method follows the idea of checking a pre-condition (before a sequence of statements is executed, the initial conditions are checked for validity) and a post-condition (results are checked after the execution of a sequence of statements). If either the pre-condition or the post-condition is not fulfilled, the processing reports the error.

For example,

```
assert < pre-condition>;
    action 1;
      :
      .
    action x;
assert < post-condition>;
```

References:

Exploiting Traces in Program Analysis. A. Groce, R. Joshi. Lecture Notes in Computer Science vol 3920, Springer Berlin / Heidelberg, 2006, ISBN 978-3-540-33056-1

Software Development – A Rigorous Approach. C. B. Jones, Prentice-Hall, 1980

Automotive SIL (ASIL)

Automotive Safety Integrity Levels (ISO 26262)

- IEC 61508 determines the SIL levels by consideration of the consequence of the hazardous event and by the probability of occurrence of this event.
- The equivalent parameters in ISO 26262 are:
  - Severity:
    - estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation
  - Exposure (actually – the probability of exposure)
    - state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

Automotive Safety Integrity Levels (ISO 26262) cont.

- ISO 26262 defines in addition also a third parameter: the controllability.
- **Controllability:**
  - ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures
- E.g., in current series implementations of driver assistance systems, the driver is requested to be alert such that he/she can take over in case of an emergency. Typically the driver needs to get in contact with the steering wheel every few seconds. This increases and enforces the controllability.

Automotive Safety Integrity Levels (ISO 26262) cont.

- Classes of Severity:

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

- Classes of Probability of Exposure:

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

- Classes of Controllability:

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

Automotive Safety Integrity Levels (ISO 26262) cont.

- QM: Quality Management – there are no hazards associated with the given application

- ASIL A: lowest automotive safety integrity level, moderate additional requirements towards the development process (on top of QM), example sub-system: retractable hardtop for convertibles
- ASIL B: example sub-system: head & tail lights
- ASIL C: example sub-system: electric drivetrain
- ASIL D: highest automotive safety integrity level, rigorous development process requirements, example sub-system: EPS (electro-mechanical power steering)

Automotive Safety Integrity Levels (ISO 26262) cont.

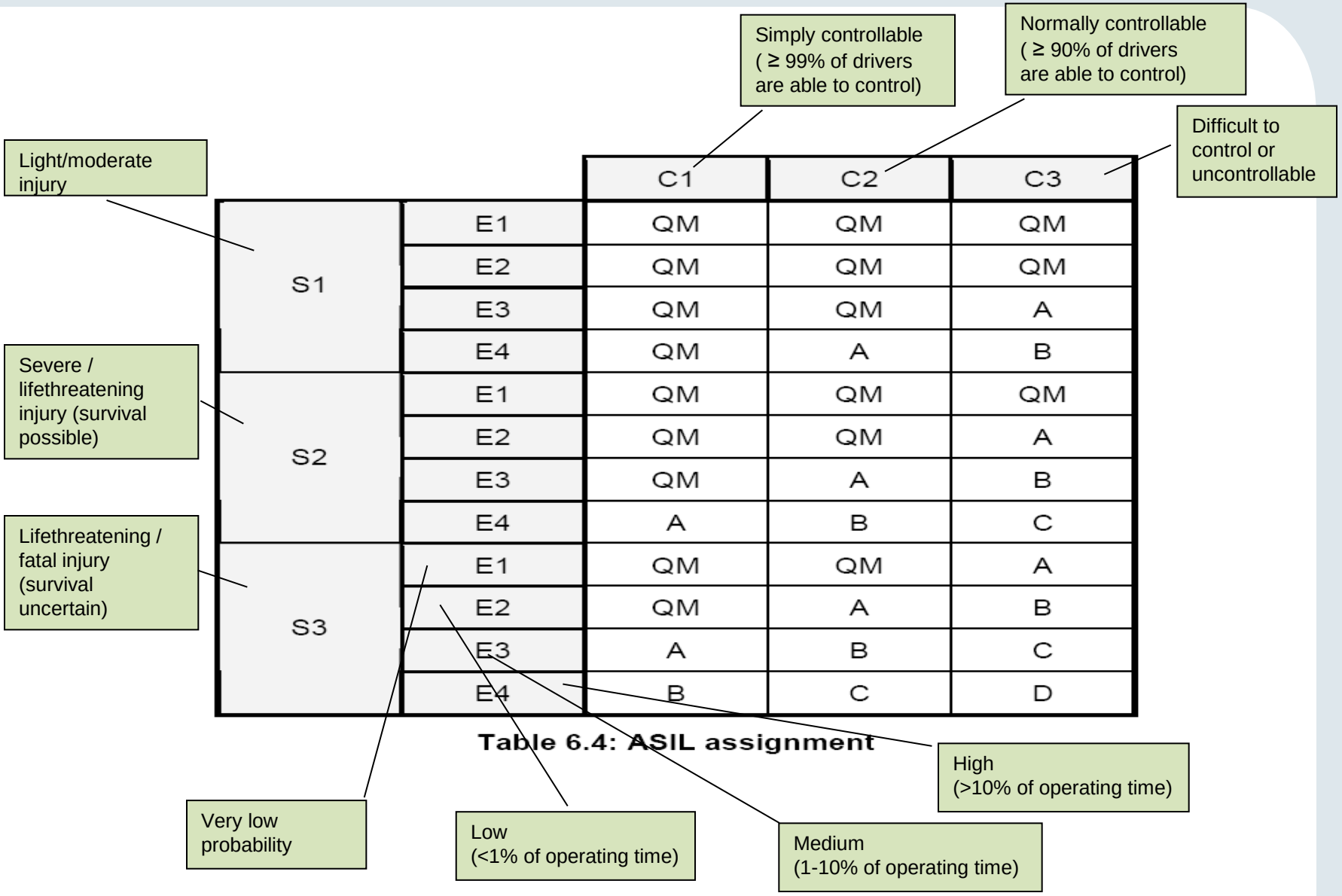
Table 4 — ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Determination of ASIL

