SIEMENS

Transportation Systems

Rail Automation

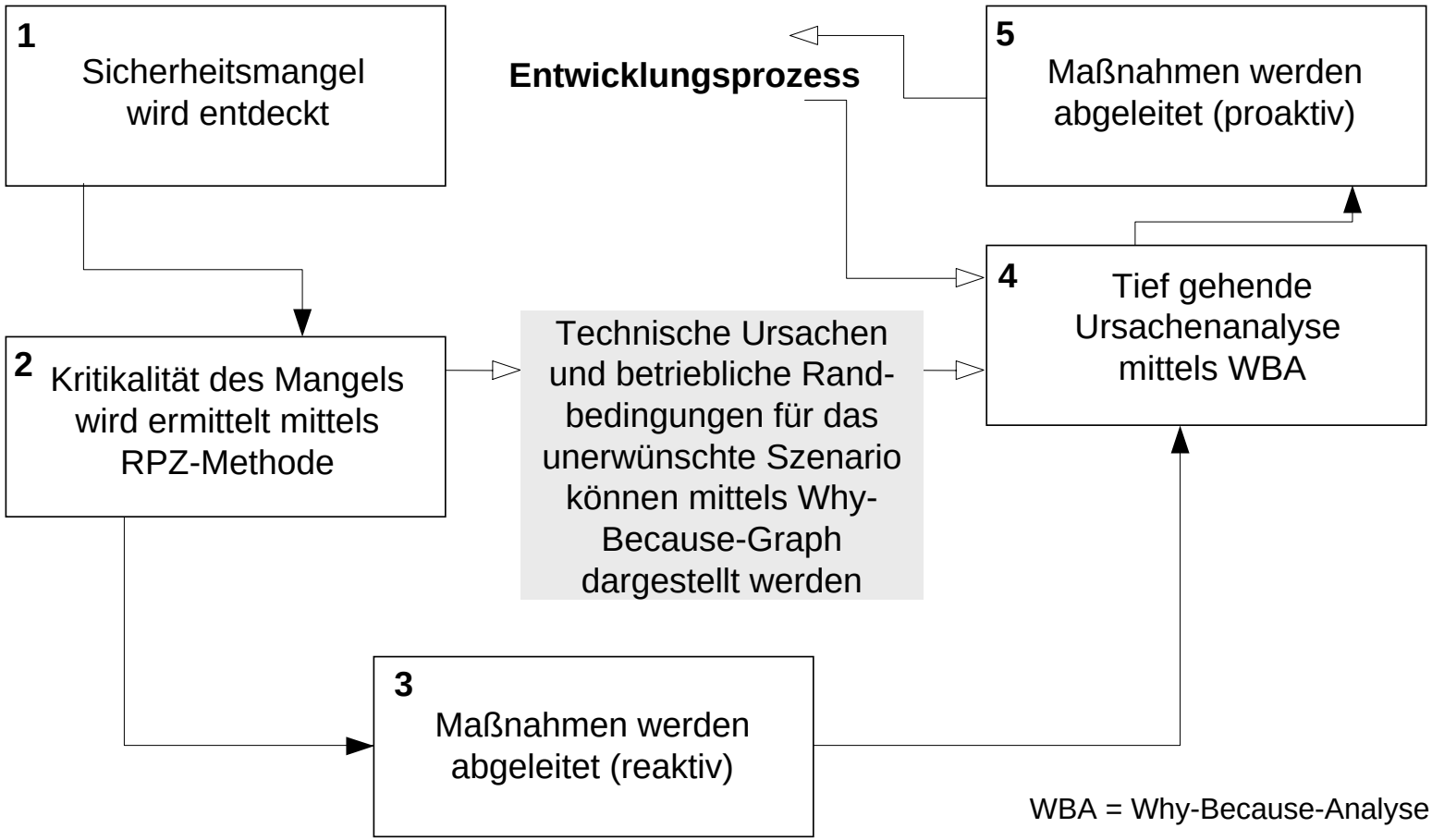
Einbinden der Why-Because-Analyse bei der Untersuchung von Produktsicherheitsmängeln

Ernesto De Stefano

Stand: 06/06/2005

Untersuchung von Produktsicherheitsmängeln

Wann wird die Why-Because-Analyse eingesetzt?



Kritikalitätsermittlung
Was ist die RPZ-Methode?

