

# Eine Generische Gefährdungsliste für Fahrerlose Transportfahrzeuge in der Intralogistik

Sönke Eilers, Thomas Peikenkamp, Dr. Stefan Rührup,  
Sören Schweigert, Dr. Tobe Toben, Hannes Winkelmann

OFFIS e.V., Escherweg 2, 26121 Oldenburg, Germany

toben@offis.de Tel. +49 441 - 779 222 28 Fax +49 441 9722 278

## Zusammenfassung

Für den Einsatz von fahrerlosen Transportsystemen in Form von autonom agierenden Fahrzeugen ist eine eingehende Sicherheitsanalyse des Gesamtsystems nötig. Grundlage dieser Sicherheitsbetrachtung ist eine vollständige Identifikation der möglichen Gefährdungen, die aus dem Betrieb der automatischen Fahrzeuge resultieren. Wir stellen in diesem Artikel eine generische Methode zur systematischen Identifikation und Bewertung von Gefährdungen vor, wie sie insbesondere in einem heterogenem Arbeitsumfeld wie dem Außenbereich eines Logistikbetriebs vorliegen. Die Methode bietet eine modellbasierte Erfassung der relevanten Systemparameter und erlaubt eine automatische Ableitung der möglichen Gefährdungen. Die Granularität der abgeleiteten Gefährdungssituationen kann durch Annotierung des zugrundeliegenden Modells flexibel verändert werden.

## 1 Einführung

Elektronische Steuergeräte, zum Beispiel in Form von Autopiloten in Flugzeugen oder Spurhalteassistenten in Automobilen, übernehmen zunehmend auch sicherheitskritische Funktionen, bei deren Fehlfunktion es insbesondere zu Personenschäden kommen kann. Es werden daher hohe Sicherheitsanforderungen an die entsprechenden Geräte gestellt. Zur Gewährleistung der funktionalen Sicherheit werden gemäß anerkannter Sicherheitsnormen (insbesondere IEC 61508 [6] und dessen Derivate) sämtliche Phasen der Planung, Entwicklung, Fertigung und Betrieb der Geräte in einen Sicherheitslebenszyklus eingebettet. Insbesondere in der Planungsphase wird eine umfassende Identifikation und Bewertung der möglichen Gefährdungen vorgenommen, auf dessen Basis die nachfolgenden Sicherheitskonzepte geplant, umgesetzt und validiert werden.

Elektronische Sicherheitsfunktionen sind nicht nur in öffentlichen Transportdomänen wie der Luftfahrt, im Bahn- oder Automobilbereich zu finden, sondern werden auch im innerbetrieblichen Bereich zum Personenschutz eingesetzt (etwa in Form von automatischen Sicherheitsabschaltungen von Schneidemaschinen). Neben fachlichen Einweisungen und baulichen

Schutzmaßnahmen haben elektronische Schutzfunktionen mittlerweile einen erheblichen Anteil an der Gesamtsicherheit von innerbetrieblichen Maschinen. Ein ebenfalls sicherheitskritischer innerbetrieblicher Bereich ist der des automatischen Materialtransports in der Intra-logistik. Hierzu zählen insbesondere Fahrerlose Transportsysteme (FTS), wie sie bereits seit den 70er Jahren in einer Vielzahl von Bauformen innerhalb von Werks- und Logistikhallen im Einsatz sind [12].

In zukünftigen FTS-Anwendungen werden sich Transportfahrzeuge durch mehr Autonomie und bessere sensorische Wahrnehmung auszeichnen. Dadurch werden sie flexibler einsetzbar und können sich auch in teil-öffentlichen Bereichen (etwa im Außenbereich von Logistikhöfen) autonom bewegen, wo sie idealerweise höhere Fahrgeschwindigkeiten erreichen. Für die Sicherheitsbetrachtung solcher Systeme werden jedoch die klassischen Verfahren einer nachgelagerten Risikominderung und der Einsatz individuell zertifizierter Schutzeinrichtungen nicht mehr ausreichen. Es kann erwartet werden, dass ähnlich zur Einführung der Sicherheitsnorm ISO 26262 [7] in der Automobilindustrie auch bei solchen Systemen die funktionale Sicherheit im gesamten Planungs-, Entwicklungs- und Betriebsprozess berücksichtigt werden muss. Insbesondere ist bereits in frühen Planungsphasen eine initiale Risikoanalyse und -bewertung erforderlich.

Motiviert durch verwandte Arbeiten im Automobil- [2] und Eisenbahnsektor [3] stellen wir in diesem Artikel eine allgemeine Systematik zur Herleitung von Gefährdungslisten für Fahrerlose Transportfahrzeuge im intralogistischen Einsatz vor. Zweck einer generischen Gefährdungsliste ist die einfache und systematische Identifikation von möglichen Gefährdungen bereits in frühen Phasen der Konzeption. Insbesondere können bereits ohne eine tiefer gehende Designphase des Systems die möglichen Gefährdungen in Bezug auf verschiedene Einsatzszenarien grob abgeschätzt und verglichen werden. Die Erkenntnisse aus dieser ersten Identifikation können als Basis für weitergehenden Risikoanalysen in späteren Planungs- und Entwurfsphasen verwendet werden. In unserem Ansatz erfolgt zudem direkt eine Risikobewertung der Gefährdungen, welche sich aus einer Annotation des Modells mit Kritikalitätsfaktoren und Aufenthaltsannahmen ergeben.

