ISO 26262
Update on development of the standard

Dr David Ward
Head of Functional Safety

January 2016

Agenda

- Why update ISO 26262?
- What is the process for updating the standard?
- Current status of Edition 2 draft and key changes
- Wider standardization activities
- Global adoption and the challenges we perceive
A frequently asked question …

- ISO 26262 was officially published on 15 November 2011
- Almost immediately on 16 November 2011 …

What’s going to be in Edition 2 of the standard?

Why update ISO 26262?

- Specific requirements to adapt ISO 26262 to
  - Extend scope to other types of vehicles (motorcycles, trucks, buses)
    - Motorcycles ISO/PAS 19695 and new Part 12 in Edition 2
  - Give additional guidance on semiconductor devices
    - ISO/PAS 19451 and new Part 11 in Edition 2
  - Address ADAS-related hazards caused by “normal operation” of the sensors
    - Currently will be proposed as a new work item for a separate PAS
- Other challenges include
  - Addressing highly distributed architectures
  - Moves towards autonomy
  - Cybersecurity
ISO 26262 for NMI: Update on development of the standard

Timescales for the revision (simplified)

- ISO timescales
  - Require at least 3 years from first publication before revision starts
  - Likely timescale for full Edition 2 is ~ 2018 based on a 36 month project
  - Specific needs will be addressed earlier in a PAS (Publicly Available Specification)

- Timescales are approximate and may be subject to change!

Key changes being considered for Edition 2

- Disclaimer: The CD is an internal committee document and many of the concepts are still subject to discussion and change!

- Key changes to be covered today include
  - New lifecycle
  - Part 1 – new definition of FTTI
  - Part 2 – link to cybersecurity
  - Product development at the hardware level
  - Product development at the software level
  - Semiconductors
  - Extensions to other types of vehicles
The structure of ISO 26262 Edition 2

Provisional information only and subject to change!

- Part 1 Vocabulary
- Part 2 Management of functional safety
- Part 3 Concept phase
- Part 4 Product development: system level
- Part 5 Product development: hardware level
- Part 6 Product development: software level
- Part 7 Production and operation
- Part 8 Supporting processes
- Part 9 ASIL-oriented and safety-oriented analyses
- Part 10 Guideline on ISO 26262 (informative)
- Part 11 Application of ISO 26262 to semiconductors
- Part 12 Adaption of ISO 26262 for motorcycles

Fault tolerant time interval

Provisional information only and subject to change!

1. Fault
2. Hazardous event develops
3. Transition to safe state
4. Safe state
5. Undetected fault
6. Diagnostic test interval
7. Fault detection
8. Fault reaction time
9. Failure time interval
10. Time

Fault tolerant time interval

Hazardous event

Normal operation

Hazardous event develops

Fault tolerant time interval

Safe state
Functional safety management

- Key new requirement to create and maintain effective communication channels between functional safety and other disciplines that are related to functional safety
  - Cybersecurity is the key activity in mind here but other disciplines can also be related

- New Annex showing example interfaces between functional safety and cybersecurity

Product development at the hardware level

- Evaluation of safety goal violations due to random hardware failures
  - Probabilistic metric (PMHF / Method 1)
    - Possibility to increase target values by up to one order of magnitude for items composed of multiple systems
  - New: residual risk assessment (“Method 3”)
    - Applied if the target values for Method 1 are not met
Product development at the software level

Software safety requirements

Attributes of requirements e.g. ASIL

Requirements defining functions

Technical safety requirements allocated to software

Safety mechanisms in software

Safety analysis to identify safety mechanisms to detect and react to software failures

Mechanisms against hardware failure

Mechanisms against system failure

Requirements defining properties

Independence

Freedom from interference

Fail operational

Safety analysis to confirm properties

Semiconductors

Common topics

• Intellectual property
• Base failure rate estimation
• Semiconductor dependent failures analysis
• Fault injection
• Production and operation
• Interfaces within distributed developments
• Confirmation measures and functional safety audit
• Clarification of hardware integration and testing

