Hardware Safety Metrics for ISO 26262 Compliance

sergio.marchese@onespin.com

Automotive Safety and ISO 26262

DVClub Europe Meeting – November 2018

making electronics reliable

Introduction to Functional Safety

The objective of functional safety:

Freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly

Functional Safety Risks	Risk drivers	Risk management through functional safety standards
• Systematic Failures ○ Design faults ○ Tool faults • Random Failures ○ Permanent faults ○ Transient faults	• Continuous increase in flow and tool complexity • Continuous increase in functionality • Increasing density of the design process node • Decreasing energy levels	• Minimize systematic failures • Safeguard against random failures

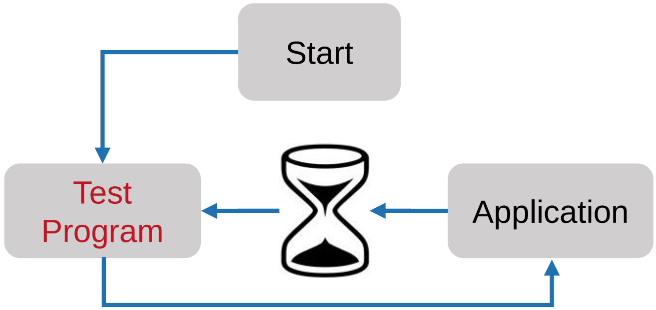
Safety Mechanisms (SMs)

Prevent faults from leading to failures – Detect faults, control failures

Random failures are caused by permanent or transient random hardware faults

- Examples of faults: single event latch-up (P); single event upset (T)

