UNFÄLLE DURCH BESTMÖGLICHEN SICHERHEITSSTANDARD VERMEIDEN

Ein **Safety Management System** für automatisierte Fahrzeuge?

In automatisierten Fahrzeugen übernehmen Fahrerassistenzsysteme teilweise die Fahraufgabe, in autonomen Fahrzeugen wird der Fahrer sogar vollständig ersetzt. Doch wenn kein Verantwortlicher mehr das Fahrzeug führt, wer ist dann für die Sicherheit während des Betriebs zuständig? Dieser Artikel beschäftigt sich mit den Möglichkeiten und Vorteilen, die ein Safety Management System bringen kann.

Nach mehreren Zwischenfällen bei der Erprobung von automatisierten Fahrzeugen wird die Anwendung eines Safety Management Systems (SMS) für automatisierte Fahrzeuge vermehrt diskutiert und empfohlen. Beispielsweise hat das National Transportation Safety Board (NTSB) nach der Evaluierung eines tödlichen Unfalls bei der Erprobung eines automatisierten Fahrzeugs der Advanced Technologie Group von Uber Technologies, Inc. die Einführung eines Safety Management Systems befürwortet [1].

Was ist ein Safety Management System?

Safety Management Systeme werden bereits in anderen sicherheitskritischen Domänen wie der Luftfahrt, Schifffahrt und dem Schienenverkehr angewendet. Nach der Australian Civil Aviation Safety Authority (CASA) wird ein Safety Management System wie folgt definiert: „Ein Sicherheitsmanagementsystem ist ein systematischer Ansatz für das Sicherheitsmanagement, einschließlich Organisationsstrukturen, Verantwortlichkeiten, Richtlinien und Verfahren. Ein SMS ist skalierbar, sodass es an die Größe und Komplexität des Unternehmens angepasst werden kann“ [2].

Das Modell der Luftfahrt beruht auf vier Komponenten – Safety Policy, Safety Risk Management, Safety Assurance, Safety Promotion – und fünfzehn Elementen, die nach dem Standard der International Civil Aviation Organization (ICAO) vorgeschrieben werden [3].
Selbst wenn das Rahmenwerk des Safety Management Systems aus der Luftfahrt auf die Automobilindustrie und die Anwendung für automatisierte Fahrzeuge übertragen werden kann, sind zur Optimierung eventuelle Anpassungen notwendig. Tabelle 1 zeigt eine detaillierte Zusammenstellung der Elemente, inklusive Ergänzungen für die Automobilindustrie.

Allgemein ist die Safety Policy für das Management-Engagement und die Definition von Prozessen und organisatorischen Strukturen zuständig. Das Safety Risk Management dient der Identifizierung von Gefährdungen und dem Bewerten und Mildern von Risiken. Die Safety Assurance ist für das Bewerten der kontinuierlichen Effektivität der Risikomanagementstrategien da und die Safety Promotion trägt zur Verbreitung einer positiven Sicherheitskultur durch Training, Kommunikation und andere Aktionen bei [4].

SMS vs. Einsatz bekannter Sicherheitsstandards

Bestehende Sicherheitsstandards, die in der Automobilindustrie zum Einsatz kommen, sind gut etabliert und beinhalten unter anderem das Safety Management. Wozu wird dann ein Safety Management System benötigt?

Functional Safety Management wird nach dem Standard für funktionale Sicherheit von elektronischen-sicherheitsrelevanten Systemen definiert. Alle Akti-

vitäten, die während der Phasen des Produkt-/Prozesslebenszyklus der funktionalen Sicherheit erforderlich sind, werden hierzu beschrieben. Neben Aktivitäten werden auch Verantwortlichkeiten im Rahmen des Functional Safety Management definiert. Diese sind spezifisch für Personen und Positionen, Abteilungen und Organisationen. [5]

Für den sicheren Betrieb eines automatisierten Fahrzeugs wird eine allgemeine Sicherheit des Systems inklusive äußerer Einflüsse benötigt. Die funktionale Sicherheit von Straßenfahrzeugen beschreibt die „Abwesenheit eines unangemessenen Risikos aufgrund von Gefährdungen durch Fehlverhalten von E/E-Systemen" [6].

