ISO 26262 Hardware Faults and Metrics

Carsten Gebauer, Robert Bosch GmbH, Corporate Research and Advance Engineering

Content

- Short introduction into ISO 26262
- Hardware fault classes of ISO 26262
- Most common misunderstandings
- Metrics concerning random HW faults

ISO 26262 – what is it?

- Standard on „**Functional Safety**“ for road vehicles
- Valid for all systems with eletrical/electronical components („**E/E systems**“)
- The „**Final Draft International Standard (ISO/FDIS)**“ published in April 2011, is currently in voting phase; last international vote by the end of June
- **The publication of the ISO 26262 is expected mid of 2011**


FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/FDIS
26262-2

Road vehicles — Functional safety —

Part 2:
Management of functional safety

Functional Safety - ISO 26262

- Based on the generic standard for Functional Safety **IEC 61508** the ISO working group TC22/SC3/WG16 elaborates an **automobile-specific adaptation ISO 26262**. Release expected by 08/2011.

- ISO 26262 will include requirements for:
  - **Development processes** and **organization**
  - **Technical requirements** for systems, HW and SW.

- The complete **product life cycle** will be addressed, e.g. system-description, hazard analysis, system development, HW- and SW-development, production, field, scrapping.

BOSCH

HW fault classes of ISO 26262

- Total failure rate: $\lambda_{total} = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}$

  $= \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF,DP} + \lambda_{MPF,L} + \lambda_{S}$

  with

  λ_{SPF} = **S**ingle-**P**oint **F**aults

  λ_{RF} = **R**esidual **F**aults

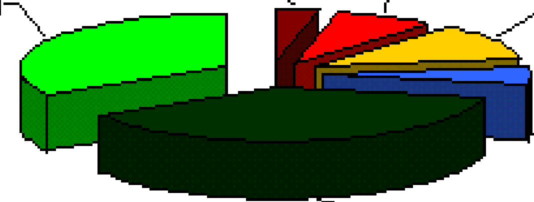
  λ_{S} = **S**afe **F**aults

  λ_{MPF} = **M**ultiple-**P**oint **F**aults

  $\lambda_{MPF,DP}$ = Detected / perceived MPFs

  $\lambda_{MPF,L}$ = Latent MPFs

  $\lambda_{MPF} = \lambda_{MPF,DP} + \lambda_{MPF,L}$



ISO 26262 HW fault class description

- A fault that has the potential to **violate** a **safety goal**, i.e. can lead to a safety critical malfunction, is classified (dependent on the presence of safety mechanisms) either as
  - a **S**ingle-**P**oint **F**ault (**SPF**) or
  - a **R**esidual **F**ault (**RF**)

- A fault that has the potential to **violate** a **safety goal** only in combination with a **second** independent fault is classified as
  - **dual-point** fault

- If a **dual-point** fault is **not detected** within a prescribed time interval it is classified as
  - **latent** fault (**M**ultiple-**P**oint **F**ault, **L**atent = **MPF, L**)

BOSCH

Examples of HW faults

- Single-point fault (**SPF**)
  - Open of a resistor which can lead to a **violation** of a **safety goal**. The resistor itself is **not supervised** at all

- Residual fault (**RF**)
  - For a memory which is checked via a **parity** bit: A fault resulting in an **even number** of erroneous bits which is **not detected** by the parity monitoring and which can lead to a **violation** of a **safety goal**

Examples of HW faults

- Latent (dual-point) faults (**MPF, L**)
  - For a memory which is checked via an **Error Correction Code (ECC)**:
    - A **single bit** fault which is **corrected** but **not signalled** and which has the potential to **violate** a **safety goal** if the **ECC** correction **fails**
    - A fault which renders the **ECC ineffective** and is **not detected** by the startup test

Most common misunderstandings

➔ The ISO 26262 definitions of fault classes are **not** always **intuitive**

Single-point fault (ISO 26262) ≠ **Single** fault

Latent fault (ISO 26262) ≠ **Latent** fault (common understanding)

Most common misunderstandings

STOP

- Within the ISO 26262 a **multiple-point** fault analysis is required. However

  - in general the analysis is limited to **dual-point** fault scenarios. Fault scenarios with **three or more** independent faults can in be considered as **safe**, unless they are shown to be relevant.

