FMEA auf einer Seite

FehlerModus- und Effektanalyse

Was es ist

Ein Test fragt: „Tut das System, was es soll?" FMEA fragt vorher: **„Auf welche Weise kann es nicht tun, was es soll? Was passiert dann? Wer merkt es zuerst?"** Kurz: ein Pre-Mortem – systematisch statt aus dem Bauch.

Die Brücke aus der IT

Wer Threat Modeling (STRIDE) oder Failure-Analysen aus dem Betrieb kennt, kennt das Prinzip. Der Unterschied: Bei FMEA kommt die Gefahr nicht nur vom Angreifer, sondern von jeder Abweichung – Bauteil, Bedingung, Bedienung, Umgebung.

Fünf Schritte

1. **Struktur:** System zerlegen wie im Komponentendiagramm – System → Komponente → Merkmal.
2. **Merkmal:** Jede Komponente bekommt ihre prüfbaren Eigenschaften, z. B. „Ablaufzeit des Tokens wird geprüft".
3. **Fehler = Verneinung des Merkmals:** „Ablaufzeit wird nicht geprüft". Dann die Kette bauen: Ursache → Fehler → Folge → … → Folge für Kunde oder System.
4. **Bewerten:** drei Zahlen von 1 bis 10.
   - **B – Bedeutung:** Wie schlimm ist die oberste Folge der Kette?
   - **A – Auftreten:** Wie wahrscheinlich ist die Ursache?
   - **E – Entdeckung:** Wie sicher fällt der Fehler auf, bevor er Schaden macht?
5. **Maßnahmen:** Vermeiden (anders auslegen) oder Entdecken (früher merken). Was zuerst drankommt, sagt die Aufgabenpriorität Hoch / Mittel / Niedrig aus einer festen Tabelle.

Beispiel

Komponente	Merkmal	Fehler	Ursache	Folge (bis ganz oben)	B	Vermeidung	Entdeckung
Token-Validierung	Ablaufzeit des Tokens wird geprüft	Ablaufzeit wird nicht geprüft	Prüfung fehlt nach Library-Update	Abgelaufene Sitzung bleibt gültig → Fremder sieht Kundendaten	9	Library mit Pflicht-Prüfung der Ablaufzeit; als Anforderung in der Spec	Test „abgelaufenes Token → 401" in der Pipeline

Drei Regeln zum Merken

- **Die Bedeutung kommt von oben.** Eine fehlende Prüfung ist für sich harmlos. Sie ist so schlimm wie das Schlimmste, wozu sie führen kann.
- **Vermeiden ist Design, Entdecken ist Sensorik.** Die Entdeckung gehört an die erste Folge, nicht ans Ende der Kette.
- **Nicht multiplizieren.** B × A × E (die alte Risikoprioritätszahl) versteckt schwere Fehler hinter kleinen Zahlen. Hohe Bedeutung zieht immer zuerst.
  Die Aufgabenpriorität (AP) ersetzt seit dem AIAG-VDA-Handbuch 2019 die Risikoprioritätszahl. Sie ordnet jeder Kombination aus B, A und E über eine feste Tabelle die Stufe Hoch, Mittel oder Niedrig zu, statt die drei Werte zu multiplizieren. Dabei wiegt die Bedeutung am stärksten, danach das Auftreten, zuletzt die Entdeckung. Bei „Hoch" muss das Team Maßnahmen festlegen oder schriftlich begründen, warum es keine gibt; bei „Mittel" sollte es das tun; bei „Niedrig" kann es das tun.

Was FMEA nicht ist

Ein Risiko-Register mit Bauchzahlen und kein Abnahmedokument fürs Qualitätsmanagement.
FMEA ist das Werkzeug dessen, der das System baut.