## **2 FTF in der Intra-logistik**

Fahrerlose Transportsysteme sind “innerbetriebliche, flurgebundene Fördersysteme mit automatisch geführten Fahrzeugen, deren primäre Aufgabe der Materialtransport [...] ist” [13]. Entsprechende Systeme sind innerhalb von Gebäuden seit langem im industriellen Einsatz [12]. Da hier die Fahrwege klar definiert sind und mit vergleichsweise geringer Geschwindigkeit befahren werden, kann ein zuverlässiger Personenschutz durch nachgelagerte Sicherheitstechnik erreicht werden. Stand der Technik hierbei ist der Einsatz von zertifizierten Laserscannern

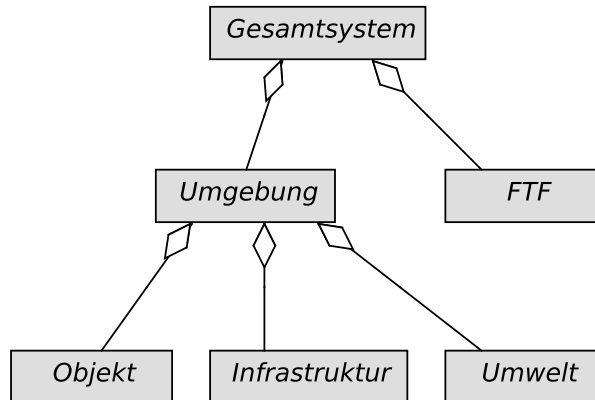


Abbildung 1: Basiskomponenten als UML Diagramm

oder Berührungssensoren, welche bei Erkennung von Hindernissen eine automatische Bremsung des Transportmittels auslösen. Entsprechende Sicherheitsanforderungen und Prüfverfahren sind in [5] beschrieben.

Der Betrieb von fahrerlosen Transportfahrzeugen (FTF) im *Außenbereich* bietet einerseits neue vielversprechende Möglichkeiten in der Automatisierung des Materialtransports, stellt aber andererseits erhöhte Anforderungen an die Sicherheitstechnik. Die Anforderungen ergeben sich im Wesentlichen aus den folgenden vier Problemklassen:

1. **Objekte:** Da der Außenbereich typischerweise weniger stark vom Betriebsgeschehen abgeschottet ist, liegt ein heterogenerer Fremdverkehr vor. Neben dem Personal ist etwa mit weiterem Anlieferungsverkehr, auch durch betriebsfremde Personen, zu rechnen. Auch statische Hindernisse sind in verschiedenen Ausprägungen zu erwarten.
2. **Infrastruktur:** Während im Hallenbetrieb eine überschaubare Fahrumgebung vorliegt, wird sich ein FTF im Außenbereich in verschiedensten Infrastrukturen bewegen müssen. Neben einer Ladezone sind typischerweise etwa lange Fahrbahnen vorhanden, eventuellen liegen auch Kreuzungssituationen oder frei navigierbare Flächen vor.
3. **Umwelt:** Im Außenbereich ist mit störenden Umwelteinflüssen zu rechnen, welche sowohl die Sensorik als auch die Aktorik des Fahrzeug beeinflussen können. Typische Ausprägungen sind Blendung, Nebel oder Glätte.
4. **FTF:** Das FTF als autonomes Fahrzeug besteht aus einer Menge von Teilfunktionen, welche prinzipiell fehlerbehaftet sein können. So muß ein FTF neben Funktionen zur Wahrnehmung der Umgebung etwa auch eine Entscheidungslogik zur Fahrplanung sowie eine Komponente zur Ansteuerung der Aktorik besitzen.

In Abbildung 1 sind die beschriebenen Aspekte als UML-Modell [10] strukturiert. Das Gesamtsystem besteht aus dem FTF in seiner Umgebung, welche sich wiederum aus den Objekten, den Infrastrukturen und den möglichen Umweltbedingungen zusammensetzt. Je nach

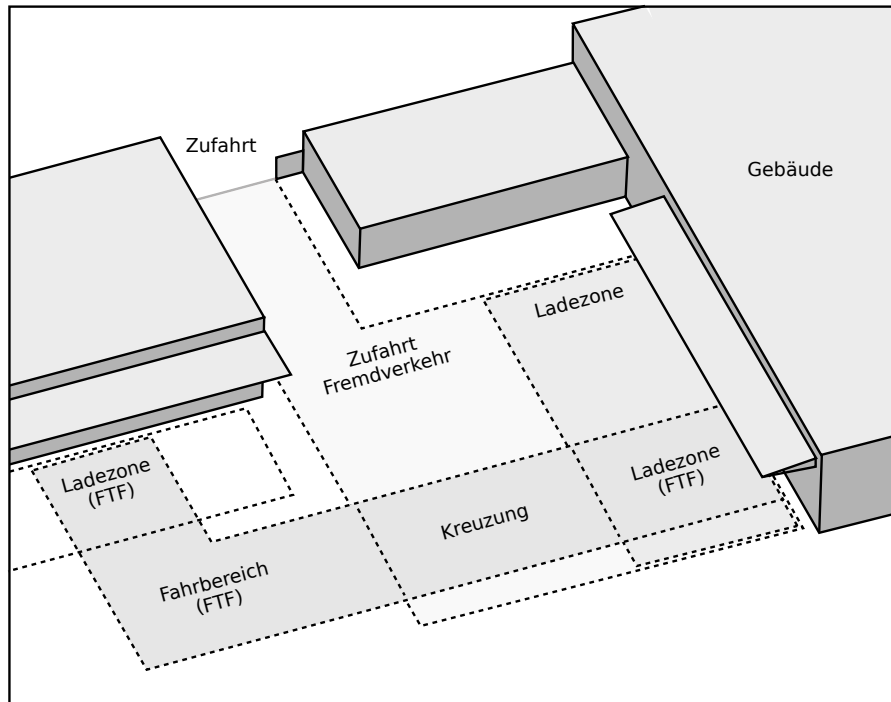


Abbildung 2: Exemplarisches Layout eines Logistikhofes

Einsatzort und -zweck werden verschiedene Ausprägungen dieser Umgebungskomponenten vorhanden sein (in obiger Aufzählung wurden bereits einige Beispiele genannt), und je nach den vorhandenen Ausprägungen ergeben sich bestimmte Gefährdungssituationen beim Betrieb des fahrerlosen Fahrzeugs.