- RPZ ist die Abkürzung für Risikoprioritätszahl.
- Mit der RPZ-Methode kann ermittelt werden, wie kritisch ein Produktsicherheitsmangel (PSM) ist.

  Ein PSM liegt vor, wenn eine sicherheitsgerichtete Funktion nicht anforderungsgemäß erbracht wird und nicht ausgeschlossen werden kann, dass das Produkt mit Rechtsgütern Dritter in Berührung kommen kann.
- Die für TS RA entwickelte RPZ-Methode ist aus der FMECA-Methode (Failure Mode, Effects and Criticality Analysis) abgeleitet, die insbesondere in der Automobilindustrie ein bewährtes Verfahren für qualitative Risikobewertungen ist.
- Die Anwendung der RPZ-Methode auf PSM wurde bei Siemens Transportation Systems – Rail Automation – Research & Development (TS RA RD) seit 12/2003 pilotiert, und seit 08/2004 wird die Methode bei TS RA auf alle PSM angewendet.

Ziele der RPZ-Methode

Was soll mit der Methode erreicht werden? (1/2)

Eine einheitliche und risikobasierte Vorgehensweise soll:

- innerhalb eines Tages Ergebnisse liefern, aus denen zu ersehen ist, wie kritisch der Mangel ist,
- eine sachlich begründete Entscheidung ermöglichen, mit welcher Dringlichkeit Maßnahmen zum Beheben des Mangels der in Betrieb befindlichen Produkte durchgeführt werden müssen,
- das Ableiten von in ihrer Tragweite vergleichbaren Maßnahmen für ähnlich kritische Produktsicherheitsmängel ermöglichen,
- der Zulassungsbehörde eine klare Darstellung des Mangels und seiner Kritikalität bereitstellen und als Entscheidungsgrundlage für die weitere Vorgehensweise dienen,

Ziele der RPZ-Methode

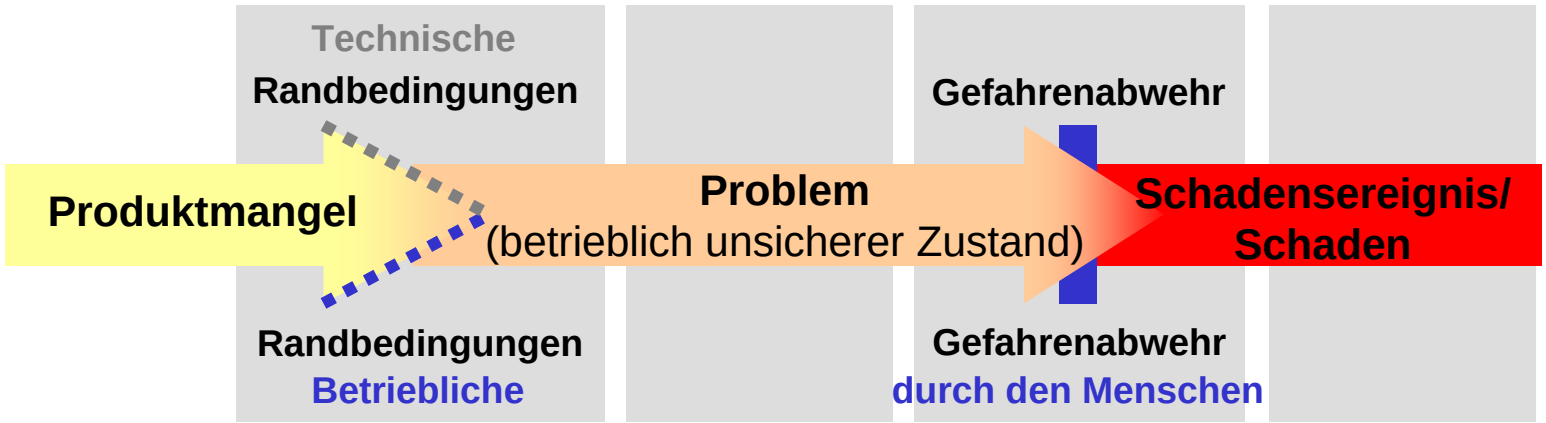
Was soll mit der Methode erreicht werden? (2/2)

Eine einheitliche sowie risikobasierte Vorgehensweise soll:

- eine solide Grundlage für eine tief gehende Ursachenanalyse schaffen,
- einen Vergleich der Kritikalität der Produktsicherheitsmängel über deren Risikoprioritätszahl erlauben,
- Metriken liefern, die erlauben, die Entwicklung der Sicherheit unserer Produkte zu verfolgen.

