

FMEA für SysML-basierte Systembeschreibungen

Maßnahmen zur Steigerung und Sicherstellung der Qualität von Systemkomponenten rücken in der Automobilindustrie wieder zunehmend in den Fokus. Die Notwendigkeit hierfür ergibt sich auch aus der erschreckend wachsenden Zahl an Rückrufen, die in jüngster Zeit eine schwindelerregende Höhe erreicht hat. In Nordamerika stieg die Rückrufquote* alleine im ersten Halbjahr 2014 auf ca. 455 % im Vergleich zu 142,5% im 1. Halbjahr 2013. Ursache für diese hohe Zahl ist unter anderem die Verwendung von gleichen Systemkomponenten in unterschiedlichen Baureihen bei verschiedenen Fahrzeugherstellern. Diese Qualitätsprobleme können für betroffene Unternehmen existenzgefährdend sein.

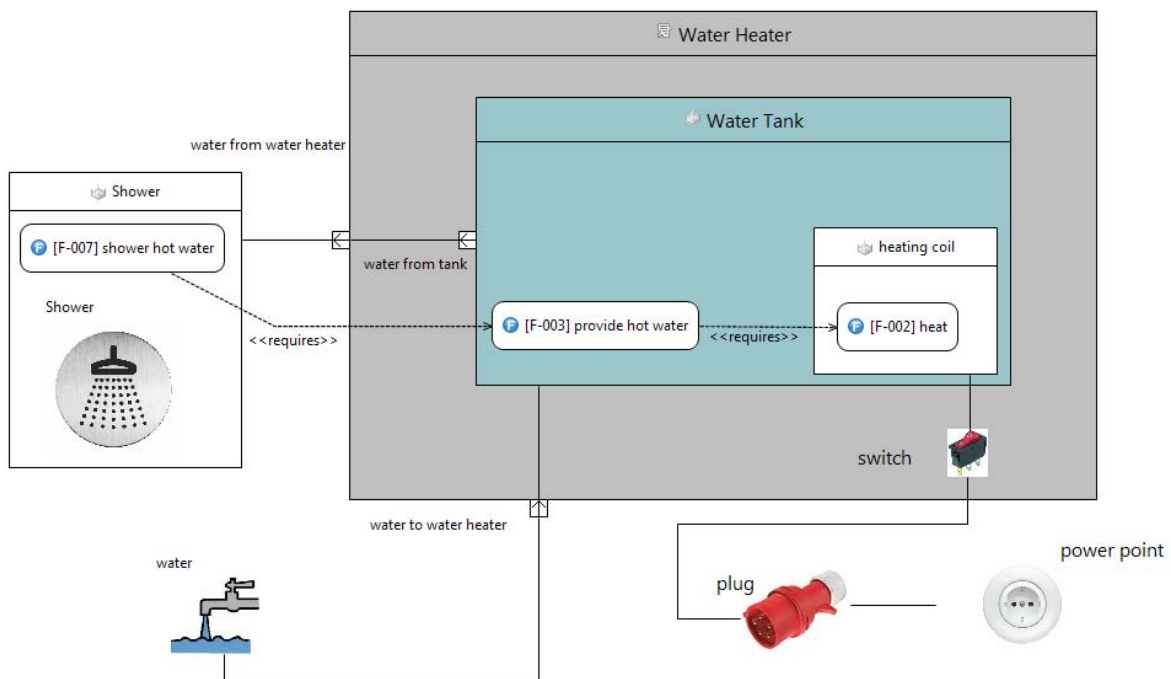
Eine Methode zur frühzeitigen Vermeidung von Qualitätsproblemen ist die konsequente Anwendung der FMEA, mit der schon während des Systemdesigns potentielle Fehler und Risiken erkannt und durch entsprechende Gegenmaßnahmen nachvollziehbar kontrolliert und minimiert werden können. Da die FMEA allerdings eine bereits weit verbreitete Methode ist, stellt sich somit die Frage nach der Effektivität und eventuell vorhandenen Schwachstellen im täglichen Einsatz der Methode, die zum Auftreten der beschriebenen Probleme beitragen können.