### Gefährdungsanalyse

Basierend auf dem generischen Systemmodell aus Abbildung 1 stellen wir in nächsten Kapitel die systematische Herleitung der möglichen Gefährdungen vor. Wir bieten mit unserem Ansatz ein einfaches Vorgehen an, mit welchem ein komplexes Einsatzszenario in seine relevanten Teilkomponenten zerlegt werden kann und darauf aufbauend eine erste Abschätzung der möglichen Gefährdungen ermöglicht. Neben der Konkretisierung der Umgebung können in dem Systemmodell auch die Funktionen des FTF in verschiedenen Verfeinerungsstufen betrachtet werden. Hierdurch kann etwa unterschieden werden, ob eine Gefährdung durch eine fehlerhafte (sensorische) Wahrnehmung oder durch eine fehlerhafte Ansteuerung oder Ausführung der Aktorik gegeben ist.

### Anwendungsszenario

In Abbildung 2 ist ein einfaches Anwendungsszenario in Form eines Logistikhofs beispielhaft skizziert. Ein FTF hat in diesem Beispiel die Aufgabe, Container zwischen den beiden Ladezonen zu transportieren. In dem Hoflayout sind die möglichen Infrastrukturen in Form von

verschiedenen Fahr- und Ladezonen eingezeichnet. So gibt es in diesem Fall neben den Ladezonen noch exklusive Fahrbereiche sowie einen Kreuzungsbereich, in welchem Fremdverkehr den Fahrweg des FTF kreuzt. Für dieses Anwendungsszenario werden wir die Herleitung der Gefährdungen im Folgenden beispielhaft durchführen.

### 3 Generische Gefährdungen von FTF in der Intralogistik

Die Gefährdungen, die durch den Einsatz von automatisierten Fahrzeugen in der Intralogistik entstehen, basieren auf den vier wesentlichen Komponenten, welche wir im vorherigen Kapitel identifiziert haben: Die Objekte, die Infrastruktur, die Umweltbedingungen, und die Funktionen des FTF. Das Zusammenspiel dieser vier Komponenten stellt den generischen Gefährdungsraum des Gesamtsystems wie folgt dar:

*In Infrastruktur I unter Umweltbedingung U kann ein Fehler  
in der Funktion F eine Kollision mit Objekt O verursachen.*

Wir erfassen in der generischen Liste lediglich die Gefährdungsklasse der *Kollisionen*, welche zweifelsfrei die Hauptgefährdung durch automatische Fahrzeuge darstellt. Weitere Gefährdungen, wie Brand oder auslaufende Flüssigkeiten, werden in unserem Ansatz nicht erfasst und müssen separat identifiziert werden. Da allerdings die Art der Objekte vom Benutzer spezifizierbar ist können auch spezielle Gefährdungen erfasst werden, zum Beispiel das Verlassen des Fahrgebietes durch eine "Kollision mit nicht-befahrtem Gebiet".

Die generische Gefährdungsliste ergibt sich gerade aus dem Kreuzprodukt aller möglichen Ausprägungen aller vier Komponenten (Infrastruktur, Umwelt, Objekte und FTF) in allen möglichen Einsatzszenarien von automatischen Fahrzeugen in der Intralogistik. Diese Liste ist entsprechend groß beziehungsweise im Allgemeinen nicht einmal geschlossen repräsentierbar, da kaum eine Beschreibung aller Möglichkeiten vorliegen wird. Wir schlagen daher vor, diese generische Liste nicht explizit zu repräsentieren, sondern auf der symbolischen Ebene des obigen Kreuzprodukts zu belassen. Für den Übergang dieser generischen Gefährdungsbeschreibung zu einer spezifischen Identifikation der Gefährdungen wird eine Konkretisierung der vier Komponenten für das jeweils betrachtete Einsatzszenario vorgenommen. Das hierdurch gewonnene Wissen über die konkreten Ausprägungen der abstrakten Komponenten erlaubt eine Ableitung von entsprechend spezialisierten Gefährdungslisten.

Dieses Vorgehen unterscheidet sich leicht vom klassischen Einsatz von generischen Gefährdungslisten wie zum Beispiel im Eisenbahn- oder Automobilbereich. Dort wird ausgehend von einer festen Matrix von Gefährdungseinflüssen der jeweils für eine betrachtete Funktionalität relevante Ausschnitt betrachtet und als Liste von spezifischen Gefährdungen interpretiert. In unserem Fall liegt die generische Matrix nur symbolisch vor, und der relevante Teilbereich wird jeweils dynamisch anhand der Konkretisierungen der Komponenten erzeugt.

### 3.1 Vorgehen

Wir schlagen somit folgendes Vorgehen zur Ableitung einer Gefährdungsliste für fahrerlose Transportfahrzeuge in der Intralogistik vor.

0. **Systemmodell:** Als Basis benutzen wir das generisches Systemmodell aus Abbildung 1, welches eine Unterteilung in die vier relevanten Komponenten Infrastruktur, Objekte, Umwelt und FTF vorgibt.
1. **Gefährdungserfassung:** Um die Gefährdungen eines gegebenen Einsatzzwecks zu identifizieren wird jede dieser Komponenten verfeinert. Es gilt hierbei alle möglichen Ausprägungen zu erfassen die in dem betrachteten Einsatzszenario vorkommen. Jede Komponente sollte getrennt bearbeitet werden, ohne sich bereits von möglichen Zusammenhängen beeinflussen zu lassen.
2. **Parametrisierung:** Durch Typisierung von verfeinerten Klassen entstehen verschiedene Sichten mit verschiedenen Detaillierungsgraden auf das verfeinerte Systemmodell. Dies erzeugt eine Flexibilität in der Erzeugung entsprechend unterschiedlich fokussierter Gefährdungslisten auf Basis eines gemeinsamen Datenbestands.
3. **Risikobewertung:** Durch Hinzunahme von Risikoparametern wird eine weitere Fokussierung der Gefährdungslisten auf kritische Elemente erzeugt. Dieser Schritt ermöglicht einen direkten Übergang in die Riskobewertung der identifizierten Gefährdungen.

