Sachbericht Teil 1 (Kurzbericht)

BMBF-Verbundprojekt SATiSFy:
Frühzeitige Validierung von Safety- und Security Anforderungen in autonomen Fahrzeugen

Zuwendungsempfänger:	**DFKI GmbH**
Vorhabenbezeichnung:	SATiSFy
Förderkennzeichen:	16KIS0821K
Projektlaufzeit:	01.05.2018 bis 30.07.2021
Erstelldatum:	18.01.2022
Autor:	Dr. Julian-Steffen Müller
Ansprechpartner:	Dr. Julian-Steffen Müller

Der vorliegende Kurzbericht gibt eine Übersicht über die von der Volkswagen AG durchgeführten Tätigkeiten und erzielten Ergebnisse im Forschungsprojekt „Frühzeitige Validierung von Safety- und Security Anforderungen in autonomen Fahrzeugen“, kurz SATiSFy.
Im Rahmen von Arbeitspaket 1 wurden der Stand von Wissenschaft und Technik abgebildet. Hierzu wurde insbesondere eine intensive Literaturrecherche zum Thema Entscheidungs- und Votingmechanismen bei redundanten E/E/PE-Systemen durchgeführt. Weitere Recherchen sind u.a. zur Thematik Optimierungsalgorithmen für Netzstrukturen durchgeführt worden. Es konnte festgestellt werden, dass für viele Anwendungen auf autonome Fahrzeuge keine Standards vorhanden sind. Auch eine Recherche im Bereich angrenzender Industrien, beispielsweise der Luft- und Raumfahrt sowie der Bahnindustrie, konnte in diesen Bereichen keine zufriedenstellenden Lösungen aufzeigen. Um vor diesem Hintergrund die Herausforderungen des autonomen Fahrens besser abbilden zu können, wurde im Rahmen von Arbeitspaket 2 und 3 ein Ebenenmodell erarbeitet. Dieses stellt die Wechselwirkungen zwischen dem Fahrzeug und der Umwelt einerseits auf der Umsetzungs- und andererseits auf der Systemebene dar. Die Umwelt und das Fahrzeug dienen in diesem Modell als Input. Die Umwelt besitzt dabei dynamische Eigenschaften/Parameter, welche sich aufgrund variabler Umgebungsbedingen ständig ändern können (dynamischer Input). Das Fahrzeug hingegen stellt ein statisches Architekturgerüst zur Verfügung, welche in der Umsetzungsebene und der Systemebene bestmöglich auf die Sicherheitsanforderungen, welche aus der Umweltebene entstammen, angepasst werden muss. Der konkrete Ablauf der Umsetzungsebene wurde in Arbeitspaket 4 realisiert. Basierend auf dem FDIR-Prozess aus der Luft- und Raumfahrt wurde der so definierte FDIRO-Prozess entwickelt, welcher Änderungen der Systemkonfiguration veranlassen kann. Diese Änderungen können einerseits durch sich ändernde Sicherheitsanforderungen aus der Umweltebene entstehen, andererseits aber auch durch Ausfälle und Fehler in der aktuellen Systemkonfiguration. Für den Fall eines Fehlers wurde im FDIRO-Prozess eine Strategie zum Fehlermanagement hinterlegt, welche auf unterschiedliche Fehler, beispielsweise Hard- oder Softwarefehler, reagieren kann und versucht, die erforderliche Systemkonfiguration wieder herzustellen. Die Umsetzung der Fahrzeugebene wurde im Rahmen von Arbeitspaket 5 adressiert. In diesem Rahmen wurde der C-PO Ansatz erarbeitet, welcher das Ziel einer kontextbasierten Application-Placement-Optimierung verfolgt. Konkret geht es hierbei um die Zuordnung von Software-Bausteinen, sogenannten Applications, auf die verfügbaren Rechenknoten im Fahrzeug. C-PO stellt sicher, dass bei einem Absinken des Sicherheitsniveaus eines Systems

aufgrund eines auftretenden Fehlers dieses wieder hergestellt wird. Sobald das höchste Sicherheitsniveau erreicht ist, optimiert C-PO die Applikationsplatzierung entsprechend der aktuellen Fahrsituation.
Zur Evaluation der erarbeiteten Modelle wurde das Tool AT-CARS im Rahmen von Arbeitspaket 6 umgesetzt. Dieses Tool, welches mittels MATLAB umgesetzt wurde, bietet die Möglichkeit, unterschiedliche Systemkonfigurationen, mit und ohne integrierten FDIRO-Prozess, zu vergleichen. Für diesen Vergleich wurde einerseits eine Auswertung hinsichtlich der Zuverlässigkeit des Systems durchgeführt, andererseits wurde auch die Sicherheit des Systems beurteilt. Diese Sicherheitsbewertung berücksichtigt u.a. inwieweit das Monitor-Control-Prinzip eingehalten wurde oder welche Fehlertoleranz vorliegt. Das Tool wurde als Simulationstool, basierend auf der Monte-Carlo-Simulation, entwickelt.
Die Veranschaulichung des FDIRO-Prozesses wurde im Rahmen von Arbeitspaket 7 im Rahmen eines Demonstrators verdeutlicht. In diesem werden einerseits sicherheitsrelevante, andererseits Komfort-Funktionen dargestellt, welche jeweils ausfallen können. Die Applikationen werden dabei auf vier Raspberry Pis dargestellt. Auf einem zusätzlichen Tablet wird das Fahrzeug, der aktuelle Zustand und aktuelle Schritt im Fehlermanagement abgebildet.