Das Grundmodell

Welche Bereiche werden berücksichtigt?



Ablauf der RPZ-Ermittlung

Wie ist die Vorgehensweise?

Schritt 1: Problem
- Problembeschreibung

Schritt 2: Randbedingungen
- Darstellung der Randbedingungen
- Einschätzung der Wahrscheinlichkeit, mit der die Randbedingungen eintreten

Schritt 3: Schaden
- Darstellung des Schadensereignisses
- Einschätzung der Anzahl Betroffener, des Unfalltyps und der maßgeblichen Geschwindigkeit

Schritt 4: Gefahrenabwehr
- Darstellung der Möglichkeiten zur Gefahrenabwehr
- Einschätzung der Wirksamkeit der Gefahrenabwehr

Parameterwert Häufigkeit (h)

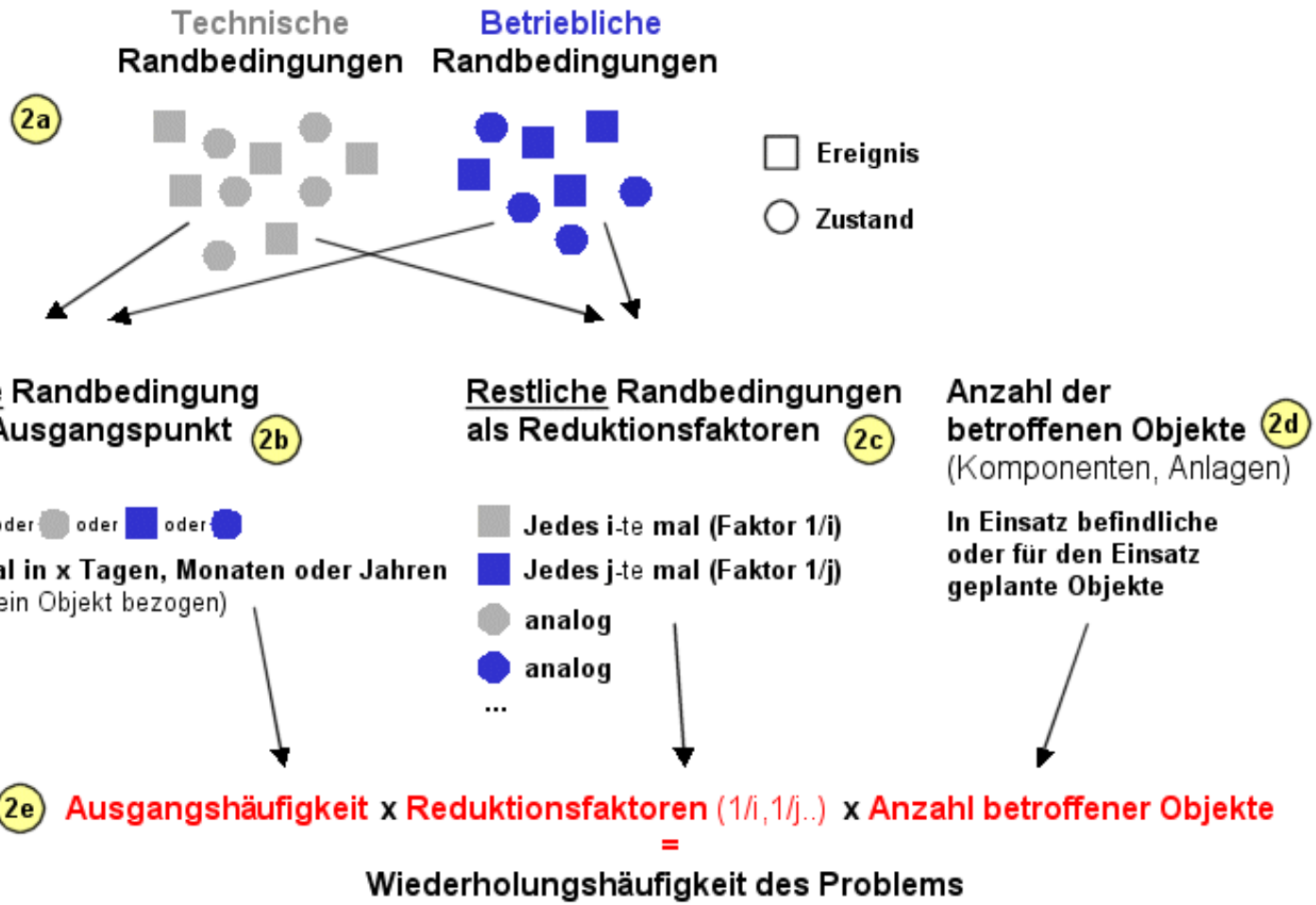
+

Parameterwert Schadensausmaß (s)

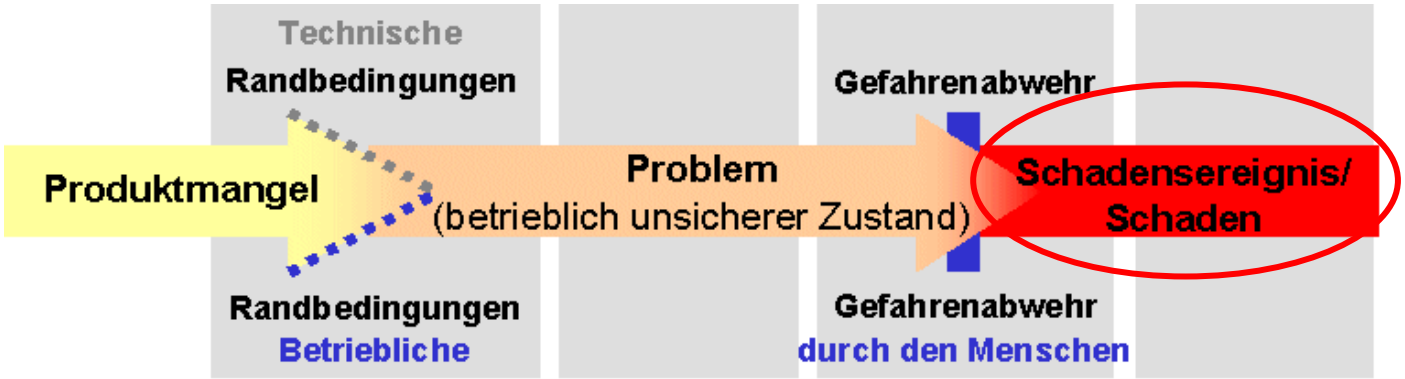
+

Parameterwert Gefahrenabwehr (g) **= RPZ**

Ablauf der RPZ-Ermittlung
Häufigkeit (Schritte 2a–e)



Ablauf der RPZ-Ermittlung
Parameter Schadensausmaß



Betrachtungseinheit ist ein Zug

Tabellenwerte der folgenden Subparameter gehen ein:

Unfalltyp (T) + Anzahl Betroffener (A) + Maßgebliche Geschwindigkeit (V)

Schadensausmaß (S) = T + A + V

Fiktives Beispiel
Randbedingungen

- **Technische Randbedingung TR1:**
  Ausfall Hauptfaden Rotlampe. Der Mangel besteht in diesem Beispiel darin, dass die Fadenüberwachung den Ausfall der Lampe nicht erkennt und nicht auf den Nebenfaden umgeschaltet wird.

- **Betriebliche Randbedingung BR1:**
  Eine Zugfahrt (Zug A) findet statt, die das Signal als deckendes Signal benötigt.