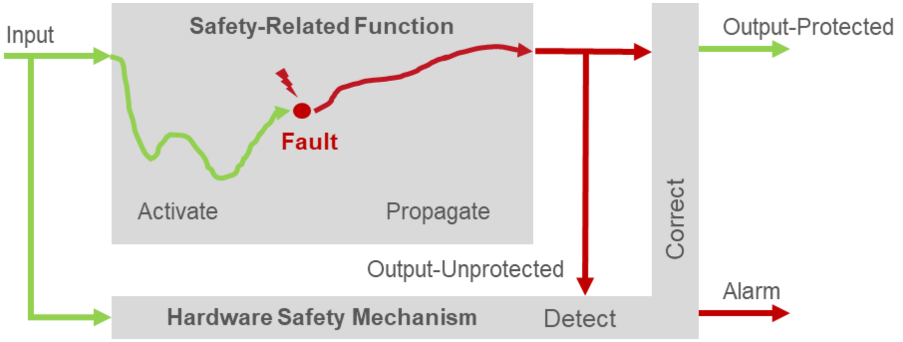
Software Safety Mechanism



Note

- **SM must correct output if alarm (optional) is not present or inactive**

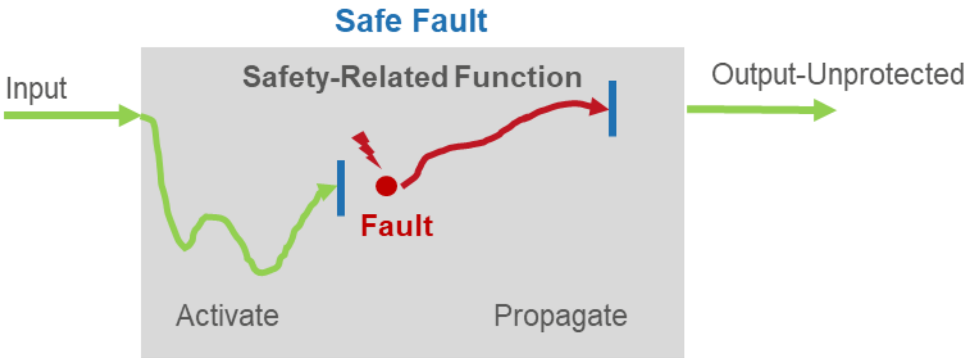
Hardware Safety Mechanism



Alarm
- Inactive
- Active

Output (Alarm Inactive)
- Correct
- Wrong

Safe Faults
Faults that cannot cause failures

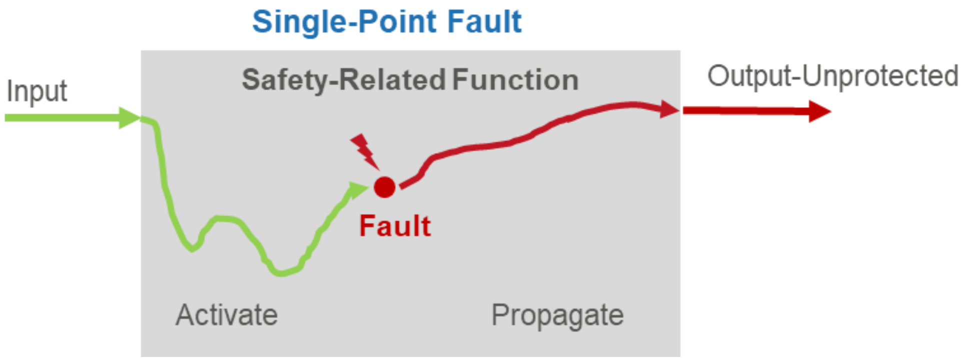


Note

- **Example: stuck-at 0 fault on net tied low does not change functionality**
- **Hardware often has many safe faults**

