J. Michael, J. Pfeiffer, A. Wortmann (Hrsg.): Software Engineering 2022 Workshops,
80 Digital Library, Gesellschaft für Informatik 2022

# Erweiterung von Gefahren- und Risikoanalysen der Funktionalen Sicherheit um Aspekte der Produktsicherheit nach ISO 12100

Moritz Emig[1], Pierre Metz[2] und Ralf Reißing[3]

**Abstract:** Bei der Brose Fahrzeugteile SE & Co. KG wird eine Gefährdungs- und Risikoanalyse (HARA) nach der ISO 26262 [DI18] angewandt. Diese Analyse betrachtet zufällige oder systematische Fehlfunktionen, die durch E/E-Probleme (Elektrik/Elektronik) verursacht werden. Die HARA soll nun um die Produktsicherheit (ProSi) erweitert werden. Diesbezüglich existiert bereits ein Brose-interner Ansatz, mit welchem allerdings nur funktionale Aspekte ermittelbar sind. Bei der ProSi-HARA sollen allerdings auch nicht-funktionale Gefährdungen (NFH) berücksichtigt werden.

Damit bei der ProSi-HARA-Durchführung so viele NFH wie möglich ermittelt werden können, wurde als Hilfsmittel eine Checkliste generiert. Diese basiert auf der Tabelle B.1 der ISO 12100 [DI11], die sich mit der Sicherheit von Maschinen beschäftigt. Anschließend wurden drei alternative Konzepte zur Integration der Checkliste in die ProSi-HARA erarbeitet. Die Konzepte wurden in einem Pilotprojekt bei Brose erprobt. Dabei hat sich eines der Konzepte klar mit dem besten Aufwand-Nutzenverhältnis durchgesetzt. Mittels dieser Vorgehensweise konnten mit der Checkliste eine Vielzahl eigenständiger NFH identifiziert werden, die mit der herkömmlichen HARA nicht erkannt worden wären. Mit eigenständig sind hier NFH gemeint, die nicht in Zusammenhang mit funktionalen Fehlern oder Use Cases (funktionalen Anwendungsfälle) stehen.

**Keywords:** Gefährdungs- und Risikoanalyse, HARA, Produktsicherheit, ProSi-HARA, nicht-funktionale Gefährdungen

## 1 Hintergrund

Die bei Brose verwendete HARA auf Basis der ISO 26262 berücksichtigt lediglich auftretende Gefährdungen, welche auf zufälligen bzw. systematischen funktionalen Fehlern (Functional Failures – FF) basieren. Zusätzlich werden ebenfalls nominale Use Cases (UC) wie auch Misuse Cases (MUC – bewusst falsche Verwendung eines Systems) eines betrachteten Systems miteinbezogen, die in gewissen Betriebsszenarien für Benutzer oder Passanten gefährlich werden können. Damit jedoch bei der Durchführung der HARA gleichermaßen NFH ermittelt werden können, soll die herkömmliche HARA um nicht-E/E-bedingte Produktfehlfunktionen erweitert werden. Die Herausforderung hierbei ist,

[1] Robert Bosch GmbH, FCEV, Robert-Bosch-Straße 40, 96050 Bamberg, moritz.emig@de.bosch.com
[2] Brose Fahrzeugteile SE & Co. KG, Bamberg, ZVE-EP, Berliner Ring 1, 96052 Bamberg, pierre.metz@brose.com
[3] Hochschule Coburg, Fakultät Maschinenbau und Automobiltechnik, Friedrich-Streib-Straße 2, 96450 Coburg, ralf.reissing@hs-coburg.de

dass aktuell keine normative Definition für den Begriff „Produktsicherheit“ existiert. Daher besteht kein Stand der Technik. Aus diesem Grund wird bei Brose die Produktsicherheit als proprietärer Oberbegriff für nachfolgende überlappende Teildomänen definiert:

- Gebrauchssicherheit
- Elektrische Sicherheit
- Mechanische Sicherheit
- Stoffliche Aspekte (z.B. chemische Reaktionen)
- Funktionale Sicherheit
- SOTIF (ISO 21448)

Da der Bereich potenzieller NFH sehr weitläufig und vielfältig erscheint, sollte daher während einer Masterarbeit ein Konzept erarbeitet werden, das die NFH-Ermittlung erleichtert. Außerdem soll das Konzept eine möglichst hohe Fehlervollständigkeit gewährleisten und zusätzlich wirtschaftlich sein. Als mögliche Idee wurde verfolgt, die Tabelle B.1 des Annex B der ISO 12100 [DI11] als Basis heranzuziehen, da diese eine Vielzahl an potenziell gefährlichen Aspekten aufzeigt, wie nachfolgend beispielhaft dargestellt:

| **Kategorie** | **Gefährdung** | **Verletzungsfolge** |
|---|---|---|
| Mechanik | Scharfe Kanten | Abscherung, Schneiden |
| Akustik | Hohe Frequenzen | Desorientierung |
| Thermik | Explosion | Verbrennung |