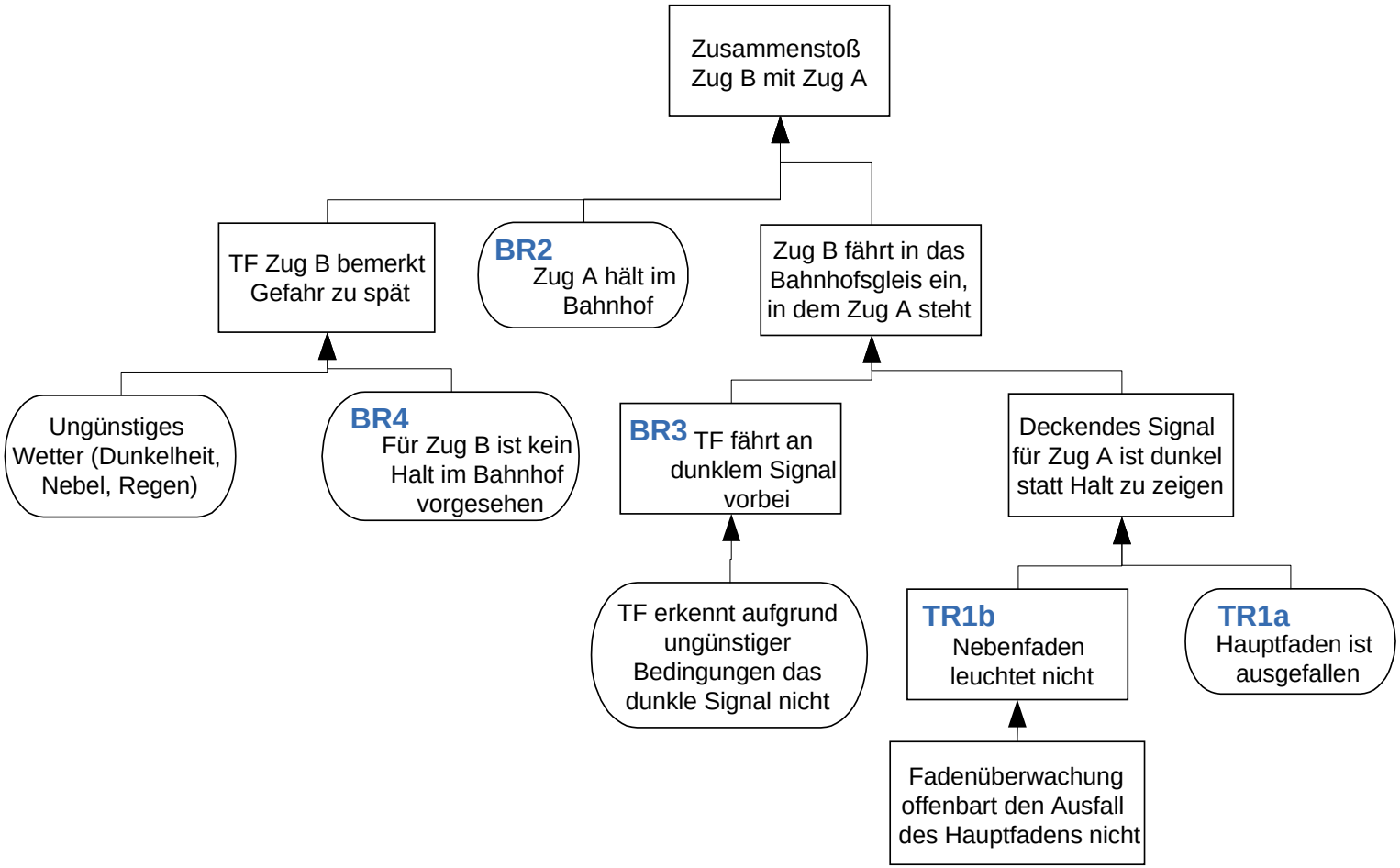
- **Betriebliche Randbedingung BR2:**
  Zug A hält im Bahnhof.

- **Betriebliche Randbedingung BR3:**
  Triebfahrzeugführer (Zug B) fährt an dunklem Signal vorbei.

- **Betriebliche Randbedingung BR4:**
  Für Zug B ist kein Halt im Bahnhof vorgesehen.

Fiktives Beispiel

Randbedingungen als Why-Because-Graph



TF = Triebfahrzeugführer

Umgang mit der ermittelten RPZ

Hilft die RPZ als absolute Zahl weiter?