Die Schritte 1-3 werden im Folgenden genauer beschrieben und anhand des Anwendungsszenarios durchgeführt.

### 3.2 Gefährdungserfassung

Die Verfeinerung der Komponenten lässt sich sehr gut im Rahmen des graphischen Systemmodells aus Abbildung 1 durchführen. Gemäß des obigen Vorgehens gilt es im ersten Schritt die generischen Komponenten zu instantiieren. Hierzu benutzen wir die Ableitungsrelation aus der UML. Es ist hierbei meist sinnvoll, den Ableitungsbaum weiter zu strukturieren, um insbesondere in den späteren Schritten verschiedene Parametrisierungsmöglichkeiten bezüglich der Ableitung von Gefährdungslisten nutzen zu können.

Für das Anwendungsszenario “Containertransport auf einem Logistikhof” stellen wir eine Verfeinerung des generischen Systemmodells in Abbildung 3 dar. Um die Modellgröße im Rahmen dieses Artikels übersichtlich zu halten, konzentrieren wir uns auf eine relative kleine Anzahl von konkreten Ausprägungen der jeweiligen Komponenten. Für die *Objekte* betrachten wir vier mögliche Ausprägungen: Container, Palette, Person und LKW. Durch Einführung zweier weiterer Klassen unterteilen wir diese in die Gruppen Statisch und Beweglich. Gemäß

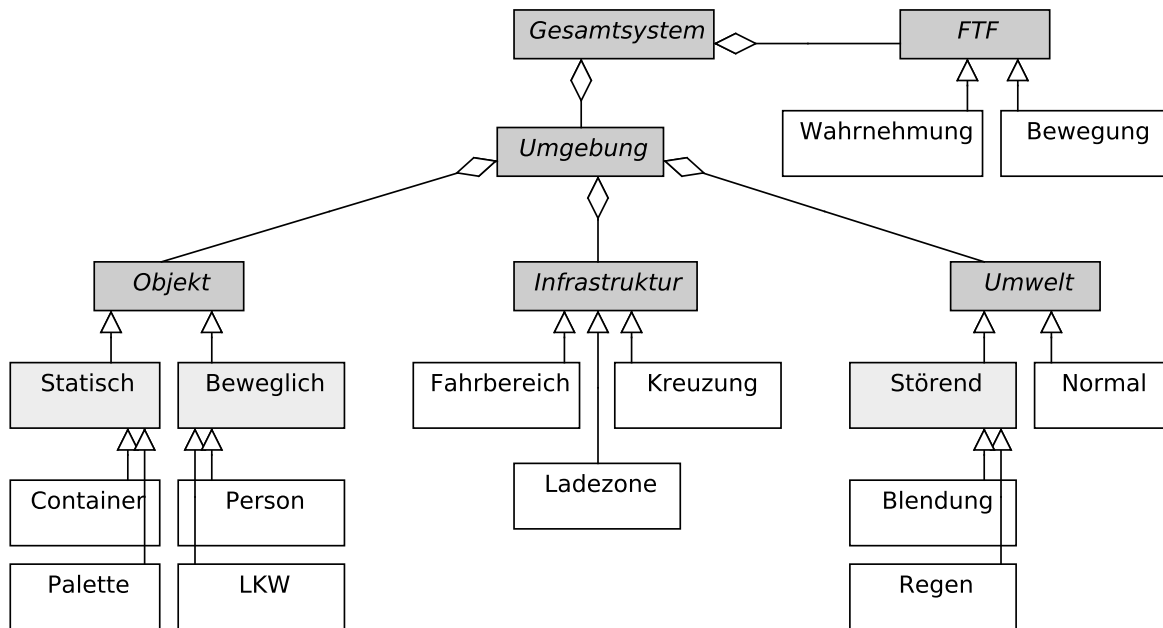


Abbildung 3: Erste Verfeinerung des Systemmodells für das Anwendungsszenario

Abbildung 2 unterteilt sich der Hof in drei verschiedene *Infrastruktur*-Bereiche: Fahrbereich, Kreuzung und Ladezone. Die *Umwelt* wird in zwei Klassen unterteilt, Normal und Störend, wobei letztere weiter verfeinert wird in Blendung und Regen. Als Funktionen des FTF konzentrieren wir uns auf die zwei Aspekte Wahrnehmung und Bewegung.

Auf Basis dieser Systemverfeinerung kann bereits eine erste Liste von Gefährdungen abgeleitet werden. Diese entspricht gerade dem Kreuzprodukt aller Blätter im verfeinerten Systemmodell, welches insgesamt 72 Elemente enthält. Die Liste ist ausschnittsweise in Tabelle 1 zu sehen. Jeder Gefährdung wird eine eindeutige Nummer zugewiesen. So entspricht zum Beispiel die Gefährdung 1 der Möglichkeit einer Kollision mit einer Person die sich unter normalen Umweltbedingungen in der Ladezone befindet, wobei die Kollision durch einen Fehler in der Wahrnehmung durch das FTF ausgelöst wird. Analog entspricht Gefährdung 2 derselben Situation, wobei hier ein Fehler in die Bewegung des FTF vorliegt (etwa ein fehlerhafte Ansteuerung oder ein Versagen der Bremsen).

