EXPECTATIONS & REQUIREMENTS FROM A TIER 1 TO IT’S SUPPLIERS

C. GEBAUER

BOSCH CENTER OF COMPETENCE “FUNCTIONAL SAFETY”
ROBERT BOSCH GMBH

IQPC FIRST INTERNATIONAL CONFERENCE SEMICONDUCTORS ISO 26262, MÜNCHEN
Expectations & Requirements of a Tier 1

**Agenda**

- General Topics
- Practical Topics
- Summary
General Topics
Expectations & Requirements of a Tier 1

What does the customer want (regarding safety)?

- Safety expectations to the suppliers: The product is safe
  - Safe = Absence of unreasonable safety risk as well as of safety risks that can be avoided through measures, which are possible and reasonable according to the state of the art.
    - Compliance with the state of the art is a legal requirement
  - Safety culture is an important prerequisite in order to be able to develop, produce and deliver safe products
Expectations & Requirements of a Tier 1

Compliance with the state of the art?

- The compliance with the state of the art requires the **implementation of measures** for avoidance of hazard and damage that are **constructively possible** and seem to be **adequate** and **sufficient** for preventing damage **according** to the sound knowledge of recognized **experts**.

- A **standard** offers a **reference**. However the **state of the art** can have **evolved beyond** the requirements of a standard.
  - I.e. if you **know** it better, do it better
  - Compliance to **ISO 26262** is a **minimum** requirement
  - **ISO 26262** does **not** cover all safety aspects of a product

- It is the **responsibility of the supplier** to ensure the **compliance** of his product with the **state of the art** and to provide adequate **evidence**
ISO 26262 in a Nutshell

Safety Goal (ASIL X)

• Adequate development & production activities
  • (HW & SW safety mechanisms to prevent the safety goal violation)

Focus: Prevent systematic faults

• Safety mechanisms to prevent the safety goal violation
  • (Dedicated measures to ensure low HW failure rate)

Focus: Control random HW faults

Systematic faults typically have a larger impact on safety than random HW faults

Requirements concerning the avoidance of safety goal violations due to systematic faults in hardware and software (ASIL X)

Requirements concerning the avoidance of safety goal violations due to random hardware faults (ASIL X)

HW Metrics
SPFM, LFM, PMHF/EEC

Realization

Requirement on vehicle level

Requirements on lower levels
For a supplier of a HW element compliance is **not limited to** only **part 5**

- **Other parts** need to be **complied with**, too
  - Part 2 Management of functional safety
  - Part 7 Production and operation
  - Part 8 Supporting processes
  - Part 9 Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
  - Depending on the product
    - Part 4 Product development at the system level
    - Part 6 Product development at the software level

- **Part 10** and **part 11** offer very **useful** guidelines **but** they do **not** address all issues
Expectations & Requirements of a Tier 1
Compliance with ISO 26262

- The **requirements** of ISO 26262 need to be **tailored** accordingly, e.g.

- **7.4.2.1** The organization shall appoint persons with the responsibility and the corresponding authority, in accordance with 5.4.2.9, to achieve and maintain the functional safety of the item during production, operation, service and decommissioning.

  → Supplier is **responsible** for the **aspects** of his **product**, not the whole item

- **Confirmation reviews**, functional safety **audits** and functional safety **assessments** of the supplier are executed by the supplier **within** the **scope** of his **product**, not the whole item.
Practical Topics
Expectations & Requirements of a Tier 1

Disjoint safety requirements for random HW faults

- The **failure modes** on product (e.g. sensor) level shall be **disjoint**

- Failure modes are disjoint if every **fault** of each **HW element of the product** can **contribute** to exactly **one failure mode on product level**
  - Ensure that **failure rates** of an HW element are only **counted once**

- Example: Sensor ABC failure modes
  
<table>
<thead>
<tr>
<th>Disjoint set</th>
<th>Overlapping set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only output A incorrect</td>
<td>Output A incorrect</td>
</tr>
<tr>
<td>Only output B incorrect</td>
<td>Output B incorrect</td>
</tr>
<tr>
<td>Only output C incorrect</td>
<td>Output C incorrect</td>
</tr>
<tr>
<td>One or more outputs incorrect</td>
<td></td>
</tr>
</tbody>
</table>

```text
Sensor ABC
Output A, B, C
```

```
Transducer A → Processing Logic A

Transducer B → Processing Logic B

Transducer C → Processing Logic C
```

```
Microcontroller
```

Output A, B, C
Base Failure Rate

Part 11 offers several procedures to calculate the base failure rates with very different results, e.g. IEC TR 62380 temperature derating

\[ \lambda_{die} \sim \frac{1}{\tau_{on} + \tau_{off}} \]

where

\[ \tau_{off} \] time ratio of being in storage or dormant

\[ \tau_{on} \] total working time ratio

\[ \tau_{off} + \tau_{on} = 1 \]

- Calculation possible with \( \tau_{off} \neq 0 \) \( \rightarrow \lambda_{calendar\ hours} \)
- Calculation possible with \( \tau_{off} = 0 \) \( \rightarrow \lambda_{operating\ hours} \)

\[ \lambda_{operating\ hours}/\lambda_{calendar\ hours} = 1 + \frac{\tau_{off}}{\tau_{on}} \]

\( \rightarrow \) factors of 8 to 17 have been seen in applied failure rate calculations
Expectations & Requirements of a Tier 1
Base Failure Rate

- Bosch typically prefers the more conservative calculation, e.g. IEC TR 62380:
  \[ \tau_{\text{off}} = 0 \]

- Typical used sources for base failure rate calculations
  - SN 29500
  - ISO TR 62380

- General recommendation: Define the to be used base failure rate calculation procedure at the beginning of the project
Expectations & Requirements of a Tier 1
HW safety requirements implemented by SW

Supplier task (SW provided by the supplier)

- Development compliant with ISO 26262-6
- Determination of the DC
- Verification of the DC
- Dependent failure analysis between HW and SW elements

Supplier task (SW specified by the supplier)

- SW specification compliant with ISO 26262-6
- Determination of the DC
- Verification of the DC
- Dependent failure analysis between HW and SW elements
Summary
Expectations & Requirements of a Tier 1

Expectations & requirements to the supplier

- **A safe product, compliant with the state of the art**
  - The state of the art might have evolved beyond requirements of ISO 26262 (if you know it better, do it better)
  - Functional safety does not necessarily address all relevant safety aspects (e.g., toxicity, flammability)

- **Compliance with ISO 26262**
  - Compliance with all relevant normative parts (2, 4, 5, 6, 7, 8, 9) with adequate tailoring
  - Part 11 provides very useful guidelines but does not address everything

- **Disjoint failure modes on product level** in case of quantitative safety analysis

- **Conservative base failure rate** estimation, typically according to SN 29500 or IEC TR 62380

- In case of **SW safety mechanisms**
  - Estimation & Verification of the DC
  - Dependent Failure Analysis between HW & SW elements
Expectations & Requirements of a Tier 1

Questions?