Demnach behandelt die funktionale Sicherheit Risiken bei Systemausfällen, deckt aber keine Sicherheitsrisiken ab, die ohne Systemausfall entstehen. Um den weiteren Gefährdungsbereich abzudecken, wurde der Standard „Safety Of The Intended Functionality" (SOTIF) eingeführt. Diese Norm soll zur Sicherheit in Situationen ohne Systemausfall beitragen und betrachtet hierfür System und Operational Design Domain (ODD). Der spezifizierte Betriebsbereich beinhaltet beispielsweise Parameter wie Straßentypen, Geschwindigkeitsbereich und Umgebungsbedingungen, in dem das automatisierte Fahrzeug operiert.
Im Rahmen der SOTIF wird zwischen vorhersehbaren und unvorhersehbaren Gefährdungen ohne Systemausfall unterschieden. Außerdem werden Gefährdungen auf Grundlage von vorsätzlichem Missbrauch des Systems betrachtet [7].

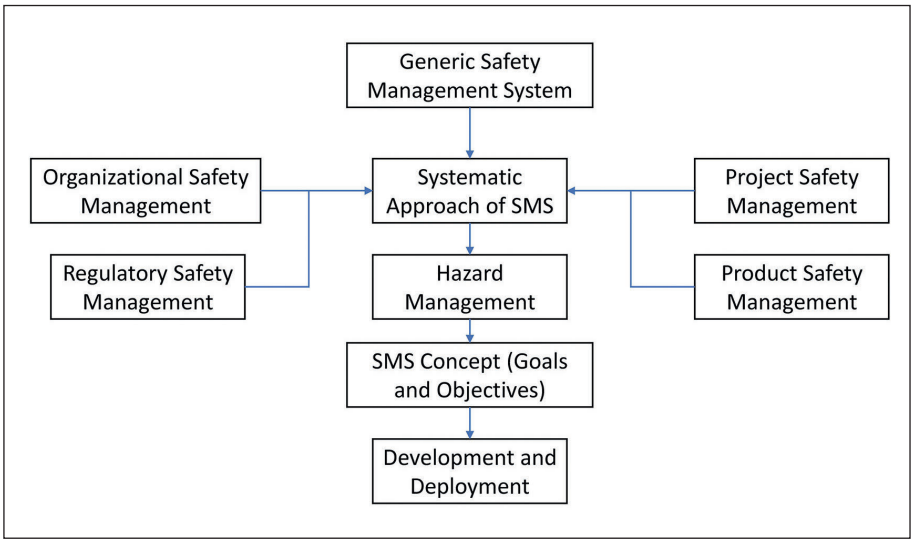

Bild 1: Systematische Herangehensweise für ein Safety Management System © Hochschule Kempten

Selbst wenn das Safety Management in den Sicherheitsstandards erwähnt wird, ist dieses nicht für das komplexe System eines automatisierten Fahrzeugs ausgelegt. Einige Elemente, Definitionen und Methoden stimmen mit den Inhalten des vorgesehenen Safety Management Systems überein, sind aber nicht ausreichend, um die allgemeine Sicherheit während der Entwicklung, Operation und Rückgang des automatisierten Fahrzeuges zu gewährleisten.

Components	Elements
Safety Policy	Management Commitment and Responsibility
	Safety Accountabilities
	Appointment of Key Safety Personnel
	Safety Managment System Implementation
	Contractors / Third Party Interfaces
	Coordination of Emergency Response Planning
	Safety Managment System Documentation
Safety Risk Management	Hazard Identification
	Risk Analysis (Severity and Exposure, Controllability)
	Risk Mitigation
	Human Factors in Risk Management
Safety Assurance	The Management of Change
	Safety Performance Monitoring and Measurement
	Safety Information System (SIS)
	Continuous Improvement of the Safety Managment System
	Documentation and Data Information Management
Safety Promotion	Training and Education
	Safety Communication

Tabelle 1: SMS-Komponenten und -Elemente für automatisierte Fahrzeuge © Hochschule Kempten

Ziele und Vorteile eines Safety Management Systems

Zusätzlich zum bereits erwähnten Ziel, den bestmöglichen Sicherheitsstandard für automatisierte Fahrzeuge zu gewährleisten, soll die allgemeine Sicherheit des Fahrsystems, sowie das Safety Management System an sich, kontinuierlich verbessert werden.

