BMBF-Verbundprojekt: SATiSFy

Förderkennzeichen: 16KIS0821K

Projektlaufzeit: 01.05.2018 bis 30.04.2021 (Verlängerung bis 31.07.2021)

Schlussbericht Teil 1: Kurzbericht

Requirements Engineering zur frühzeitigen Validierung von Safety-und Security-Anforderungen in autonomen Fahrzeugen

Version: 1

Erstelldatum: 26.01.2022

Autoren: Philip Stolz und Markus Eberhardt (HOOD)

Zuwendungsempfänger: HOOD GmbH (HOOD)

1 Ziel des Forschungsprojekts

Das Ziel des Teilvorhabens „Requirements Engineering zur frühzeitigen Validierung von Safety- und Security-Anforderungen in autonomen Fahrzeugen“ war:

- Methoden zur gesamtheitlichen Spezifikation zu analysieren
- Geeignete Methoden und Praktiken zur Ermittlung von Safety- und Security-Anforderungen zu identifizieren
- Informationsmodelle zur Strukturierung von Safety- und Security-Anforderungen zu entwickeln
- Modellierungstechniken zur Visualisierung von Safety- und Security Anforderungen zu untersuchen
- Agile Vorgehensweisen zur frühzeitigen Validierung von Safety-und Security-Anforderungen zu erproben

Der Stand von Wissenschaft und Technik, auf dem aufgesetzt wurde, ist ausführlich im Kapitel 3 der Teilvorhabensbeschreibung beschrieben.

2 Inhalt des Forschungsprojekts

Nachfolgende Inhalte waren Bestandteil des Forschungsprojektes:

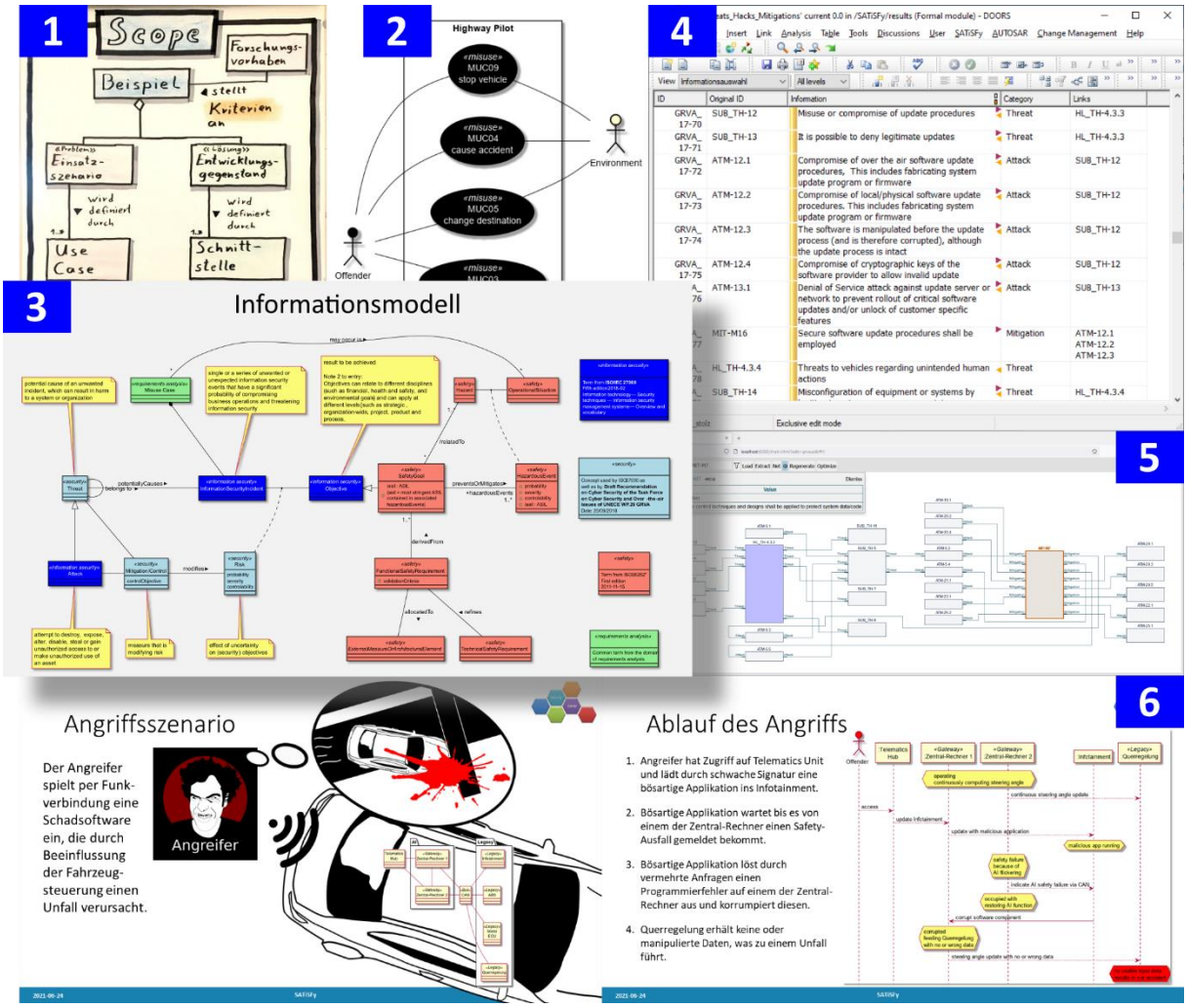
- Analyse des Stands der Wissenschaft zu Verifikations- und Validierungsstrategien
- Definition eines Bedrohungsszenarios für SAF basierend auf Misuse-Cases
- Ableiten von Kriterien an ein kombiniertes Informationsmodell für Safety und Security aus den Validierungsstrategien
- Evaluation möglicher Informationsmodelle und Identifikation sich daraus ergebender Kriterien
- Entwicklung eines geeigneten Informationsmodells basierend auf den o.g. Kriterien
- Definition einer geeigneten Werkzeugintegration zur Nutzung und Visualisierung des Informationsmodells
- Validierung des entwickelten Informationsmodells mittels einer Werkzeugintegration

Für die die Bearbeitung der Inhalte fand eine Zusammenarbeit mit folgenden Konsortialpartnern statt: Concept Engineering, DFKI, EKUT, KAOS, Bosch, Volkswagen.

3 Ergebnis des Forschungsprojekts

HOOD hat ein Vorgehen entwickelt, um mit den Konsortialpartnern den Betrachtungsgegenstand zu definieren und dabei eine klare Trennung zwischen Einsatzszenario und Entwicklungsgegenstand vorzunehmen [1]. Basierend darauf entstand im Konsortium frühzeitig eine Einigung über die Fokussierung auf einen Autobahnpiloten. Mit Hilfe eines Angreifermodells des Konsortialpartners KAOS hat HOOD Misuse-Cases im Kontext dieses Autobahnpilotens gebildet, um weiter in die Anforderungsanalyse einzusteigen [2].

Für eine weitere Anforderungsanalyse hat HOOD nach vorheriger Ermittlung der zu erfüllenden Kriterien, ein Informationsmodell entwickelt, welches als Metamodell für ein kombiniertes Safety- und Security-Anforderungsmodell genutzt werden kann [3]. Dieses Informationsmodell wurde exemplarisch in einem Anforderungsmanagementwerkzeug implementiert [4]. Die darin abgebildeten Sicherheitsanforderungen wurden durch die Integration des Werkzeugs EEvision unseres Konsortialpartners Concept Engineering explorierbar gemacht [5].



In einem gemeinsam eruierten Angriffsszenario für den Autobahnpiloten, konnte HOOD mit Hilfe der erarbeiteten Ergebnisse Anforderungen ermitteln, welche durch die Beiträge der Konsortialpartner entlang eines Produktentwicklungszyklusses erfüllt werden konnten [6].

Der Einsatz von künstlicher Intelligenz (KI) im Kontext des RE wurde nicht untersucht, da der Fokus des Projektes auf einem gemeinsamen Informationsmodell für Safety- und Security-Anforderungen lag. Eine diesbezügliche Hypothese von HOOD konnte nicht validiert werden.

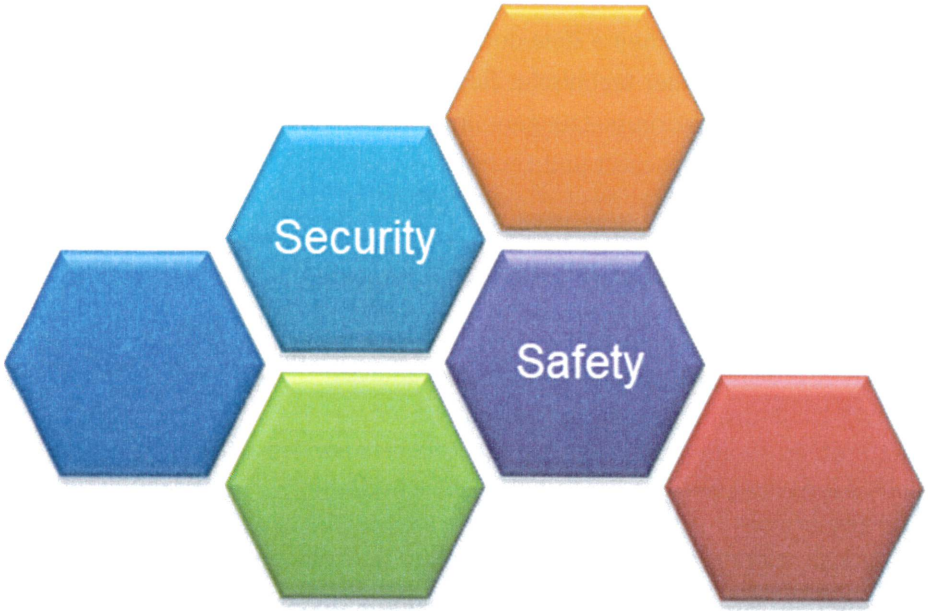
Es hat keine weitere Zusammenarbeit mit anderen Forschungseinrichtungen stattgefunden.

4 Nutzen und Anwendungsmöglichkeiten der Projektergebnisse

HOOD beabsichtig, nach Ende des Forschungsprojektes, basierend auf dem im Forschungsprojekt genutzten Verfahren, ein generelles Verfahren zur Anpassung von Anforderungsmanagementwerkzeugen zu entwickeln, mit dem das erarbeitete Informationsmodell potenziell in jedem verfügbaren Anforderungsmanagementwerkzeug umgesetzt werden kann.

Gemäß unserer Untersuchung zur Dissemination der Ergebnisse, beabsichtigt HOOD, im Modus „online, asynchron“ die erarbeiteten Ergebnisse an seine Kunden zu vermitteln. Daraus soll für HOOD idealerweise eine erhöhte Nachfrage an Beratung im Bereich Safety- und Security-Requirements-Engineering entstehen.

HOOD beabsichtigt außerdem die erarbeiteten Inhalte, wie z.B. das Informationsmodell, in stattfindenden systems-engineering-spezifischen Workshops, wie z.B. auf der REConf (www.REConf.de), kontextspezifisch zu vermitteln.



BMBF-Verbundprojekt: SATiSFy
Förderkennzeichen: 16KIS0821K
Projektlaufzeit: 01.05.2018 bis 30.04.2021 (Verlängerung bis 31.07.2021)

Schlussbericht Teil 2: Fachbericht

Frühzeitige Validierung von SAfeTy-und Security-Anforderungen in autonomen Fahrzeugen Teilvorhaben: Requirements Engineering zur frühzeitigen Validierung von SAfeTy-und Security-Anforderungen in autonomen Fahrzeugen

Version: 1
Erstelldatum: 18.01.2022
Autoren: Philip Stolz, Markus Eberhardt
Zuwendungsempfänger: HOOD GmbH (HOOD)
Ansprechpartner: Philip Stolz
Keltenring 7
82041 Oberhaching

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS0821K gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

I. Ziele

I.1 Problemstellung und allgemeine Ziele des Vorhabens

Das Ziel des Teilvorhabens „Requirements Engineering zur frühzeitigen Validierung von Safety- und Security-Anforderungen in autonomen Fahrzeugen" war:

- Methoden zur gesamtheitlichen Spezifikation zu analysieren
- Geeignete Methoden und Praktiken zur Ermittlung von Safety- und Security-Anforderungen zu identifizieren
- Informationsmodelle zur Strukturierung von Safety- und Security-Anforderungen zu entwickeln
- Modellierungstechniken zur Visualisierung von Safety- und Security Anforderungen zu untersuchen
- Agile Vorgehensweisen zur frühzeitigen Validierung von Safety-und Security-Anforderungen zu erproben

I.2 Wissenschaftliche und/oder technische Ziele des Vorhabens

Die Aufgabe und Arbeitsziele von SATiSFy liegen darin, die komplexe Verbindung von Security und Safety-Anforderungen für den Kontext eines SAF als heterogenes Mehrkomponentensystem frühzeitig beherrschbar (mittels der Erfassung geeigneter Sicherheitsanforderungen und -komponenten im Designprozess) und nachvollziehbar (mittels geeigneter Verifikations- und Validationsmethoden) zu machen.

I.3 Ausgangssituation und Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

I.3.1 Der Stand von Wissenschaft und Technik

Im agilen Kontext gibt es derzeit wenige verbreitete Techniken zur Anforderungserhebung und -validierung (1). Die meisten agilen Praktiken konzentrieren sich auf die Softwareerstellung im Nicht-Embedded-Bereich. Es existieren aber bereits erste Konzepte für agile Praktiken im sicherheitsrelevanten und regulierten Bereich wie z.B. SafeSCRUM (2), es sind aktuell aber keine agilen Praktiken bekannt, die durchgängig die Safety-und Security Thematik im Umfeld des autonomen Fahrens in der erforderlichen Tiefe adressieren. Im klassischen Requirements Engineering (3) (4) gibt es im Automobil Sektor etablierte Techniken zur Identifikation und Abstimmung von Anforderungen, die vor allem von der Herstellerinitiative Software (HIS) (5) getrieben sind. Ein Beispiel hierfür ist der OMG ReqIF Standard (6) zum elektronischen Austausch von Anforderungen.

I.3.2 Neuheit und Attraktivität des Lösungsansatzes

Die verbreitetsten Vorgehensweisen wie z.B. automotive SPICE (7) werden in der Praxis primär vertrags-getriggert gelebt, orientieren sich aber nicht am tatsächlichen Bedarf der Entwicklungsprojekte. Aufgrund dieser Erkenntnis ist der Themenkomplex „Agile Vorgehensweisen zur frühzeitigen Validierung von Safety-und Security-Anforderungen" in diesem Forschungsvorhaben aufgenommen worden.

I.3.3 Bisherige Arbeiten des Antragstellers

Wesentliche Beiträge und bisherige Arbeiten im Arbeitsgebiet des Vorhabens von HOOD sind u.a.:

- HOOD Generic RM&EProcess zur Konsolidierung von Anforderungen über mehrere Ebenen im Informationsmodell
- Unterstützung des Agire (http://agile-requirements-institute.org/) bei Schulungen von Requirements Engineeringim agilen Kontext (CARS)
- Mitarbeit im Programmausschuss wichtiger Konferenzen wie OOP, Manage Agile, REConf
- Mitarbeit im Requirements-Engineering bei den namhaften deutschen OEM im Automotivebereich
- Coaching agiler Projekte
- Konzeption eines Informationsmodells für die Begriffswelt der ISO26262

I.4 Abgrenzung und Zusammenarbeit mit anderen Projekten

HOOD sind keine anderen Projekte bekannt, welches sich mit den Zielen dieses Vorhabens direkt beschäftigen.