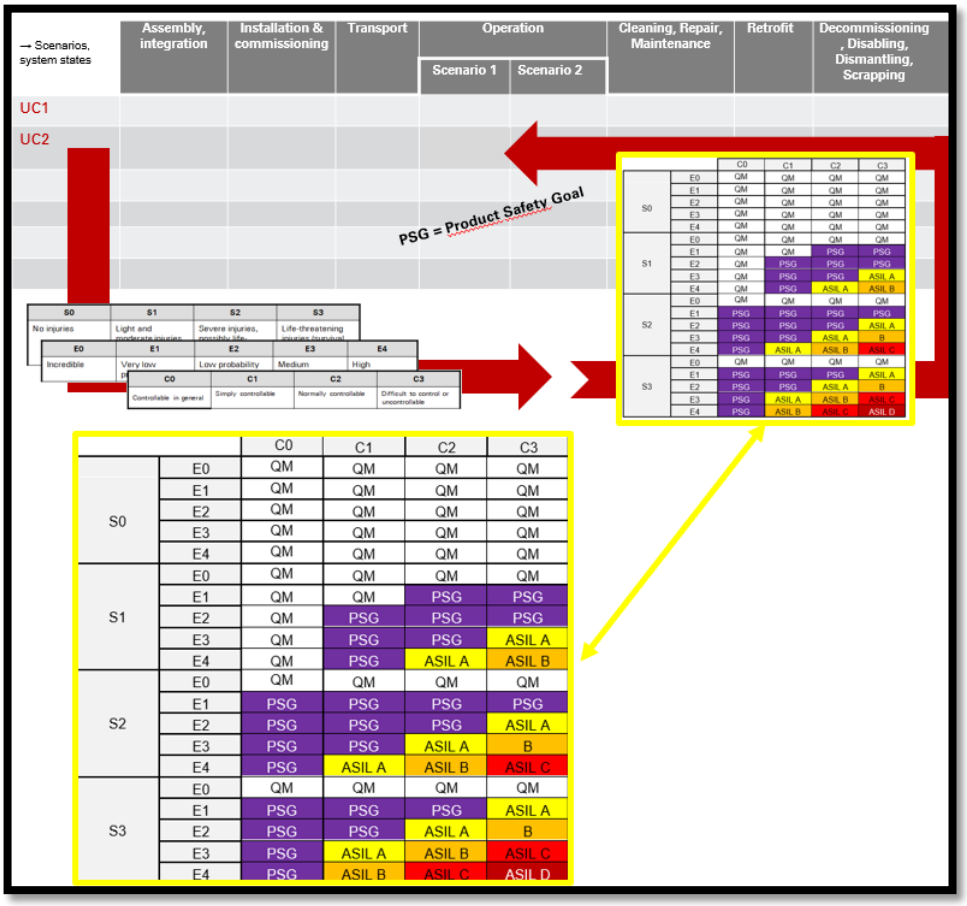
Da die Tabelle B.1 in Bezug zur Maschinensicherheit steht, musste diese an den Kontext der Produktentwicklung in der Automobilindustrie angepasst werden. Hierbei ist zu erwähnen, dass Brose bereits eine vorläufige, aber unvollständige ProSi-HARA generierte. Daher musste die angepasste automobilrelevante Tabelle (als Checkliste Annex B Automobil) ebenfalls in diese vorläufige ProSi-HARA integriert werden.

## 2 ProSi-HARA

Bei der ProSi-HARA spielen folgende Aspekte eine Rolle: Use Cases (UC), Functional Failures (FF), Misuse Cases (MUC), Mutual Functional Dependencies (FD) und Commanded Failures (CF). Auf diese funktionalen Fälle wird im folgenden Kapitel detailliert eingegangen.