### 3.3 Parametrisierung

Bereits an diesem kleinen Anwendungsfall ist ersichtlich, dass der naive Ansatz des vollen Kreuzprodukts der verfeinerten Komponentenbeschreibung im Allgemeinen zu einer zu großen und zu unfokussierten Gefährdungsliste führt. Sie enthält insbesondere viele Redundanzen da viele ähnliche Gefährdungen getrennt gelistet werden. So ist es etwa nicht zwingend nötig, Kollisionen mit einem Container und einer Palette getrennt zu betrachten.

Das Wissen über sinnvolle Zusammenfassungen kann explizit in das Modell integriert und

ID	Objekt	Infrastruktur	Umwelt	FTF-Funktion
1	Person	Ladezone	Normal	Wahrnehmung
2	Person	Ladezone	Normal	Bewegung
3	Person	Ladezone	Blendung	Wahrnehmung
4	Person	Ladezone	Blendung	Bewegung
5	Person	Ladezone	Regen	Wahrnehmung
6	Person	Ladezone	Regen	Bewegung
...	...	...	...	...
...	LKW	...	...	...
...	...	...	...	...
71	Palette	Kreuzung	Regen	Wahrnehmung
72	Palette	Kreuzung	Regen	Bewegung

Tabelle 1: Initiale Gefährdungsliste

entsprechend bei der Generierung der Liste beachtet werden. Gemäß Schritt 2 unseres Vorgehens stellen wir die hierzu möglichen Annotationen im folgenden Abschnitt vor. Des Weiteren lässt sich eine Fokussierung der Liste auf kritische Situationen erreichen, indem Wissen über die Auftretenshäufigkeit von Objekten und Umweltbedingungen sowie über die Vermeidbarkeit und Schwere von möglichen Kollisionen in das Modell kodiert werden. Hiermit lässt sich insbesondere eine initiale Risikobewertung der Gefährdungen ableiten. Als Vorbereitung für Schritt 3 unseres Vorgehens stellen wir die hierzu möglichen Parameter im darauffolgenden Abschnitt über “Risikoparameter” vor.

### 3.3.1 Annotationen

Zur Gruppierung von abgeleiteten Systemkomponenten führen wir drei UML Stereotypen ein: `<<barrier>>`, `<<join>>` und `<<ignore>>`. Durch Annotation des verfeinerten Systemmodells mit diesen Stereotypen lassen sich verschiedene Sichten auf die Menge der Gefährdungen sehr flexibel erzeugen. Wir beschreiben die Bedeutung der Stereotypen zunächst, und wenden sie danach in dem Beispielszenario exemplarisch an.

Die Annotation `<<barrier>>` für eine Klasse  $K$  führt dazu, dass ledig die Klasse  $K$ , nicht aber die abgeleitete Klassen von  $K$ , in das Kreuzprodukt der Gefährdungen aufgenommen werden. Damit wird der Teilbaum unterhalb von  $K$  nicht mehr explizit aufgefaltet, sondern gruppiert unter der Bezeichnung  $K$  geführt. Eine Variation von `<<barrier>>` stellt der Stereotyp `<<join>>` dar. Auch hier wird der Teilbaum unter  $K$  nicht mehr getrennt betrachtet, sondern lediglich gruppiert unter einer neuen Bezeichnung geführt, welche der Menge aller abgeleiteten Klassen von  $K$  entspricht. Durch den Stereotyp `<<ignore>>` können gewissen Klassen explizit von

	(E)xposure	(C)ontrollability	(S)everity
0	Unvorstellbar	Immer beherrschbar	Keine Verletzungen
1	Sehr niedrig	Einfach beherrschbar	Leichte bis mittlere Verl.
2	Niedrig	Normalerweise beherrschbar	Schwere Verletzungen
3	Mittel	Schwierig beherrschbar	Lebensgefährliche Verl.
4	Hoch		

Tabelle 2: Risikoparameter und -domänen auf Basis der ISO 26262 Norm

der Betrachtung ausgeschlossen werden. Wir fordern, dass jede Klasse mit maximal einem dieser Stereotypen annotiert ist und werten die Annotationen beginnend von den Blättern des Systemmodells rekursiv aus.

Zur Demonstration der Stereotypen setzen wir für das Beispielszenario folgenden Annotationen: `Statisch:⟨⟨join⟩⟩`, `Störend:⟨⟨barrier⟩⟩`, und `Fahrbereich:⟨⟨ignore⟩⟩`. Hierdurch werden die Umweltbedingungen `Blendung` und `Regen` unter der Klasse `Störend` zusammengefasst, die statischen Objekte werden unter einer Bezeichnung `‘Container,Palette’` geführt, und die Infrastruktur `Fahrbereich` aus der aktuellen Betrachtung ausgeschlossen. Mit dieser Parametrisierung ergeben sich 24 Gefährdungen, jeweils acht pro Objekt unter den zwei Infrastrukturen mit zwei möglichen Umweltbedingungen und zwei Funktionen des FTF.

### 3.3.2 Risikoparameter

Neben der Möglichkeit bestimmte Teilkomponenten zusammenzufassen bzw. auszublenden, kann eine weitere Fokussierung der Liste durch Annotation von Häufigkeit und Relevanz erreicht werden. Diese Daten stellen zudem wichtige Information für die nachfolgende Risikobewertung der identifizierten Gefährdungen dar. Wir betrachten die folgenden *Risikoparameter*:

- $E_O$ : Auftretenshäufigkeit von Objekten in Infrastrukturen
- $E_U$ : Auftretenshäufigkeit von Umweltbedingungen in Infrastrukturen
- $C$ : Kontrollierbarkeit für Objekte in Infrastrukturen
- $S$ : Schadenshöhe von Objektkollisionen in Infrastrukturen

Als Wertedomänen benutzen wir die Klassifizierung aus der kommenden Sicherheitsnorm ISO 26262 [7] für den Automobilbereich, welche wir in Tabelle 2 zusammenfassen. Hierbei korrespondiert die Auftretenshäufigkeit zu einem Exposure-Wert, die Kontrollierbarkeit zur Controllability und die Schadenshöhe zur Severity. Die Kontrollierbarkeit gibt in unserem Ansatz an, wie gut eine drohende Kollision vom Objekt selbst noch verhindert werden kann. Andere Domänen für die Risikoparameter sind in unserem Ansatz problemlos verwendbar.

