Standards and Legislation

Namhoon Kim

Standards

- Two international standard applied in industries
  - IEC 61508
    - **Functional Safety**
  - ISO 26262
    - **Road vehicles -- Functional safety**

IEC 61508

- Title “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”
- A basic functional safety standard for all kinds of industry
- Covers the complete life cycle
  - Initiation, specification, design, development, and decommission

IEC 61508

- 16 phases life cycle
  - Phase 1-5 - analysis
  - Phase 6-13 - realization
  - Phase 14-16 - operation

- “Zero risk can never be reached”
- “Safety must be considered from the beginning”

Hazard and Risk Analysis

- Failure occurrence categories

Category	Definition	Failure per year
Frequent	Many times in system lifecycle	$> 10^{-3}$
Probable	Several times in system lifecycle	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	$< 10^{-7}$

Hazard and Risk Analysis

- Consequence categories

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

Hazard and Risk Analysis

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

Class I: Unacceptable in any circumstance

Class II: Tolerable only if risk reduction is impracticable

Class III: Tolerable if the cost of risk reduction would exceed the improvement

Class IV: Acceptable

Safety Integrity Level (SIL)

- A risk assessment effort yields a target SIL
- A target SIL is a requirement for the final system
- Part 2 and 3 of IEC 61508

SIL	**Low demand:** **Average probability of failure on demand**	**High demand:** **Probability of dangerous failure per hour**
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$ *
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

High demand: operate continuously or more than once per year

Low demand: operate intermittently and at most once a year

* 1 dangerous failure in 1140 years

Testing

- Software need to be unit tested or require MCDC c ode coverage criterion (depend on SIL)

- Unit testing
  - Testing method by individual units of source code
  - The smallest testable part of an application
  - An entire module, individual procedure, or class…
  - Limitations
    - Testing will not catch every error
    - It will not catch integration errors or system-level errors

MCDC code coverage criterion

- MCDC (modified condition/decision coverage) is a code coverage criterion
- Requires all conditions during testing
  1. Each entry and exit point is invoked
  2. Each decision tries every possible outcome
  3. Each condition in a decision takes on every possible outcome
  4. Each condition in a decision is shown to independently affect the outcome of the decision
- MCDC is used in avionics software guidance DO-178B/C and highly recommended for ASIL D in ISO 26262

ISO 26262

- Title “Road vehicles – Functional safety”
  - The first edition published on Nov. 2011
  - Apply to electrical and/or electric systems installed in “series production passenger cars” with a maximum gross weight of 3500 kg
  - Address possible hazards caused by the malfunctioning behavior of electronic and electrical systems

ISO 26262

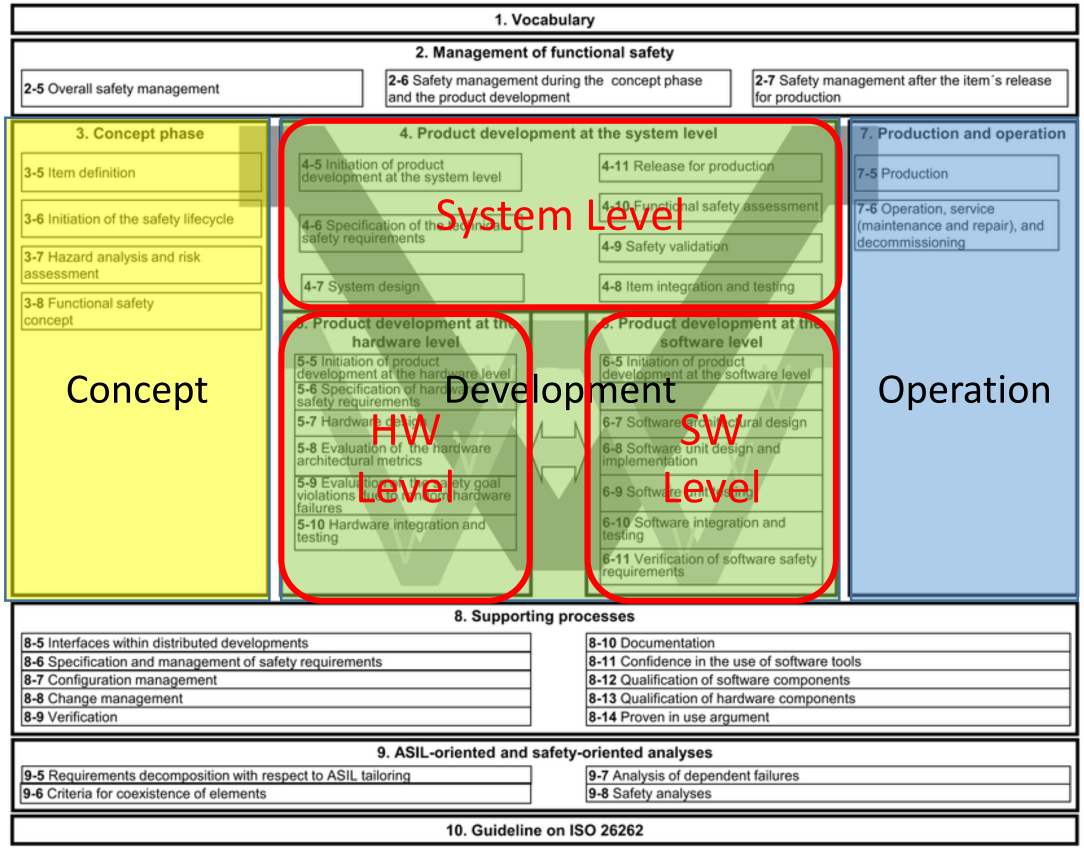
- Adapted from the previous, more generic safety standard IEC 61508
- Before ISO 26262, automotive industry uses the Motor Industry Software Reliability Association (MISRA) guidelines