## 2.1 Use Cases

Brose verwendet sowohl für die Durchführung der HARA nach ISO 26262 als auch für die vorläufige ProSi-HARA einen Matrix-Ansatz (vgl. Abbildung 1). Hierbei werden auf der y-Achse alle Fälle (z.B. UC, FF, MUC, NFH) aufgeführt.




| | | C0 | C1 | C2 | C3 |
|---|---|---|---|---|---|
| S0 | E0 | QM | QM | QM | QM |
| | E1 | QM | QM | QM | QM |
| | E2 | QM | QM | QM | QM |
| | E3 | QM | QM | QM | QM |
| | E4 | QM | QM | QM | QM |
| S1 | E0 | QM | QM | QM | QM |
| | E1 | QM | QM | PSG | PSG |
| | E2 | QM | PSG | PSG | PSG |
| | E3 | QM | PSG | PSG | ASIL A |
| | E4 | QM | PSG | ASIL A | ASIL B |
| S2 | E0 | QM | QM | QM | QM |
| | E1 | PSG | PSG | PSG | PSG |
| | E2 | PSG | PSG | PSG | ASIL A |
| | E3 | PSG | PSG | ASIL A | B |
| | E4 | PSG | ASIL A | ASIL B | ASIL C |
| S3 | E0 | QM | QM | QM | QM |
| | E1 | PSG | PSG | PSG | ASIL A |
| | E2 | PSG | PSG | ASIL A | B |
| | E3 | PSG | ASIL A | ASIL B | ASIL C |
| | E4 | PSG | ASIL B | ASIL C | ASIL D |

Abbildung 1: Schematische Darstellung der Brose-HARA-Matrix, inklusive der Beurteilungsparameter (S, E, C – unten links) und einer Matrix zur Bestimmung der ProSi-Integrity Level (unten), nach [ME21]

Im Gegenzug sind auf der x-Achse sämtliche Systemzustände beziehungsweise Szenarien im Lebenszyklus eines Systems dargestellt. Beispiele hierfür sind:

- Transport
- Betrieb
- Instandhaltung, Wartung, Reparatur
- Montage
- Demontage
- Verschrottung

Mit Bezug auf die Vorgehensweise sollen nach der Festlegung der Systemzustände (x-Achse) zu Beginn die UC bestimmt werden [EM21a]. Das ProSi-HARA-Team muss sich hierbei an den wesentlichen Funktionen beziehungsweise dem Systemeinsatz orientieren. Wie in Abbildung 1 zu erkennen, werden die UC untereinander aufgeführt, wodurch in Kombination mit den Systemzuständen mehrere Zellen in der Matrix entstehen. Jede Zelle kann, falls diese Kombination aus UC und Systemzustand technisch möglich ist, somit eine potenzielle Gefährdung darstellen. Analog zur HARA nach der ISO 26262 muss jede Zelle mittels folgender Parameter einzeln beurteilt werden. Dadurch ist die potenzielle Gefährdung, die durch eine Zelle dargestellt werden kann, evaluierbar.

1. Severity (S): Schweregrad der Verletzung
   ➔ S0 (keine Verletzung) – S3 (lebensgefährlich)
2. Exposure (E): Wahrscheinlichkeit, dass eine Person der Gefährdung ausgesetzt ist
   ➔ E0 (unwahrscheinlich) – E4 (hohe Wahrscheinlichkeit)
3. Controllability (C): Kontrollierbarkeit der Gefahrensituation
   ➔ C0 (generell kontrollierbar) – C3 (schwer kontrollierbar)

Basierend auf der S-, E-, C-Einschätzung muss anschließend jede Gefährdung (hier: resultierend aus den UC) mit Hilfe der ProSi-Integrity-Level-Matrix (vgl. Abbildung 1 unten/mittig rechts) eingestuft werden [EM21a]. Der Unterschied der ProSi-Integrity-Level-Matrix zur herkömmlichen Automotive-Safety-Integrity-Level-Matrix nach ISO 26262 besteht darin, dass eine neue Art eines Sicherheitsziels resultieren kann. Dies ist, wie in Abbildung 1 zu erkennen, das Product Safety Goal (PSG). Wird einer Gefährdung ein farbiges Feld (PSG oder ASIL A-D – vgl. Abbildung 1) zugewiesen, so müssen daraus Risikoreduzierungsmaßnahmen abgeleitet werden. Alle weißen QM-Felder (vgl. Abbildung 1) benötigen hingegen keine weiteren Maßnahmen.

## 2.2 Functional Failures

Der nächste Schritt bei der Durchführung der ProSi-HARA ist die Ermittlung der FF [EM21a]. Es kann eine Vielzahl der potenziellen FF von den UC abgeleitet werden (siehe Abbildung 2). Hierzu wird eine Tabelle mit Guide Words und dessen Bedeutungen herangezogen. Diese Vorgehensweise ist an dem HAZOP-Verfahren nach ISO DIN EN 61882 [DI17] angelehnt.