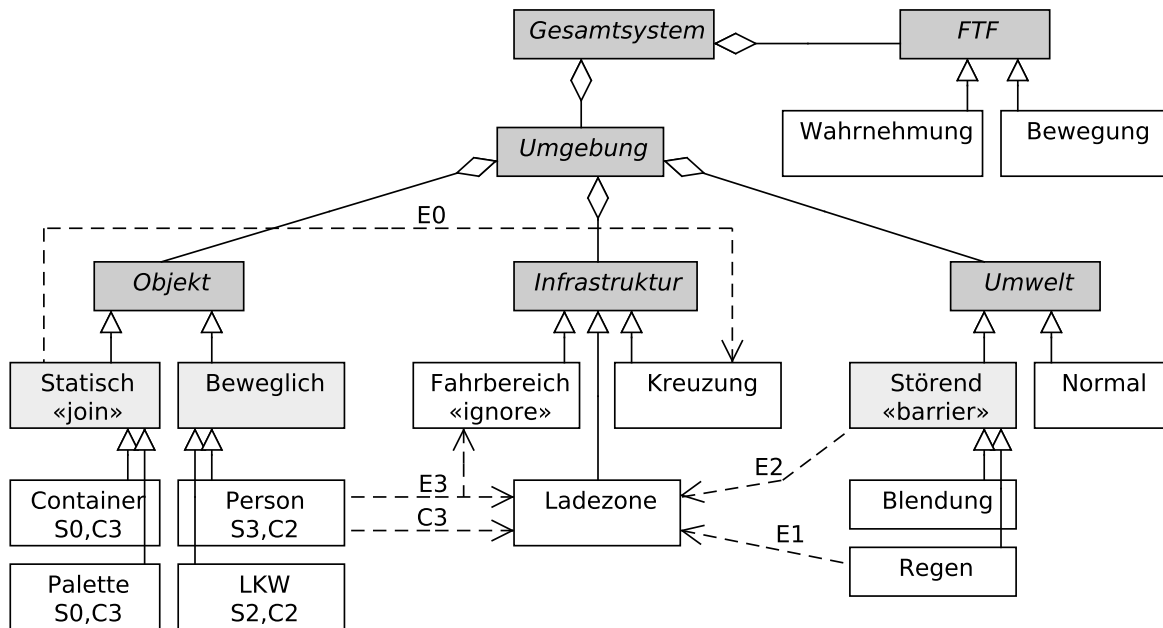


Abbildung 4: Erweiterung des Systemmodells um Risikoparameter

Wir zeigen eine mögliche Angabe von Risikoparametern in Abbildung 4, die wie folgt zu interpretieren ist: Parameter, die direkt einer Klasse zugeordnet sind, werden als Standardwerte interpretiert. Diese können durch explizit angegebene Werte überschrieben werden. So wird bei einer Person generell eine Kontrollierbarkeit von C2 erwartet, diese aber innerhalb der (unübersichtlichen) Ladezone auf C3 herabgesetzt. Die Schadenshöhe ist unabhängig von der Infrastruktur bei Personen auf S3 gesetzt. Angaben vererben sich grundsätzlich an die Kinderklassen, können dort aber explizit überschrieben werden. Störende Umwelteinflüsse etwa werden mit geringer Wahrscheinlichkeit (E2) in der Ladezone erwartet. Dieser Wert wird für Blendung vererbt, für Regen hingegen wird explizit eine sehr geringe Wahrscheinlichkeit (E1) angegeben (etwa wegen einer Überdachung der Ladezone). Die Auftretenshäufigkeit von Personen im Fahrbereich und in der Ladezone liegt bei E3 (mittel). Es wird explizit ausgeschlossen, dass sich statische Objekte in einer Kreuzung befinden (E0). Ist für eine Relation keine explizite oder vererbte Angabe vorhanden, so wird der jeweils höchste Wert angenommen. So sagt das Modell implizit, dass etwa bei Kreuzungen eine hohe Wahrscheinlichkeit für das Auftreten von Personen vorliegt (E4).

Zusammen mit den Gruppierungs-Stereotypen ergibt sich mit dieser Risikoparametrisierung eine Liste von 20 Gefährdungen, siehe Tabelle 3. Die Risikoparameter aus dem Modell werden hierbei in entsprechenden Spalten mit den Bezeichnungen  $S$ ,  $C$ ,  $E_O$  und  $E_U$  transformiert. Die Anordnung der Spalten der beiden Wahrscheinlichkeiten ist gerade so gewählt, dass jeweils die Auftretenswahrscheinlichkeit der beiden benachbarten Komponenten angegeben wird. Es entspricht zum Beispiel die Gefährdung Nummer 1 einer Kollision mit einer Person die sich unter normalen Umweltbedingungen in der Ladezone befindet, wobei die Kollision