Single-Point and Residual Faults

Both may cause failures



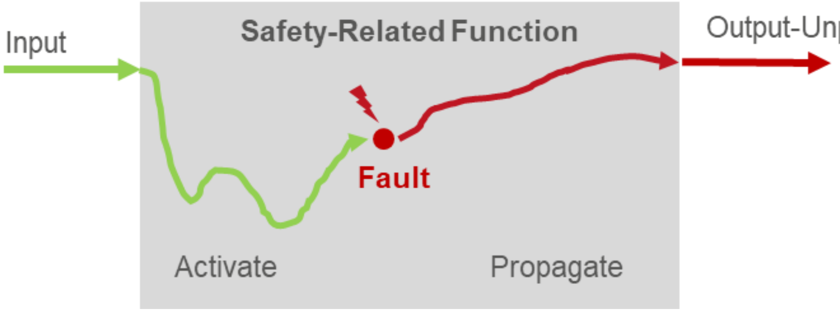
Note

- **Single-point faults compromise unprotected safety-related functions**

Single-Point and Residual Faults

Both may cause failures

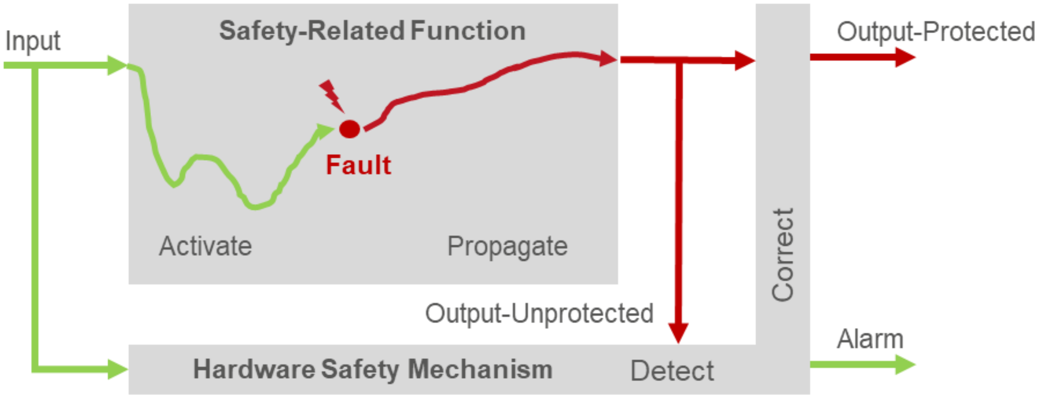
Single-Point Fault



Note

- **Single-point faults compromise unprotected safety-related functions**

Residual Fault

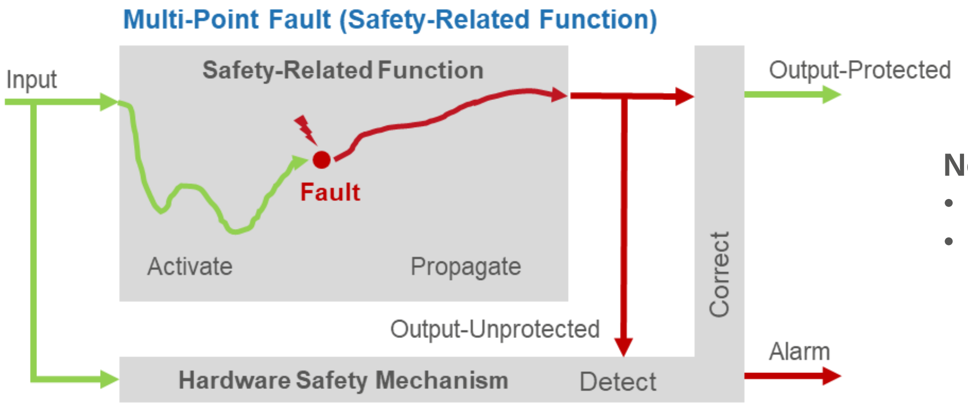


Note

- **Residual faults compromise protected safety-related functions**

Multi-Point Faults

Two or more multi-points faults (together) may cause failures



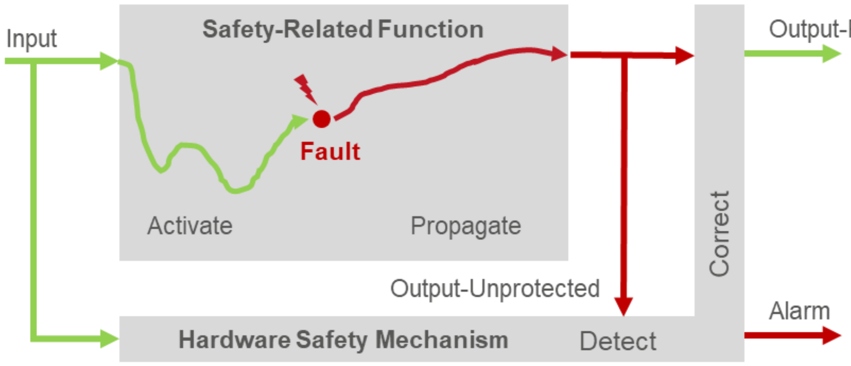
Note

- **Does not cause failures (on its own)**
- **Fault detected/corrected by safety mechanism**

Multi-Point Faults

Two or more multi-points faults (together) may cause failures

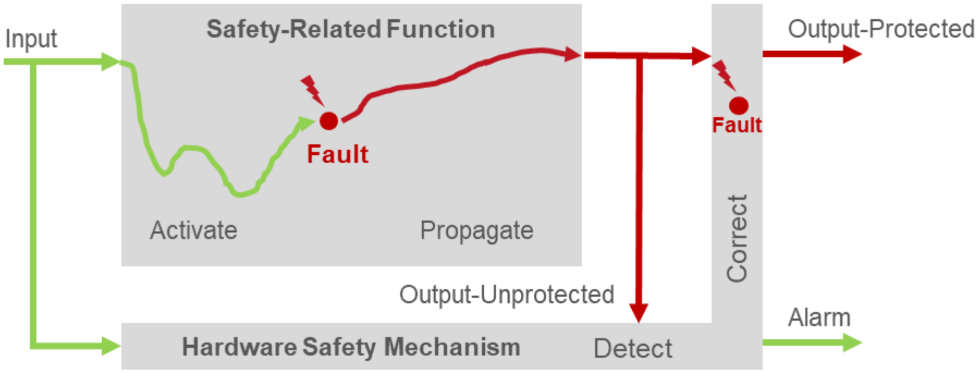
Multi-Point Fault (Safety-Related Function)