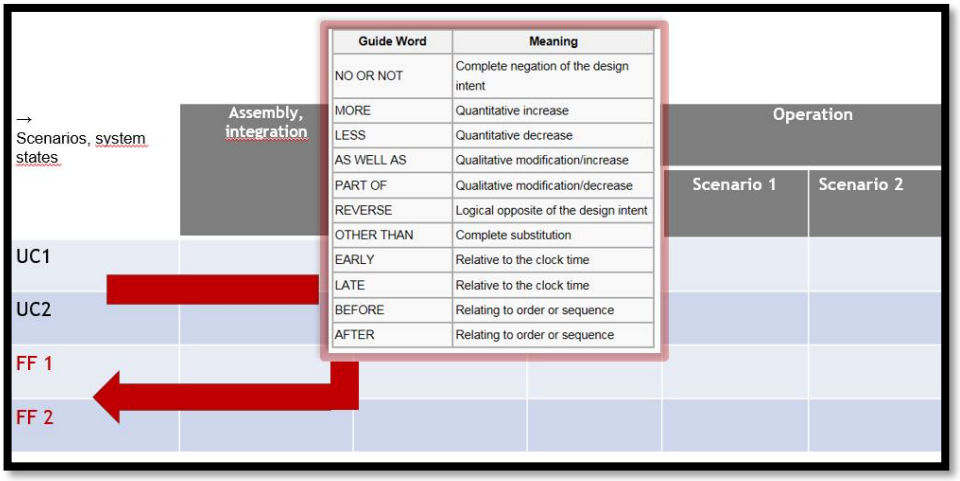



Abbildung 2: Schematische Darstellung der Ableitung der FF von den UC mit Hilfe einer Guide Word-Tabelle [EM21b]

Ein Beispiel für diese Vorgehensweise ist nachfolgend anhand eines E-Bikes im Systemzustand Betrieb dargestellt [EM21a]:

| **UC** | **Guide Word** | **FF** |
|---|---|---|
| Einstellung einer E-Motor-Unterstützungsstufe. Benutzer tritt in die Pedale. E-Motor unterstützt den Benutzer beim Beschleunigen des E-Bikes oder beim Halten der Geschwindigkeit. | NO OR NOT | Keine E-Motor-Unterstützung beim Beschleunigen oder Halten der Geschwindigkeit. |

Nach der Identifizierung der FF müssen die daraus resultieren Gefährdungen in den Betriebsszenarien / Systemzuständen (Zellen in der ProSi-HARA-Matrix) analog zu Abschnitt 2.1 UC mit S, E und C bewertet werden (vgl. Abbildung 1) [EM21a]. Das Gleiche gilt für die Zuweisung der Sicherheitsziele. Alle nachfolgenden Fälle (z.B. MUC oder NFH) werden nach dem gleichen Schema beurteilt bzw. eingestuft.

## 2.3 Misuse Cases, Mutual Functional Dependencies und Commanded Failures

Weitere funktionale Fälle, die durch das ProSi-HARA-Team zu ermitteln sind, sind die MUC, FD und die CF [EM21a]. In Bezug auf die herkömmliche bei Brose verwendete HARA nach ISO 26262 werden mit den FD und den CF zwei weitere Gefährdungsarten berücksichtigt. Nachfolgend sind die drei funktionalen Gefährdungsarten erläutert.

MUC: Als MUC werden bewusst falsche Handhabungen eines Systems durch einen Benutzer oder Passanten bezeichnet [EM21a]. Dadurch resultieren Gefährdungen durch vorhersehbaren Fehlgebrauch eines Systems.

FD: FD sind Gefährdungen, die durch Abhängigkeiten von mehreren Komponenten eines Systems auftreten können. Ein Beispiel hierfür ist die Vernachlässigung der Trägheitseigenschaften beim automatischen Heckklappenschließsystem von Brose [ME21]. Das System weist zwei Softwarefunktionen auf. Die Erste ist das Soft-Closing zum sanften, kraftschlüssigen Schließen der Heckklappe. Die zweite Funktion ist der Einklemmschutz. Am Ende des automatischen Schließvorgangs passiert die Heckklappe einen Sensor, der das sanfte Schließen initiiert. Ist im Schließbereich-Ende beispielsweise eine Hand platziert (z.B. spielendes Kind), muss der Einklemmschutz auslösen und die Heckklappe stoppen beziehungsweise reversieren. Schwingt die Heckklappe aufgrund ihrer Trägheit nach, kann diese den Soft-Closing-Sensor passieren. Dadurch startet das Soft-Closing und die Hand wird eingeklemmt.

