Toolbox: Produktfehler quantifizieren

Das Auftreten technischer Ereignisse und Fehler abschätzen

IHRE SITUATION

Sie stehen kurz vor Projektende oder haben bereits Serienteile geliefert. Die Dokumentation ist freigegeben. Ressourcen, Zeit und Budget sind aufgebraucht. Gerade jetzt tritt ein Produktfehler auf. Das, obwohl Ihr Team sorgfältig nach Stand der Technik entwickelte. Sie verwerfen Ihren ersten Impuls, einen Hotfix zu liefern. Denn Sie wissen: Es gibt bei Software immer den nächsten Fehler. Ein Dilemma: Das Änderungsrisiko eingehen oder den Fehler belassen?

UNSER ANSATZ

Wir reduzieren die Entscheidung auf eine Frage: Ist das erwartete Risiko tolerierbar, wenn Sie den Fehler beibehalten? Dafür schätzen wir das Risiko quantitativ und setzen es in Relation zum Stand der Technik. In Euro und Cent wenn Sie wünschen. Doch das ist nur ein Teil: Kunden, Manager, Qualitäter, Auditoren und andere Interessenten müssen Ihre Entscheidung mittragen. Das geht nur, wenn sie das Risiko verstehen. Dafür erstellen wir einen klaren Bericht.

SO GEHT ES

Wir zerlegen den Produktfehler in unabhängige Basisereignisse und berechnen deren absolute Auftretenswahrscheinlichkeiten P_X:

$$\underbrace{P_{Szenario}}_{\text{System-umwelt}} * \underbrace{P_{Fehler\,1} * \cdots * P_{Fehler\,n}}_{\text{Unabhängige Produktfehler}} * \underbrace{P_{t-kritisch}}_{\text{Kritische Fehlerzeit}} = \underbrace{P_{Gesamt} < \mathrm{P}_{Tolerabel}}_{\text{Entscheidungsregel}}$$

AUTOMOTIVE TYPISCHE ABSOLUTE UND RELATIVE HÄUFIGKEITEN

ASIL	Grenzwerte zufälliger Fehler[1]	FIT $1\,FIT = 10^{-9}h^{-1}$
A[2]	$< 10^{-6}h^{-1}$	$< 1.000\,FIT$
B	$< 10^{-7}h^{-1}$	$< 100\,FIT$
C	$< 10^{-7}h^{-1}$	$< 100\,FIT$
D	$< 10^{-8}h^{-1}$	$< 10\,FIT$

Tab. 1

Exposure aus G&R[4]	Relative Häufigkeit[3]
E1	-
E2	<1%
E3	<10%
E4	>10%

Tab. 2

Lebensdauer[2]	$15\,a$
Betriebsstunden[2]	$8.000\,h$
Ladestunden[2]	$40.000\,h$
Betriebszeit[3]	$400\,h/a$
Fahrzyklen[3]	$1000\,/a$
Fahrzyklus[3]	$24\,\mathrm{min}$
Laufleistung[3]	$20.000 km/a$
Unbekannte Fehler[2]	50%

Tab. 3

(1) gem. ISO 26262-5:2018 Table 6
(2) konservativer Erfahrungswert
(3) gem. VDA 702 Situationskatalog E-Parameter
(4) gem. ISO26262-3:2018

Klick oder Scan

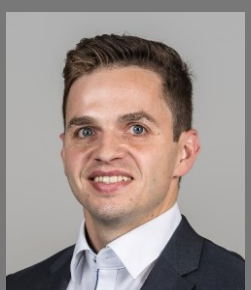
© Nico Litschke:
International (CC BY-NC-SA 4.0)

Projekt- und Safety Ingenieur in Automotive.

Nico Litschke
Dachtlerstr. 20
70499 Stuttgart

Telefon: +49 711 469 122 48
Mail: info@nicolitschke.com

www.nicolitschke.com

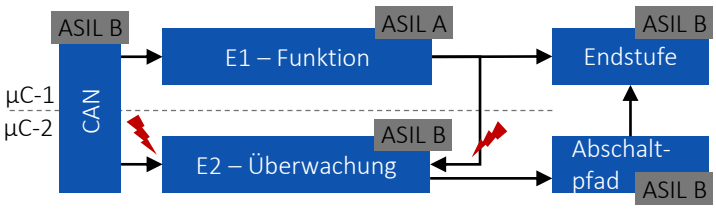


Toolbox: Produktfehler quantifizieren

Das Auftreten technischer Ereignisse und Fehler abschätzen

Schritt 1. Den Fehler qualitativ verstehen

Zunächst gilt es, den Fehler und die Fehlerkette qualitativ zu erfassen. Natürlich analysieren die Entwickler die Details; teilweise bis zum Code. Abstrahieren Sie die Analyse auf das notwendige Maß, um schätzen zu können – und auch um die Analyse an Andere zu kommunizieren.