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

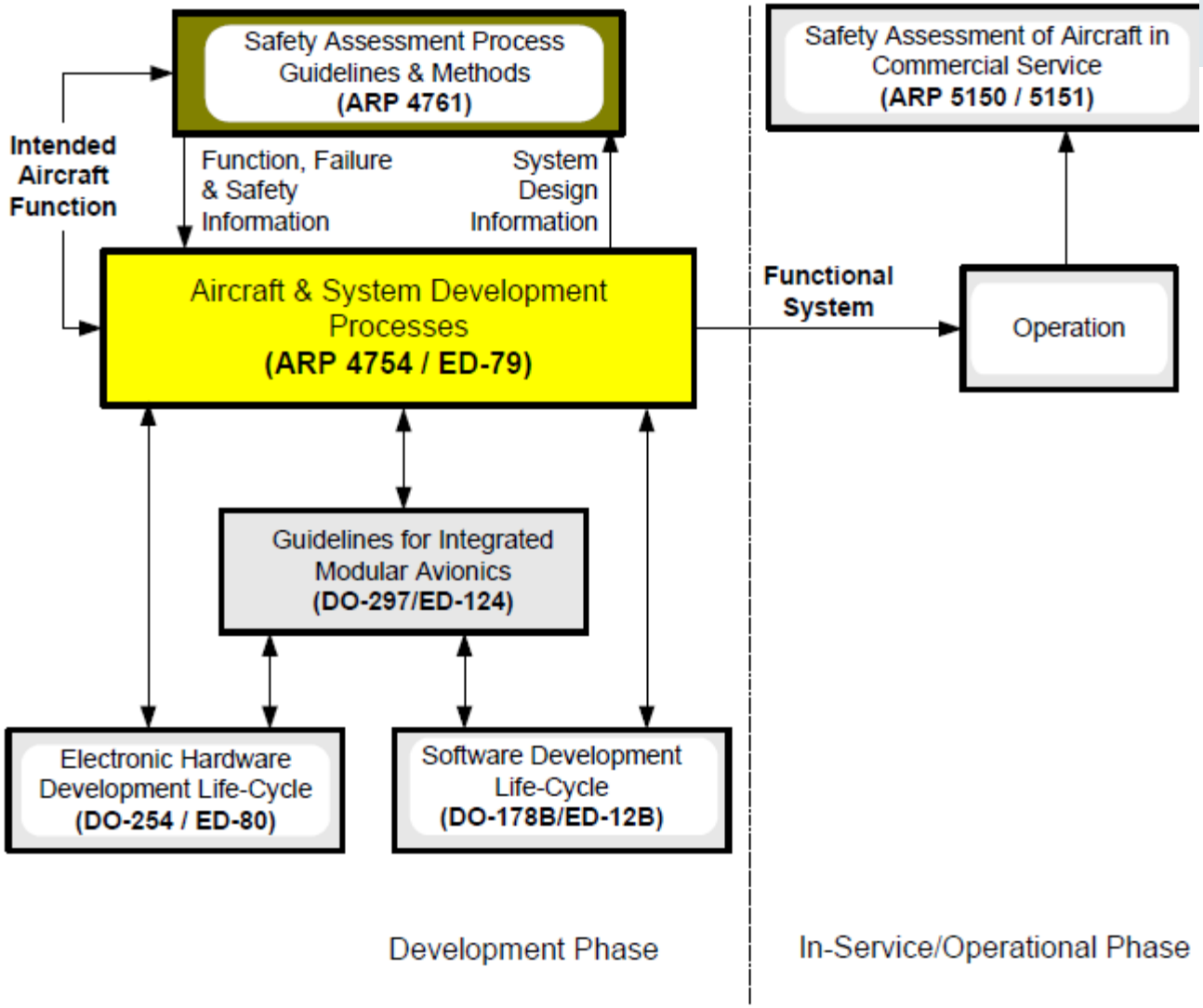
Table 6.4: ASIL assignment



		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Table 6.4: ASIL assignment

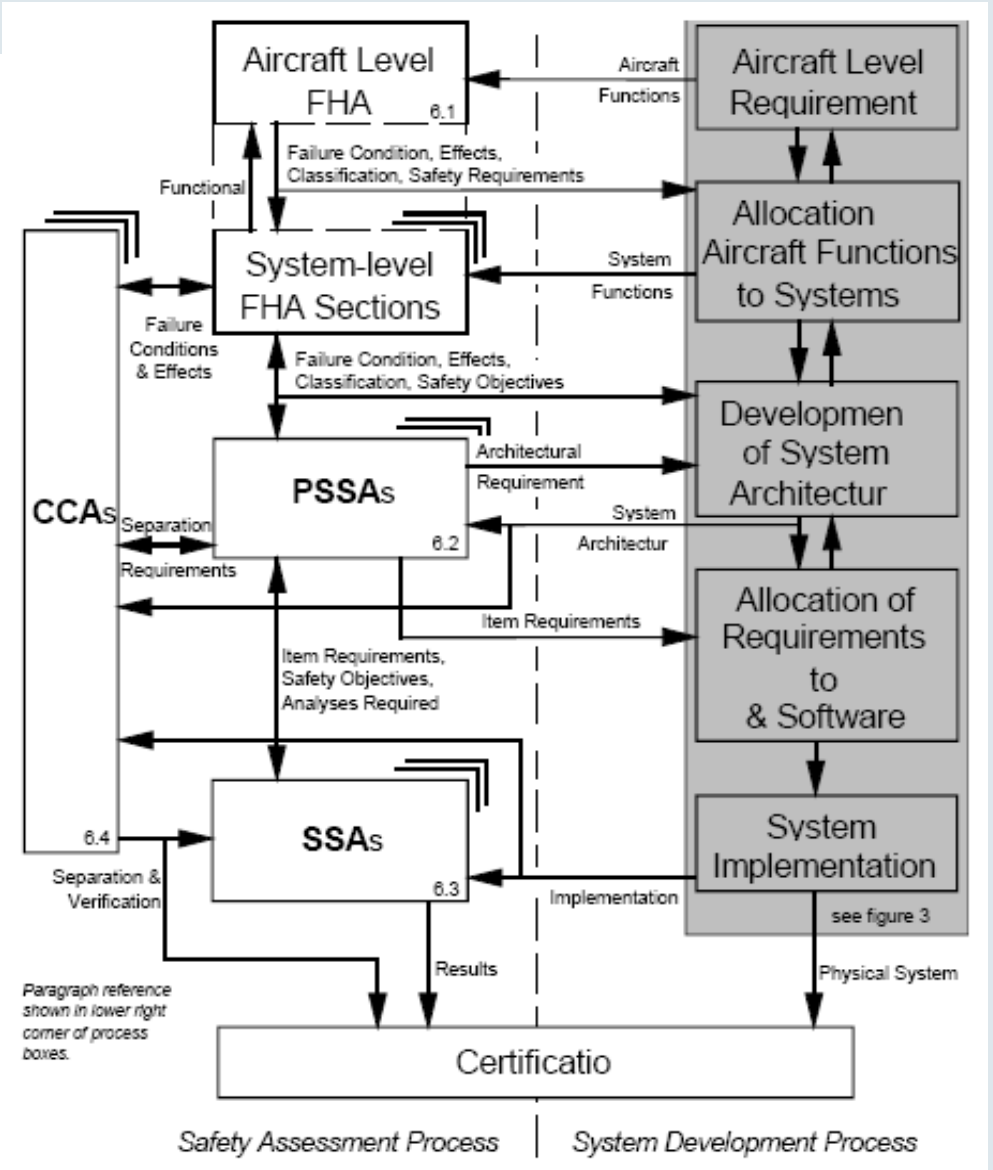
ARP 4754, 4761, DO 178, DO 254



SAE ARP 4754A

FIGURE 1 - GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES

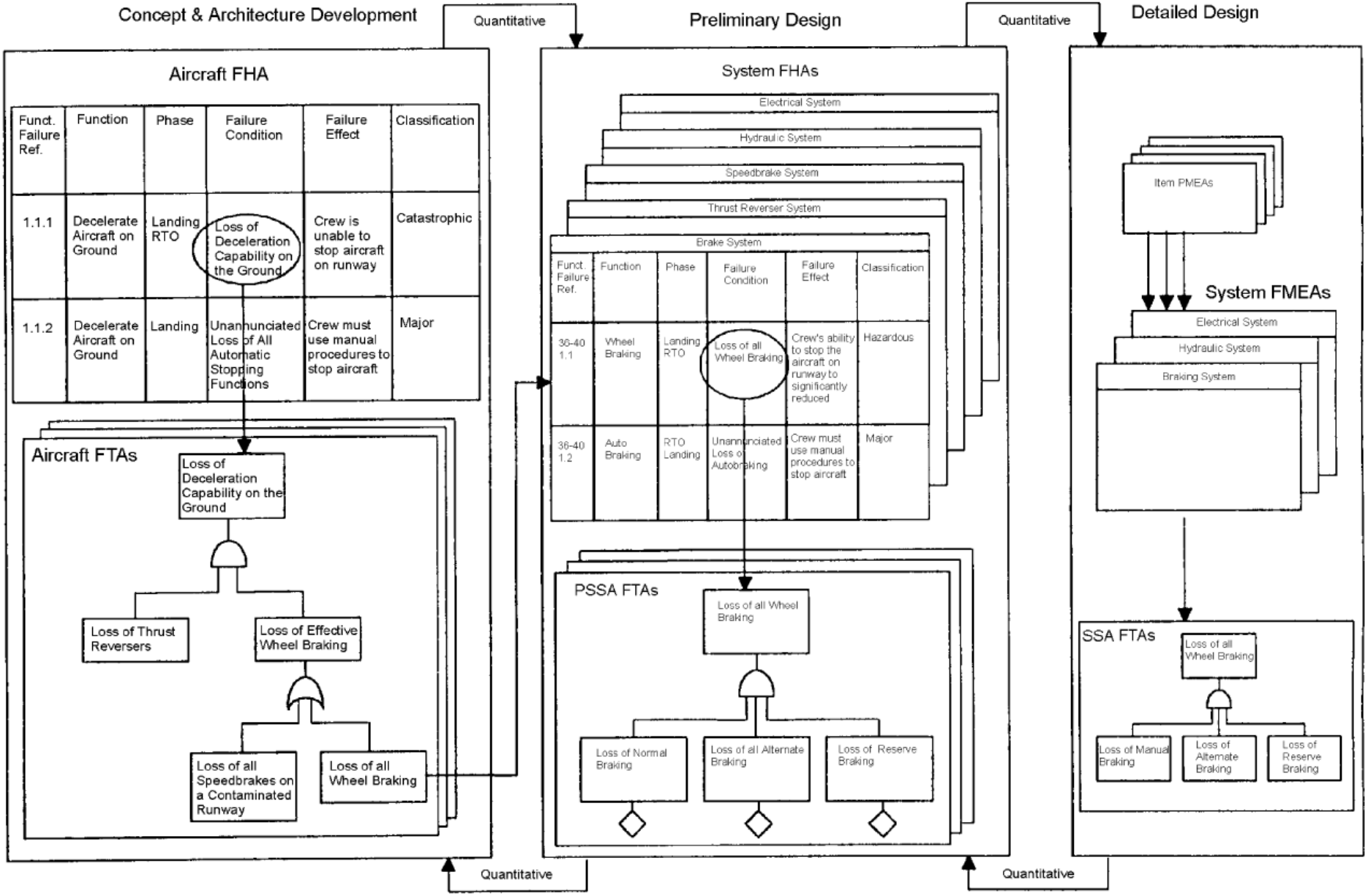
- Aircraft level functional requirements are allocated to aircraft systems
- Iterative analysis with Functional Hazard Assessment (FHA)
  - Determines severity of failures
- Development of System Architecture
  - Allocation, Redundancy, Partitioning, etc.
- Preliminary System Safety Assessment (PSSA) of design, iteratively (top-down)
  - Determines Safety Requirements and
  - Development Assurance Levels
- Allocation of requirements to hardware and software items
- HW/SW item development according to DO-254 and DO-178B, respectively
- *System Safety Assesments* (SSAs) analyze implementation (bottom-up)