In der Praxis lassen sich bei der FMEA-Anwendung häufig die folgenden problematischen Aspekte beobachten:

- Die FMEA findet parallel zu anderen Entwicklungs-Aktivitäten statt, aber ist nicht ausreichend mit diesen integriert, daher entstehen Konsistenzprobleme und zusätzlicher Aufwand. Im Extremfall entspricht die FMEA nicht dem aktuellen Systementwicklungsstand, so dass Fehler nicht erkannt werden können oder die geplanten Maßnahmen nicht ausreichend sind.
- Die Nachverfolgung der in der FMEA identifizierten Maßnahmen ist unzureichend. Diese müssen in den Anforderungsmanagementprozess einfließen, das ist häufig nicht einfach möglich oder unterbleibt.
- Die verschiedenen FMEAs für Bauteile, Komponenten, Teilsysteme und Systeme sind nicht ausreichend miteinander verknüpft, daher werden die möglichen Auswirkungen von Fehlern von der Bauteilebene bis hinauf auf die Fahrzeugebene nicht vollständig sichtbar und analysiert.
- Die Wiederverwendbarkeit ist nur eingeschränkt möglich - aus Fehlern soll gelernt werden, aber wenn FMEAs getrennt von Systemmodellen entstehen, können sie nur schwer wiederverwendet werden, d.h. bereits erkannte Fehler werden bei Designvarianten oder bei Wiederverwendung von Komponenten schlicht vergessen. Umgekehrt bringt ein Verweis bei einer Systemweiterentwicklung auf eine existierende FMEA des Vorgängersystems keinen ausreichenden Nachweis über alle potentiellen Fehler und deren Effekte.

Die Lösung der aufgezeigten Probleme erfordert einerseits Prozessanpassungen und eine konsequente, regelkonforme Anwendung der FMEA und andererseits eine bessere Anbindung der FMEA an die Systementwicklung. Steht dann noch eine geeignete Werkzeugunterstützung bereit, lassen sich Konsistenzprobleme einfacher und schneller aufdecken und beheben.

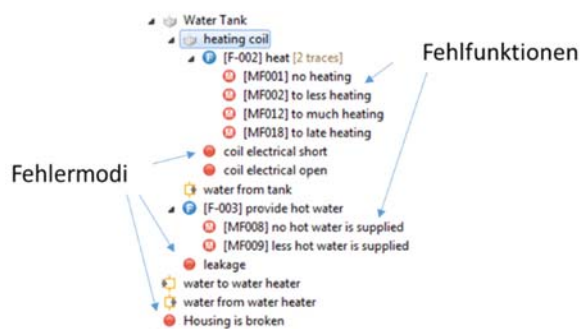
Solch eine bessere Verzahnung der FMEA mit den Aktivitäten des Systementwicklungsprozesses sowie die Lösung von Konsistenz- und Effizienzproblemen lässt sich durch ein modellbasiertes Vorgehen unter Verwendung einer semi-formalen Notation (z.B. SysML) im Systemdesign erreichen.



In dem im Bild dargestellten Beispiel eines Wassererhitzers sind im Systemmodell die Systemkomponenten, ihre hierarchische Struktur sowie die Verbindungen zwischen den Systemkomponenten enthalten. Weiterhin sind auch bereits die den Systemkomponenten zuzuordnenden

Systemfunktionen sowie deren Abhängigkeiten modelliert. Die verwendete Modellierungssprache ist ein SysML-Profil.

Damit stehen für die FMEA bereits wesentliche Informationen bereit. Um Inkonsistenzen und mehrfache Arbeitsschritte zu vermeiden, können für die Komponenten ihre Fehlermodi sowie für die Funktionen die entsprechenden Fehlfunktionen direkt im Systemmodell hinterlegt werden. Gewonnen werden die Fehlfunktionen z.B. über eine HAZOP-Analyse. Die Fehlermodi können z.B. Bauteilbibliotheken entnommen werden (im Falle von zufälligen Hardwarefehlern) oder im Falle von systematische Fehlern z.B. aus Statistiken oder Erhebungen über den bisherigen Einsatz im Feld stammen.



