FUNKTIONALE SICHERHEIT

Die System-FMEA im Safety-Projekt

Artikelserie Functional Safety, Teil 6

Einleitung

Die Entwicklung funktional-sicherer Komponenten stellt den Entwickler vor zusätzliche Herausforderungen. Im Gegensatz zu Standardproduktentwicklungen ergeben sich normative Anforderungen, die die Komplexität der Produktentwicklung weiter erhöhen.

Hierzu zählen beispielsweise die Architekturanforderungen der IEC 61508-2. Abhängig vom zu erreichenden Sicherheitsintegritätslevel macht diese Norm konkrete Vorgaben bezüglich der zu erreichenden Hardware-Fehlertoleranz (HFT) sowie dem Anteil sicherer Fehler (SFF). Neben fehlersicheren Design-Prinzipien sind Diagnosemassnahmen der Schlüssel zu einer hohen SFF.

Da die Norm applikationsunabhängig und abstrakt ist, ergeben sich für den Anwender in der Praxis häufig Probleme bei der Interpretation. Der Beitrag soll helfen, den Schritt von den normativen Anforderungen zur praktischen Anwendung zu meistern. Im Fachartikel werden die typischen Anforderungen der Fabrikautomation herangezogen (max. SIL3, Anforderungsrate: High Demand).

Hintergrund

Die IEC 61508-2 fordert Massnahmen zur Vermeidung, beziehungsweise zur Beherrschung von Fehlern.
Fehler lassen sich einteilen in systematische und zufällige Fehler. Systematische Fehler können in den verschiedenen Phasen des Produktlebenszyklus auftreten. Entsprechend formuliert die Norm Verfahren und Massnahmen zur Vermeidung von systematischen Fehlern, wie zum Beispiel Anwendung eines Projektmanagements, strukturierter Entwurf, Dokumentation und Tests auf mehreren Ebenen. Diese Methoden sind somit von qualitätssichernder Natur. Mit diesen soll erreicht werden, dass Fehler erst gar nicht in das Produkt eingebracht werden.

Davon abzugrenzen sind Methoden zur Beherrschung von Fehlern.
Der Beherrschung von Fehlern wird einerseits mit einer erhöhten Robustheit des Produkts, zum Beispiel gegen EMV-Einflüsse, und andererseits mit einer Erkennung der Fehler (im Betrieb) und darauf folgender Fehlerreaktion reagiert. Eine typische Massnahme ist die Überführung des Systems in den sicheren Zustand. Der Schlüssel für die Erkennung von Fehlern (im Betrieb) sind Diagnosemassnahmen, die additiv zur gewünschten Sicherheitsfunktion im Produkt implementiert werden.

In diesem Beitrag werden die grundsätzlichen Schritte bei der Berücksichtigung der IEC 61508-2 zur Identifikation, Implementierung und Bewertung von Diagnosemassnahmen erläutert. Ein geeignetes Werkzeug hierfür ist die Failure Mode and Effects Analysis – die FMEA (dt.: Ausfallarten- und Auswirkungsanalyse).

Die FMEA im Safety-Projekt

FMEAs werden in der Praxis vielfältig angewendet und mit unterschiedlichen Begriffen bezeichnet (Prozess-FMEA, Konstruktions-FMEA, …). Für das Ziel dieses Artikels ist die System-FMEA am zweckmässigsten.

Den weiteren Betrachtungen liegt folgendes zugrunde:

- Unter System wird das zu entwickelnde Produkt aufgefasst. Formal korrekt aus Sicht der IEC 61508 wäre die Bezeichnung Subsystem, da es sich bei dem Produkt i.d.R. nur um einen Teil der gesamten Sicherheitskette handelt.
- Systemelemente sind die Bestandteile der Highlevel-Produktarchitektur. Die Betrachtung von einzelnen Bauteilen erfolgt erst in der nachgelagerten Ausfallratenberechnung (FMEDA).
- Die Methode wird meist iterativ angewendet werden, da sich durch die FMEA ggf. erforderliche Anpassungen an der ursprünglichen Architektur ergeben.
- Wie geschildert, steht hier als Analyseziel die Festlegung von fehlervermeidenden Massnahmen und Diagnosemassnahmen im Vordergrund. Andere Massnahmen, die sich ebenfalls aus der FMEA ergeben können, werden in diesem Fall nicht betrachtet, wie etwa Ermittlung von Schulungsbedarfen für Mitarbeiter oder Verwendungshinweise für das Produkt.