CF: Die CF sind Gefährdungen, die durch externe inkorrekte oder fehlende, meist elektrische Signale verursacht werden [EM21a]. Dies ist möglich, wenn das System nicht nachvollziehen kann, ob die Signale von außerhalb seines Scopes korrekt beziehungsweise plausibel sind.

## 3 Checkliste Annex B Automobil

Die aus der Tabelle B.1 des Annex B der ISO 12100 abgeleitete Checkliste Annex B Automobil ist eine Tabelle, die potenzielle nicht-funktionale Gefährdungen eines Systems im Automobilbereich ausweist [EM21a]. Diese Gefährdungen sind zur Steigerung der Übersichtlichkeit kategorisiert (siehe Abbildung 3).

| Nr. | Typ oder Gruppe | Gefahren durch |
|---|---|---|
| 1 | **Mechanische Gefahren** | - Oberflächen (z.B. kantig; scharf; spitz; eckig; rau; glatt; rutschig)<br>- Schwerkraft<br>- Bewegliche Elemente (Fallhöhe; „Spiel“ / Toleranzen; fallen, gleiten, rollen, lösen, umherfliegen)<br>- Hoher Druck<br>- Instabilität; elastische Elemente<br>- Gespeicherte Energie |
| 2 | **Elektrische Gefahren** | - Elektrotechnische Phänomene (elektromagnetisch, elektrostatisch)<br>- Unter Spannung stehende Teile<br>- Überspannung / Überlast<br>- Lichtbogen |
| 3 | **Thermische Gefahren** | - Explosion / Flamme<br>- Objekttemperatur / Strahlung<br>- Kälteschäden |
| 4 | **Gefahren durch Lärm** | - Bewegende Teile<br>- Schabende Oberfläche (z.B. zu geringe Toleranzen, Verschleiß)<br>- Unwucht bei Rotationsteile (z.B. zu große Toleranzen, Verschleiß) |

Abbildung 3: Ausschnitt aus der Checkliste Annex B Automobil [EM21c]

Aufgrund der Unterschiede in den Einsatzgebieten erfuhr die Checkliste mehrere Modifikationen [EM21a]. Zum einen mussten Punkte gelöscht werden, die im Normalfall bei Systemen im Automobilbereich nicht zu Gefährdungen führen (z.B. hat Sauerstoffmangel typischerweise keinen Einfluss auf Fahrerassistenzsysteme). Ebenso waren Tabellenpunkte zu streichen, die bereits im Zusammenhang mit UC, MUC oder FF betrachtet wurden (z.B. S-Bewertung), um Redundanz zu vermeiden. Zum anderen mussten Punkte hinzugefügt werden, die zwar nicht für die Sicherheit der Maschinen, aber für die Sicherheit im Automobil durchaus relevant sind (z.B. chemische Einflüsse, mechanischer Druck). Des Weiteren wurden zwei zusätzliche Gefahrengruppen aufgenommen:

- Gefahren durch gesetzliche Einschränkungen
- Gefahren in Verbindung mit informationstechnologischen Aspekten

Weitere Modifikationen haben im Zusammenhang mit dem Tabellenformat und den Zusatzinformationen stattgefunden [EM21a]. Hierbei wurde beispielsweise die Spalte mit potenziellen Verletzungen gelöscht, da im Normalfall die ProSi-HARA-Teammitglieder (Fachleute für deren Teilbereich) in der Lage sein sollten Folgen aus auftretenden Gefährdungen herzuleiten. Diese Anpassungen dienten zur Steigerung der Übersichtlichkeit und somit zur verbesserten Anwendbarkeit der Checkliste.

# 4 Integration der Checkliste in die ProSi-HARA

Im vierten Kapitel werden potenzielle Konzepte dargestellt, die eine reibungslose Integration der Checkliste in die bestehende ProSi-HARA gewährleisten. Damit die Checkliste als Werkzeug der ProSi-HARA bei der Ermittlung der NFH unterstützen kann, wurden drei Konzepte beziehungsweise Anwendung der Checkliste erarbeitet [EM21a].

**Konzept 1: Eine S-Detaillierung der UC, FF, MUC, FD, CF durchführen [EM21a]:** Hierbei resultiert eine unterschiedliche Betrachtung der Schweregrade aufgrund von veränderten nicht-funktionalen Eigenschaften, wie z.B. FF: Zerbersten eines Verdichters durch zu hohen Druck. In diesem Fall können durch scharfe oder heiße Splitter verschiedene Verletzungsschweregrade auftreten. Die NFH nach Konzept 1 werden somit bei der Beurteilung der funktionalen Fälle (UC, MUC, FF…) im Zuge der S-Bewertung berücksichtigt. Aus diesem Grund sind die NFH lediglich bei der S-Argumentation zu dokumentieren und erhalten keinen Eintrag in die ProSi-HARA-Matrix.