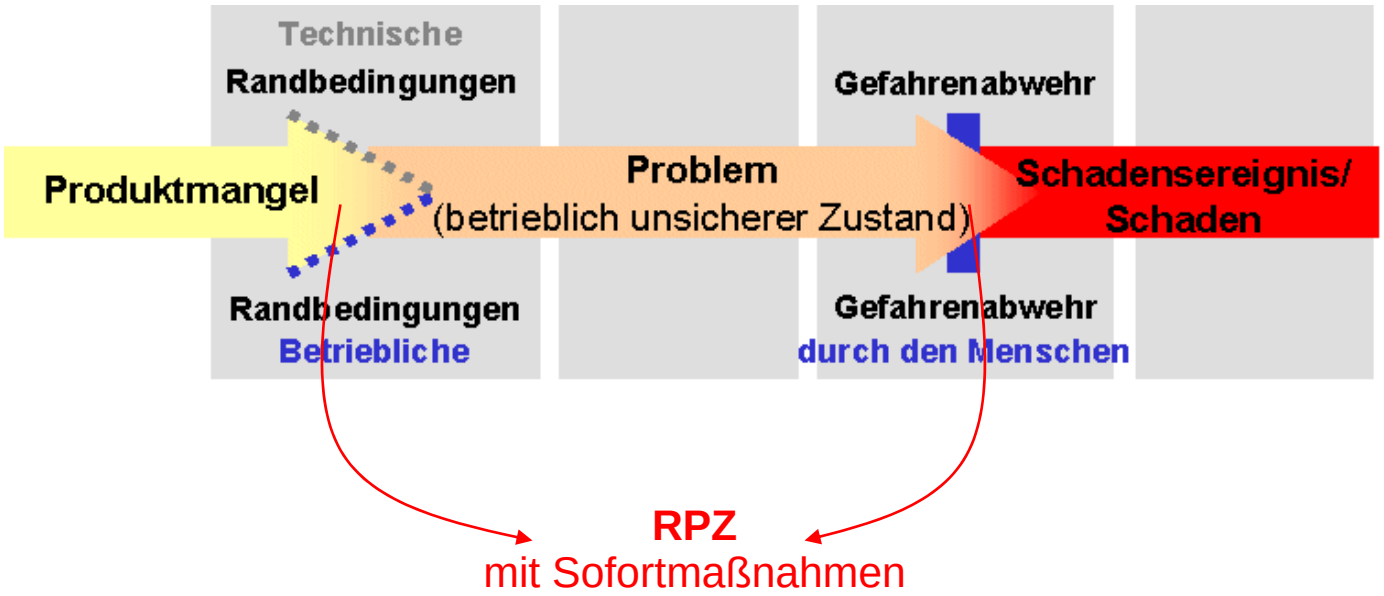
- Die absolute Höhe der Kritikalität eines PSM (RPZ mit Mangel) ist für sich allein gesehen nicht geeignet, sich über Dringlichkeit und Ausmaß einzuleitender Maßnahmen klar zu werden. Benötigt wird noch das Wissen, wie groß die Erhöhung des Risikos gegenüber dem Produkt ohne Mangel ist.

- Das bei der Ermittlung der RPZ mit Mangel betrachtete Schadensereignis ist auch bei dem Produkt ohne Mangel denkbar. Jedoch müssten noch weitere Randbedingungen vorliegen, damit dieses auch eintritt. Betrachtet man diese Randbedingungen, kann eine RPZ des Produktes ohne Mangel für dieses Schadensereignis ermittelt werden (RPZ ohne Mangel).

- Zusammen mit dem absoluten Wert RPZ mit Mangel liefert die Differenz RPZ mit Mangel – RPZ ohne Mangel eine Entscheidungshilfe, ob und in welchem Ausmaß dem Betreiber Sofortmaßnahmen vorgeschlagen werden.

Umgang mit der ermittelten RPZ

Welche Auswirkungen haben Maßnahmen auf die RPZ?



Obwohl die Wirksamkeit von Sofortmaßnahmen in Form einer Reduktion der RPZ dargestellt und bewertet werden kann, ändert sich dadurch nicht die RPZ des eigentlichen Produktsicherheitsmangels, sondern bestenfalls die Dringlichkeit einzuleitender Maßnahmen für dessen Behebung.

Referenzen

Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), IEC 60812

Bowles, J.: An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis, Proc. RAMS2003, Tampa, January 2003

Bowles, J.: Failure Modes, Effects, And Criticality Analysis: What It Is And How To Use It, Tutorial, RAMS2000

Braband, J.: Improving the Risk Priority Number Concept, Journal of System Safety, 3, 2003, 21-23

Potential Failure Mode and Effects Analysis In Design (Design FMEA) and Potential Failure Mode and Effects Analysis In Manufacturing and Assembly Processes (Process FMEA), Reference Manual, Society of Automotive Engineers, Surface Vehicle Recommended Practice, J1739, July 1994.