ID	S	Objekt	C	E <sub>o</sub>	Infrastruktur	E <sub>U</sub>	Umwelt	FTF-Funktion
1	S3	Person	C3	E3	Ladezone	E4	Normal	Wahrnehmung
2	S3	Person	C3	E3	Ladezone	E4	Normal	Bewegung
3	S3	Person	C3	E3	Ladezone	E2	Störend	Wahrnehmung
4	S3	Person	C3	E3	Ladezone	E2	Störend	Bewegung
5	S3	Person	C2	E4	Kreuzung	E4	Normal	Wahrnehmung
6	S3	Person	C2	E4	Kreuzung	E4	Normal	Bewegung
7	S3	Person	C2	E4	Kreuzung	E4	Störend	Wahrnehmung
8	S3	Person	C2	E4	Kreuzung	E4	Störend	Bewegung
9	S2	LKW	C2	E4	Ladezone	E4	Normal	Wahrnehmung
...	...	...	...	...	...	...	...	
19	S0	Cont.,Palette	C3	E4	Ladezone	E2	Störend	Wahrnehmung
20	S0	Cont.,Palette	C3	E4	Ladezone	E2	Störend	Bewegung

Tabelle 3: Gefährdungsliste nach Gruppierung und Risikoparametrisierung

durch einen Fehler in der Wahrnehmung durch das FTF ausgelöst wird. Die Situation wird als schwierig durch die Person beherrschbar und mit potentiell lebensgefährlichen Verletzungen eingeschätzt, wobei sich Personen mit geringer Wahrscheinlichkeit in der Ladezone aufhalten und normale Umweltbedingung mit hoher Wahrscheinlichkeit vorliegen.

In die resultierende Gefährdungsliste werden keine Szenarien mehr aufgenommen, bei denen die Auftretenshäufigkeit mit E0 (unvollstellbar) angegeben wurde. In unserem Beispiel sind dies die vier möglichen Kollisionsszenarien mit statischen Objekten an Kreuzungen. Mögliche Kollisionen mit Objekten bei absoluter Kontrollierbarkeit (C0) oder ohne jegliche Verletzungsgefahr (S0) bleiben explizit in der Liste, können aber typischerweise in nachfolgenden *Sicherheitsbetrachtungen* vernachlässigt werden.

### 3.4 Risikobewertung

In Anlehnung an den Begriff SIL aus der IEC 61508 Norm wird im Automobilbereich für das Risikomaß der Begriff ASIL (Automotive Safety Integrity Level) benutzt. Hierbei stellt A das geringste und D das höchste Risiko dar. Das Riskomaß ergibt sich aus der Kombination der Schwere (S), der Häufigkeit (E) und der Kontrollierbarkeit (C). Ist für mindestens einer der Parameter der Wert '0' angegeben so wird kein dedizierter ASIL Wert zugewiesen und der Gefährdung muss nicht durch dedizierte Sicherheitsmaßnahmen begegnet werden. Für die sonstigen Werte wird der resultierende ASIL anhand einer Matrix bestimmt, welche durch die ISO 26262 Norm vorgeben wird [7].

ID	Objekt	Infrastruktur	Umwelt	S	C	E	R
1,2	Person	Ladezone	Normal	S3	C3	E3	C
5,6	Person	Kreuzung	Normal	S3	C2	E4	C
7,8	Person	Kreuzung	Störend	S3	C2	E4	C
9,10	LKW	Ladezone	Normal	S2	C2	E4	B
13,14	LKW	Kreuzung	Normal	S2	C2	E4	B
15,16	LKW	Kreuzung	Störend	S2	C2	E4	B
3,4	Person	Ladezone	Störend	S3	C3	E1	A
11,12	LKW	Ladezone	Störend	S2	C2	E2	–
17,18	Cont.,Palette	Ladezone	Normal	S0	C3	E4	–
19,20	Cont.,Palette	Ladezone	Störend	S0	C3	E2	–

Tabelle 4: Risikobewertung der abgeleiteten Gefährdungen aus Abbildung 4.  $E = E_O \cdot E_U$  bezeichnet die kombinierte Wahrscheinlichkeit und  $R$  das Risikomaß in Form des ASIL.

Durch die Risikoparametrisierung im Modell sind wir hiermit grundsätzlich bereits in der Lage jeder Gefährdung eine Risikomaß zuzuordnen und hierdurch die Gefährdungsliste weiter zu klassifizieren. Die Häufigkeit der Gefährdung ist bei uns allerdings durch zwei Werte gegeben,  $E_O$  und  $E_U$ . Um diese zu einem Häufigkeitswert sinnvoll zusammenfassen zu können muss sichergestellt werden, dass nicht etwa *eine risikoreiche* Gefährdung durch *eine Vielzahl risikoarmer* Gefährdungen ersetzt wird. Dies wäre der Fall wenn lediglich viele verschiedene Umweltbedingungen mit sehr geringer Wahrscheinlichkeit angegeben werden, ohne eine “Standard”-Umweltbedingung mit Häufigkeit E4 hinzuzufügen. In unserem Beispiel benutzen wir hierfür die Umweltbedingung Normal. Ist diese Bedingung erfüllt können die beiden Parameter  $E_O$  und  $E_U$  kombiniert werden. Wir weisen hierzu jedem Exposure-Begriff E1 bis E4 seinen Wert  $V(E_x) = 10^{x-4}$  zu, und definieren die Kombination aus  $E_O$  und  $E_U$  als

$$E_O \cdot E_U := V^{-1}(\max\{10^{-3}, V(E_O) \cdot V(E_U)\})$$

Wir erreichen hierdurch eine angemessene Reduktion der Gesamtwahrscheinlichkeit, wobei mindestens der Wert E1 erhalten bleibt um keine Gefährdung vollständig zu unterdrücken. Zu beachten ist, dass das Rechnen mit Wahrscheinlichkeiten durchaus fehlerträchtig ist, insbesondere wenn die Wahrscheinlichkeiten nicht unabhängig voneinander sind. Es sollte daher im Einzelfall geprüft werden ob die Rechenvorschrift plausible Werte ergibt. Nach diesem Schritt können die Werte  $S$ ,  $C$  und  $E = E_O \cdot E_U$  gemäß ISO 26262 zu einem ASIL Wert kombiniert werden. Für die Tabelle 3 ergibt sich damit die Risikobewertung aus Tabelle 4, absteigend sortiert nach dem Risikomaß wobei beide FTF-Funktionen zusammengefasst wurden.

