PLATO Functional Safety

Funktionale Sicherheit (ISO 26262) und FMEDA

Hersteller komplexer Produkte mit elektrischen, elektronischen und programmierbaren Komponenten müssen dafür sorgen, dass eine sichere Beherrschung von Ausfällen und Störungen gewährleistet ist.

Die Normen ISO 26262 und IEC 61508 beschreiben die Forderungen an Funktionale Sicherheit.
Sie beinhalten die Durchführung einer Gefährdungsanalyse mit Risikoabschätzung und den Nachweis mit quantitativer Berechnung über FMEDA.

PLATO liefert dazu eine zertifizierte Lösung, die in die Systemanalyse integriert ist und individuell anpassbare Formblätter und Berechnungen möglich macht.

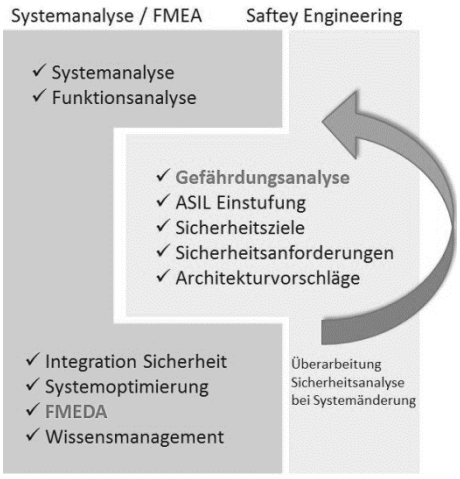


Abb.1: Systemanalyse und Funktionale Sicherheit verwenden und ergänzen das Unternehmenswissen

Ihr Nutzen

▪ Individuelle Analysen	Maßgeschneiderte Analysen fördern die Akzeptanz bei Nutzern
▪ Berechnungen	Modelle zur Berechnung von Fehlermetriken
▪ Flexible Formblattgestaltung	Spalten und Inhalte werden unternehmensspezifisch angepasst
▪ Web-Anwendung	Arbeiten im Browser erleichtert verteiltes Arbeiten und einfache Software-Bereitstellung
▪ Datenbank nutzen	Unternehmenswissen wird genutzt und ergänzt
▪ Zeitersparnis	Aufwand und Pflege von Daten sind für den Nutzer minimiert
▪ Kataloge	Verwendung von Katalogen für Bauteildaten
▪ Integration von Unternehmensdaten	Daten aus SAP®, MES, PLM usw. können genutzt werden

Individuelle Anwendung

e1ns.methods enthält Standardformblätter und Berechnungsverfahren für Gefährdungsanalyse und FMEDA. Sie sind die Basis für unternehmensspezifisch angepasste Formblätter, die im Rahmen einer Formblattkonfiguration entwickelt werden. Erweiterungen um zusätzliche Formblätter für Varianten einer Methode oder Varianten der Berechnungsverfahren sind möglich.

Eine Formblattkonfiguration beinhaltet:

- Spezifikation des Formblattes
- Umsetzung des Formblattes (ca. 1-2 Tage – abhängig vom Funktionsumfang)
- Installation des Formblattes - Remote / optional (0,5 Tage)

info@plato.de +49.451.930 986-0 www.plato.de

PLATO Functional Safety

Funktionale Sicherheit (ISO 26262) und FMEDA

Gefährdungsanalyse mit Risikoabschätzung

Durchführung:

- Identifizierung potenzieller Gefährdungen des Systems
- (Fahr-)Situationsanalyse
- Einstufung der Schwere (S), Häufigkeit der Situation (E), Beherrschbarkeit der Fehlfunktion (C)).
- Einstufung des Sicherheitslevels (ASIL / SIL)
- Sicherheitsziele definieren

Abb.2: Gefährdungsanalyse und Risikograf zur ASIL-Klassifizierung

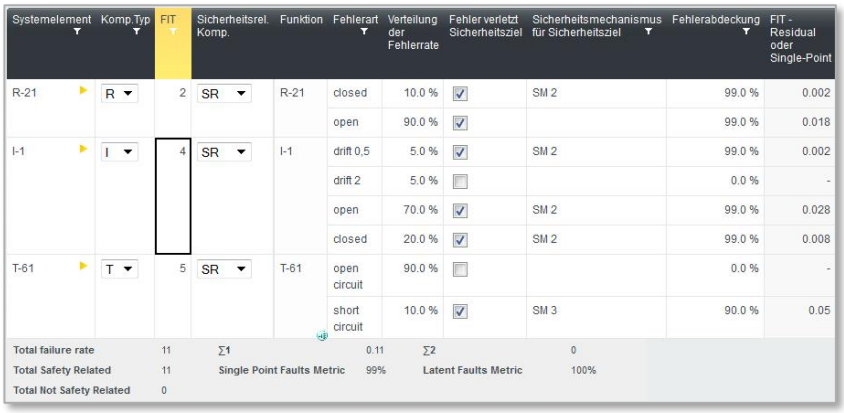
Sicherheits- und Diagnosekonzept

- Sicherheitskonzept beschreiben und ASIL Dekomposition durchführen
- Diagnosekonzept definieren

FMEDA

FMEDA = Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse

- Erfassung quantitativer Kenngrößen
- Berechnung von Ausfallraten mit individuellen Verfahren und Modellen
- Werte-Kataloge für Bauteile bieten eine komfortable Vorbereitung
- Sicherheitsfunktion, Diagnosemechanismus und Bauteilfehler sind über die Methoden verknüpft und liefern die Grundlage für eine normenkonforme Berechnung und Traceability.



Systemelement	Komp.Typ	FIT	Sicherheitsrel. Komp.	Funktion	Fehlerart	Verteilung der Fehlerrate	Fehler verletzt Sicherheitsziel	Sicherheitsmechanismus für Sicherheitsziel	Fehlerabdeckung	FIT - Residual oder Single-Point
R-21	R	2	SR	R-21	closed	10.0 %	☑	SM 2	99.0 %	0.002
					open	90.0 %	☑		99.0 %	0.018
I-1	I	4	SR	I-1	drift 0,5	5.0 %	☑	SM 2	99.0 %	0.002
					drift 2	5.0 %	☐		0.0 %	-
					open	70.0 %	☑	SM 2	99.0 %	0.028
					closed	20.0 %	☑	SM 2	99.0 %	0.008
T-61	T	5	SR	T-61	open circuit	90.0 %	☐		0.0 %	-
					short circuit	10.0 %	☑	SM 3	90.0 %	0.05
Total failure rate		11	Σ1			0.11	Σ2		0	
Total Safety Related		11	Single Point Faults Metric			99%	Latent Faults Metric		100%	
Total Not Safety Related		0								

Abb. 3: Ausschnitt aus dem FMEDA-Formblatt

info@plato.de +49.451.930 986-0 www.plato.de