Note

- **Does not cause failures (on its own)**
- **Fault detected/corrected by safety mechanism**

Multi-Point Failure

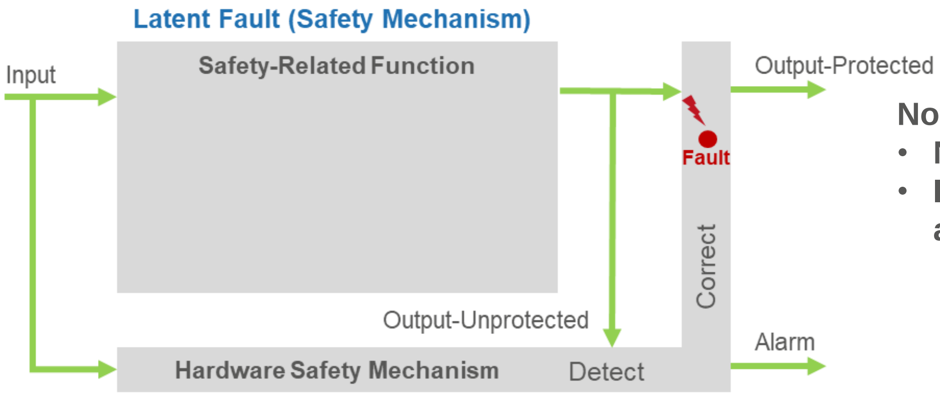


Note

- **Two multi-point faults may cause a failure**
- **Important to consider because of latent faults**

Latent Faults

A special class of multi-point (permanent) faults

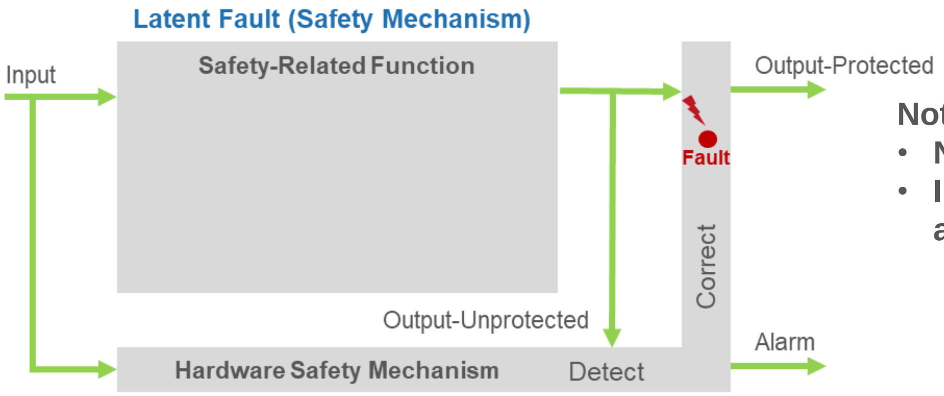


Note

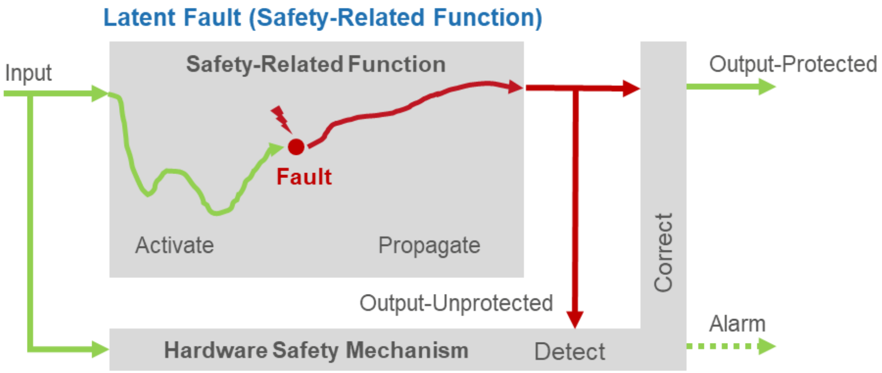
- **No alarm raised (fault remains latent)**
- **Important to consider: may compromise protection of a large portion of the safety-related function**