Das höchste Risikomaß erhalten drei Gefährdungen bezüglich einer Kollision mit einer Person, insbesondere da hierbei mit einer hohen Schadenshöhe gerechnet wird. Die mögliche Kollision mit einer Person an einer Ladezone unter störenden Umweltbedingungen erhält ein geringeres Maß, da die Gesamtwahrscheinlichkeit für dieses Szenario nur sehr gering ist. Insbesondere Kollisionen mit statischen Objekten erreichen keinen ASIL Wert aufgrund der Tatsache dass hierbei keine Verletzungen entstehen.

## 4 Zusammenfassung und Ausblick

Wir haben in diesem Artikel ein modell-basiertes Vorgehen zur systematischen Identifikation und Bewertung von Gefährdungen beim Einsatz von fahrerlosen Transportfahrzeugen, insbesondere für den Außenbereich, vorgestellt. Die modell-basierte Erfassung der Systemkomponenten und -parameter kann sehr gut in einem gemeinsamen Prozess aller Systembeteiligter (Anwender, Betreiber, Hersteller, Entwickler, Personal, usw.) erfolgen. Ähnliche Herangehensweisen finden sich etwa bei UML-basierten HAZOP Analysen [8, 9] oder der Gefährdungsanalyse auf Szenarienbasis [1].

Wie auch bei generischen Gefährdungslisten in anderen Anwendungsdomänen [3, 2, 4] ermöglicht unsere Methodik eine einfache Abschätzung von Gefährdungssituationen in frühen Phasen der Systemkonzeption, und ist damit eine Form der “preliminary hazard analysis” (PHA). Die identifizierten Gefährdungen können in späteren Phasen unter Zuhilfenahme klassischer Analysemethoden [14] detaillierter betrachtet werden. In unserem Ansatz nehmen wir zudem eine *Bewertung* der Gefährdungen vor, welche sich automatisch aus den Risikoparametrisierungen des Systemmodells ableiten lassen. Damit sind unmittelbar die verschiedenen Risiken der identifizierten Gefährdungen ersichtlich.

Als Ausblick auf mögliche weiterführenden Arbeiten bietet der modell-basierte Ansatz einen direkten Übergang in die Identifikation von technischen Gefährdungen, die sich aus späteren design- und implementierungsspezifischen Entscheidungen ergeben. Dies erfordert im Wesentlichen eine Ausarbeitung der FTF-Komponente in unserem Modell. Liegen die Sicherheitsanforderungen, die sich aus den identifizierten Gefährdungen ableiten lassen, in einer entsprechend formalisierten Sprache vor, ließe sich das entstandene Systemmodell zudem für eine modell-basierte Sicherheitsanalyse [11] verwenden.

### Acknowledgement

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Technologie unter dem Förderkennzeichen 01MA09037 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

## Literatur

- [1] K. Allenby and T. Kelly. Deriving safety requirements using scenarios. In *5th IEEE International Symposium on Requirements Engineering*, pages 228–235. IEEE Computer Society, 2001.
- [2] D. Beisel, C. Reuß, E. Schnieder, and U. Becker. Automotive Generic Hazard List. In *11. Braunschweiger Symposium Automatisierungs-, Assistenzsysteme und eingebettete Systeme für Transportmittel*, Februar 2010.
- [3] J. Drewes and J. May. Structured approach of a generic (signalling) hazard list for railway (interlocking) systems. In *Proc. of the 5th European Congress and Exhibition on Intelligent Transport Systems and Services*, Hannover, 2005.
- [4] C.A. Ericson. *Hazard Analysis Techniques for System Safety*. Wiley, New York, 2005.
- [5] European Committee for Standardization (CEN). DIN EN 1525, Sicherheit von Flurförderzeugen: Fahrerlose Flurförderzeuge und ihre Systeme, 1997.
- [6] International Electrotechnical Commission (IEC). IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, 1998.
- [7] International Organization for Standardization (ISO). ISO 26262, Road vehicles – Functional safety. Final Draft International Standard, 2010.
- [8] P. Johannessen, C. Grante, A. Alminger, U. Eklund, and J. Torin. Hazard analysis in object oriented design of dependable systems. In *International Conference on Dependable Systems and Networks*, pages 507–512. IEEE Computer Society, 2001.
- [9] D. Martin-Guillerez, J. Guiochet, D. Powell, and C. Zanon. A UML-based method for risk analysis of human-robot interactions. In *Proceedings of SERENE 2010*, London, United Kingdom, April 2010.
- [10] Object Management Group (OMG). Unified Modeling Language: Superstructure, Version 2.3, Mai 2010.
- [11] T. Peikenkamp, A. Cavallo, L. Valacca, E. Böde, M. Pretzer, and E. M. Hahn. Towards a unified model-based safety assessment. In *SAFECOMP*, volume 4166 of *LNCS*, pages 275–288. Springer, 2006.
- [12] G. Ullrich, F. Simen, and T. Sommer-Dittrich. Quo vadis, FTS? In: *Hebezeuge und Fördermittel*, 45, HUSS-MEDIEN GmbH, 2005.
- [13] Verein Deutscher Ingenieure (VDI). Fahrerlose Transportsysteme (FTS). VDI Richtlinie 2510, Beuth Verlag, Berlin, 2005.
- [14] J.W. Vincoli. *Basic Guide to System Safety*. Wiley, New York, 2nd edition, 2006.