Das Projekt SAFE4I („Sicherer Automatischer Software-Entwurf für Industrieanlagen"; Förderkennzeichen „01IS17032G"; Projektlaufzeit 01.10.2017 - 30.09.2021) beschäftigt sich mit Safety-Anforderungen und ihrer Umsetzung in sicherer Software und Firmware. Im Gegensatz zu SATiSFy liegt bei SAFE4I der Fokus auf Software in der Internet of Things / Industrial Automation Domäne und nicht im Automotivebereich. Die in SATiSFy adressierte frühzeitige Validierung der Anforderungen wird nicht erforscht

Das Projekt autoSWIFT („Schneller entlang der Automobil-Wertschöpfungskette mit Innovationen für Technologieführerschaft sorgen"; Förderkennzeichen „16ES0356-61"; Projektlaufzeit 01.09.2015 – 31.08.2018) konzentriert sich auf die Beschleunigung von Mikroelektronik-Innovationen entlang der Wertschöpfungskette in der Automobilbranche und erforscht hierzu passende Modelle der Zusammenarbeit sowie neu technologische Ansätze. Die in SATiSFy adressiere Safety- und Security Thematik wird in autoSWIFT nicht betrachtet.

Im Projekt SATiSFy fand keine weitere Zusammenarbeit mit anderen Projekten oder Forschungsvorhaben statt.

Während des Projektes sind keine Ergebnisse von dritter Seite bekannt geworden, welche für die Durchführung des Vorhabens relevant waren.

II. Technische Ergebnisse

Die Arbeiten von HOOD haben als zentrales Element ein Anforderungsinformationsmodell. In einem typischen Produktentwicklungszyklus wäre dies in der Spezifikationsphase einsetzbar.

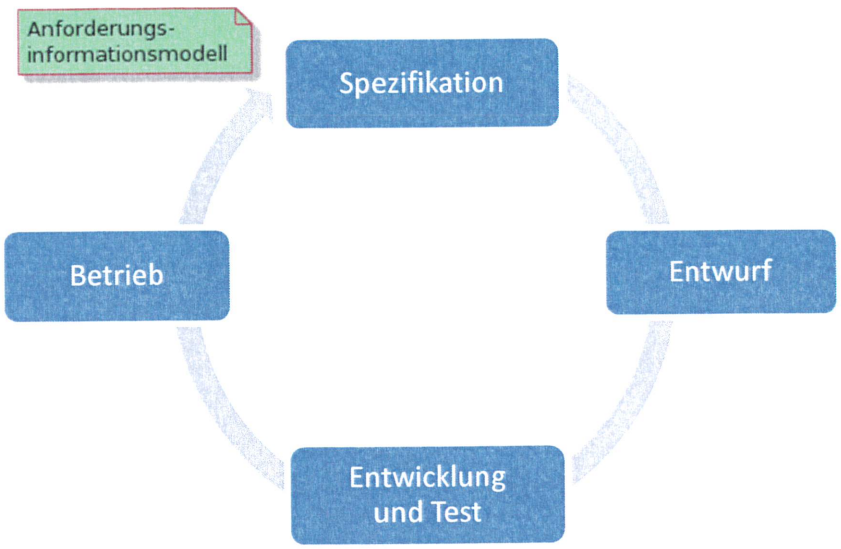


Abbildung 1 Das Anforderungsinformationsmodell im Produktentwicklungszyklus

II.1 Arbeitspaket 1: Sicherheits- und Anforderungsanalyse

AP1 umfasst zum einen die Analyse möglicher Bedrohungsszenarien und daraus resultierenden Attacken und zum anderen eine Bestandsaufnahme existierender Designmechanismen und -komponenten für SAF-Systeme.

II.1.1 Teil AP 1a: Bedrohungs-und Anforderungsanalyse

II.1.1.1 Problemstellung und Ziele aus der Teilvorhabensbeschreibung

Aus der Analyse möglicher Bedrohungsszenarien werden potentielle Angriffsarten bzw. -muster ermittelt. Dies betrifft insbesondere Bedrohungen, die sich aus der Autonomie der Fahrzeuge und damit den potentiellen Veränderungen in ihrer Umgebung ergeben. Zusammen mit einer zu spezifizierenden Modellierung des Angreifers bilden sie den Ausgangspunkt für die Definition des Schutzbedarfs eines SAFs sowie den daraus resultierenden Sicherheitsanforderungen an die Architektur bzw. die Komponenten des SAF.
Ziele sind die:

- Analyse der Bedrohungsszenarien
- Spezifikation des Angreifermodells
- Identifikation von Safety-Anforderungen (nach Komponenten/Gesamtsystem gegliedert)
- Identifikation von Security-Anforderungen (nach Komponenten/Gesamtsystem gegliedert)

II.1.1.2 Lösungsweg aus der Teilvorhabensbeschreibung

- Kriterien in Hinblick auf die Erstellung eines geeigneten Informationsmodells für Safety- und Security-Anforderungen identifizieren
- Analyse der Bedrohungsszenarien und der Identifikation der verschiedenen Anforderungen im SAF-Kontext unterstützen

II.1.1.3 Ergebnisse

II.1.1.3.1 Herleitung und Identifikation der Bedrohungsszenarien

HOOD hat ein Metamodell entwickelt, dass zum Finden von Bedrohungsszenarien genutzt werden kann. Das Modell kam außerdem zu Beginn des Forschungsprojektes zum Einsatz, um mit den Konsortialpartnern einen gemeinsamen Systemkontext zu finden.

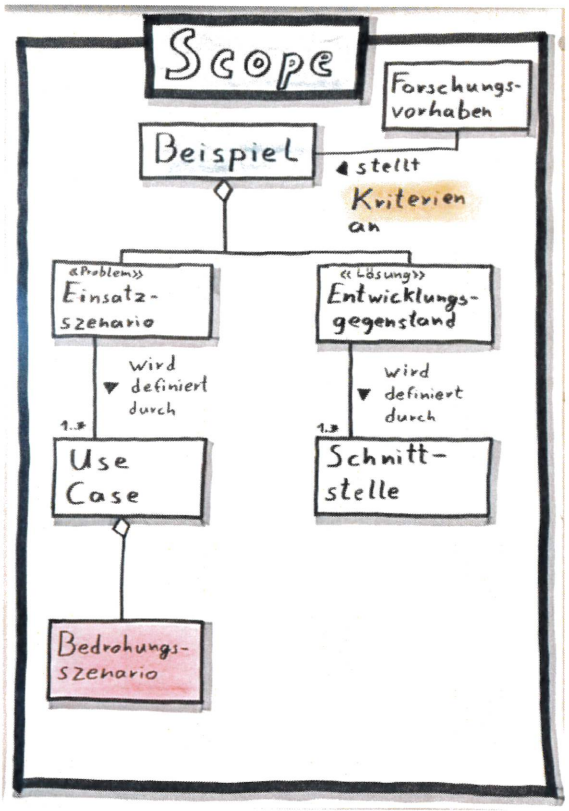


Abbildung 2 HOOD-Metamodell zum Erheben des gemeinsamen Systemkontexts

Im Konsortium wurde als gemeinsamer Entwicklungs-/Betrachtungsgegenstand ein Systemszenario identifiziert, in welchem zwei Zentralrechner die notwendigen Funktionen für einen Autobahnpilot realisieren.
Ausgehend davon, haben wir uns entschieden, das Bedrohungsszenario als Einstiegspunkt in eine Security-Analyse zu wählen. Zu dem gemeinsamen Systemszenario haben wir zunächst Use Cases identifiziert. Danach konnten wir einen Partnerbeitrag integrieren, indem wir auf der Basis eines Angreifermodells des Konsortialpartners KAOS mit demselben Vorgehensprinzip ergänzend Misuse Cases identifiziert haben.

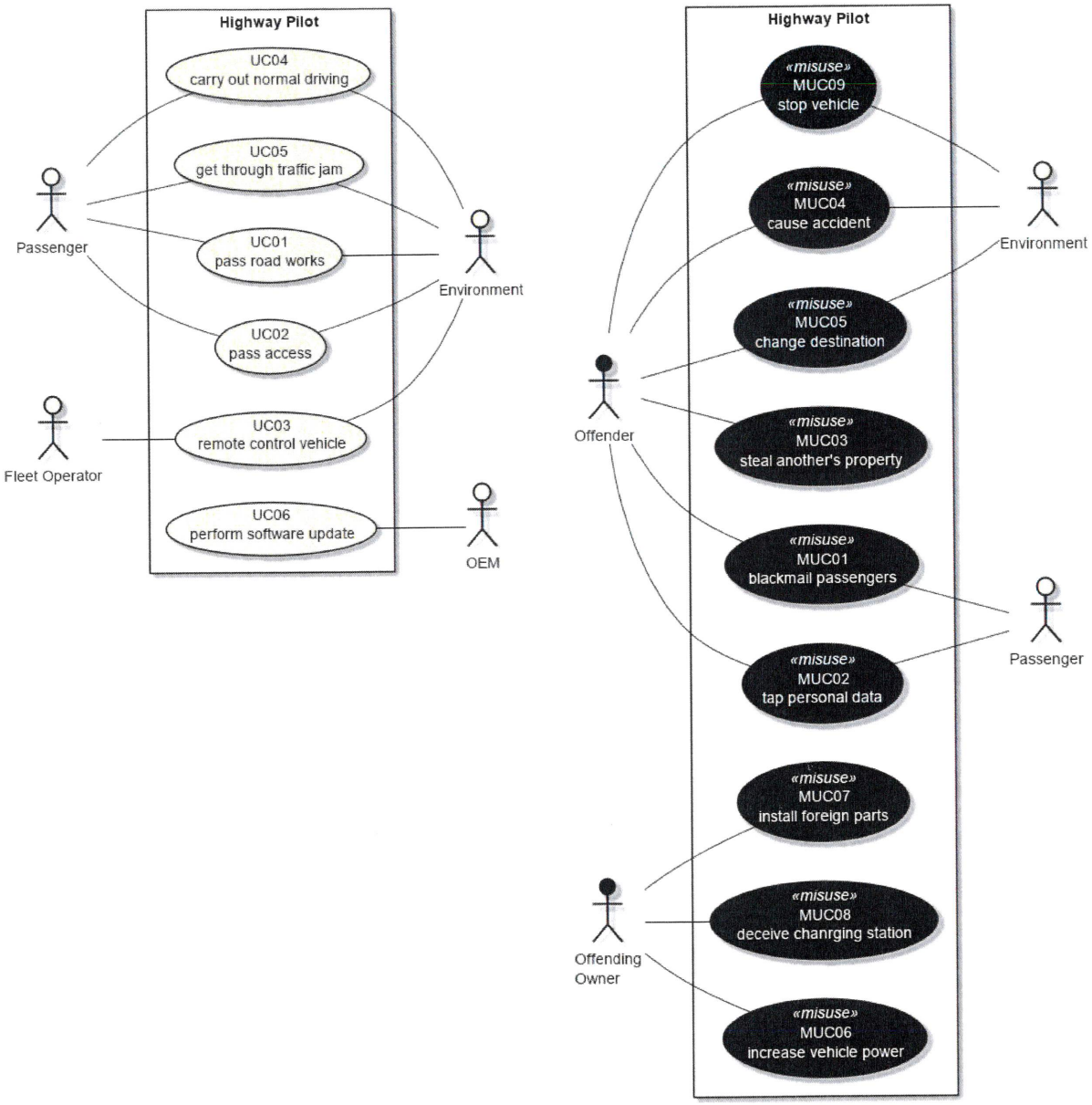


Abbildung 3 Use Cases und Misuse Cases für den Autobahnpiloten

II.1.1.3.2 Kriterien an ein kombiniertes Safety- und Security-Anforderungs-Informationsmodell

Ausgehend von den durch diese Analyse gewonnen Erkenntnissen konnten wir folgende Kriterien an ein kombiniertes Safety- und Security-Anforderungs-Informationsmodell ableiten:

1. das Informationsmodell muss den Misuse Case als Element enthalten
2. das Informationsmodell muss Safety- und Security miteinander in Beziehung setzen
3. die Elemente des Informationsmodells müssen Informationseinheiten repräsentieren, die sich bzgl. Security aus der Analyse von Bedrohungsszenarien ermitteln lassen

Weitere Details hierzu sind dem HOOD-Meilensteinbericht M01 (8) zu entnehmen.

II.1.1.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Analyse der Bedrohungsszenarien	Erfüllt
Spezifikation des Angreifermodells	Erfüllt

Ziel aus Teilvorhabensbeschreibung	Bewertung
Identifikation von Safety- und Security-Anforderungen (nach Komponenten/Gesamtsystem gegliedert)	*Erfüllt für das Gesamtsystem, auf eine Gliederung nach Komponenten wurde verzichtet, da eine Betrachtung auf Szenarienebene weiterverfolgt wurde.*

II.1.2 Teil AP 1b: Aufarbeitung des Standes der Forschung und Technik für Safety- und Security Methoden

II.1.2.1 Problemstellung und Ziele aus der Teilvorhabensbeschreibung

Es erfolgt eine Analyse und Wertung des Standes der Forschung und Technik zu existierenden Methoden sowie Designelemente zur Überprüfung der Einhaltung von Sicherheitsanforderungen (Security & Safety). Die Erfassung dieser existierenden Schutzmechanismen und Techniken fließt in die Spezifikation des gesamtheitlichen Betrachtungsansatzes ein.
Ziele sind:

- Stand der Verifikation/Validation von Safety-Anforderungen für SAF-Systeme
- Stand der Verifikation/Validation von Security-Anforderungen für SAF-Systeme
- Stand formaler Beschreibungssprachen für kombinierte Safety-und Security-Anforderungen

II.1.2.2 Lösungsweg aus der Teilvorhabensbeschreibung

- branchenübergreifende Methoden zur Verifikation und Validierung aufbereiten
- Partnerbeiträge integrieren
- Gemeinsam mit den Partnern, Stand zu Technik und Forschung aufarbeiten und abgleichen
- Implikation auf mögliche Informationsmodelle untersuchen

II.1.2.3 Ergebnisse

II.1.2.3.1 Stand der Technik zu Verifikation und Validierung von sicherheitskritischen Systemen

Die folgende Tabelle fasst den von uns erfassten Stand zusammen. Die Spalte Verifikations- / Validierungs-Kategorie stellt dabei generelle Vorgehensweisen dar, die wir durch Literaturrecherche extrahieren konnten. Die Spalte Charakteristika enthält unsere Einordnung in Bezug auf die Nutzung eines Modells und die Charakteristik eines darauf basierenden Tests.