	HARWARE-FEHLERTOLERANZ FÜR SICHERHEITSBEZOGENE ELEMENTE					
	HFT=0		HFT=1		HFT=2	
ANTEIL SFF	**TYP A**	TYP B	**TYP A**	TYP B	**TYP A**	TYP B
< 60%	**SIL 1**	—	**SIL 2**	SIL 1	**SIL 3**	SIL 2
60% – < 90%	**SIL 2**	SIL 1	**SIL 3**	SIL 2	**SIL 4**	SIL 3
90% – < 99%	**SIL 3**	SIL 2	**SIL 4**	SIL 3	**SIL 4**	SIL 4
≥ 99%	**SIL 3**	SIL 3	**SIL 4**	SIL 4	**SIL 4**	SIL 4

Abbildung 1: Zusammenhang HFT und SFF

MESCO Engineering AG | Klosterzelgstrasse 1a | 5210 Windisch | Schweiz | Tel. +41 065 560 37 00 | Fax +41 61 641 67 28 | info@mesco.ch | www.mesco.ch

Einflussfaktoren Entwicklung nach IEC 61508-2

Ein Überblick über die Einflussfaktoren bei einer Produktentwicklung nach IEC 61508-2 schafft Transparenz. Die funktionalen Anforderungen und die Anforderungen an die Sicherheitsintegrität ergeben sich aus der Safety Requirements Specification, die in der Praxis oft mit dem Lastenheft gleichgesetzt wird. Direkt aus der IEC 61508-2 ergeben sich mehrere Anforderungen, die teilweise in Wechselbeziehung zueinander stehen.

Architektur-Anforderungen

Die Norm definiert einen Zusammenhang zwischen der Hardware-Fehlertoleranz (HFT) eines Elements, dem geforderten SIL und dem Anteil sicherer Fehler (SFF). Darüber hinaus macht die Norm eine Unterscheidung zwischen Elementen, die nur aus einfachen Bauteilen (Typ A) und Elementen, die zumindest ein komplexes Bauteil umfassen (Typ B). Die Zusammenhänge sind in Abbildung 1 (s. S. 1) zusammengestellt.

Zum besseren Verständnis: Ein Element in diesem Kontext, sind zum Beispiel alle Schaltungsteile eines Produkts, die der Stromversorgung dienen.

Diagnosetestintervall und Prozessicherheitszeit (PST)

Für die Anforderungsrate High Demand beziehungsweise Continous Mode gilt folgendes:

Bei einkanaligen Elementen können nur Diagnosemassnahmen berücksichtigt werden, die innerhalb der Prozesssicherheitszeit den Fehler erkennen und das System in den sicheren Zustand überführen. Bei mehrkanaligen Systemen darf die festgelegte Mittlere Dauer bis zur Wiederherstellung (MTTR) als maximales Diagnosetestintervall genutzt werden.

Fehlermodelle und DC

Mit steigendem angestrebten Diagnosedeckungsgrad (DC) für ein Element sind zunehmend komplexere Fehlermodelle zu berücksichtigen und das System auf deren Auswirkungen hin zu untersuchen. Beispielsweise muss bei einem angestrebten DC von 60% ein digitaler Ausgang nur auf die einfachen Fehlermodelle Stuck-at Low und Stuck-at High hin betrachtet werden. Bei einem DC von 99% hingegen müssen – über die einfachen Fehlermodelle hinaus – auch das DC-Fehlermodell, Drift und Oszillation berücksichtigt werden.

Der höhere DC wiederum kann nur in Anspruch genommen werden, wenn nachgewiesen wird, dass diese komplexeren Fehler auch erkannt werden.

Diagnosemassnahmen und erreichbarer DC

Die Norm benennt konkrete Diagnosemassnahmen und deren höchstens erreichbaren DC. Als Hilfestellung sind die benannten Diagnosemassnahmen in der IEC 61508-7 etwas detaillierter beschrieben. Da die Wirksamkeit der Diagnosemassnahme nachzuweisen ist, kann es in der Praxis ratsam sein, nicht pauschal immer den maximal erreichbaren DC zu beanspruchen.

Ausfallgrenzwerte für eine Sicherheitsfunktion in der Betriebsart High Demand / Continuous Mode

In Abhängigkeit vom zu erreichenden SIL sind konkrete Grenzwerte für die Rate der gefährlichen Ausfälle einzuhalten.

Im Falle der Betriebsart High Demand / Continuous Mode ist deren Bezeichnung die PFH (Probability of dangerous failure per hour – mittlere Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion pro Stunde).

Anmerkung: Für Produkte / Subsysteme wird in der Regel die Erreichung eines bestimmten prozentualen Anteils der PFH vorgegeben.