Beim Initialisieren des Systems beginnt die E2 ihre Überwachung mit einer Verzögerung zwischen 10ms und 60ms. In diesem Zeitraum ist die E2-Überwachung inaktiv. Bei einem E1-Fehler wird auch das ASIL B Sicherheitsziel verletzt. Die Verzögerung fluktuiert in Abhängigkeit von 2 unabhängigen CAN-Frames.

Schritt 2. Konservative Annahmen abstimmen

Mit unserem Kunden stimmen wir ab:

- Lebensdauer: $6.000\ \text{h}$ über $15a$
- Betriebszeit: $400\ h/a$
- Auftreten CAN-1: $5\ /a$
- Auftreten CAN-2: $10\ /a$
- Fahrzyklen: $1.000/\text{a}\ je\ 24min$ (vgl. Tab. 3)
- Kritische Zeit: $60ms$ (Worst Case)
- Tolerabel: $100FIT$ (ASIL B)

Prüfen Sie in Fahrzeug- und Test-Logs, ob die realen Werte zu den Annahmen passen. Als Anhaltspunkt können Sie auch Tab. 3 nutzen.

Schritt 3. $P_{Szenario}$ schätzen

Wie häufig kann der Fehler durch die Systemumwelt angestoßen werden? Hier: der Empfang der unabhängigen Frames CAN-1 und CAN-2:

$$P_{Szenario} = \frac{(5+10)/a}{400h/a} = 0{,}0375h^{-1}$$

Im Beispiel kann der Kunde die absoluten Häufigkeiten direkt angeben. Ist das nicht möglich, können Sie die Exposure ermitteln und Tab. 2 nutzen. Sie finden die Exposure in:

- Gefahren- und Risikoanalyse (HARA)
- VDA 702 Situationskatalog E-Parameter

Schritt 4. $P_{E1\text{-}Fehler}$ schätzen

Eine Verletzung des Sicherheitsziels setzt eine fehlerhafte Berechnung in E1 voraus. Derartige Softwarefehler sind nicht bekannt. Somit ist ein Hardwarefehler notwendig. E1 und E2 laufen auf unabhängiger Hardware. E1 ist in ASIL A implementiert. Somit lesen wir aus Tab. 1 ab:

$$P_{E1-Fehler} = 10^{-6}h^{-1}$$

Wenn verfügbar, können Sie auch das Ergebnis aus der FMEDA heranziehen.

Schritt 5. $P_{E2\text{-}Fehler}$ schätzen

Der E2-Fehler tritt immer dann auf, wenn der E1-Fehler auftritt. Somit gilt:

$$P_{E2-Fehler} = 1$$

6. $P_{t\text{-}kritisch}$ schätzen

Der Fehler ist in den ersten 60ms je 24min der jährlich 1.000 Fahrzyklen kritisch. Somit gilt:

$$P_{t-krit} = \frac{0{,}06s}{3600s/h} * \frac{24}{60}h * \frac{1000}{365*24h} = 7{,}61*10^{-7}h$$

Schritt 6. P_{Gesamt} schätzen

$$= P_{Szenario} * P_{E1-Fehler} * P_{E2-Fehler} * P_{t-kritisch}$$
$$= 0{,}0375h^{-1} * 10^{-6}h^{-1} * 1 * 7{,}61 * 10^{-7}h$$
$$= 2{,}8510^{-14}h^{-1} = 0{,}0000285 * 10^{-9}h^{-1}$$

Schritt 7. Vergleich mit $P_{Tolerabel}$ und entscheiden

$$P_{Gesamt} = 0{,}0000285\ FIT \ll 100\ FIT = P_{Tolerabel}$$

Das Auftreten eines kritischen Fehlers ist sehr unwahrscheinlich und viel kleiner als der Grenzwert. Ein sofortiger Bug Fix ist nicht notwendig.

Risikohinweis: Der Ansatz dient der Entscheidungsfindung. Im Schadenfall zählt stets der Stand der Technik. Es ist niemals unsere Intention, »schlechtere« Technik »schön zu beten«.