Tabelle 1 Verifikations- / Validierungs-Kategorien

Lfd. Nr.	Verifikations- / Validierungs-Kategorie	Kurzbeschreibung	Charakteristika
1	Modellbasiertes Testen	Testfälle werden aus einem Verhaltensmodell des Systems oder des Systemkontexts generiert.	Modell: Abbildung der Problemdomäne: Verhalten Test: dynamisch
2	Formale Methoden	Die formale Verifikation verwendet mathematische Methoden, um zu beweisen, dass eine Eigenschaft auf einem bestimmten System gilt.	Modell: Abbildung der Problemdomäne: Eigenschaften Abbildung der Lösungsdomäne: Struktur & Verhalten Test: statisch
3	Semi-formale Verfahren	Anforderungsspezifikationen werden semi-formal beschrieben, so dass Techniken der formalen Verifikation und Simulation zur automatischen Testgenerierung kombiniert werden können.	Modell: Abbildung der Problemdomäne: Struktur & Verhalten Test: dynamisch
4	Laufzeitverifikation	Definition des erlaubten Laufzeitverhaltens durch formal spezifizierte Korrektheitseigenschaften. Die Korrektheitseigenschaften werden zur Laufzeit geprüft. (9)	Modell: Abbildung der Problemdomäne: statische Regeln Test: dynamisch
5	Physisches Prototyping	Prüfen des Systemverhaltens im Zusammenspiel von Hardware, Software, Mechanik, Hydraulik etc. durch prototypische Integration.	Modell: Abbildung der Lösungsdomäne: statisch & dynamisch.

			Test: dynamisch & statisch
6	Informale Methoden	Prüfen mittels menschlicher Interpretation und Beurteilung	Modell: Modellbildung möglich, aber nicht charakteristisch. Test: dynamisch & statisch
7	Konformitätstest (conformance testing / compliance testing)	*Der Konformitätstest ist eine Black-Box-Testtechnik, die darauf abzielt, zu überprüfen, ob eine Implementierung mit ihrer Spezifikation konform ist.* Übersetzt aus (10)	Modell: Falls Modellbildung erfolgt, dann zur Abbildung der Problemdomäne: statisch & dynamisch. Test: dynamisch & statisch
8	Akzeptanzprüfung	Validierungsmethode, die bei ausreichender Abdeckung die Sicherheit bietet, dass ein System die informalen Kundenanforderungen erfüllt (11)	Modell: Falls Modellbildung erfolgt, dann sind Abbildung der Problemdomäne oder Lösungsdomäne möglich, sowohl statische als auch dynamische. Test: dynamisch (z.B. durch Simulation) & statisch
9	Abdeckungs- und Überdeckungsmessungen (coverage measurements)	Metriken zur Vollständigkeitsprüfung von Tests	Modell: Modellbildung über Problemdomäne kann Messung von Anforderungsüberdeckung unterstützen, sowohl bzgl. Verhalten als auch Struktur. Test: dynamisch & statisch

Weitere Details hierzu sind dem HOOD-Meilensteinbericht M01 (8) zu entnehmen.

II.1.2.3.2 Abgeleitete Kriterien für das Informationsmodell

Unsere Literaturrecherche hat ergeben, dass der Großteil der Ansätze, die im Umfeld von Validierung- und Verifikation in der Forschung veröffentlicht werden auf einer Form von Modellbildung basieren.
Wir konnten die Modellbildungen entlang von zwei Dimensionen kategorisieren:

1. Modellgegenstand: Anforderungen oder Systeme bzw. Problem- oder Lösungsdomäne
2. Modellinhalt: statisch oder dynamisch, d.h. bildet das Modell statische Eigenschaften (z.B. durch Regeln) ab oder bildet es Abläufe, z.B. in Form von Szenarien oder Zustandsautomaten ab.

Tabelle 2 Modellkategorisierung

		Modellgegenstand	
		Problemdomäne	**Lösungsdomäne**
Modellinhalt	**statisch**	1. Abbildung von Eigenschaften und Bedingungen die gelten müssen.	2. Abbildung von Systemstrukturen
	dynamisch	3. Abbildung von Abläufen, die erwartet werden.	4. Abbildung des Systemverhaltens

Nach diesen Betrachtungen sind wir zu dem Schluss gekommen, dass als Kriterien an ein entsprechendes Informationsmodell, dieses die Kategorien 1 und 3 abdecken muss. D.h., es muss möglich sein, sowohl Abläufe als auch Eigenschaften zu erfassen.
Weitere Details hierzu sind dem HOOD-Meilensteinbericht M01 (8) zu entnehmen.

II.1.2.3.3 Potenzielle Informationsmodelle

Als potenzielle Informationsmodelle wurden ein einfaches Ebenenmodell für Anforderungen, ein allgemeines Informationsmodell für Anforderungen, ein komplexes Ebenenmodell für

Anforderungen, ein komplexes Modell einer einzelnen Anforderung und der HOOD-Ansatz zum Erheben des gemeinsamen Systemkontextes gefunden.
Weitere Details hierzu sind dem HOOD-Meilensteinbericht M02 (12) zu entnehmen.

II.1.2.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Stand der Verifikation/Validation von Safety- und Security-Anforderungen für SAF-Systeme	Erfüllt
Stand formaler Beschreibungssprachen für kombinierte Safety-und Security-Anforderungen	Erfüllt

II.2 Arbeitspaket 2: Framework für sichere SAF-Architekturen

AP 2 umfasst die Erstellung des grundlegenden Frameworks und Methodik zur Erfassung, Integration und Verifikation der Safety-und Securityanforderungen eines SAF. Dazu wird zunächst die Architektur der einzelnen Komponenten betrachtet (Komponentenebene). Im nächsten Schritt werden die verschiedenen Sicherheitsanforderungen hinsichtlich ihrer wechselseitigen Kompatibilität untersucht und Mechanismen entwickelt, um solche Anforderungen in verschiedenen Richtungen hinsichtlich einer späteren Verifikation zu dekomponieren.

II.2.1 Teil AP 2a: Definition von Zielkriterien für Sicherheitsanforderungen

II.2.1.1 Problemstellung und Ziele aus der Teilvorhabensbeschreibung

Die verschiedenartigen Sicherheitsanforderungen (Safety und Security) werden (im Sinne einer multilateralen Sicherheit) hinsichtlich ihrer Integrationsmöglichkeit und ihren statischen und dynamischen Abhängigkeiten analysiert und entsprechend klassifiziert. Es werden Zielkriterien für die Gewichtung der verschiedenen Anforderungen entwickelt, um zum einen konkurrierende Safety-und Security-Anforderungen gegeneinander ausbalancieren und zum anderen die Notwendigkeit von Anforderungen in verschiedenen Betriebsphasen (z.B. Normalbetrieb, Notbetrieb, Recovery, etc.) beurteilen zu können, u.a.:

- Festlegung von Zielkriterien für Sicherheitsanforderungen an SAF-Systeme
- Analyse der Abhängigkeiten der verschiedenen Sicherheitsanforderungen
- Integrierbarkeit und Verträglichkeit solcher Sicherheitsanforderungen
- Identifikation möglicher Abschwächungen von Sicherheitsanforderungen

II.2.1.2 Lösungsweg aus der Teilvorhabensbeschreibung

- Zielkriterien konzipieren
- Potentielle Informationsmodelle aus AP 1 parametrisieren

II.2.1.3 Ergebnisse

II.2.1.3.1 **Safety- und Security-Anforderungsinformationsmodell**

Details zu den nachfolgend aufgeführten Ergebnissen sind dem HOOD-Meilensteinbericht M02 (12) zu entnehmen.

II.2.1.3.1.1 Zielkriterien an ein geeignetes Informationsmodell

ZK-1 Das Informationsmodell muss Informationseinheiten klassifizieren (beispielsweise durch Klassen).

ZK-2 Das Informationsmodell darf Eigenschaften von Informationseinheiten als Attribute definieren.

ZK-3 Das Informationsmodell muss Beziehungen zwischen Informationseinheiten definieren (beispielsweise durch Assoziationen).

ZK-4 Das Informationsmodell darf Generalisierungen nutzen.

ZK-5 Das Informationsmodell muss es ermöglichen, eine Information als Misuse Case zu klassifizieren.

ZK-6 Das Informationsmodell muss Safety- und Security miteinander in Beziehung setzen.

ZK-7 Das Informationsmodell muss es ermöglichen, das Risiko sowohl für Safety- als auch Security-Erwägungen zu erfassen.

ZK-8 Das Informationsmodell muss es ermöglichen, Risiken gemäß ihrer Eintrittswahrscheinlichkeit, der Schwere ihrer Auswirkung und der Beherrschbarkeit zu bewerten.

ZK-9 Das Informationsmodell muss es ermöglichen, risikoreduzierende Maßnahmen zu erfassen.

II.2.1.3.1.2 Dokumentation des Informationsmodells

Das hier aufgeführte Informationsmodell wurde mit dem Ziel entwickelt, die aufgestellten Zielkriteren zu erfüllen. Zur Modellierung kam das UML-Klassendiagramm zum Einsatz. Eine Dokumentation über die genaue Verwendung von UML kann dem HOOD-Meilensteinbericht M02 **(12)** oder auch aus Kapitel II.2.3.3.1 entnommen werden.Im Folgenden wird die grafische Repräsentation des Informationsmodells dargestellt.

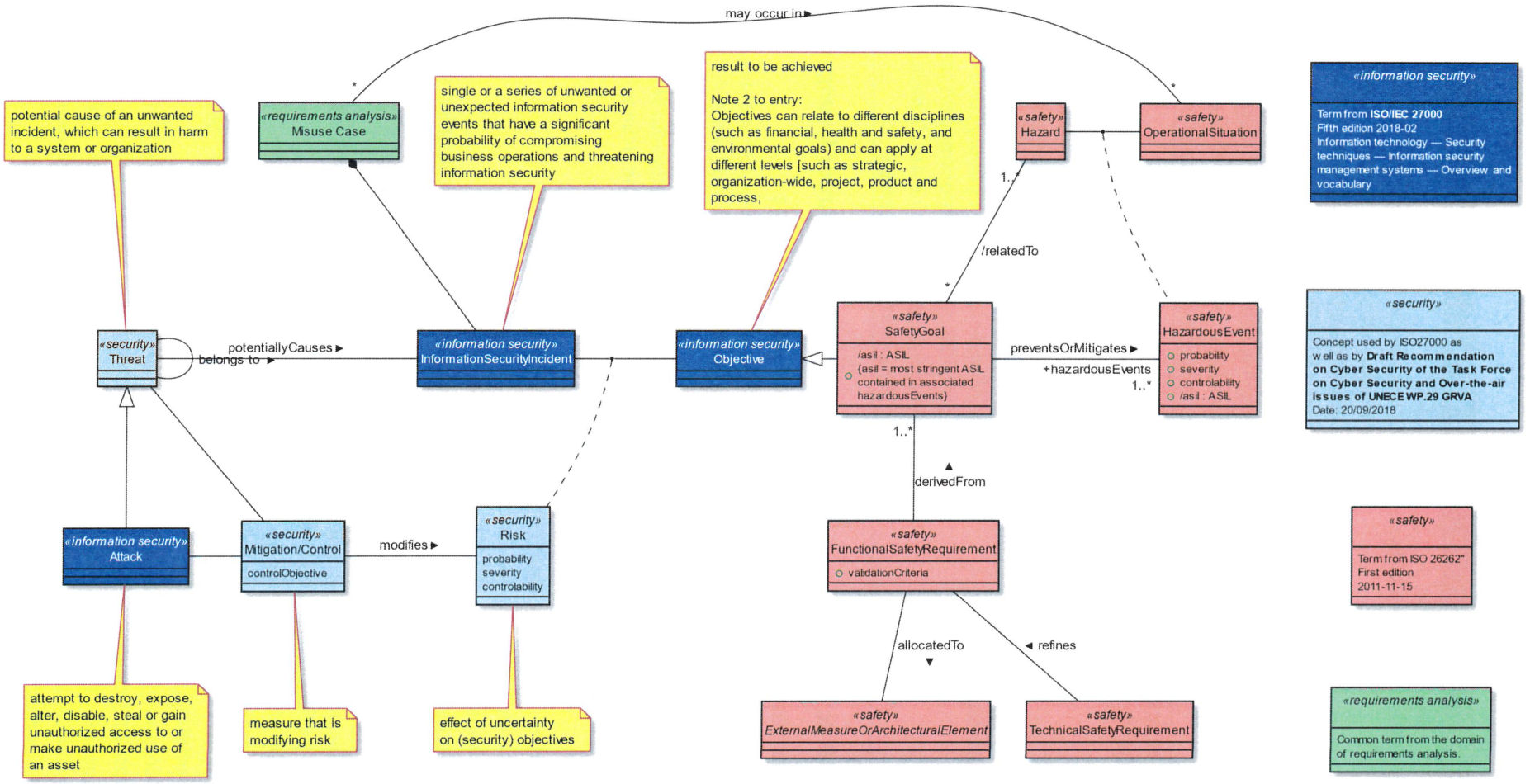


Abbildung 4 Kombiniertes Safety- und Security-Informationsmodell

II.2.2 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Festlegung von Zielkriterien für Sicherheitsanforderungen an SAF-Systeme	Erfüllt *Es wurden Zielkriterien auf einer abstrakten Ebene an ein Informationsmodell konzipiert, um in möglichst vielen konkreten SAF-Systemkontexten Anwendung finden zu können.*
Analyse der Abhängigkeiten der verschiedenen Sicherheitsanforderungen	Erfüllt *Verschiedene Sicherheitsanforderungstypen wurden identifiziert und deren Abhängigkeiten wurden im Informationsmodell als Assoziationen abgebildet.*
Integrierbarkeit und Verträglichkeit solcher Sicherheitsanforderungen	Erfüllt *Safety- und Security-Anforderungsartefakte wurden im Informationsmodell so integriert, dass deren Verträglichkeit in einer Anforderungsanalyse mittels des Informationsmodells sichergestellt werden kann.*
Identifikation möglicher Abschwächungen von Sicherheitsanforderungen	Erfüllt *Die Modellelemente Mitigation/Control sowie SafetyGoal des Informationsmodells lassen in der Anforderungsanalyse eine Abschwächung gegebener Sicherheitsanforderungen zu.*

II.2.3 Teil AP 2c: Formalisierung der Safety- und Security-Anforderungen

II.2.3.1 Problemstellung und Ziele aus der Teilvorhabensbeschreibung

Die identifizierten Anforderungsklassen und Sicherheitsmechanismen für SAF werden, soweit möglich, formal erfasst. Es werden Wechselwirkungen zwischen verschiedenen Anforderungsklassen analysiert und deren formale Fassbarkeit erarbeitet. Entsprechend den entwickelten Architekturmodellen werden Techniken zur Dekomposition der Sicherheitsanforderungen (sowohl Security als auch Safety) sowie zugehörige Kompositionsresultate für eine sichere Integration der Komponenten entwickelt (Security-by-Design).
Ziele sind u.a.:

- Definition/Festlegung einer formalen Beschreibungssprache
- Formale Beschreibung von Safety- und Security-Anforderungen
- Dekompositionstechniken für Safety- und Security-Anforderung
- Kompositionsfähigkeit der Garantien aus den Komponenten hinsichtlich einer Garantie des Gesamtsystems

II.2.3.2 Lösungsweg aus der Teilvorhabensbeschreibung

- gemeinsame Auswahl und Definition einer formalen Beschreibungssprache unter Berücksichtigung des Informationsmodells unterstützen
- Transformation von informellen und semi-formalen Safety- und Security-Anforderungen in die formale Beschreibung aufzeigen
- Modellierungstechniken zur Absicherung der Konsistenz der Safety- und Security-Anforderungen anwenden
- Anforderungs-Informationsmodells um Kategorien zur Klassifizierung verschiedener Ausprägungen von Safety- und Security-Anforderungen anreichern
- adäquater Relationen zwischen Anforderungen verschiedener Hierarchie-Ebenen zur nachvollziehbaren Beschreibung der Dekomposition der S&S Anforderungen identifizieren und anwenden

- Abbildung des Relations-Modells in datenbankbasierten Entwicklungswerkzeugen konzipieren
- Traceability-Reports, mit denen die Komposition der Garantien der Teilsysteme zur Garantie für das Gesamtsystem nachvollziehbar aufgezeigt werden kann, entwickeln
- Metriken und Analysen auf Basis der Relationen zwischen den S&S Anforderungen entwerfen

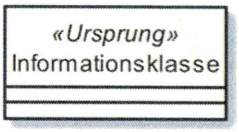
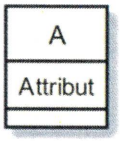
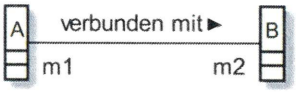
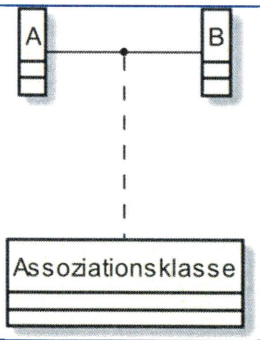
II.2.3.3 Ergebnisse

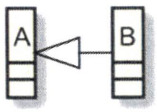
Details zu den nachfolgend aufgeführten Ergebnissen sind dem HOOD-Meilensteinbericht M02 (12) zu entnehmen.