ISO 26262 Contents

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development at the system level
5. Product development at the hardware level
6. Product development at the software level
7. Production and operation
8. Supporting processes
9. Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis
10. Guideline on ISO 26262

Overview of ISO 26262

Figure 1 — Overview of ISO 26262



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

6-6 Specification of software safety requirements

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

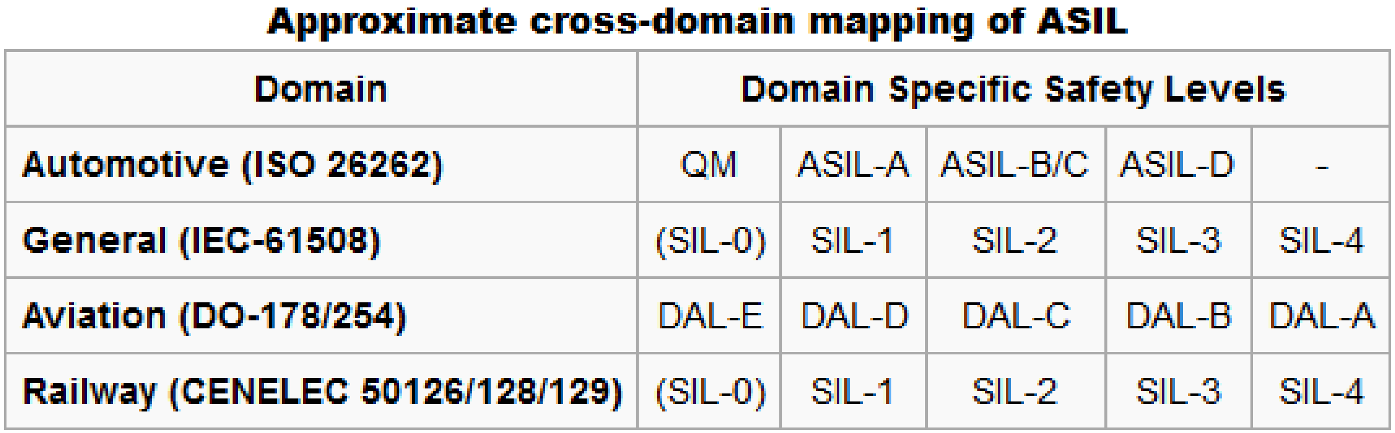
image credit: ISO 26262

Risk Classification

- Automotive Safety Integrity Level (ASIL)
  - Defined by the ISO 26262
  - Adaptation of the Safety Integrity Level (SIL) used in IEC 61508
  - Established by performing a risk analysis of a potential hazard
  - 4 ASILs and QM (Quality management)
    - QM: no hazards
    - ASIL A: the lowest integrity requirement
    - ASIL B
    - ASIL C
    - ASIL D: the highest integrity requirement