  - it is **not** requested to investigate **all** possible dual-point fault **scenarios** but those that **derive** from the **safety concept** (e.g. simultaneous fail of the main function and its monitoring)

BOSCH

Requirements concerning random HW faults

- The ISO 26262 has explicit requirements concerning **random HW faults** addressing the necessary **reduction** of
  - single-point faults (**SPF**)
  - residual faults (**RF**)
  - latent (dual-point) faults (**MPF,L**)

- The requirements are **expressed** as **target values** in form of the
  - **S**ingle-**P**oint **F**ault **M**etric (**SPFM**)
  - **L**atent (Dual-Point) **F**ault **M**etric (**LFM**)
  - **P**robabilistic **M**etric for random **H**ardware **F**ailures (**PMHF**) or evaluation of **E**ach **C**ause of **S**afety **G**oal **V**iolation (**ECSGV**)

Relative metrics

Absolute metrics

BOSCH

Relative HW metrics and target values

$$\mathrm{SPFM} = 1 - \frac{\sum_{\mathrm{SR,HW}} (\lambda_{\mathrm{SPF}} + \lambda_{\mathrm{RF}})}{\sum_{\mathrm{SR,HW}} \lambda}$$

Table 4 — Possible source for the derivation of the target "single-point fault metric" value

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

$$\mathrm{LFM} = 1 - \frac{\sum_{\mathrm{SR,HW}} (\lambda_{\mathrm{MPF,latent}})}{\sum_{\mathrm{SR,HW}} (\lambda - \lambda_{\mathrm{SPF}} - \lambda_{\mathrm{RF}})}$$

Table 5 — Possible source for the derivation of the target "latent-fault metric" value

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

- Sum over all **S**afety **R**elated **HW** elements of the **item**
- **Target** values can be derived from
  - values calculated for **similar** well-trusted **designs**, or
  - **tables** 4 and 5

Absolute HW metrics and target values

- **First option**: Evaluation of Probabilistic Metric for random Hardware Failures (**PMHF**)
  - On **item level**: Probability per hour of a potential violation of the safety goal

Table 6 — Possible source for the derivation of the random hardware failure target values

ASIL	Random hardware failure target values
D	$<10^{-8}\ h^{-1}$
C	$<10^{-7}\ h^{-1}$
B	$<10^{-7}\ h^{-1}$

NOTE The quantitative target values described in this table can be tailored as specified in 4.1 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).

- **Target** values can be derived from
  - values calculated for **similar** well-trusted **designs**, or
  - **table** 6, or
  - **field** experience

Absolute HW metrics and target values

- **Second option**: Evaluation of each cause of safety goal violation (**ECSGV**)
  - On **hardware part level**
  - Regarding **residual** and **single-point faults** (effective requirements)
    - ASIL **D**: $\lambda_{RF} + \lambda_{SPF} \leq \boldsymbol{\lambda}_{\mathbf{FRC\ 1}}$
    - ASIL **C**: $\lambda_{RF} + \lambda_{SPF} \leq \lambda_{FRC\ 1}$ *** 10**
    - ASIL **B**: $\lambda_{RF} + \lambda_{SPF} \leq \lambda_{FRC\ 1}$ *** 10** (recommended)

with $\boldsymbol{\lambda}_{\mathbf{FRC\ 1}}$ = ASIL D item target / n
and n = 100 if no rational for a smaller number is provided

Absolute HW metrics and target values

- **Second option**: Evaluation of each cause of safety goal violation (**ECSGV**) (continued)
  - Regarding **latent** (dual-point) **faults**
    - **either** they can be regarded as **not plausible**, which they are **if** for
      - ASIL **D**: **Both** involved HW parts have a **LFM ≥ 90 %**
      - ASIL **C**: **Both** involved HW parts have a **LFM ≥ 80 %**
    - **or** each **part** fulfills by **itself** following requirement

Table 9 — Targets of failure rate class and coverage of hardware part regarding dual-point faults

ASIL of safety goal	Diagnostic coverage with respect to latent faults		
	>= 99 %	>= 90 %	<90 %
D	Failure rate class 4	Failure rate class 3	Failure rate class 2
C	Failure rate class 5	Failure rate class 4	Failure rate class 3

where HW part ϵ failure rate class n if $\lambda_{\text{HW part}} \leq \lambda_{\text{FRC 1}} * 10^{(n-1)}$

BOSCH

Requirements concerning random HW faults

➔ The metrics provide a way to **evaluate** the **design**

- They are **model calculations** based on expert judgement and engineering practises (e.g. using an equal distribution for unkown probability distributions)

- They are **not** a **realistic forcast** of the to be expected **incidents**