Eine höhere Sicherheit macht sich durch weniger Vorfälle und Unfälle bemerkbar. Des Weiteren ist die Schwere des Ereignisses neben der Auftretenswahrscheinlichkeit zu beachten. Die Stärken eines Safety Management Systems werden in anderen sicherheitskritischen Domänen bereits dokumentiert. Ein Rückgang an Vorfällen und Unfällen, eine Reduzierung von direkten und indirekten Kosten, Versicherungsprämien, Verbesserung der Mitarbeiterproduktivität und eine nachweisliche Sorgfalt bei rechtlichen und behördlichen Sicherheitsuntersuchungen, ist in der Luftfahrt zu verzeichnen [8].

Um solche Ergebnisse auch beim automatisierten Fahren zu erreichen, sind spezifische Anpassungen der Struktur notwendig. Idealerweise ist ein Rahmenwerk mit einem generischen Aufbau des Safety Management Systems vorhanden, das von jeder Organisation und für jedes Projekt angewendet und individuell erweitert werden

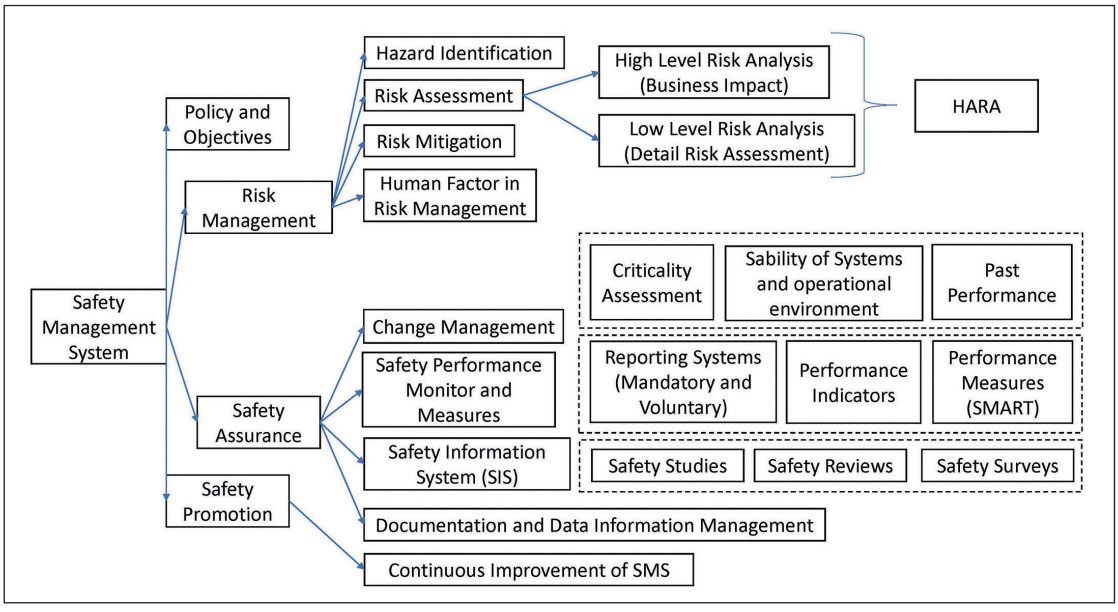

Bild 2: Detaillierte SMS-Komponenten, -Elemente und -Methoden

© Hochschule Kempten

kann. Diese Herangehensweise wird in Bild 1 veranschaulicht [9].

Um eine systematische und durchsichtige Struktur zu erhalten, werden das organisatorische, regulatorische, projekt- und produktspezifische Safety Management mit einbezogen. Anschließend werden die Gefährdungen bestimmt, um das individuelle Risiko-Management zu gestalten. Auf Basis der konkreten Gefährdungen lässt sich ein spezifisches SMS-Konzept zur Erreichung der Ziele definieren, bevor mit der Entwicklung und Bereitstellung begonnen wird.