Hazard Analysis and Risk Assessment

- A hazard is assessed based on the relative impact a nd relative likelihood
- ASIL = Severity × (Exposure × Controllability)



Approximate cross-domain mapping of ASIL

Domain	Domain Specific Safety Levels				
Automotive (ISO 26262)	QM	ASIL-A	ASIL-B/C	ASIL-D	-
General (IEC-61508)	(SIL-0)	SIL-1	SIL-2	SIL-3	SIL-4
Aviation (DO-178/254)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
Railway (CENELEC 50126/128/129)	(SIL-0)	SIL-1	SIL-2	SIL-3	SIL-4

image credit: http://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level#Comparison_with_Other_Hazard_Level_Standards

ASIL Assessment

Severity	
S0	No injuries
S1	Light to moderate injuries
S2	Severe to life-threatening injuries
S3	Life-threatening to fatal injuries

Exposure	
E0	Incredibly unlikely
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

ASIL Assessment

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

Controllability: the relative likelihood that the driver can act to prevent the injury

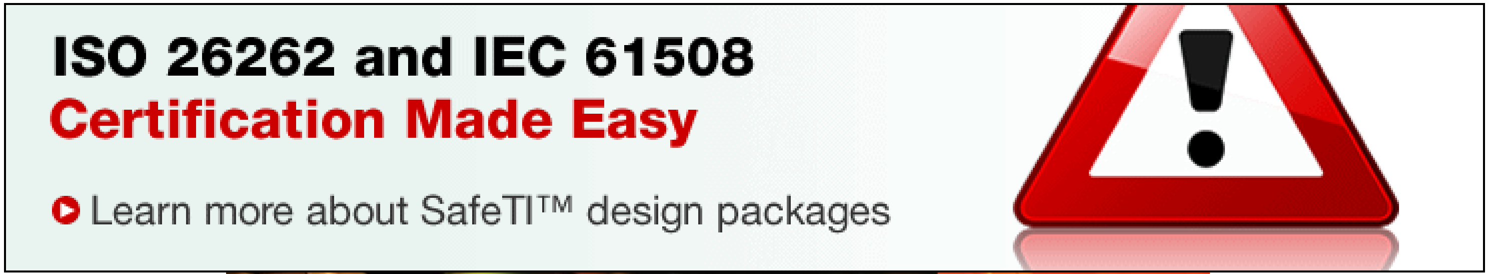
ASIL D = S3 x (E4 x C3)
ASIL C = S3 x (E4 x C2) or S3 x (E3 x C3) or S2 x (E4 x C3)
…
Each single reduction in any one classification, a single level reduction in the ASIL

Software Test

- Both unit level and system level testing are recommended
  - System level testing includes functional tests and structural coverage test
    - Statement coverage
    - Branch coverage
    - MCDC
- Part 6 addresses the recommendations for software testing and verification

HW and SW for Certification

- HW vendors provide specialized MCUs



ISO 26262 and IEC 61508

Certification Made Easy

Learn more about SafeTI™ design packages

Hercules™ TMS570 safety MCUs

Accelerate ISO26262 and IEC61508 development for motor control

Get started

HW and SW for Certification

- Software testing and verification tools
  - Static code analysis
  - Coverage tests
  - Condition tests
  - …. and etc.

Legislation

- The ECE-Homologations are international agreed
  - Unified technical regulations for vehicles and their comp onents
  - Three safety-critical systems are presented
    1. Vehicle stability control systems
    2. Steering systems
    3. Braking systems

Legislation

- The World Forum for Harmonization of Vehicle Regulations (WP29) of the United Nations Economic Commission for Europe (UN-ECE) is responsible for a technical regulation for ESC (Electronic stability control)

- ESC (Electronic stability control) is mandatory
  - From September 2011 in US and Canada
  - From November 2011 in the European Union

Legislation

- Steer-by-wire systems
  - An electronic connection is used instead of mechanical connection
  - The mechanical linkage between the driver and the road contact is dispensable
  - Steer-by-wire systems without mechanical backup are allowed
    - The UNECE approved the regulation ECER79 for road vehicles
  - Other regulations (e.g. self-centering) are still mandatory

Legislation

- Brake-by-wire systems
  - For new electric regenerative brakes in a HEV, electric and magnetic fields shall not affect the braking system
  - A static total braking force when ignition and start switch switched off has to be generated
  - The ECER13 is the regulation for brake systems