II.2.3.3.1 Genutzte Modellierungselemente

Zur Modellierung des Informationsmodells hat sich das UML-Klassendiagramm als geeignetes Mittel erwiesen. Im Folgenden werden die verwendeten Elemente aufgelistet und deren Bedeutung bzgl. des Informationsmodells erläutert:

Tabelle 3 Modellierungselemente des Informationsmodells

Name	Symbolik	Bedeutung
Klasse		Klassen wurden genutzt, um Klassen von Informationen in der Anforderungsinformation zu identifizieren. Dabei bezeichnet der Klassenname die Kategorie der Information. Z.B. „Misuse Case“. Der Stereotyp der jeweiligen Klasse identifiziert die Herkunft der Informationsklasse.
Attribut		Das Informationsmodell benutzt Attribute, um gewisse Eigenschaften der jeweiligen Informationskategorie zu identifizieren. Dabei können diese Eigenschaften als erforderliche Teilinformationen der jeweiligen Informationskategorie betrachtet werden. Für die Klasse „Risiko“ wäre z.B. das Attribut „Eintrittswahrscheinlichkeit“ eine zu erwartende Teilinformation.
Assoziation		Assoziationen wurden im Informationsmodell genutzt, um auszudrücken, dass Informationen einer Kategorie mit Informationen einer anderen Kategorie verbunden sein können. Die Multiplizitäten (im Bild durch „m1“ und „m2“ angedeutet) geben dabei an, mit wie vielen Informationsobjekten ein Informationsobjekt verbunden sein muss bzw. kann. Der Assoziationsname (im Bild angedeutet durch „verbunden mit“) identifiziert die Bedeutung der Assoziation, wobei die Leserichtung durch eine schwarze Pfeilspitze angedeutet ist.
Assozia-tionsklasse		Assoziationsklassen wurden genutzt, um auszudrücken, dass ein Informationsobjekt zwei Informationsobjekte einer bestimmten Informationsklasse miteinander verbindet.

Name	Symbolik	Bedeutung
Generali-sierung		Generalisierung wurde genutzt, um auszudrücken, dass eine Informationsklasse eine spezielle Form einer anderen Informationsklasse ist. Im Bild links ist B eine spezielle Form von A.

II.2.3.3.2 Erweiterte Dokumentation der Informationsmodelle aus den Literaturquellen hinsichtlich der Transformationen zur Konsolidierung in einem formalen Informationsmodell

Zur Entwicklung des Informationsmodells wurden zunächst Konzepte aus dem Bereich von Safety- und Securityanforderungen identifiziert. Dies geschah durch Analyse von Safety- und Security-Literatur. Ein erster Start zur Identifikation dieser Konzepte bot das Glossar der jeweiligen Literaturquelle.
Das Verständnis der gefundenen Konzepte wurde über Assoziationen und Attribute abgebildet. Dabei blieben an einigen Stellen Lücken zwischen den Konzepten offen, die durch Bilden eines Verständnisses mittels Analyse von Prozessbeschreibungen der Literaturquellen geschlossen und ebenfalls im Modell abgebildet werden konnten.
Das Vernetzen von Safety- und Security geschah durch Optimierung des Modells auf Basis der gefundenen Zielkriterien. Dabei wurden, wo nötig, zusätzliche Elemente ergänzt.

II.2.3.3.3 Erweiterte Dokumentation der Informationsmodelle hinsichtlich der Relationen und Metriken

II.2.3.3.3.1 Aussage der Metriken

Beim Entwurf der Metriken war zunächst die Frage, worüber eine Metrik bzgl. Anforderungsanalyse im Safety- und Security-Umfeld eine Aussage treffen sollte.
Bei der Beantwortung dieser Frage orientierten wir uns an der Überlegung welcher generelle Aspekt sowohl im Umfeld der Safety- als auch im Umfeld der Security-Analysen als kritisch erachtet werden kann. Dies ist erstens die Gefahr der Unvollständigkeit einer Analyse. D.h., dass Dinge nicht erfasst wurden. Und zweitens die Gefahr, dass Fehler gemacht worden sind.
Projiziert man diese zwei Aspekte auf die Merkmale eines Informationsmodells, so erhält man die folgenden Modellaspekte, über die eine Aussage getroffen werden muss:

1. Vollständigkeit
2. Konsistenz

II.2.3.3.3.2 Entworfene Metriken

Die nachfolgend entworfenen Metriken beziehen sich auf Aspekte, die direkt anhand der Relationen einer nach dem Informationsmodell abgebildeten Safety- und Security-Analyse gemessen werden. Nicht betrachtet wurden dabei qualitative Aspekte der erfassten Informationsobjekte.

Tabelle 4 Safety- und Security-Metriken

Bezeichnung	Definition	Detaillierte Aussage
Safety- und Security-Probleminterferenz	Anzahl der Relationen zwischen Misuse Cases und Operational Situations.	Geringe Anzahl kann ein Indiz dafür sein, dass Misuse Cases oder Operational Situations unvollständig erfasst sind oder dass die Relationen unvollständig erfasst sind.
Hazard-Irrelevanz	Anzahl der Hazards, zu denen keine Operational Situations existieren.	Drückt aus, dass entweder Betriebsszenarien nicht betrachtet wurden oder dass Hazards dokumentiert wurden, welche für das betrachtete Szenario irrelevant sind.
Fehlende Security Goals	Anzahl der kritischen Hazardous Events, zu denen	Drückt aus, dass für bestimmte Hazardous Events keine Maßnahmen definiert

Bezeichnung	Definition	Detaillierte Aussage
	keine Security Goals existieren.	wurden.
Fehlende Safety-Verfeinerung	Anzahl der Safety Goals und Anzahl der Functional Safety Requirements, zu denen kein abgeleitetes Element über „refines“, „derivedFrom“ oder „allocatedTo“ existiert.	Drückt aus, dass die Safety-Analyse nicht vollständig ist.
Unnötige Functional Safety Requirements	Anzahl der Functional Safety Requirements, zu denen kein Safety Goal existiert.	Drückt aus, dass entweder Safety Goals fehlen oder dass Fehler bei der Safety-Analyse gemacht wurden durch Einführung unnötiger Maßnahmen.
Unnötige Technical Safety Requirements	Anzahl der Technical Safety Requirements, zu denen kein Functional Safety Requirement existiert.	Drückt aus, dass entweder Functional Safety Requirements fehlen oder dass Fehler bei der Safety-Analyse gemacht wurden durch Einführung unnötiger technischer Maßnahmen.
Fehlende Information Security Incidents	Anzahl der Misuse Cases, aus denen keine Security Incidents hervorgehen.	Drückt aus, dass die Misuse-Case-Analyse unvollständig ist.
Falsche Information Security Incidents	Anzahl der Information Security Incidents ohne Relation zu mindestens einem Objective.	Drückt aus, dass die Security-Analyse inkonsistent ist. Entweder fehlen Objectives oder die Security Incidents sind falsch.
Fehlende Threats	Anzahl der Security Incidents, zu denen kein verursachender Threat identifiziert wurde.	Drückt aus, dass die Analyse der Systemschwachstellen unvollständig ist.
Fehlende Security-Maßnahmen	Anzahl der kritischen Risks ohne Mitigations/Controls.	Drückt aus, dass für ein Security-Risiko noch keine Maßnahmen getroffen wurden.

II.2.3.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Definition/Festlegung einer formalen Beschreibungssprache	Erfüllt
Formale Beschreibung von Safety- und Security-Anforderungen	Erfüllt *Formale Beschreibung ist durch Instanzbildung, z.B. mittels Objektdiagrammen möglich.*
Dekompositionstechniken für Safety- und Security-Anforderung	Erfüllt *Dekomposition erfolgt durch Nutzung entsprechender Assoziationen aus dem Informationsmodell.*
Kompositionsfähigkeit der Garantien aus den Komponenten hinsichtlich einer Garantie des Gesamtsystems	Erfüllt *Geforderte Garantien werden abgebildet als Eigenschaften der jeweiligen Sicherheitsanforderungen. Da diese dekomponiert werden können, ist Komposition von Garantien ebenfalls möglich.*

II.2.4 Teil AP 2d: Validierungstechniken für Safety- & Security-Garantien

II.2.4.1 Problemstellung und Ziele aus der Teilvorhabensbeschreibung

Anforderungen im Bereich Security und Safety für SAF werden hinsichtlich der Verifikation/Validation der erwarteten Sicherheitsgarantien untersucht und klassifiziert. Hierbei sind mehrere Aspekte zu unterscheiden. Einerseits ist die Frage welche Anforderungen statisch zur Entwicklungszeit, welche zur Laufzeit oder welche in beiden Phasen überprüft werden müssen. Andererseits ist es wichtig, dass ein Nachweis der Anforderung auch graduelle Ergebnisse liefern kann; d.h. welche Teile der Anforderungen sind auch im Notfall -bei Wegfall von einzelnen Annahmen -noch gültig.
Ziele des Arbeitspakets:

- Klassifikation der Sicherheitsanforderungen hinsichtlich des Prüfaufwandes/-zeitraums
- Bewertung der zu erwartenden Kosten, Seitenbedingungen und Abdeckung der zugeordneten Schutzmaßnahmen durch verfügbare/erweiterte Sicherheitsarchitekturen

II.2.4.2 Lösungsweg aus der Teilvorhabensbeschreibung

- Generische Verifikations-Strategien in Hinsicht auf das identifizierte Informationsmodell ermitteln
- Kategorien zur Klassifizierung von Verifikationsstrategien, z.B. nach Formalisierungsgrad, Kosten, Schutzmaßnahmen, aufstellen
- Verifikationsstrategien bewerten und in die Kategorien einordnen
- Verifikationsstrategie und Verifikationskategorien mit den Kategorien von S&S Anforderungen verbinden
- Verifikationskategorien auf die damit nachweisbaren Garantien zuordnen
- Verifikationskategorien mit Elementen der Sicherheits-Architekturen verbinden

II.2.4.3 Ergebnisse

Details zu den nachfolgend aufgeführten Ergebnissen sind dem HOOD-Meilensteinbericht M02 (12) zu entnehmen.

II.2.4.3.1 Erweiterte Dokumentation des Informationsmodells hinsichtlich der Verifikations-Strategien und Klassifizierungen

Es wurden die Modellelemente auf ihre Nutzbarkeit bei den Verifikationsmethoden aus Teil AP 1b beurteilt (siehe Kapitel II.1.2.3.1 Stand der Technik zu Verifikation und Validierung von sicherheitskritischen Systemen):

Tabelle 5 Nutzbarkeit der Modellelemente

Informationsmodellklasse	1 Modellbasiertes Testen	2 Formale Methoden	3 Semi-formale Verfahren	4 Laufzeitverifikation	5 Physisches Prototyping	6 Informale Methoden	7 Konformitätstest	8 Akzeptanzprüfung	9 Abdeckungs- und Überdeckungsmessungen
Misuse Case	✓	✗	✓	✗	✓	✓	✓	✓	✓
Hazard	✓	✓	✓	✗	✓	✓	✓	✓	✓

Operational Situation	✓	✗	✓	✗	✓	✓	✓	✓	✓
Threat	✓	✓	✓	✗	✓	✓	✓	✓	✓
Information Security Incident	✓	✓	✓	✗	✓	✓	✓	✓	✓
Objective	✓	✓	✓	✓	✓	✓	✓	✓	✓
Safety Goal	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hazardous Event	✓	✓	✓	✗	✓	✓	✓	✓	✓
Attack	✓	✓	✓	✗	✓	✓	✓	✓	✓
Mitigation/Control	✓	✓	✓	✓	✓	✓	✗	✓	✗
Risk	✓	✓	✓	✗	✓	✓	✓	✓	✓
Functional Safety Requirement	✓	✓	✓	✓	✓	✓	✗	✓	✗
External Measure Or Architectural Element	✓	✓	✓	✓	✓	✓	✗	✓	✗
Technical Safety Requirement	✓	✓	✓	✓	✓	✓	✗	✓	✗

II.2.4.3.1.1 Detaillierte Beurteilung

II.2.4.3.1.1.1 Modellbasiertes Testen

Beim modellbasierten Testen werden Testfälle aus einem Verhaltensmodell des Systems oder des Systemkontexts generiert.
Demzufolge können alle Klassen des Informationsmodells als nutzbar betrachtet werden, die sich in einem solchen Verhaltens- oder Kontextmodell so formalisieren lassen, dass automatisch Testfälle daraus abgeleitet werden könnten.
Dies trifft auf alle Klassen des Informationsmodells zu, da jede Klasse entweder den Kontext oder das System und damit auch potenziell dessen Verhalten beschreibt.

II.2.4.3.1.1.2 Formale Methoden

Für die Verifikation durch formale Methoden sind alle Klassen des Informationsmodells nutzbar, die durch Formalisierung vollständig beschrieben werden können.
Dieses Kriterium weisen die Klassen Misuse Case und Operational Situation nicht auf, da es sich dabei um Szenarien handelt, welche im Kontext eines Gesamtfahrzeugs nur beispielhaft, jedoch niemals vollständig erfasst werden können.

II.2.4.3.1.1.3 Semi-formale Verfahren

Die semi-formalen Verfahren bilden eine Spezialform des modellbasierten Testens auf natürlichsprachlicher Basis. Daher ist die Nutzbarkeit der Klassen des Informationsmodells mit derselben Begründung wie für modellbasiertes Testen für semi-formale Verfahren übertragbar.

II.2.4.3.1.1.4 Laufzeitverifikation

Laufzeitverifikation nutzt formal definierte Korrektheitseigenschaften. Daher sind alle Klassen des Informationsmodells in diesem Kontext nutzbar, wenn sie dazu genutzt werden können, formal definierte Korrektheitseigenschaften zu beschreiben.
Dies sind zum einen alle Klassen, die eine gewisse Form der Anforderung repräsentieren:

- Objective

- Safety Goal
- Functional Safety Requirement
- Technical Safety Requirement

Zum anderen sind dies alle Klassen, die das System beschreiben:

- Mitigation/Control
- External Measure Or Architectural Element

II.2.4.3.1.1.5 Physisches Prototyping

Für physisches Prototyping sind alle Klassen nutzbar, die dabei helfen, ein besseres Verständnis für die Problemstellung oder für das System zu entwickeln. Dies trifft auf alle Klassen des Informationsmodells zu.

