PLATO e1ns

FMEDA certified acc.

ISO 26262-8:2018; clause 11.4.4

Created by:

PLATO AG
Maria-Goeppert-Straße 15
23562 Lübeck
Tel.: +49 451 930986-0

Fax: +49 451 930986-09

E-Mail: info@plato.de

Inhalt

1 Purpose of this document

This document describes the structure of the methodology and the calculations used to perform FMEDA according to ISO 26262 with PLATO e1ns.

2 Abbreviations

DC	Diagnostic coverage
FIT	Failure in time
FR	Failure rate
λ	Lambda, failure rate
LF	Latent fault
LFM	Latent fault metric
MPF	Multiple point fault
MPF,L	Latent multiple-point fault
MPF,D	Detected multiple-point fault
MTTF	Mean time to failure
NSR	Not safety related
RF	Residual fault
S	Safe (e.g. λ_S)
SM	Safety mechanism
SPF	Single point fault
SPFM	Single point fault metric
SR	Safety related
PMHF	Probabilistic metric of random hardware failure

3 FMEDA acc. to ISO 26262

FMEDA is a structured approach to define failure modes, failure rate, and diagnostic capabilities of a hardware component. Based on the component functionality, the FMEDA hierarchy is structured in parts/subparts/elementary subparts failure modes (ISO 26262: Road vehicles — Functional safety). Each failure mode is categorized as to whether it affects the safety goal or not.

For each failure mode defined and affecting safety goals, basic needed inputs include:

- Failure rate (FR): the rate at which the component experiences faults, i.e., the reliability
- Safety mechanism (SM): whether there is a safety mechanism to detect the failure mode
- Diagnostic coverage (DC): the effectiveness of the safety mechanism at detecting faults

The failure rate is the measure of the reliability of a component, which is expressed in FIT. The FIT rate of a component is the number of failures expected in one billion hours of operation. (FIT rate equal to 1 means, the device has a mean time to failure (MTTF) of 1 billion hours, ISO 26262: Road vehicles — Functional safety).

Per ISO 26262, the estimated failure rates for hardware parts shall be determined in one of three ways:

- Estimated by application of industry reliability data books
- Derived from observation of field incidents, such as analysis of material returned as field failures
- Derived from experimental testing

When an initial FMEDA is setup to assess the safety readiness of a system, the DC for the safety mechanisms can be estimated based on the achievable values (low, medium, high) defined in ISO 26262:2011-5, Annex D.

The outputs to assess the level of functional safety readiness are the hardware architectural metrics **Single Point Fault Metric (SPFM)**, **Latent Fault Metric (LFM)** and **Probabilistic Metric of random Hardware Failures (PMHF).**

Based on these three metrics, the FIT for ASIL levelling can be addressed.

4 Performing FMEDA using PLATO e1ns

FMEDA in PLATO e1ns can be done per system element (e.g. printed circuit board) consisting of several thousand HW components supplying to several safety goals. The final fault metrics are calculated per safety goals.

4.1 Analysis per system element (FMEDA item)

The following analysis steps are performed in PLATO e1ns.FMEDA:

- Defining hardware components and its functions
- Link safety goals to hardware component functions
- The subsequent steps are working acc. the flow chart of the ISO 26262.5:2018E, figure B.2 and verified via TÜV SGN certificate in May 2021:

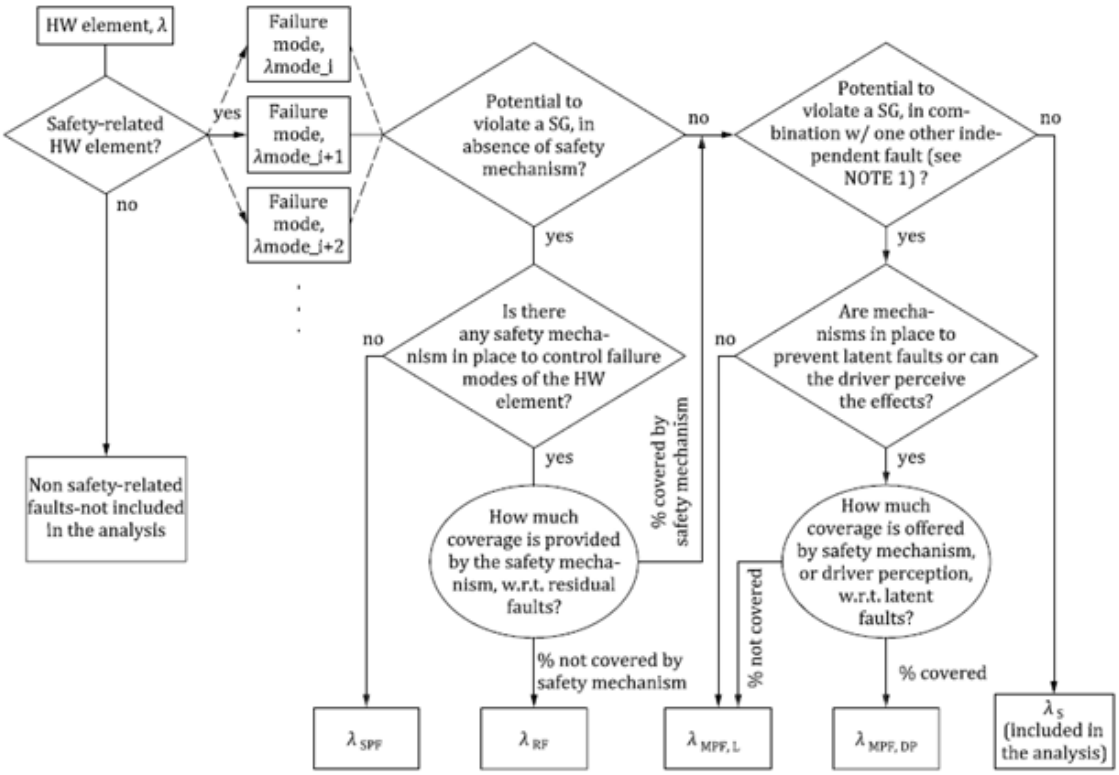

Figure B.2 — Example of flow diagram for failure mode classification

Origin: ISO 26262-5:2018 (E), page 37

4.2 Calculation of final metrics per safety goal

The final metrics per safety goal are calculated as written below:

(1) **Total failure rate (SR)** = $\sum\lambda_{SR}$ [FIT]

(2) **Residual and single-point fault failure rate** = $\sum(\lambda_{SPF} + \sum\lambda_{RF})$ [FIT]

(3) **Single-point fault metric (SPFM [%])** = $1 - \sum(\lambda_{SPF} + \lambda_{RF}) / \sum\lambda_{SR}$ [%]

(4) **Latent multiple-point fault failure rate** = $\sum\lambda_{MPF,\,L}$ [FIT]

(5) **Latent multiple-fault metric (LMF [%])** = $1 - \sum\lambda_{MPF,\,L} / \sum(\lambda_{SR} - \lambda_{RF} - \lambda_{SPF})$[%]

(6) **Detected multiple-point fault failure rate** = $\sum\lambda_{MPF,\,D}$ [FIT]

(7) **Probabilistic metric for random HW failures (PMHF)** = $\sum$PMHF

5 History of FMEDA 26262 certified plugin

June 2021:

Certification of the plugin FMEDA executable for PLATO e1ns version 3.3.3 successfully completed.

- Certified acc. ISO 26262-8:2018; clause 11.4.4
- Suitable in development of safety related systems up to ISO 26262 up to ASIL D

December 2021, valid for versions as of PLATO e1ns 4.0.0 and higher:

Technical conversion of the plugin from python 2.7 to python 3.9 for runnability of FMEDA from PLATO e1ns 4.0.0 and higher. No changes were made to processing, design, SW components or application methodology.

February 2022, valid for versions as of PLATO e1ns 4.0.3 and higher:

Due to performance optimizations, the following 2 operations were physically separated from each other in the FMEDA application:

- Data entry and calculations per hardware element
- Calculation of metrics per safety goal

No changes were made to processing, design, SW components or application methodology.

Dortmund, 07.03.2022

PLATO AG