Specific semiconductor technologies and use cases

• Digital components and memories
• Analogue/mixed signal components
• Programmable logic devices
• Multi-core components
• Sensors and transducers
**ISO 26262 for NMI: Update on development of the standard**

**What types of vehicles are in the future scope of ISO 26262?**

*Provisional information only and subject to change!*

<table>
<thead>
<tr>
<th>Class of vehicle</th>
<th>In scope?</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1/L2</td>
<td>Excluded</td>
<td></td>
</tr>
<tr>
<td>L3/L4/L5</td>
<td>In scope</td>
<td>PAS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integration into Edition 2</td>
</tr>
<tr>
<td>L6/L7</td>
<td>Not defined</td>
<td></td>
</tr>
<tr>
<td>M1</td>
<td>In scope</td>
<td>Edition 1</td>
</tr>
<tr>
<td>M2/M3</td>
<td>In scope</td>
<td>Integration into Edition 2</td>
</tr>
<tr>
<td>N1/N2/N3</td>
<td>In scope</td>
<td>Integration into Edition 2</td>
</tr>
<tr>
<td>O1/O2/O3</td>
<td>In scope</td>
<td>Integration into Edition 2</td>
</tr>
<tr>
<td>Other categories</td>
<td>Not defined</td>
<td></td>
</tr>
</tbody>
</table>

**Motorcycles**

*Provisional information only and subject to change!*

- Part 12 contains requirements for
  - Functional safety management (concept phase and product development)
    - Maximum I2 independence
  - Hazard analysis and risk assessment
    - Use of MSILs
    - Example tables
- Chapters from PAS on vehicle integration and testing and safety validation appear not to be included in Part 12
Trucks and buses

Provisional information only and subject to change!

- Unlike motorcycles, truck and bus requirements are integrated into the main Parts of the standard e.g.
  - Some specific requirements for hazard analysis and risk assessment
    - Management of variants in performing the analysis
    - Integration of truck and bus examples in the tables of Annex B
  - New supporting processes for
    - Development of a base vehicle for an application out of scope of ISO 26262
    - Integration of safety elements developed out of scope of ISO 26262

Link to other activities

- Related standardization activities include
  - SAE J2980™ (functional safety guidebook)
  - SAE J3061™ (cybersecurity guidebook)
SAE J2980™ – Considerations for ISO 26262 ASIL hazard classification

- Original objectives
  - Develop a global harmonized approach to determining ISO 26262 ASIL classifications for vehicle level hazards
  - Develop global harmonized ASIL classifications for vehicle level hazards
  - Develop global standard hazard metrics for harmonized ASIL classified hazards
- Membership started with US OEMs but has grown to include Europe and Japan
- Now mostly concerned with guidance on a consistent process
  - Found very quickly it was not possible to agree on "global harmonized ASIL classifications"

SAE J3061™ Recommended Practice – Cybersecurity Guidebook

- Tailors a cybersecurity process framework from the ISO 26262 process framework
  - Cybersecurity and functional safety share parallel processes e.g.
    - Threat analysis and risk assessment vs hazard analysis
    - Attack tree analysis vs fault tree analysis
  - Security countermeasures should be consistent with safety measures and safety mechanisms
  - The cybersecurity and functional safety teams need to interact
What are the challenges we perceive?

- Differing approaches to interpreting and applying the standard still exist globally
- Discussions on cybersecurity highlight the narrow focus of ISO 26262 compared to system safety and wider issues of system dependability
- Some issues associated with autonomous vehicles have been acknowledged but it is unlikely the standard will fully address autonomy in the timescales being discussed for their deployment
- Vision for 2025 (personal opinion!)
  - Edition 3 of ISO 26262?
  - Majority of cars on the road will have at least one SAE Level 1 (or above) application
  - Level 3+ systems will become more prevalent along with new entrants / new modes

Conclusions

- ISO 26262 is already well established as the "state of the art" in development of automotive safety-related systems
- Still some variance in actual practice
- Edition 2 is under preparation addressing some of the issues in application of Edition 1 and future trends
- Further work remains to be done, particularly addressing wider issues for example
  - System assurance
  - Driverless vehicles