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

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Failure per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>Many times in system lifecycle</td>
<td>&gt; 10^{-3}</td>
</tr>
<tr>
<td>Probable</td>
<td>Several times in system lifecycle</td>
<td>10^{-3} to 10^{-4}</td>
</tr>
<tr>
<td>Occasional</td>
<td>Once in system lifetime</td>
<td>10^{-4} to 10^{-5}</td>
</tr>
<tr>
<td>Remote</td>
<td>Unlikely in system lifetime</td>
<td>10^{-5} to 10^{-6}</td>
</tr>
<tr>
<td>Improbable</td>
<td>Very unlikely to occur</td>
<td>10^{-6} to 10^{-7}</td>
</tr>
<tr>
<td>Incredible</td>
<td>Cannot believe that it could occur</td>
<td>&lt; 10^{-7}</td>
</tr>
</tbody>
</table>
Hazard and Risk Analysis

- Consequence categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Multiple loss of life</td>
</tr>
<tr>
<td>Critical</td>
<td>Loss of a single life</td>
</tr>
<tr>
<td>Marginal</td>
<td>Major injuries to one or more persons</td>
</tr>
<tr>
<td>Negligible</td>
<td>Minor injuries at worst</td>
</tr>
</tbody>
</table>
Hazard and Risk Analysis

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Frequent</td>
<td>Class I</td>
</tr>
<tr>
<td>Probable</td>
<td>Class I</td>
</tr>
<tr>
<td>Occasional</td>
<td>Class I</td>
</tr>
<tr>
<td>Remote</td>
<td>Class II</td>
</tr>
<tr>
<td>Improbable</td>
<td>Class III</td>
</tr>
<tr>
<td>Incredible</td>
<td>Class IV</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>SIL</th>
<th>Low demand: Average probability of failure on demand</th>
<th>High demand: Probability of dangerous failure per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
</tr>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>$\geq 10^{-9}$ to $&lt; 10^{-8}$</td>
</tr>
</tbody>
</table>

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 code 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
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 and relative likelihood

• ASIL = Severity × (Exposure × Controllability)

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

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

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0</td>
<td>No injuries</td>
</tr>
<tr>
<td>S1</td>
<td>Light to moderate injuries</td>
</tr>
<tr>
<td>S2</td>
<td>Severe to life-threatening injuries</td>
</tr>
<tr>
<td>S3</td>
<td>Life-threatening to fatal injuries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E0</td>
<td>Incredibly unlikely</td>
</tr>
<tr>
<td>E1</td>
<td>Very low probability</td>
</tr>
<tr>
<td>E2</td>
<td>Low probability</td>
</tr>
<tr>
<td>E3</td>
<td>Medium probability</td>
</tr>
<tr>
<td>E4</td>
<td>High probability</td>
</tr>
</tbody>
</table>
ASIL Assessment

<table>
<thead>
<tr>
<th>Controllability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0</td>
<td>Controllable in general</td>
</tr>
<tr>
<td>C1</td>
<td>Simply controllable</td>
</tr>
<tr>
<td>C2</td>
<td>Normally controllable</td>
</tr>
<tr>
<td>C3</td>
<td>Difficult to control or uncontrollable</td>
</tr>
</tbody>
</table>

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

ASIL D = S3 \times (E4 \times C3)

ASIL C = S3 \times (E4 \times C2) or S3 \times (E3 \times C3) or S2 \times (E4 \times 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

**MAKE THE SWITCH**

**Hercules™ TMS570 safety MCUs**

- Accelerate ISO26262 and IEC61508 development for motor control

- Get started

freescale.com/automotive
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 components
  • 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