II.2.4.3.1.1.6 Informale Methoden

Genau wie beim physischen Prototyping sind bei den informalen Methoden zur Überprüfung mittels menschlicher Interpretation und Beurteilung alle Klassen nutzbar, die dabei helfen, ein besseres Verständnis für die Problemstellung oder für das System zu entwickeln. Dies trifft auf alle Klassen des Informationsmodells zu.

II.2.4.3.1.1.7 Konformitätstest

Zur Nutzung bei einem Konformitätstest kommen nur diejenigen Klassen des Informationsmodells infrage, die die Problemdomäne statisch oder dynamisch abbilden können.
Dazu zählt ein Großteil der Klassen des Informationsmodells, jedoch nicht diejenigen, die das System oder das Systemverhalten definieren.
Klassen, die das System oder das Systemverhalten definieren, sind folgende:

- Mitigation/Control
- Functional Safety Requirement
- External Measure Or Architectural Element
- Technical Safety Requirement

II.2.4.3.1.1.8 Akzeptanzprüfung

Da bei der Akzeptanzprüfung modellbasiertes Testen mit informalen Methoden kombiniert werden kann, lassen sich alle Klassen des Informationsmodells in diesem Kontext nutzen.

II.2.4.3.1.1.9 Abdeckungs- und Überdeckungsmessungen

Da Modellbildung über die Problemdomäne die Messung von Anforderungsüberdeckung unterstützen kann, sind alle Klassen des Informationsmodells nutzbar, die die Problemdomäne statisch oder dynamisch abbilden können.
Dazu zählt ein Großteil der Klassen des Informationsmodells, jedoch nicht diejenigen, die das System oder das Systemverhalten definieren.
Klassen, die das System oder das Systemverhalten definieren, sind folgende:

- Mitigation/Control
- Functional Safety Requirement
- External Measure Or Architectural Element
- Technical Safety Requirement

II.2.4.3.2 Zwischenevaluation nach Refinement der Anforderungen

Im Folgenden wurden die in Teil AP 2a konzipierten Zielkriterien hinsichtlich der Erfüllung durch das in Teil AP 2a definierte Informationsmodell ausgewertet:

Tabelle 6 Zielkriterienerfüllung durch das Informationsmodell

Bez.	Zielkriterium	Erfüllungsgrad
ZK-1	Das Informationsmodell muss Informationseinheiten klassifizieren (beispielsweise durch Klassen).	✓
ZK-2	Das Informationsmodell darf Eigenschaften von Informationseinheiten als Attribute definieren.	✓
ZK-3	Das Informationsmodell muss Beziehungen zwischen Informationseinheiten definieren (beispielsweise durch Assoziationen).	✓
ZK-4	Das Informationsmodell darf Generalisierungen nutzen.	✓
ZK-5	Das Informationsmodell muss es ermöglichen, eine Information als Misuse Case zu klassifizieren.	✓
ZK-6	Das Informationsmodell muss Safety- und Security miteinander in Beziehung setzen.	✓
ZK-7	Das Informationsmodell muss es ermöglichen, das Risiko sowohl für Safety- als auch Security-Erwägungen zu erfassen.	✓
ZK-8	Das Informationsmodell muss es ermöglichen, Risiken gemäß ihrer Eintrittswahrscheinlichkeit, der Schwere ihrer Auswirkung und der Beherrschbarkeit zu bewerten.	✓
ZK-9	Das Informationsmodell muss es ermöglichen, risikoreduzierende Maßnahmen zu erfassen.	✓

II.2.4.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Klassifikation der Sicherheitsanforderungen hinsichtlich des Prüfaufwandes/-zeitraums	Erfüllt *Die Beurteilung der Informationsmodellklassen, welche verschiedenen Arten von Sicherheitsanforderungen entsprechen, hinsichtlich ihrer Nutzbarkeit innerhalb einer bestimmten Verifikationsstrategie, lässt im konkreten Fall einen Rückschluss auf einen möglichen Prüfaufwand und -zeitraum zu.*
Bewertung der zu erwartenden Kosten, Seitenbedingungen und Abdeckung der zugeordneten Schutzmaßnahmen durch verfügbare/erweiterte Sicherheitsarchitekturen	Teilweise erfüllt *Die Bewertung ist mit Hilfe der Informationsmodellklassen möglich.* *Die Zuordnung von Schutzmaßnahmen wurde im Demonstrator über den Produktlebenszyklus anschaulich dargestellt.* *Die zu erwartenden Kosten konnten allerdings nicht allein auf Basis von Anforderungen bewertet werden.*

II.2.5 Teil AP 2e: Entwicklung einer Methodik zur Restrisikoanalyse

II.2.5.1 Problemstellung und Ziele

Hinsichtlich der zu erwartenden Abdeckungsbandbreite der erforderlichen Anforderungen eines SAF durch Sicherheitsarchitekturen (AP 2b und AP 2d) wird eine Metrik zur Restrisikoanalyse entwickelt. Diese wird insbesondere in AP 4 zur Festlegung von Resilienzstrategien und Aktionsplänen im Störungsfall benötigt.
Ziele sind u.a.:

- Restrisikoanalyse für nicht vollständig erreichte Sicherheitsanforderungen
- Entwicklung einer Risikometrik zur Erstellung geeigneter Aktionspläne

II.2.5.2 Lösungsweg

- Konzept für die Restrisikoanalyse und geeigneter Risikometriken unter Berücksichtigung branchenübergreifender Erfahrungen erarbeiten
- Anforderungs-Informationsmodells um die Behandlung von Hazard-und Risks erweitern
- Risk-Control-Measures aus den identifizierten Risiken ableiten und Restrisiken ermitteln
- Ableitung von technischen Safety-Requirements aus Risk-Control-Measures konzipieren
- Ableitung von Verifikations-Strategien aus Risk-Control-Measures konzipieren
- Strategien zur Ermittlung von Schwellen der gesellschaftlichen Rest-Risiko-Akzeptanz, bzw. von Requirements der Gesellschaft an diese Schwelle, analysieren

II.2.5.3 Ergebnisse

II.2.5.3.1 Verifikationsstrategien in Bezug auf die Restrisiko-Akzeptanz

Details zur erweiterten Dokumentation des Informationsmodells hinsichtlich der Risiko-Aspekte, sind dem HOOD-Meilensteinbericht M01 (8) zu entnehmen.

II.2.5.3.1.1 Restrisikoanalyse und geeignete Risikometriken

Das Restrisiko bezeichnet in unserem Kontext das nach Anwendung aller risikomindernden Maßnahmen verbleibende Risiko eines Entwicklungsgegenstandes. [in Anlehnung an (13)]
Die Restrisikoanalyse ist damit Teil jeder Produktrisikoanalyse, bei der Ereignisse und deren Auswirkungen analysiert werden, geeignete Maßnahmen definiert werden und das Risiko nach Anwendung der definierten Maßnahmen erneut quantifiziert wird.
Als Risikometriken kommen dabei immer die Größen "Eintrittswahrscheinlichkeit" und "Auswirkungsschwere" zum Einsatz. In manchen Umfeldern wird ergänzend noch die "Beherrschbarkeit" beurteilt.

II.2.5.3.1.2 Strategien zur Ermittlung von Schwellen der gesellschaftlichen Rest-Risiko-Akzeptanz, bzw. von Requirements der Gesellschaft an diese Schwelle

Die Risikoakzeptanz sagt aus inwieweit ein Individuum oder eine Gesellschaft bereit ist, ein Restrisiko zu tragen.
In vielen Kontexten der Produktentwicklung existieren anerkannte Regeln der Technik, welche zu treffende technische Maßnahmen vorgeben und die jeweilige Produktentwicklungsorganisation von einer Produktrisikoanalyse befreien. In diesem Fall kann das Restrisiko als gesellschaftlich akzeptiert betrachtet werden.
In Umfeldern, Systemen oder zu Funktionen, zu denen noch keine anerkannten Regeln der Technik existieren, muss eine Produktrisikoanalyse durchgeführt werden. Dabei gibt es zwei Fälle, die unterschieden werden:

1. Branchenspezifische Standards geben ein Risikobewertungsschema vor und nennen auch einen Schwellwert, unterhalb dessen ein Risiko als tolerabel betrachtet wird. Damit existiert implizit eine gesellschaftliche Akzeptanz des Restrisikos.
   Beispiele für Prinzipien hinter solchen Schwellwerten sind (14):
   a. GAME: Globalement Au Moins Equivalent
   b. ALARP: As Low As Reasonably Practicable
   c. MEM: Minimum Endogenous Mortality
2. Eine Produktrisikoanalyse muss durchgeführt werden und macht das Restrisiko durch Quantifizierung transparent. Jedoch gibt es keinerlei Vorgaben oder Anhaltspunkte, ab welcher Schwelle das Risiko gesellschaftlich akzeptiert wird.

Faktoren, die einen Einfluss auf die Risikoakzeptanz haben sind folgende:

1. Individueller Grad der Selbstbestimmung
   Dabei handelt es sich um die subjektive Einschätzung, welchen Einfluss der einzelne auf das Risiko hat.
   Beispiel: Ein Autofahrer ist bereit, ein höheres Unfallrisiko zu tolerieren als ein Bahnfahrer, weil sein eigener Einfluss ihm dabei größer erscheint.

2. Potenzielles Schadensausmaß
   Dabei handelt es sich um eine Abschätzung, wie viele Individuen im Pessimalfall betroffen sind.
   Beispiel: Ein Atomkraftwerk besitzt eine geringere Restrisikoakzeptanz der Gesellschaft als ein Automobil, da im Falle eines GAUs mehr Menschen betroffen sind als bei einem Autounfall.
3. Tatsächliches Eintreten von Restrisiken
   Beispiel: Das Restrisiko von Kernkraft wurde in Deutschland nicht mehr akzeptiert, nachdem ein sich ein größerer Unfall in einem japanischen Atomkraftwerk ereignete.

II.2.5.3.1.3 Verifikationsstrategien

Abschließend können folgende Verifikationsstrategien der Restrisikoakzeptanz identifiziert werden:

1. Literaturrecherche:
   Identifikation branchenspezifischer Standards und anerkannter Regeln der Technik, welche eine gesellschaftliche Restrisikoakzeptanz implizieren.
2. Analyse politischer Entscheidungen:
   Politische Entscheidungen reflektieren den gesellschaftlichen Konsens und zeigen, dass der gesellschaftliche Wert einer Technologie als höher erachtet wird als das damit einhergehende Restrisiko.
3. Umfragen zu gesellschaftlicher Restrisikoakzeptanz:
   Wenn keine anerkannten Regeln der Technik existieren, dann ist der einzige Weg, die Restrisikoakzeptanz zu verifizieren, indem das ermittelte Restrisiko transparent gemacht wird und dann durch Befragung relevanter Stichproben der Gesellschaft die Restrisikoakzeptanz ermittelt wird.

II.2.5.3.1.4 Abgeleitete Kriterien für das Informationsmodell

Unsere Recherche zur Restrisikoanalyse und geeigneten Risikometriken hat ergeben, dass das Informationsmodell folgenden Kriterien genügen muss:

1. Das Informationsmodell muss es ermöglichen, das Risiko sowohl für Safety- als auch Security-Erwägungen zu erfassen.
2. Das Informationsmodell muss es ermöglichen, Risiken gemäß ihrer Eintrittswahrscheinlichkeit, der Schwere ihrer Auswirkung und der Beherrschbarkeit zu bewerten.
3. Das Informationsmodell muss es ermöglichen, risikoreduzierende Maßnahmen zu erfassen.

II.2.5.3.2 Erweiterte Dokumentation des Informationsmodells hinsichtlich der Risiko Aspekte

Details zur erweiterten Dokumentation des Informationsmodells hinsichtlich der Risiko-Aspekte, sind dem HOOD-Meilensteinbericht M02 (12) zu entnehmen.
Die konzipierten Zielkriterien für das Informationsmodell bzgl. der Risikoaspekte aus Teil AP 2a lauten wie folgt:

Tabelle 7 Zielkriterien hinsichtlich der Risikoaspekte

Bezeichner	Beschreibung
ZK-7	Das Informationsmodell muss es ermöglichen, das Risiko sowohl für Safety- als auch Security-Erwägungen zu erfassen.
ZK-8	Das Informationsmodell muss es ermöglichen, Risiken gemäß ihrer Eintrittswahrscheinlichkeit, der Schwere ihrer Auswirkung und der Beherrschbarkeit zu bewerten.
ZK-9	Das Informationsmodell muss es ermöglichen, risikoreduzierende Maßnahmen zu erfassen.

Im Folgenden wird die Umsetzung der beschriebenen Zielkriterien im Informationsmodell dokumentiert.

II.2.5.3.2.1 Risikoabbildung für Safety und Security (ZK-7)

II.2.5.3.2.1.1 Safety-Risiko-Aspekte

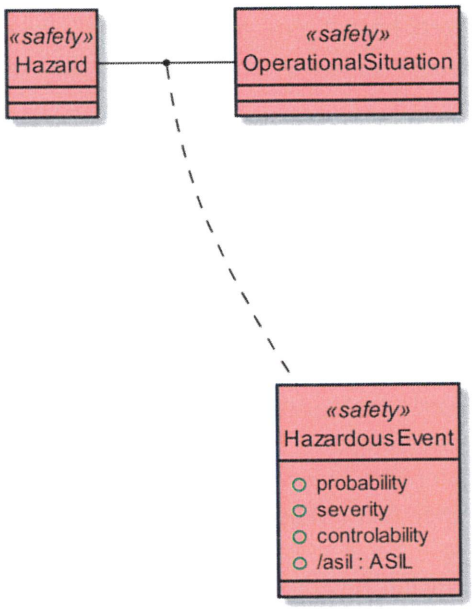


Abbildung 5 Hazardous Event im Informationsmodell

Bezüglich Safety ist der Begriff des Risikos in Form des sog. „Hazardous Events" (deutsch Gefärdungsereignis) abgebildet. Das „Hazardous Event" stellt ein Ereignis dar, welches den „Hazard" (deutsch Gefahr) mit einer „Operational Situation" (deutsch Betriebsszenario) verknüpft. Das „Hazardous Event" kann in einem Betriebsszenario auftreten und stellt eine Gefahr dar.

II.2.5.3.2.1.2 Security-Risiko-Aspekte

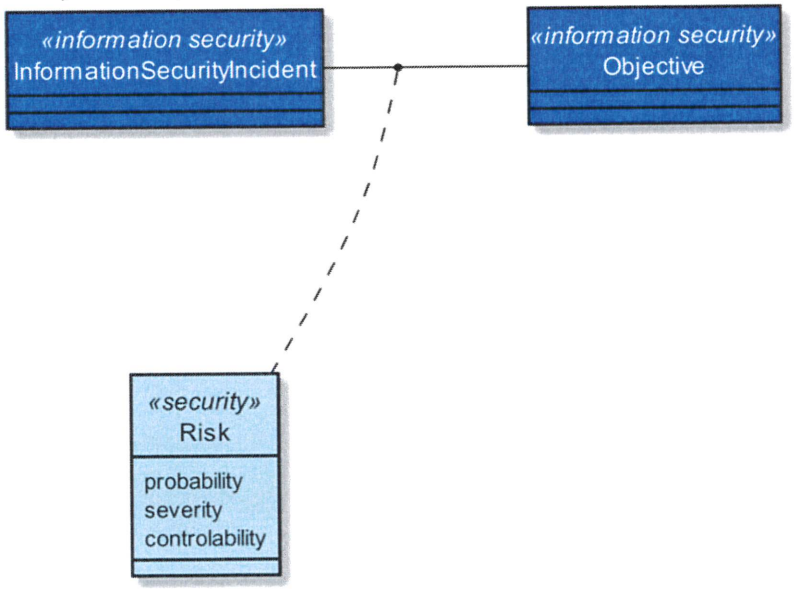


Abbildung 6 Risk im Informationsmodell

Bezüglich Security ist der Begriff des Risikos in Form des „Risks" (deutsch Risiko) abgebildet. Das „Risk" verknüpft den „Information Security Incident" (deutsch Informationssicherheitsvorvall) mit einem „Objectiv" (deutsch Ziel) verknüpft.