	PFH	
SIL	max.	min.
3	100 FIT	10 FIT
2	1000 FIT	100 FIT
1	10.000 FIT	1.000 FIT

Abbildung 2: Ausfallgrenzwerte PFH

Zusammenhänge und Ablauf in der Praxis

Die Vielfalt und die gegenseitige Abhängigkeit der Einflussfaktoren erschweren gerade Neueinsteigern die Anwendung und führen bei falscher Anwendung oft zu sub-optimalen Ergebnissen. Typische negative Folgen in der Praxis sind die Notwendigkeit von Anpassentwicklungen, die erst spät im Entwicklungszyklus erkannt werden, aber auch Over-Engineering von Sicherheitsmassnahmen, die zu Lasten der Verfügbarkeit des Produkts gehen und das Produkt unnötig verteuern.

Die System-FMEA sollte als Hilfsmittel betrachtet werden, das bereits zu einem frühen Zeitpunkt in der Entwicklungsphase zum Einsatz kommt.

Es empfiehlt sich folgender Ablauf:

- Entwurf der Systemarchitektur (ohne Diagnosemassnahmen)
- Erstellung des zugehörigen Reliability-Block Diagrams (RBD)
- Durchführung der System-FMEA anhand von Blockschaltbild und RBD
- Ermittlung von Diagnosemassnahmen und dem zu erreichenden DC
- Ergänzung der Diagnosemassnahmen in der Systemarchitektur. Ggf. Vornahme von Änderungen an der Architektur und RBD, wenn die Erreichung der Architektur-Anforderungen nicht realistisch erscheint (z.B. die mehrkanalige Ausführung der Elemente, zur Reduktion der Anforderungen für die SFF)
- Erneute Durchführung der System-FMEA und Abschätzung, ob alle Anforderungen der SRS und Norm damit erreichbar sind

Bauteil	Ausfallrate λ	Ausfallart	Anteil	Auswirkung	Ausfallrate / Ausfallart	λ_s	λ_{dd} = DC *λ_d	λ_{du}
R1	**10 FIT**					**4 FIT**	**5,4 FIT**	**0,6 FIT**
		Kurzschluss	40%	sicherer Ausfall	4 FIT			
		Unter-brechung	**50%**	**gefährlicher Ausfall**	**5 FIT**			
		Drift	**10%**	**gefährlicher Ausfall**	**1 FIT**			
R2		…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…
∑						**650 FIT**	**800 FIT**	**78 FIT**

Abbildung 3: Exemplarische FMEDA

Ist die Architektur stabil kann eine Umsetzung entsprechend dem Hardware-Pfad nach IEC 61508-2 erfolgen. Sofern für sicherheitsrelevante Teile Software zum Einsatz kommt, gilt hierfür der entsprechende Software-Pfad nach IEC 61508-3.
Die Ermittlung der Ausfallraten der (Element-)Sicherheitsfunktion erfolgt gegen Ende der Design & Development-Phase, auf Basis des Stromlaufplans und der Materialstückliste, im Rahmen der FMEDA.

Die FMEDA lässt sich prinzipiell als Erweiterung der FMEA auffassen. Wurden auf der Ebene der (System)-FMEA Elemente als Blackbox betrachtet, liegen nun Details zum inneren Aufbau dieser Elemente vor.

Die (Basis-)Ausfallrate jedes verwendeten Bauteils kann dem Herstellerdatenblatt oder einer geeigneten Datenbank entnommen werden. Entsprechend der individuellen Ausfallarten des Bauteils ergibt sich auf der Ebene des Elements ein sicherer oder ein gefährlicher Ausfall, wodurch sich eine Verteilung der Basisausfallrate *λ* auf *λ_safe* und *λ_dangerous* ergibt.

Jetzt kommt die Diagnose nutzbringend zur Wirkung, da mit ihr ein Teil der gefährlichen Fehler entdeckt und das Produkt als Fehlerreaktion in den sicheren Zustand überführt wird. Aus Sicht der Funktionalen Sicherheit sind die entdeckten gefährlichen Fehler somit nicht mehr relevant. Für den Vergleich mit dem geforderten SIL-Ausfallratengrenzwert sind nur noch die gefährlichen unentdeckten Fehler *λ_du* relevant.

Für den Fall von einkanaligen (Sub-)Systemen gilt der einfache Zusammenhang:
- *PFH=λ_du*

Autor: Dr. Johann Pohany
Managing Director
Medidtcine Consultants
www.medidtcine.com

Autor: Armin Götzmann
Geschäftsführer
MESCO Systems GmbH
www.mesco.de