SAE ARP 4754

Common Cause Analysis

- Common Cause Analysis (CCA) targets design errors that may invalidate subsystem *failure independence assumptions* required by the (P)SSA.
  - **Zonal Safety Analysis:**
    should examine each physical zone of the aircraft to ensure that equipment installation and potential physical interference with adjacent systems do not violate the independence requirements of the systems.
  - **Particular Risk Assessment**:
    should examine those common events or influences that are outside the system(s) concerned but which may violate independence requirements. These particular risks may also influence several zones at the same time, whereas zonal safety analysis is restricted to each specific zone.
  - **Common Mode Analysis:**
    provides evidence that the failures assumed to be independent are truly independent. The analysis also covers the effects of design, manufacturing, and maintenance errors and the effects of common component failures.



ARP 4761, p.18

Failure Mode Classification – Consequences, e.g., Aircraft

Minor: 10E-5 per flight hour or greater

no significant reduction of aeroplane safety, a slight reduction in the safety margin

Major: between 10E-5 and 10E-7

significant reduction in safety margins or functional capabilities, significant increase in crew workload or discomfort for occupants

Hazardous: between 10E-7 and 10E-9

large reduction in safety margins or functional capabilities, causes serious or fatal injury to a relatively small number of occupants

Catastrophic: less than 10E-9

these failure conditions would prevent the continued safe flight and landing of the aircraft

Design Assurance Levels (ARP, DO 178, DO 254)

- Design Assurance Levels are determined only by the effects on the aircraft:
  - DAL A: Catastrophic
  - DAL B: Hazardous failure condition
  - DAL C: Major
  - DAL D: Minor
  - DAL E: No Effect

- DO 178 and DO 254 are process prescriptive,
  - i.e., the DAL defines which processes need to be executed and how.
- DO 178 and DO 254 are not product prescriptive,
  - i.e., the DAL does not require specific functions in an end product

Assurance Cases / Safety Cases

Definitions

- *“An assurance case provides arguments to justify certain claims about a system, based on evidence concerning both the system and the environment in which it operates.” [Rushby]*
- A safety case is a special kind of assurance case in which the claims being argued concern safety properties.

Prescriptive Method vs. Performance-Oriented Method

- Prescriptive methods can be product prescriptive and/or process prescriptive.
  - We have discussed IEC 61508 and ISO 26262 as product prescriptive methods.
  - We have discussed DO 178b/c and DO 254 as project prescriptive methods.
- In performance-oriented methods, "*the certification authority specifies a threshold of acceptable performance and a means for assuring that the threshold has been met. [...] it is up to the assurer to decide how to accomplish that goal." [Leveson].*