II.2.5.3.2.2 Risikoquantifizierung (ZK-8)

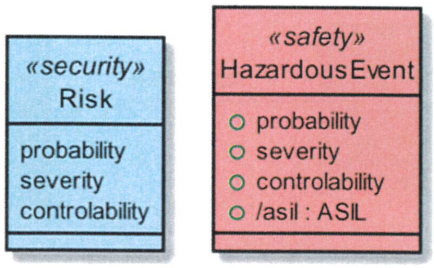


Abbildung 7 Risikoquantifizierung im Informationsmodell

Beide Informationsmodellklassen, welche den Risikobegriff repräsentieren, verfügen über die folgenden Attribute zur Quantifizierung des Risikos:

1. Probability (entspricht der Eintrittswahrscheinlichkeit)
2. Severity (entspricht der Schwere des Risikos)
3. Controlability (entspricht der Beherrschbarkeit des Risikos).

II.2.5.3.2.3 Risikoreduzierende Maßnahmen (ZK-9)

II.2.5.3.2.3.1 Safety-Risikoreduzierende Maßnahmen

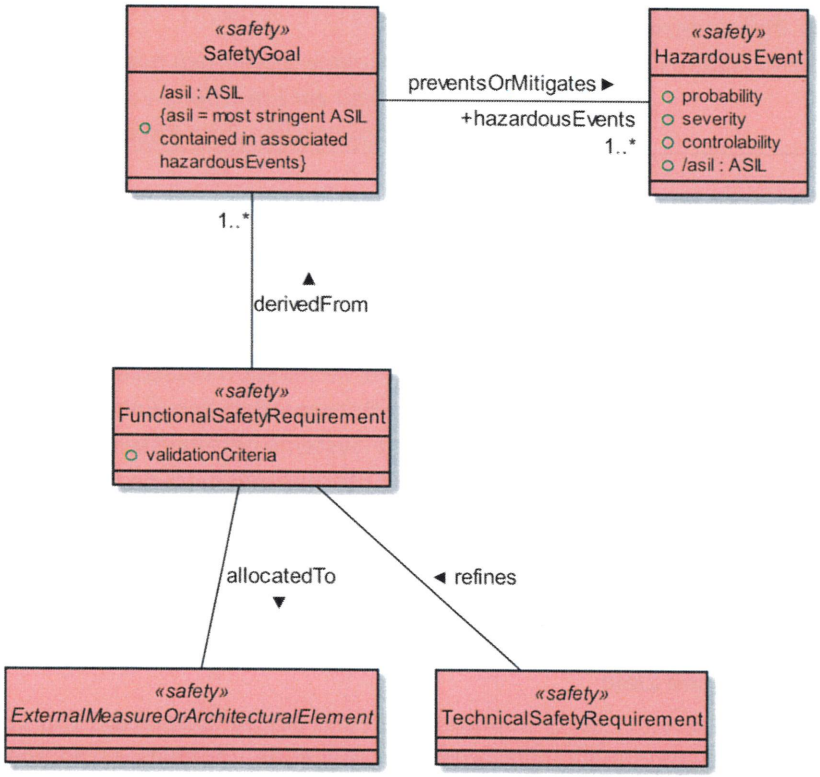


Abbildung 8 Risikoreduzierende Maßnahmen für Safety

Die risikoreduzierende Maßnahme, die das Informationsmodell bzgl. Safety bietet, ist die Definition eines sog. „Safety Goals" (deutsch Sicherheitsziel). Dieses verhindert oder mildert das Risiko. Aus dem „Safety Goal" können sog. „Functional Safety Requirements" (deutsch funktionale Sicherheitanforderungen) als detailliertere Maßnahmen abgeleitet werden, wovon wiederum „Technical Safety Requirements" (deutsch technische Sicherheitsanforderungen) abgeleitet werden können.
Zudem ermöglicht es das Informationsmodell ein „Functional Safety Requirement" an eine externe Maßnahme oder ein Architekturelement zu richten, welche oder welches die jeweilige Anforderung als Maßnahme umsetzt.

II.2.5.3.2.3.2 Security-Risikoreduzierende Maßnahmen

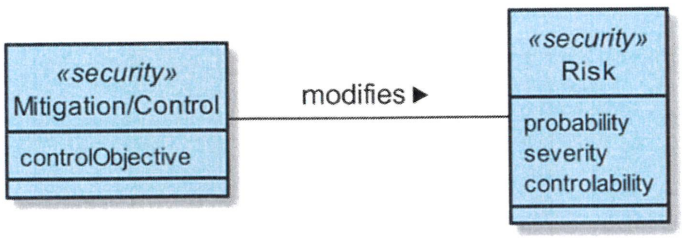


Abbildung 9 Risikoreduzierende Maßnahmen für Security

Die risikoreduzierende Maßnahme, die das Informationsmodell bzgl. Security bietet, ist die Definition sog. „Mitigations/Controls" (deutsch Abhilfemaßnahmen/Überwachungsmechanismen). Die „Mitigations/Controls" sind Maßnahmen, welche das Risiko verändern bzw. reduzieren.

II.2.5.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Restrisikoanalyse für nicht vollständig erreichte Sicherheitsanforderungen	Erfüllt *Das Restrisiko ist über die jeweiligen Risikomodifkatoren Mitigation/Control bzw. SafetyGoal abbildbar.*
Entwicklung einer Risikometrik zur Erstellung geeigneter Aktionspläne	Erfüllt *Aktionspläne lassen sich aus den identifizierten Strategien zur Ermittlung von Schwellen der gesellschaftlichen Rest-Risiko-Akzeptanz ableiten.*

II.3 Arbeitspaket 5: Werkzeugentwicklung

AP 5 beinhaltet die Entwicklung eines Demonstrator-Werkzeugs, das die Integration und den Verifikationsprozess von Sicherheitsanforderungen von SAF-Einzelkomponenten sowie dem SAF-Gesamtsystem begleitet. Das Demonstrator-Werkzeug verbindet in Form eines hierarchischen Top-Down-Ansatzes mehrere Module zur Spezifikation und Verifikation verschiedener Sicherheitsanforderungen auf einer SAF-Architektur. Dazu werden dem Entwickler sowohl eine Visulisierung über die funktionale Architektur des SAF-Systems bereitgestellt, die jeweils die Perspektiven (a) Safety-Anforderungen, (b) Security-Anforderungen, (c) der Komposition Safety & Security-Anforderungen, aufgeschlüsselt je nach deren Zeitraums zur Sicherstellung zur (i) Entwicklungszeitoder (ii) Laufzeit.

II.3.1 Teil AP 5c: Implementierung der Werkzeugmodule

II.3.1.1 Problemstellung und Ziele

Die einzelnen Module für Bottom-Level-Komponenten und der komponierten Top-Level Architektur werden für ihre spätere Einbindung implementiert. Vorliegende Verifikationsmodule (AP 3c) werden dabei berücksichtigt. Zur Einbindung externer Tools für die Verifikation von Teilkomponenten werden entsprechende APIs vorbereitet, um die externe Software mit dem entwickelten Werkzeug zu verknüpfen.
Ziele sind u.a.:

- Entwicklung einzelner Verifikationsmodule (Bottom-Level)
- Entwicklung einer API zur Einbindung externer Verifikationstools
- Entwicklung der Verifikationsengine für die Top-Level Verifikation (ggf. unter Einbindung eines existierenden Tools)

II.3.1.2 Lösungsweg

- Integrationsrelevante Inhalte der einzelnen Werkzeugkomponenten identifizieren
- Kompatibilität und Integrationsfähigkeit des Informationsflusses zwischen Werkzeugkomponenten auf Basis der identifizierten integrationsrelevanten Inhalte prüfen

II.3.1.3 Ergebnisse

Details zu den nachfolgend aufgeführten Ergebnissen sind dem HOOD-Meilensteinbericht M03 (15) zu entnehmen.

II.3.1.3.1 Spezifikation der integrationsrelevanten Inhalte

II.3.1.3.1.1 Auszutauschende Daten

Die in DOORS abgebildeten Daten mussten zum Zwecke der Visualisierung auf das Objektmodell des Visualisierungswerkzeugs abgebildet werden. In unserem Fall handelte es sich um EEvision in der Version 7.3.7.

II.3.1.3.1.1.1 Daten in DOORS

Zur Visualisierung der Strukturen gemäß des Anforderungsinformationsmodells, müssen in DOORS nur Anforderungsinformationen betrachtet werden, strukturierende Elemente, wie Kapitelüberschriften, können ignoriert werden. Die Anforderungsinhalte werden in DOORS-Objekten gespeichert und innerhalb dieser in sog. Attributen gegliedert. Abbildung 10 stellt die Attribute dar, deren Inhalt dafür in EEvision abgebildet werden muss.

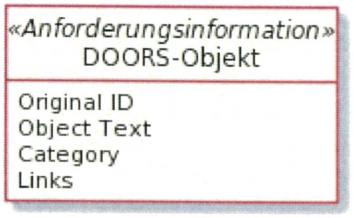


Abbildung 10 Anforderungsinformation in DOORS

II.3.1.3.1.1.2 Daten in EEvision

In EEvision müssen Daten gemäß des sog. EDB-Objektmodells abgebildet werden (siehe Abbildung 11). EDB steht dabei für „Electric Wiring Database".

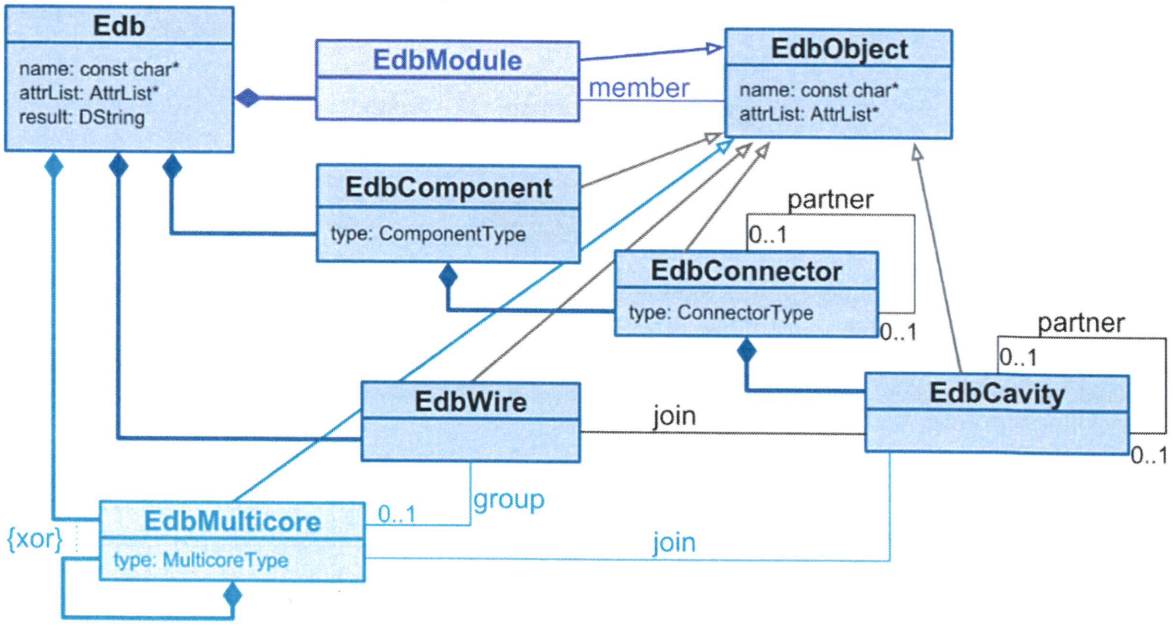


Abbildung 11 EDB Object Model - aus EEvision 7.3.7

II.3.1.3.1.1.3 Kompatibilität und Integrationsfähigkeit des Informationsflusses

Tabelle 8 Abbildung von DOORS-Daten im EDB-Objektmodell

Daten in DOORS	Abbildung im EDB-Objektmodell	Bemerkung
DOORS-Objekt	EdbObject	
Original ID	EdbObject::name	
Object Text	EdbObject::attrList	abgelegt in einem Attribut mit dem Namen „Text“
Category	EdbConnector EdbCavity EdbWire	

II.3.1.3.2 Definition einer geeigneten Schnittstelle für die Werkzeugintegration

EEvision visualisiert Daten, die in sogenannten EDB-Dateien gespeichert sind. Zur Erzeugung solcher EDB-Dateien stellt EEvision das EDB Creator API bereit, über welches mittels verschiedener Programmiersprachen Daten in EDB-Dateien gespeichert werden können.
Anforderungsdaten in DOORS können durch das DXL API ausgelesen werden. DXL steht dabei für „DOORS Extension Language“.
Die Werkzeugintegration liest Anforderungsdaten aus DOORS durch Nutzung des DXL APIs und schreibt mittels des EDB Creator APIs die aufbereiteten Daten in eine EDB-Datei, welche durch EEvision visualisiert werden kann.

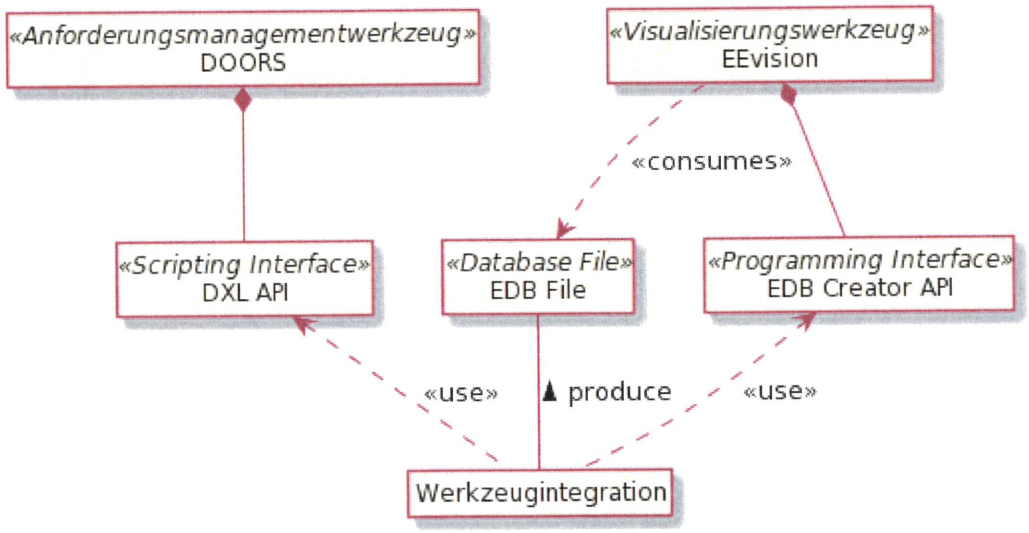


Abbildung 12 Werkzeugintegration DOORS - EEvision

II.3.1.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Entwicklung einzelner Verifikationsmodule (Bottom-Level)	Erfüllt
Entwicklung einer API zur Einbindung externer Verifikationstools	Erfüllt
Entwicklung der Verifikationsengine für die Top-Level Verifikation (ggf. unter Einbindung eines existierenden Tools)	Erfüllt

II.3.2 Teil AP 5d: Gesamtintegration und Test

II.3.2.1 Problemstellung und Ziele

Die Komponenten aus AP 5c des Werkzeugs (Demonstrator) zur Entwicklungsunterstützung und Darstellung des Systemmodells hinsichtlich der Sicherheitsanforderung werden integriert und mit

einer geeigneten Visualisierungsschnittstelle für die funktionalen Komponenten, Annotationsmodelle und Sicherheitsanforderungen ausgestattet. Mehrere Perspektiven (jeweils Safety und Security einzeln und in ihrer Komposition, je zur Entwicklungs- und Laufzeit) werden integriert.
Ziele sind u.a.:

- Integration der Verifikationsmodule (Bottom-Level) mit den Top-Level Komponenten
- Implementierung der Visualisierungsengine und -perspektiven
- Einzeltest des Werkzeugs
- Visualisierung des Annotationsmodells für Aktionspläne (AP4)

II.3.2.2 Lösungsweg

- Konzeptvalidierung des entwickelten Werkzeugs hinsichtlich des abzubildenden Informationsmodells durchführen
- praktischen Erprobung unterstützen

II.3.2.3 Ergebnisse

Details zu den nachfolgend aufgeführten Ergebnissen sind dem HOOD-Meilensteinbericht M03 (15) zu entnehmen.