Latent Faults

A special class of multi-point (permanent) faults



Note
- **No alarm raised (fault remains latent)**
- **Important to consider: may compromise protection of a large portion of the safety-related function**



Note
- **Fault is corrected but SM does not indicate it**
- **Alarm inactive or not present (fault remains latent)**
- **Important to consider: may cause failures as soon as another random fault occurs**

Single-Point Fault Metric

SPFM

- Reflects the effectiveness of the safety architecture to protect from individual faults
- Many safe faults → Higher SPFM
- Effective safety mechanisms → Few residual faults → Higher SPFM
- Unprotected functions → Many single-point faults → Lower SPFM

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

λ is the failure rate

Source: ISO/FDIS 26262-5:2018

Latent Fault Metric

LFM

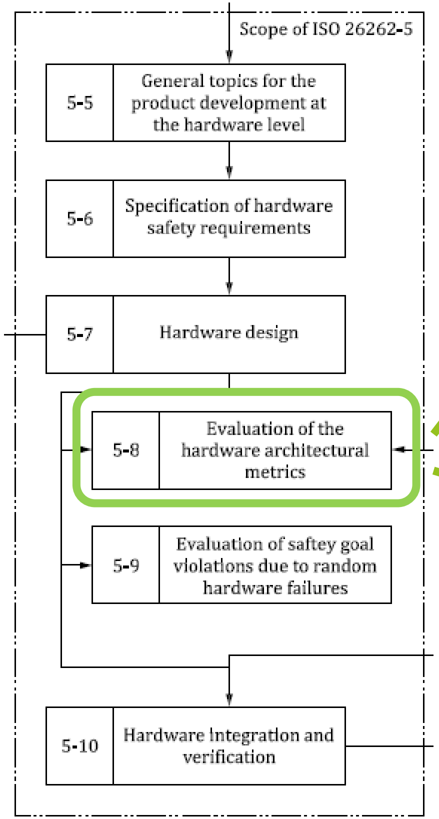
- Reflects the effectiveness of the safety architecture to protect from multi-point faults
- Many safe faults → Higher LFM
- Many single-point or residual faults → Higher LFM
- Many detected multi-point faults → Higher LFM

$$1-\frac{\sum_{SR,HW}(\lambda_{MPF,L})}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})}=\frac{\sum_{SR,HW}(\lambda_{MPF,DP}+\lambda_{S})}{\sum_{SR,HW}(\lambda-\lambda_{SPF}-\lambda_{RF})}$$

λ is the failure rate

Source: ISO/FDIS 26262-5:2018

Hardware Architectural Metrics



Evidence that the hardware safety architecture adequately prevents/controls random failures

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 %

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 %

Note

- **May require separate metrics for permanent and transient faults**

Source: ISO/FDIS 26262-5:2018

Summary

Fault Classification

- Safe faults
- Single-point and residual faults
- Multi-point faults
  - Detected
  - Latent

Key ISO 26262 Metrics

- SPFM and LFM
- Evidence that the hardware safety architecture adequately prevents/controls random failures

OneSpin

- Unique, automated solution for fault classification
- Automate FMEDA
- Reduce reliance on expert judgement
- Integrate with third-party tools
- Minimize time-consuming fault simulation

- Proven in both established and new suppliers of automotive hardware

"Computing hardware fault metrics and achieving targets set by ISO 26262 is challenging, but crucial to enable the application of our massively parallel many-core technology in autonomous vehicles. OneSpin is a trusted provider of apps, methodology and expertise to automate many steps of this process. Working cooperatively with its engineers smoothed our path to ISO 26262, savings months of project time."
Camille Jalier, director of hardware R&D, Kalray

OneSpin Provides Automated ISO 26262 Safety Analysis, Verification Flow to Kalray (Press release, 2018-06-22)

Thank you!