**Konzept 2: Eigenständige NFH ermitteln [EM21a]:** Identifizierung von NFH, die auftreten können, jedoch nicht im Zusammenhang mit UC, FF, MUC, FD oder CF stehen. Das bedeutet, diese Gefährdungen sind schwer zu ermitteln, da diese nicht von den nominalen Funktionen oder von Fehlfunktionen abgeleitet werden können. Hierbei ist außerdem zu erwähnen, dass NFH nach Konzept 2 aufgrund ihrer Eigenständigkeit einen separaten Eintrag in die ProSi-HARA-Matrix (siehe Abbildung 4) erhalten. Daher müssen die NFH in jedem Betriebsszenario beurteilt werden (vgl. Abschnitt 2.1).

Somit werden nach Konzept 2 auch NFH mit Hilfe der Checkliste ermittelt. Allerdings stehen die NFH nach Konzept 1 in Bezug zu den UC, FF, MUC, FD und CF, die NFH nach Konzept 2 jedoch nicht. Daraus resultiert der Unterschied, dass die NFH nach Konzept 2 einen separaten Eintrag in der ProSi-HARA-Matrix erhalten, wohingegen die NFH nach Konzept 1 lediglich in der S-Argumentation eines funktionalen Falles dokumentiert werden.

**Konzept 3: Sowohl eine S-Detaillierung durchführen als auch eigenständige NFH ermitteln [EM21a]** (kombinierter Ansatz aus den Konzepten 1 und 2). Bei der Vorgehensweise nach Konzept 3 werden mit Hilfe der Checkliste einerseits NFH ermittelt, die eine S-Detaillierung von funktionalen Fällen zur Folge haben und andererseits eigenständig sind. Daraus resultieren sowohl neue nicht-funktionale Einträge in der ProSi-HARA-Matrix, als auch die Berücksichtigung von NFH bei der S-Argumentation und S-Dokumentation der funktionalen Fälle.

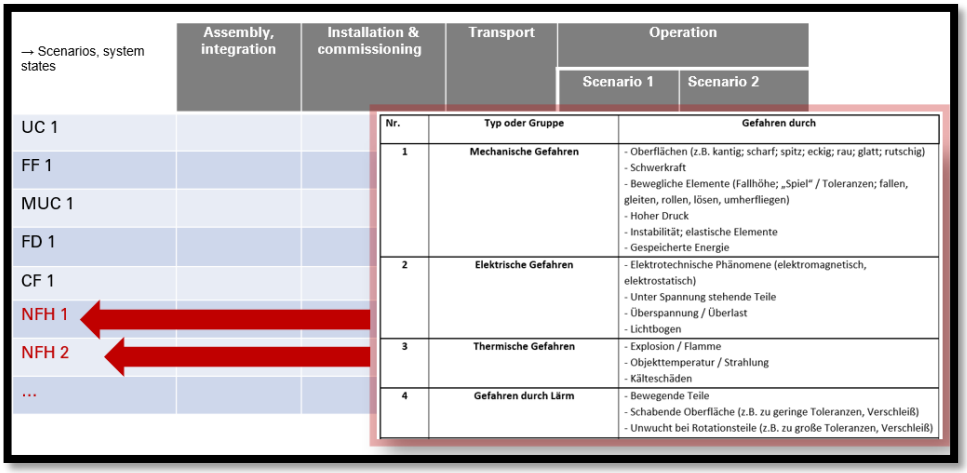



Abbildung 4: Schematische Darstellung von Konzept 2 zur Integration der Checkliste Annex B Automobil in die ProSi-HARA [EM21b]

Zur Auswahl des am besten geeigneten Konzeptes wurden alle drei Konzepte bei Brose in einem Projekt für einen elektrischen Kältemittelverdichter (eKMV) erprobt [EM21a]. Zur Beurteilung wurden zwei Kriterien herangezogen:

1. Vollständigkeit des Systemfehler-Erkenntnisgewinns, gemessen über die Anzahl an identifizierten NFH (zur S-Detaillierung bzw. als neuer Eintrag), die unter Zuhilfenahme der Checkliste Annex B Automobil identifiziert wurden
2. Methodische Komplexität, gemessen über die benötigte Zeit zur Erläuterung der Methode

Mit Bezug auf die anschließende Beurteilung wurden die Kriterien mit unterschiedlichen Prioritäten belegt [EM21a]. Da das Hauptziel der ProSi-HARA die Ermittlung möglichst aller Gefahren ist, die durch ein System ausgehen, wurde die „Vollständigkeit des Systemfehler-Erkenntnisgewinns" als wichtigstes Kriterium festgelegt. Die „methodische Komplexität" ist zu berücksichtigen, wenn bei zwei oder mehrere Konzepte die gleiche Anzahl an NFH nach Kriterium 1 resultieren.