II.3.2.3.1 Konzeptvalidierung des entwickelten Werkzeugs hinsichtlich des abzubildenden Informationsmodells

II.3.2.3.1.1 Abbildung der Security-Norm im Anforderungsmanagementwerkzeug

Eine Security-Norm wurde in DOORS abgebildet.

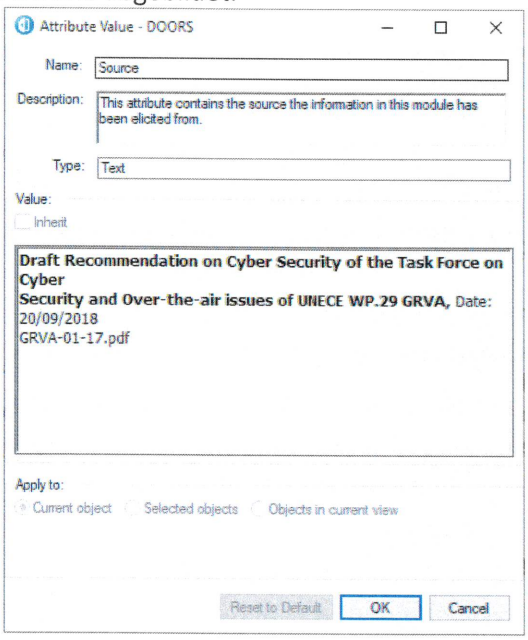


Abbildung 13 Dokumentation der Informationsquelle in DOORS

Dabei wurden die in der Norm enthaltenen Informationen gemäß dem Informationsmodell kategorisiert und, wie in der Norm abgebildet, miteinander in Beziehung gesetzt.

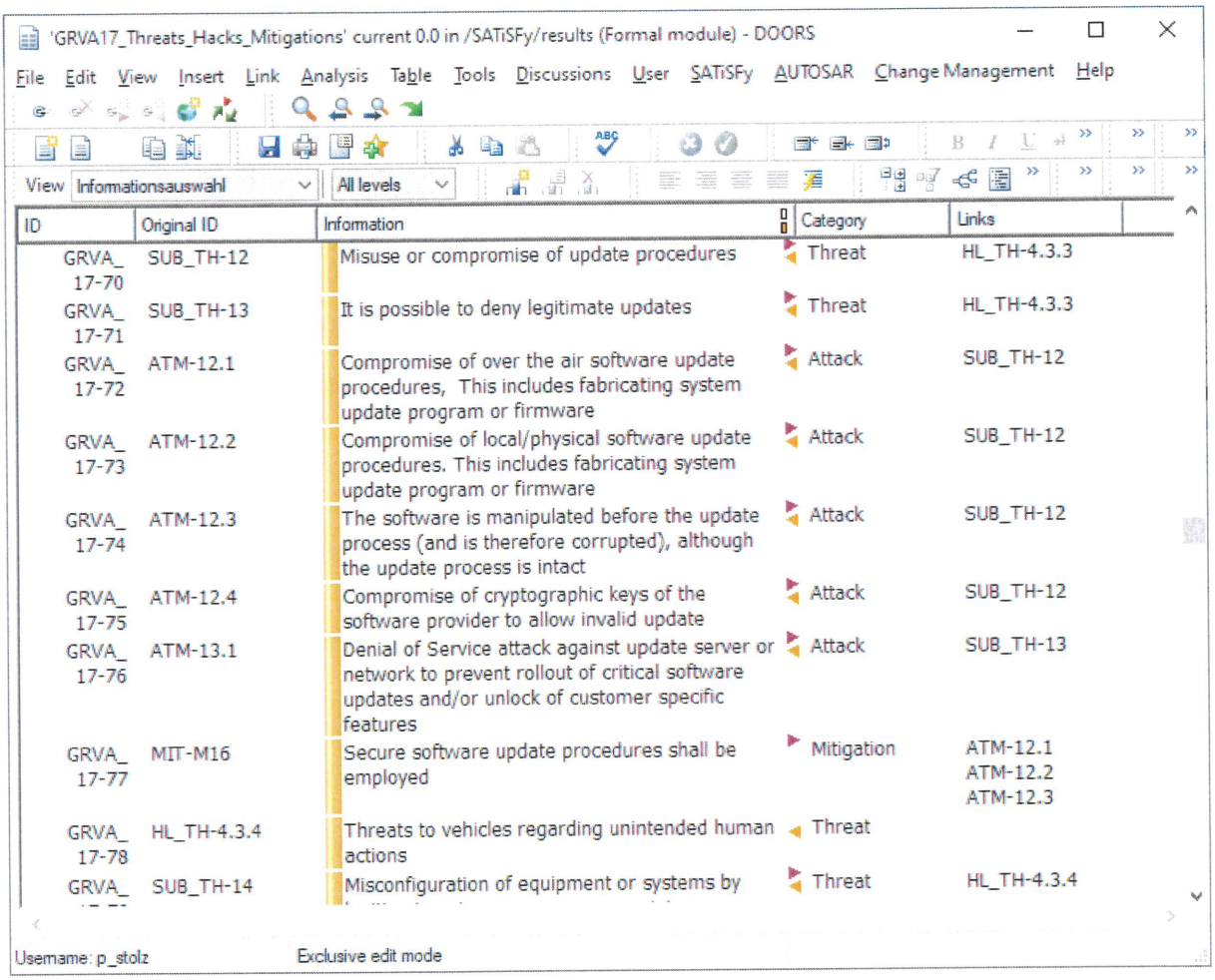


Abbildung 14 Kategorisierung der Normeninhalte und Abbildung der Beziehungen zwischen den Informationseinheiten

Die Abbildung der Security-Norm in DOORS kann im Anhang des Dokumentes ihrer tabellarischen Abbildung unter **Fehler! Verweisquelle konnte nicht gefunden werden.** nachvollzogen werden.

II.3.2.3.1.2 Abbildung der Security-Norm in der einfachen Graphenbeschreibungssprache

Es wurde eine dafür entwickelte DOORS-Erweiterung „Create EDB…“ genutzt, um die Security-Norm in die einfachen Graphenbeschreibungssprache zu transformieren.

II.3.2.3.1.3 Erzeugung der EDB-Datei

Aus der Textrepräsentation in der einfachen Graphenbeschreibungssprache wurde mittels eines dafür entwickelten Komandozeilenprogrammes „simplegraph“ erfolgreich eine EDB-Datei erzeugt.

II.3.2.3.1.4 Visualisierung der EDB-Datei mit EEvision

Die erzeugte EDB-Datei wurde mit EEvision geladen und visualisiert. Dabei war es möglich, die textuellen und strukturellen Inhalte der Security-Norm interaktiv zu explorieren.

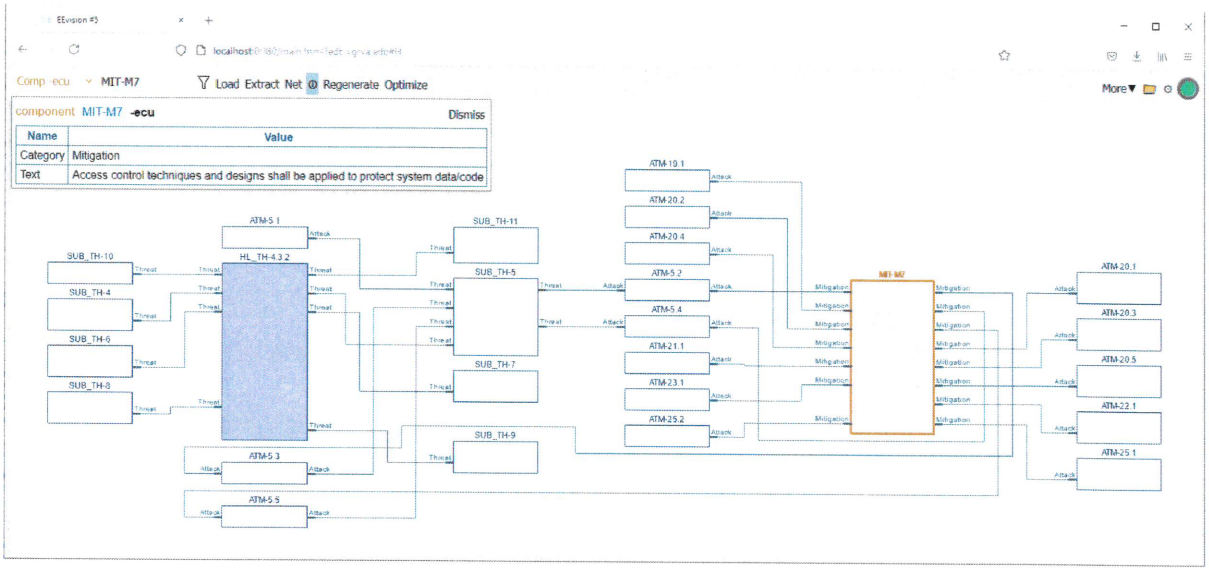


Abbildung 15 Interaktive Exploration der Security-Norm mit EEvision

II.3.2.3.2 Fazit der praktischen Erprobung

Unsere Validierung des Ansatzes hat gezeigt, dass sich durch Kategorisierung von Anforderungsinformation gemäß unseres Anforderungsinformationsmodells eine Security-Norm in einem Anforderungsmanagementwerkzeug hinsichtlich Struktur und Inhalt abbilden lässt. Zudem konnten wir zeigen, dass sich die strukturellen Zusammenhänge mit einem Visualisierungswerkzeug interaktiv explorieren lassen, was eine Alternative zum linearen Lesen von Anforderungsdokumenten ermöglicht.

II.3.2.4 Ergebnisbewertung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Integration der Verifikationsmodule (Bottom-Level) mit den Top-Level Komponenten	Erfüllt
Implementierung der Visualisierungsengine und -perspektiven	Erfüllt
Einzeltest des Werkzeugs	Erfüllt
Visualisierung des Annotationsmodells für Aktionspläne (AP4)	Nicht erfüllt *Aktionspläne waren im Kontext des betrachteten Systemszenarios nicht verfügbar. Stattdessen wurde eine Konzeptvalidierung des entwickelten Werkzeuges hinsichtlich des abzubildenden Informationsmodells durchgeführt.*

II.4 Arbeitspaket 7: Demonstration und Dissemination

In AP7 werden die entwickelte Methodik und das Demonstratorwerkzeug in zwei verschiedenen Use-Cases praktisch eingesetzt. Dabei wird nach einem Einsatz für Einzelkomponenten, Subsystem (unter Einsatz von virtuellen Prototypen) und einem vollständigen SAF-Demonstrator unterschieden.

II.4.1 Teil AP 7b: Demonstration auf Systemebene

II.4.1.1 Problemstellung und Ziele

Die Anwendung des Werkzeugs auf ein SAF-(Sub-)System wird in diesem AP durchgeführt.
Ziele des Arbeitspakets:

- Aufbau eines Testsystems (Versuchsfahrzeug, Teilsystem)
- Leistungsbewertung der Methodik und des Demonstratorwerkzeugs auf einem Labor-SAF

II.4.1.2 Lösungsweg

- Anforderungen an ein Testsystem erheben und abstimmen
- geeigneten Strategien zur Wissensvermittlung der Methodik und Werkzeuge identifizieren
- Schulungsunterlagen zur Dissemination unter Berücksichtigung der Strategien zur Wissensvermittlung konzipieren
- Workshops zur Dissemination konzipieren

II.4.1.3 Ergebnisse

II.4.1.3.1 Anforderungen an das Testsystem

Die folgenden Anforderungen an ein Testsystem zur Validierung der Ergebnisse konnten ermittelt und abgestimmt werden:

1. Das Testsystem muss realistische Anforderungen enthalten. D.h., die Anforderungen dürfen nicht von den Entwicklern des Informationsmodells aufgestellt worden sein, sondern müssen eine Qualität haben, wie sie in der Industrie zu erwarten ist.
2. Das Testsystem muss die Abbildung von Anforderungen gemäß dem Anforderungsinformationsmodell in einem Anforderungsmanagementwerkzeug demonstrieren.
3. Das Testsystem muss die Visualisierung der Anforderungen gemäß dem Informationsmodell demonstrieren.

Details hierzu sind dem HOOD-Meilensteinbericht M03 (15) zu entnehmen.

II.4.1.3.2 Erhobene Anforderungen an den Produktlebenszyklus-Demonstrator

Für eine Demonstrationsszenario, welches in der Abschlusspräsentation (16) gezeigt wurde, konnte HOOD die nachfolgenden Anforderungen ermitteln, welche durch die Beiträge der Konsortialpartner erüllt werden konnten:

Tabelle 9 Anforderungen an den Demonstrator

ID	Anforderung
MIT-M7	Access control techniques and designs shall be applied to protect system data/code
MIT-M15	Measures to detect malicious internal messages or activity should be considered
MIT-M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data. Example Security Controls can be found in OWASP.
OWASP C1	**Define Security Requirements:** A security requirement is a statement of needed security functionality that ensures one of many different security properties of software is being satisfied. Security requirements are derived from **industry standards**, **applicable laws**, and a **history of past vulnerabilities**. Security requirements define new features or additions to existing features to solve a specific security problem or eliminate a potential vulnerability. ...
OWASP C10	**Handle All Errors and Exceptions:** Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.
[ISO26262]	The hardware-software interface (HSI) requirements shall be tested with appropriate coverage, with consideration to the ASIL or a rationale shall be given that no issues with respect to the HSI remain.
MIT-M6	Systems shall implement security by design to minimize risks
MIT-M23	Cybersecurity best practices for software and hardware development shall be followed.

Quellangaben zu den Anforderungen können der Abschlusspräsentation entnommen werden.

II.4.1.3.3 Demonstration und Dissemination

Details zu den nachfolgend aufgeführten Ergebnissen sind dem HOOD-Meilensteinbericht M04 (17) zu entnehmen.

II.4.1.3.3.1 Konzepte zur Dissemination

Es wurden systematisch Strategien zur Wissensvermittlung derMethodik und Werkzeuge identifiziert.