In einem anschließenden Arbeitsschritt werden diese Informationen unter Nutzung des FMEA-Formblattes miteinander verknüpft. Durch die direkte Annotation der Fehlerinformationen im Systemmodell werden Duplikationen z.B. des Strukturbaumes in verschiedenen Werkzeugen und die damit verbundenen potentiellen Inkonsistenzen durch das Prinzip „*single source of information*“ vermieden. Die FMEA-Formblätter sind so stets bereits vorausgefüllt – die Systemstruktur inklusive der Fehlermodi wird aus dem Modell entnommen. In den Formblättern werden dann die Fehlerketten aufgedeckt, die Risikobewertungen vorgenommen und die erforderlichen Maßnahmen hergeleitet und spezifiziert.

Component	Potential Failures	Potential Failure Effects	Severity	Max	Risk	Potential Failure Causes	Occuren	Current Design Controls Prevention	Current Design Controls Detection	Detectio	RPN
Water Heater	● Housing is broken	⚠ [water heater hazards] flooding	0		N	[produce housing] [MF019] mechanically broken housing is being produced	0	[2] periodic callibration of production equipment for tank	🔍 electrical test - coil [det: 0]	0	0
		⚠ [water heater hazards] electric shock	0		N	[malfunctions at system level] [3] human misuse	0				
	→ water to water heater										
	← water from water heater										
switch	● switch electrical short	[[F-009] stop power supply if turned OFF] [MF006] power is supplied if turned OFF	7								
		[[F-008] provide power if turned ON] [MF005] no power is supplied if turned ON	1		N	[produce coil] [MF014] mechanically broken coil is produced	0	[1] periodic callibration of production equipment for coil	🔍 electrical test - coil [det: 0]	0	0
[F-008] provide power if turned ON	● [MF005] no power is supplied if turned ON	[[F-002] heat] [MF001] no heating	8		N	[switch] switch electrical open	0				
			8		N	[produce switch] [MF016] mechanically broken switch is being produced	0				

Die enge Verbindung von FMEA und SysML-Modell macht alle Veränderungen in der Modellstruktur immer auch sofort in der FMEA sichtbar. Mehr noch, durch eine komponentenorientierte Vorgehensweise bei der Erstellung des SysML-Modells lassen sich Wirkketten erstellen, mit denen Auswirkungen von Fehlern bis auf die oberste Systemebene verfolgt werden können. Durch die Ausnutzung des Typ-/Instanz-Konzeptes von SysML kann zusätzlich eine (zumindest teilweise) Wiederverwendung von FMEA-Daten erreicht werden, z.B. indem wiederverwendbare Komponenten zusammen mit ihren Fehlermodi wie auch den komponenteninternen Wirkketten in Bibliotheken organisiert werden.

Die hier skizzierte Methode der SysML-basierten FMEA erfordert für den praktischen Einsatz geeignete Werkzeuge, da ohne sie die erhofften Vorteile – Konsistenz und Effizienzverbesserungen – nicht realisiert werden können. Ebenso erhöht eine adäquate Werkzeugunterstützung nicht nur die Akzeptanz der Methode, sondern verhindert auch, dass die FMEA nur als zeitraubendes und störendes aber notwendiges Beiwerk der Systementwicklung empfunden wird.

*Statistik des Center of Automotive Management in Bergisch-Gladbach

Autoren

Dr. Marc Born

Chief Technology Officer
KPIT medini Technologies AG,
Tochterfirma der KPIT Technologies GmbH



Dr. Eckhardt Holz

Senior Advisor Functional Safety
KPIT medini Technologies AG,
Tochterfirma der KPIT Technologies GmbH



Über KPIT

KPIT medini Technologies ist Teil der **KPIT Technologies**. KPIT Technologies (BSE: 532400, NSE: KPIT) ist ein schnell wachsendes internationales Unternehmen im Bereich Produktentwicklung und IT-Beratung. Es entwickelt gemeinsam mit seinen Kunden innovative und domänenspezifische Technologielösungen für Automobil-, Transport, Produktions- und Energieversorgungsunternehmen. KPIT ist der weltweit führende Anbieter von Lösungen für die Bereiche AUTOSAR & Bordnetze, Karosserielektronik, Chassis, Sicherheits- und Fahrerassistenz, funktionale Sicherheit, Fahrzeugdiagnose, Infotainment und Antriebsstrang.

Pressekontakt:

Stefanie Köhler
Tel: +49 89 322 99 66 140
stefanie.koehler@kpit.com
www.kpit.com