Die Beurteilung der Konzepte im Pilotprojekt zeigte, dass die Checkliste keine Wirkung auf die Detaillierung von S hat (Konzept 1) [EM21a]. Eine Unterteilung von S der verschiedenen Fälle konnte durchgeführt werden, jedoch war die Expertise der ProSi-HARA-Teammitglieder hierfür ausreichend. Allerdings konnten mit Hilfe der Checkliste zehn zusätzliche eigenständige NFH identifiziert werden (Konzept 2), die bei reiner Betrachtung der funktionalen Fälle nicht erkannt worden wären. Da Konzept 3 sowohl Konzept 1 als auch 2 beinhaltet, ist Konzept 3 mit Bezug auf das erste Kriterium ebenso

gut wie Konzept 2 zu bewerten. Daraus resultiert folgendes Ranking nach der Beurteilung der drei Konzepte mit dem ersten Kriterium:

1. Platz: Konzept 2 und Konzept 3: 10 NFH

3. Platz: Konzept 1: 0 NFH

Beim Vergleich zwischen den drei Konzepten hinsichtlich des zweiten Kriteriums weisen Konzept 1 und 2 die größten Vorteile auf [EM21a]. Im Hinblick auf die Erläuterungszeit der Methode schneiden die ersten beiden Konzepte mit jeweils 5 min gleich gut ab. Konzept 3 ist aufgrund des höheren Erläuterungsaufwands schlechter zu bewerten (Erläuterungszeit: 10 min). Dies ist damit begründet, dass bei der Anwendung von Konzept 3 die Checkliste nicht nur zur Ermittlung von eigenständigen NFH (Konzept 2) herangezogen, sondern zusätzlich mit jedem UC, FF, MUC, FD sowie CF abgeglichen wird (Konzept 1). Dies steigert die Komplexität und damit den Zeitaufwand der Methode. Unter Berücksichtigung der Kriterien-Priorisierung wird daher in der Gesamtschau über beide Kriterien Konzept 2 ausgewählt:

| | | |
|---|---|---|
| **1. Platz: Konzept 2** | **10 NFH** | **5 min** |
| 2. Platz: Konzept 3 | 10 NFH | 10 min |
| 3. Platz: Konzept 1 | 0 NFH | 5 min |

Im Hinblick auf die Integration des ausgewählten Konzeptes 2 waren auch die Schritte bei der Durchführung der ProSi-HARA festzulegen [EM21a]. Im Zuge des Pilotprojektes zeigte sich, dass nachstehende Arbeitsschrittfolge die beste Wahl ist:

1. UC
2. FF
3. MUC
4. FD
5. CF

funktionale Fälle

6. NFH → nicht-funktional

Die Ermittlung der NFH nach den funktionalen Fällen ist sinnvoll, weil sich einige NFH bereits bei der Besprechung der funktionalen Fälle ergeben und somit nicht als eigenständige NFH betrachtet werden müssen. Des Weiteren war in der Praxis zu beobachten, dass durch eine spätere Ermittlung fehlender NFH Redundanzen vermieden werden konnten.

## 5 Repräsentativität der Projekt-Ergebnisse

Damit die Glaubwürdigkeit des Projektes und der Beurteilung der ProSi-HARA sichergestellt ist, werden im Anschluss drei Aspekte dargestellt, welche die Konformität der Evaluation belegen [EM21a].

**1. Bestimmung der ProSi-HARA-Teammitglieder:** Um gewährleisten zu können, dass die ProSi-HARA-Methode von Grund auf neu verstanden werden musste, wurden ausschließlich Laien ausgewählt (Konformität hinsichtlich des Kriteriums „Methodische Komplexität“) [EM21a]. Die Mitglieder waren zwar Experten auf deren fachlichen Gebiet, hatten allerdings kein Vorwissen in Bezug auf die HARA. Die Ausnahmen bildeten hierbei der Moderator und dessen Stellvertreter.