Einige methodische Vorgehensweisen des Safety Management Systems sind bereits in den Unternehmen der Automobilindustrie etabliert und lassen sich somit einfach in die neue SMS-Struktur einbinden. Die zuvor erwähnten vier Komponenten können in organisatorisch und sicherheitsrelevant untergliedert werden. Somit beziehen sich die Safety Policy and Objectives, sowie die Safety Promotion auf die organisatorischen Strukturen und Bereitstellungen in einem Unternehmen. Das Risikomanagement und die Sicherheitsgarantie umfassen ständige Bearbeitung der Ereignisse, kontinuierliche Verbesserungen und methodische Arbeitsweisen. Bild 2 gibt eine Anregung, welche bekannten Hilfsmittel und Techniken angewandt werden können, um die Elemente der SMS-Komponenten umzusetzen.

Die organisatorischen Komponenten hingegen stellen sicher, dass die Inhalte systematisch, strukturiert und transparent umgesetzt und dokumentiert werden. Die Implementierung neuer Sicherheitsziele und die Annahme anderer Rollen, Positionen, Verantwortlichkeiten und Kommunikationswege kann in einem Unternehmen eine größere Herausforderung darstellen. Dennoch ist es von großem Interesse, ein Safety Management System in der Automobilindustrie, insbesondere für automatisierte Fahrzeuge zu etablieren, weil der Schutz aller Verkehrsteilnehmer als größtes Sicherheitsziel angesehen wird. Das ist auch der ursprüngliche Grund für die Entwicklung von automatisierten Fahrzeugen gewesen. Laut des statistischen Bundesamtes werden rund 98 Prozent der Unfälle mindestens teilweise von Menschen verursacht [10].

Durch automatisierte oder zukünftig auch autonome Fahrzeuge sollen die Verkehrsunfälle auf Basis von menschlichem Versagen ausgeschlossen werden. ■ (eck)

www.hs-kempten.de/ifm

Quellenverzeichnis

[1] National Transportation Safety Board, "Collision between Vehicle Controlled by Developmental Automated Driving System and Pedestrian," Washington D.C., National Transportation Safety Board Public Meeting of November 19, 2019.

[2] CASA, "Australian Goverment Civil Aviation Safety Authority,": www.casa.gov.au/safety-management/safety management-systems/what-safety-management-and-safety-management-systems, Last modified 26th March 2020

[3] International Civil Aviation Organization, "Safety Management Manual (SMM)," ICAO publication, 2012.

[4] D. A. Ludwig, C. R. Andrews, N. R.-t. Veen and C. Laqui, "ACRP Report 1 Safety Management System for Airports," Washington D.C., Transportation Research Board, 2007.

[5] IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements," iso-org, 2010.

[6] ISO 26262–1, "Road vehicles — Functional safety: Concept Phase," iso-org, 2018.

[7] ISO/PAS 21448:2019, "Road vehicles — Safety of the intended functionality," iso-org, 2019.

[8] R. Yeun, P. Bates and P. Murray, "Aviation safety management systems," in World Review of Intermodal Transportation Research, South East Queensland, Griffith University, Vol. 5, pp. 6, 2014.

[9] M. Khatun, F. Wagner, R. Jung and M. Glaß, "An Approach of a Safety Management System for Highly Automated Driving System," Upcoming conference proceedings-5th International Conference on System Reliability and Safety (ICSRS), Manuscript Accepted September 2021.

[10] Statistisches Bundesamt (DESTATIS). Fachserie 8, Reihe 7, Verkehr, Verkehrsunfälle 2017. Germany, 2018.

Florence Wagner, Safety Management und Funktionale Sicherheit, IFM – Institut für Fahrerassistenz und vernetzte Mobilität an der Hochschule Kempten. © Hochschule Kempten

Unterstützt durch **Prof. Dr. Rolf Jung** und **Marzana Khatun**, Institut für Fahrerassistenz und vernetzte Mobiliät an der Hochschule Kempten.