PLATO Functional Safety

Functional Safety (ISO 26262) and FMEDA

Manufacturers of complex products with electrical, electronic, and programmable components must guarantee that failures and malfunctions are controlled safely.

The ISO 26262 and IEC 61508 standards describe the requirements on functional safety. They include the performance of a hazard analysis with risk assessment and verification with quantitative calculations via FMEDA.

PLATO supplies a certified solution that is integrated into the system analysis and makes individually customizable forms and calculations possible.

CERTIFIED ACC. TO
ISO 26262

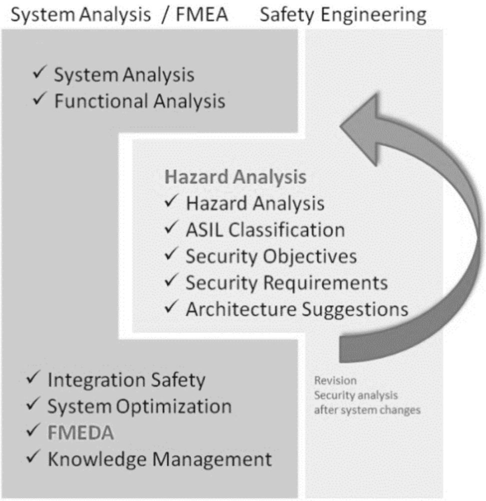


Fig.: System analysis and functional safety use and expand the corporate knowledge

Your Benefit

▪ Individual Analyses	Tailor-made analyses promote acceptance among users
▪ Calculations	Models for calculating error metrics
▪ Flexible form layouts	Columns and contents are customized specifically for the company
▪ Web application	Working in the browser simplifies distributed team work and software availability
▪ Use a database	Corporate knowledge is used and expanded
▪ Saves time	Effort and maintenance of data are minimized for the user
▪ Catalogs	Use of catalogs for component data
▪ Integration of company data	Data from SAP®, MES, PLM, etc., can be used

Individual Application

e1ns.methods contains standard forms and calculation methods for hazard analysis and FMEDA. They form the basis for company-specific forms that are developed within the framework of a form configuration. Additional forms for variants of a method or variants of the calculation methods can be added.

A form configuration contains :

- Specification of the form
- Implementation of the form (approx. 1-2 days – depending on the scope of functions)
- Installation of the form - remote / optional (0.5 days)

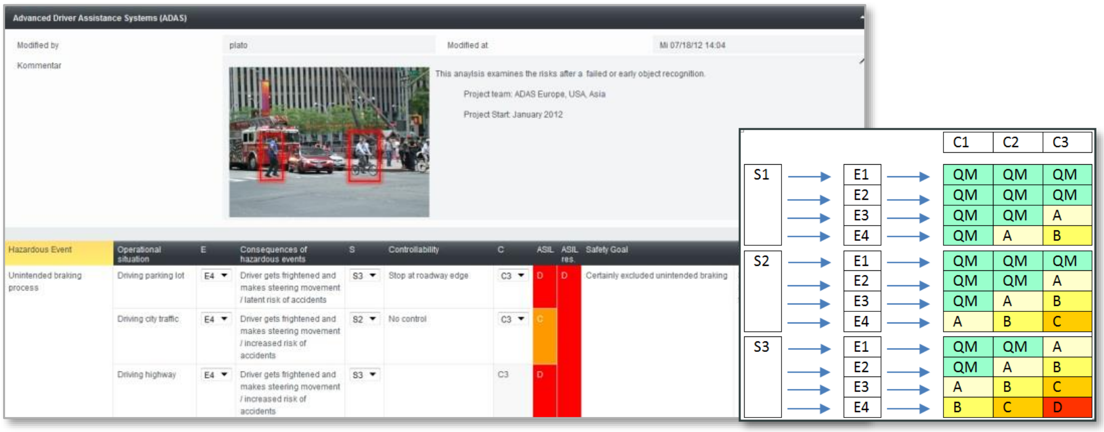
PLATO Functional Safety

Functional Safety (ISO 26262) and FMEDA

Hazard Analysis with Risk Assessment

Execution:

- Identification of potential hazards of the system
- (Driving) situation analysis
- Evaluation of severity (S), frequency of situation (E), controllability of malfunction (C).
- Classification of the safety level (ASIL / SIL)
- Definition of safety objectives



Advanced Driver Assistance Systems (ADAS)

Modified by	plato	Modified at	Mi 07/18/12 14:04
Kommentar	This anaylsis examines the risks after a failed or early object recognition. Project team: ADAS Europe, USA, Asia Project Start: January 2012		

Hazardous Event	Operational situation	E	Consequences of hazardous events	S	Controllability	C	ASIL	ASIL res.	Safety Goal
Unintended braking process	Driving parking lot	E4	Driver gets frightened and makes steering movement / latent risk of accidents	S3	Stop at roadway edge	C3	D	D	Certainly excluded unintended braking
	Driving city traffic	E4	Driver gets frightened and makes steering movement / increased risk of accidents	S2	No control	C3	C		
	Driving highway	E4	Driver gets frightened and makes steering movement / increased risk of accidents	S3		C3	D		

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Fig.: Hazard analysis and risk graph for ASIL classification

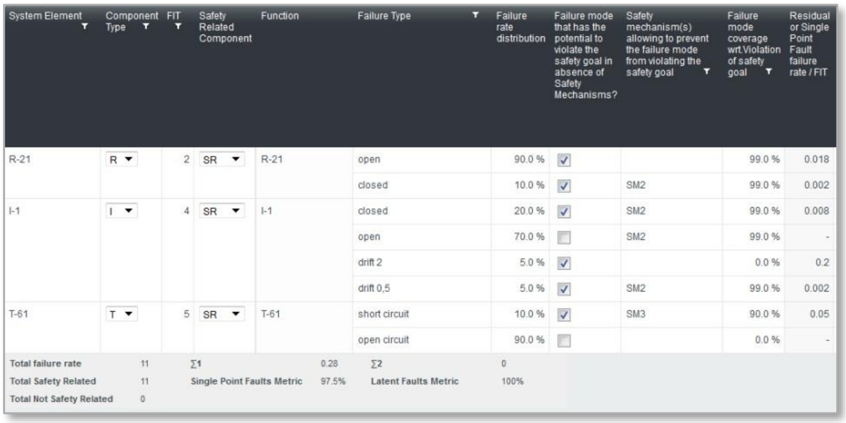
Safety and Diagnostic Concept

- Describe safety concept and execute ASIL decomposition
- Define diagnostic concept

FMEDA

FMEDA = Failure Modes, Effects and Diagnostics Analysis

- Determination of the quantitative parameters
- Calculation of failure rates with individual procedures and models
- Value catalogs for components offer convenient preparation
- Safety function, diagnostic mechanism and component faults are linked via the methods and provide the basis for standard-compliant calculation and traceability



System Element	Component Type	FIT	Safety Related Component	Function	Failure Type	Failure rate distribution	Failure mode that has the potential to violate the safety goal in absence of Safety Mechanisms?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal	Failure mode coverage wrt.Violation of safety goal	Residual or Single Point Fault failure rate / FIT
R-21	R	2	SR	R-21	open	90.0 %	☑		99.0 %	0.018
					closed	10.0 %	☑	SM2	99.0 %	0.002
I-1	I	4	SR	I-1	closed	20.0 %	☑	SM2	99.0 %	0.008
					open	70.0 %	□	SM2	99.0 %	-
					drift 2	5.0 %	☑		0.0 %	0.2
					drift 0,5	5.0 %	☑	SM2	99.0 %	0.002
T-61	T	5	SR	T-61	short circuit	10.0 %	☑	SM3	90.0 %	0.05
					open circuit	90.0 %	□		0.0 %	-

Total failure rate	11	Σ1	0.28	Σ2	0
Total Safety Related	11	**Single Point Faults Metric**	97.5%	**Latent Faults Metric**	100%
Total Not Safety Related	0				

Fig.: Excerpt from the FMEDA form