Tabelle 10 Strategien zur Wissensvermittlung der Methodik und Werkzeuge

		Interaktivität	
		Interaktiv	Nicht-interaktiv
Disseminationsmodus	Präsenz, synchron	Vor-Ort-Training mit Trainer und Teilnehmern, z.B. Transfer-Workshops	Vortrag/Vorlesung
	Präsenz, asynchron	Interaktiver Trainingsautomat mit festem Standort	Nicht relevant, aber denkbar: z.B. stationärer Schulungsvideoautomat
	Online, synchron	Online-Training mit Trainer und direktem Feedback an Teilnehmer, z.B. Transfer-Workshops	Vortrag im Live-Stream
	Online, asynchron	Jederzeit durchführbares Online-Tutorial mit Übungen und automatisiertem Feedback	Abrufbares Trainingsmaterial zum Selbststudium ohne Feedback

Die verschiedenen Strategien wurden bzgl folgender Kriterien bewertet:

1. Aufwand der Durchführung bei Wiederholung
2. Reichweite/Skalierung
3. Produktionskosten
4. Attraktivität
5. Wirksamkeit

Aus der Bewertung konnte eine Rangfolge für die verschiedenen Strategien festgelegt werden:

Tabelle 11 Rangfolge der Disseminationsstrategien

Rang	Disseminationskonzept
1	Online, asynchron, interaktiv
1	Online, asynchron, nicht-interaktiv
2	Online, synchron, nicht-interaktiv
3	Online, synchron, interaktiv
4	Präsenz, synchron, interaktiv
5	Präsenz, synchron, nicht-interaktiv
6	Präsenz, asynchron, interaktiv
7	Präsenz, asynchron, nicht-interaktiv

II.4.1.3.3.2 Konzept für Schulungsunterlagen zur Dissemination

II.4.1.3.3.2.1 Anforderungen an die Schulungsunterlagen

- Die Schulung muss online durchführbar sein
- Die Schulung muss asynchron durchführbar sein
- Die Schulung darf interaktive Elemente enthalten
- Die Schulung muss dem Teilnehmer die Motivation der Forschungsergebnisse näherbringen
- Die Schulung muss dem Teilnehmer das kombinierte Safety und Security Informationsmodell näherbringen

II.4.1.3.3.2.2 Lösungsansatz für die Schulungsunterlagen

II.4.1.3.3.2.2.1 Teil 1: Motivation

Form:	Videovortrag, Audioaufnahme oder Präsentationstext
Inhalt:	• Einschlägige Normen empfehlen die Orientierung an einem Prozessmodell, die praktische Erfahrung zeigt aber, dass eine Orientierung an Arbeitsergebnissen, statt an Aktivitäten, deutlich einfacher umzusetzen ist • Safety und Security können nicht isoliert voneinander betrachtet werden • Safety und Security erfordern bei den Beteiligten ein gemeinsames Verständnis, welches durch ein Begriffsmodell gefördert werden kann

II.4.1.3.3.2.2.2 Teil 2: Kombiniertes Safety- und Securitymodell

Form:	Browsebares Modell oder lineare Präsentation
Inhalt:	• Alle Begriffe und Assoziationen des kombinierten Safety- und Securitymodells • Ggf. zusätzliche Erläuterungen

II.4.1.3.3.2.2.3 Teil 3: Übungsaufgaben mit Musterlösungen

Form:	Lineare Liste mit Fragestellungen und verdeckter Musterlösung
Inhalt:	• Fragestellungen bezüglich Interferenz von Safety und Security • Suchaufgaben zu Begriffen • Fragen zu konkreten Beispielen • Lösungen zu den aufgeführten Fragestellungen und Aufgaben

II.4.1.3.3.2.2.4 Teil 4: Häufig gestellte Fragen

Form:	FAQ
Inhalt:	• Gesammelte Fragen von Schulungsteilnehmern • Antworten der Spezialisten

II.4.1.3.4 Konzept für Workshop zur Dissemination

Da diese Konzepte gezeigt haben, dass ein Workshop keine geeignete Disseminationsmethode für diese Materie ist, wurde die Konzeption eines solchen Workshops nicht weiter verfolgt.

II.4.1.4 Ergebnisbewerung

Ziel aus Teilvorhabensbeschreibung	Bewertung
Aufbau eines Testsystems (Versuchsfahrzeug, Teilsystem)	Teilweise erfüllt *Anforderungen für Teilsysteme in Demonstrationsszenario ermittelt*
Leistungsbewertung der Methodik und des Demonstratorwerkzeugs auf einem Labor-SAF	Teilweise erfüllt *Methodik anhand des Demonstrationsszenarios validiert, jedoch nicht differenziert evaluiert*

III. Verwertung und voraussichtlicher Nutzen

III.1 Wirtschaftliche Erfolgsaussichten

HOOD beabsichtigt spezifische Produkte zu den betrachteten Vorgehensweisen zu entwickeln, die das Produktportfolio von HOOD erweitern und tragfähiger machen. Hierunter fallen z.B. themenspezifische Workshops, Webinare, Methodentrainings und Fachvorträge. Außerdem sieht HOOD in dem Projekt die Chance, die Vernetzung über die bekannten Domänen hinaus zu verbessern.

Gemäß unserer Untersuchung zur Dissemination der Ergebnisse (17), beabsichtigt HOOD, im Modus „online, asynchron" die erarbeiteten Ergebnisse an seine Kunden zu vermitteln. Daraus soll für HOOD idealerweise eine erhöhte Nachfrage an Beratung im Bereich Safety- und Security-Requirements-Engineering entstehen.

III.2 Wissenschaftliche und technische Erfolgsaussichten

HOOD beabsichtigt die Aspekte agiler Vorgehensweisen im regulierten und sicherheitskritischen Umfeld weiter zu vertiefen, da diese auch in anderen Branchen eine große Herausforderung darstellen. Es wird angestrebt, die erzielten Ergebnisse in der betriebswirtschaftlichen und technischen Anwendungsintegration weiter zu untersuchen und in zukünftige Forschungs- und Industrie-Projekte einzubringen. Die entwickelten Methoden, Informationsmodelle und Werkzeuge können auch Anwendung in anderen Branchen/Bereichen finden, was Inhalt zukünftiger Projekte von der HOOD GmbH sein kann.
Nach Ende des Forschungsprojektes plant HOOD, basierend auf dem im Forschungsprojekt genutzten Verfahren, ein generelles Verfahren zur Anpassung von Anforderungsmanagementwerkzeugen zu entwickeln, mit dem das erarbeitete Informationsmodell potenziell in jedem verfügbaren Anforderungsmanagementwerkzeug umgesetzt werden kann.
Weiterhin besteht, durch das offene Netzwerk der HOOD GmbH, eine erprobte Möglichkeit des Forschungs- und Technologietransfers. Des Weiteren sollen die Projektergebnisse auf eigenen Konferenzen, beispielsweise der REConf, vorgestellt werden, die als Zielgruppe sowohl Wissenschaftler als auch Praktiker haben und somit einen großen Verbreitungsgrad im deutschsprachigen Raum sicherstellen. Als Plattform für die Verbreitung der Forschungsergebnisse ist darüber hinaus die Integration in Gastvorträge bei externen Veranstaltungen vorgesehen.

III.3 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

HOOD beabsichtigt, die Erkenntnisse aus dem SATiSFy Projekt auf der REConf (www.REConf.de) vorzustellen, um eine große Anzahl von RE-Experten zu erreichen.
Die REConf, als größte deutschsprachige Konferenz mit den Themen Requirements Engineering und angrenzenden Disziplinen, wird jedes Jahr von der HOOD GmbH veranstaltet und spricht mehr als 300 RE-Fachexperten aus den unterschiedlichsten Domänen an. Die entwickelten Ergebnisse stellen ein generisches Rahmenwerk bezüglich der frühzeitigen Validierung von Safety- und Security-Anforderungen dar. Die Ergebnisse tragen dazu bei, langfristig und in verschiedenen Domänen nachhaltig nutzbar zu sein. Der direkte branchenübergreifende Anwendungsnutzen wird durch die entwickelten Methoden, Modelle und Strategien herausgestellt, so dass eine Verwertung auch außerhalb des Projektkonsortiums sichergestellt wird. Die Anschlussfähigkeit wird zusätzlich durch kontinuierliche Weiterentwicklungen sichergestellt, die die Erfolgsaussichten in Richtung marktfähiger Produkte zusätzlich verbessern.

IV. Veröffentlichungen

Beitrag zu Vorstellung des Projekts auf VDI Konferenz „6th International VDI Conference - Cyber Security for Vehicles" (18)

V. Positionen des zahlenmäßigen Nachweises

In der Projektlaufzeit 01.05.2018 bis 30.04.2021 (kostenneutrale Verlängerung bis 31.07.2021) wurden die bewilligten Gesamtmittel vollständig verbraucht.
Die folgende Tabelle gibt einen Überblick über die nachgewiesenen Ausgaben, die insgesamt die bewilligten Ausgaben übersteigen:

Tabelle 12 Positionen des zahlenmäßigen Nachweises

Angaben in EUR	Bewilligte Ausgaben	Nachgewiesene Ausgaben
Material (0813)	1.941,61 EUR	1.941,61 EUR
Personalausgaben (0837)	532.052,40 EUR	535.184,42 EUR
Reisekosten (0838)	5.347,99 EUR	5.347,99 EUR
Gesamtausgaben	539.342,00 EUR	542.474,02 EUR

Die Reisekosten (0838) fielen geringer als geplant aus, da als Folge der Corona-Pandemie zahlreiche Projekttreffen durch Online-Meetings ersetzt wurden. (Umwidmung in Personalkosten)
Materialkosten (0813) waren geringer als geplant (Umwidmung in Personalkosten).

Literaturverzeichnis

1. **Mühlbauer, Susanne.** Machen Sie noch Anforderungsmanagement oder sind Sie schon READY for Scrum? (Are you still doing requirements management or are you ready for Scrum?). Zürich, Schweiz : s.n., 06 2011.
2. **Stålhane et al.** The application of SafeScrum to IEC 61508-Certifiable Software. *Safety-Critical Systems Club Newsletter, Volume 23, Number 1.* 2013.
3. **Hood, Colin und Wiebel, Rupert.** *Optimieren von Requirements Management & Engineering.* s.l. : Springer-Verlag GmbH, 2005. ISBN: 3540211780.
4. **Hood, Colin, et al.** *Requirements Management.* s.l. : Springer-Verlag GmbH, 2008. ISBN: 978-3-540-47689-4.
5. **HIS.** Herstellerinitiative Software. [Online] http://portal.automotive-his.de.
6. **Object Modelling Group.** Requirements Interchange Format (ReqIF). [Online] 07 2016. [Zitat vom: 19. 11 2021.]
7. **Wikipedia.** Automotive SPICE - Wikipedia, Die freie Enzyklopädie. [Online] [Zitat vom: 19. 11 2021.] http://de.wikipedia.org/wiki/Automotive_SPICE.
8. **Stolz, Philip, Chen, Si und Eberhardt, Markus.** *Meilensteinbericht M01: Analyse der Bedrohungen und Anforderungen: Verifikation, Validation und Restrisikoanalyse.* Oberhaching : HOOD GmbH, 2021. M01.
9. *Perceptions on the State of the Art in Verification and Validation in Cyber-Physical Systems.* **Zheng, Xi, et al.** 4, s.l. : IEEE, 2017, IEEE Systems Journal, Bd. 11, S. 2614–2627. ISSN: 2373-7816.
10. *Translating Grafcet specifications into Mealy machines for conformance test purposes.* **Provost, Julien, Roussel, Jean-Marc und Faure, Jean-Marc.** 2011, Bd. 19, S. 947-957. ISSN: 0967-0661.
11. **Dghaym, Dana, et al.** Systematic Verification and Testing. *Validation and Verification of Automated Systems.* s.l. : Springer International Publishing, 2019, S. 89–104.
12. **Stolz, Philip und Eberhardt, Markus.** *Meilensteinbericht M02: Zwischenevaluation nach Refinement der Anforderungen: Kombiniertes Safety & Security Informationsmodell.* Oberhaching : HOOD GmbH, 2021. M02.
13. **Wikipedia.** Restrisiko — Wikipedia, Die freie Enzyklopädie. [Online] 2017. [Zitat vom: 09. 01 2019.] [Online; Abruf: 09. Jan. 2019]. https://de.wikipedia.org/w/index.php?title=Restrisiko&oldid=171100980.
14. **Ernst Basler + Partner, [Hrsg.].** *Risikoorientierte Sicherheitsnachweise im Eisenbahnbetrieb.* (Stand Oktober 1996). Bonn : Bundesministerium für Verkehr, 1996.
15. **Stolz, Philip und Eberhardt, Markus.** *Meilensteinbericht M03: Werkzeugimplementierung und Test.* Oberhaching : HOOD GmbH, 2021. M03.
16. **EKUT, DFKI, CE, Bosch & HOOD.** Gesamtdemonstrator: Übersicht der Beiträge. *SATiSFy.* Online : SATiSFy, 2021.
17. **Stolz, Philip und Eberhardt, Markus.** *Meilensteinbericht M04: Dissemination.* Oberhaching : HOOD GmbH, 2021. M04.

18. *Conquering Safety & Security in Autonomous Vehicles.* **Große, Daniel.** virtuell : SATiSFy, 2020.
19. **International Organization for Standardization.** *ISO 26262 Road vehicles — Functional safety — Part 3: Concept phase.* Geneva, Switzerland : ISO, 2018. Norm.
20. **Pohl, Klaus.** *Requirements Engineering Grundlagen, Prinzipien, Techniken.* Heidelberg : dpunkt.verlag, 2008. ISBN: 9783898645508.
21. *A taxonomy of model-based testing approaches.* **Utting, Mark, Pretschner, Alexander und Legeard, Bruno.** 2012, Softw. Test. Verification Reliab., Bd. 22, S. 297–312.
22. **Ma, Canlong.** *Advances in Model-Based Testing of Programmable Controllers: Automatic Test Generation using Design-to-Test and Plant Features.* Technische Universität München. München : s.n., 2019. Dissertation.
23. *Testing with model checkers: a survey.* **Fraser, Gordon, Wotawa, Franz und Ammann, Paul E.** s.l. : John Wiley & Sons, Ltd, 9 2009, Softw. Test. Verif. Reliab., Bd. 19, S. 215–261. ISSN: 0960-0833.
24. *Simulation coverage enhancement using test stimulus transformation.* **Ip, C. Norris.** San Jose, CA, USA : IEEE, 2000. S. 127–133. ISBN: 0-7803-6445-7 ISSN: 1092-3152.
25. *Systematic Test and Validation of Complex Embedded Systems.* **Tatar, Mugur und Mauss, Jakob.** 2014. ERTS-2014 (Feb. 5-7 2014).
26. **HOOD GmbH.** *Analyse der Bedrohungen und Anforderungen: Verifikation, Validation und Restrisikoanalyse.* 2021.
27. **GRVA.** Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issue of UNECE WP.29 GRVA. *Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issue of UNECE WP.29 GRVA.* September 2018.
28. **OWASP.** OWASP. *Open Web Application Security Project®.* [Online] [Zitat vom: 31. 07 2021.] https://owasp.org.
29. **Stolz, Philip und Eberhardt, Markus.** SATiSFy Abschlusspräsentation HOOD. *SATiSFy.* virtuell : SATiSFy, 2021.

Tabellenverzeichnis

Abbildungsverzeichnis