**2. Wissen des Moderators:** Zur Vermeidung einer Verfälschung der Pilotergebnisse, musste, im Gegensatz den restlichen Teammitgliedern, der Moderator und dessen Stellvertreter ein Experte für die (ProSi-)HARA sein [EM21a]. Die wesentlichen Aufgaben des Moderators, die hohes Fachwissen und Erfahrung voraussetzen, sind nachfolgend dargestellt:

- Sicherstellung der Einhaltung der Systemgrenze
- Gewährleistung der Einhaltung des Black-Box-Charakters
- Erfahrung bei der Festlegung der S-, E- und C-Parameter

**3. Expertenvielfalt** Eine Steigerung hinsichtlich der Ergebniskonformität ist ebenfalls durch die Vielfalt an Experten diverser Fachbereiche gegeben. Somit wurde nachgewiesen, "dass ganz verschiedene entwicklungsrelevante Personengruppen die ProSi-HARA verstehen können“ [EM21a].

## 6 Fazit

Ziel dieser Arbeit war die Weiterentwicklung des Ansatzes zur Produktsicherheits-Gefährdungs- und Risikoanalyse (ProSi-HARA) der Brose Fahrzeugteile SE & Co. KG. Dadurch sollte es möglich werden, neben Gefährdungen durch Fehler von Elektrik/Elektronik-Elementen (E/E-Elemente) – inklusive Software – zusätzlich Gefährdungen ausgehend von Nicht-E/E-Elementen mit der ProSi-HARA zu identifizieren und zu bewerten.

Die HARA nach ISO 26262 basiert auf der Betrachtung der Use Cases (UC), Functional Failures (FF) und Misuse Cases (MUC). Die ProSi-HARA bei Brose betrachtet zusätzlich die Mutual Functional Dependencies (FD) wie auch die Commanded Failures (CF). Es wird eine weitere ASIL-Bewertungsstufe (PSG) zwischen QM und ASIL A eingefügt, um Sicherheitsziele zu kennzeichnen, bei denen das Produktsicherheitsgesetz relevant ist. Zur Unterstützung einer systematischen Vorgehensweise bei der ProSi-HARA wurde die

Checkliste Annex B Automobil aus der ISO 12100 abgeleitet und ein Konzept zur effektiven Verwendung der Checkliste in der ProSi-HARA erarbeitet. In einem Pilotprojekt konnte gezeigt werden, dass die Verwendung der Checkliste das ProSi-HARA-Team bei der Identifizierung sämtlicher NFH unterstützt, die von einem System ausgehen, aber unabhängig von dessen Funktionen auftreten können (z.B. Gefahren durch hohe oder niedrige Objekttemperaturen oder chemischen Einflüsse). Dadurch wird eine Steigerung der Vollständigkeit bei der Gefährdungsidentifizierung/-beurteilung und somit eine Verbesserung der Produktqualität erreicht. Zusätzlich werden u.a. Entwicklungskosten, durch frühzeitige Ermittlung von potenziellen Gefährdungen, reduziert. Außerdem können Entschädigungszahlungen bei Rückrufaktionen oder in Bezug auf die Produkthaftung vermieden werden.

Da die dargestellten Ergebnisse auf einem einzelnen Pilotprojekt basieren, sollte die Methode in Zukunft in weiteren Projekten validiert werden, um die Resultate zu bestätigen. Dies kann allerdings auch zu Anpassungen beziehungsweise Erweiterungen der ProSi-HARA-Methode führen.

## Literaturverzeichnis

[DI11] ISO 12100: Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung.

[DI17] DIN EN 61882: HAZOP-Verfahren (HAZOP-Studien) - Anwendungsleitfaden (IEC 61882:2016).

[DI18] ISO 26262-3: Straßenfahrzeuge - Funktionale Sicherheit - Teil 3: Konzeptphase.

[EM21a] Emig, M.: Erweiterung von Gefahren- und Risikoanalysen der Funktionalen Sicherheit um Aspekte der Produktsicherheit nach DIN EN ISO 12100 (Masterarbeit), Bamberg, 2021.

[EM21b] Emig, M., Metz, P.: Produktsicherheits-Gefährdungs- und Risikoanalyse (ProSi-HARA) (internes Dokument), Coburg, 2021.

[EM21c] Emig, M.: Erweiterung von Gefahren – und Risikoanalysen der Funktionalen Sicherheit um Aspekte der Produktsicherheit nach DIN EN ISO 12100 (Masterarbeit), Hochschule Coburg, 2021.

[ME21] Metz, P.; Emig, M.; Schilde, B.: Product Safety Hazard & Risk Analysis (ProdSa HARA), VDA Automotive SYS Conference, Berlin, 2021