Sachbericht Teil 2 (Eingehende Darstellung)

BMBF-Verbundprojekt SATiSFy:
Frühzeitige Validierung von Safety- und Security Anforderungen in autonomen Fahrzeugen

Zuwendungsempfänger:	DFKI GmbH
Vorhabenbezeichnung:	SATiSFy
Förderkennzeichen:	16KIS0821K
Projektlaufzeit:	01.05.2018 bis 30.07.2021
Erstelldatum:	18.01.2022
Autor:	Dr. Julian-Steffen Müller
Ansprechpartner:	Dr. Julian-Steffen Müller

1 Einleitung

Das vorliegende Dokument stellt den Abschlussbericht des Vorhabens SATiSFy dar. SATiSFy wurde durch das Bundesministerium für Wirtschaft und Technologie (BMWi, Förderkennzeichen 16KIS0821K) gefördert.

Dieser Abschlussbericht folgt dabei dem in der Anlage 2 zum NKBF 98 gegebenen Muster. In Kapitel 2 wird eine kurze Darstellung des Projektes gemäß Punkt I gegeben, Kapitel 3 stellt die inhaltlichen Entwicklungen in einer eingehenden Darstellung gemäß Punkt II des Musters dar. Die Punkte III (Erfolgskontrollbericht) und IV (Berichtsblatt bzw. Document Control Sheet) werden durch gesondert abgegebene Dokumente erfüllt.

Die dargestellten Arbeiten umfassen alle von der Volkswagen AG geleisteten Arbeiten im Vorhaben SATiSFy.

2 Kurzdarstellung

In diesem Kapitel wird zunächst die Aufgabenstellung des Projektes beschrieben (Abschnitt 1.1). Anschließend werden die Voraussetzungen des Vorhabens (Abschnitt 2.2) sowie Planung und Ablauf des Vorhabens (Abschnitt 2.3) behandelt. Es folgen Erläuterungen zum wissenschaftlichen Stand (Abschnitt 2.4) und zur Zusammenarbeit mit anderen Stellen (Abschnitt 2.5).

2.1 Aufgabenstellung

Die Volkswagen AG möchte im Projekt SATiSFY Erkenntnisse über die Auswirkungen unterschiedlicher Fahrzeugarchitekturen auf die grundlegenden Eigenschaften wie Safety und Security erlangen. Eines der Ziele ist dabei die Definition hilfreicher Metriken zur Bewertung von Fahrzeugarchitekturen. Für diese Metriken sollen dann Bewertungsmethoden entwickelt werden, mit denen die Unterschiede verschiedener Fahrzeugarchitekturvarianten bezüglich der zu untersuchenden Eigenschaften quantifiziert werden können.

Dadurch sollen dann die Auswirkungen der Einführung redundanter Komponenten in die Fahrzeugarchitektur als auch anderer Mechanismen zur Erhöhung der Sicherheit überprüft werden. Der Fokus der Untersuchung soll dabei auf der Designzeit der Systeme liegen, damit die entwickelten Bewertungsmethoden später auch für die Entwicklung realer Fahrzeuge eingesetzt werden können.
Zusätzlich sollen Methoden untersucht werden, um die identifizierten Metriken zur Laufzeit der Fahrzeuge zu messen und zu bewerten. Eine solche Form der Laufzeitüberwachung kann aus unterschiedlichen Gründen hilfreich sein. Einerseits kann gegebenenfalls vorsorglich auf sich abzeichnende Fehler im System reagiert werden, andererseits können die Metriken möglicherweise hilfreiche Einblicke in die Funktionsweise der aktiven Systeme geben um für nachfolgende Produkte Optimierungen oder Verbesserungen zu implementieren.
Schlussendlich sollen Techniken zum Validieren und/oder Verifizieren der Wirksamkeit der eingeführten Mechanismen und redundanten Systeme entwickelt werden, welche es ermöglichen die Verbesserung der Sicherheit nachzuweisen.

2.1.1 Technische und wissenschaftliche Arbeitsziele

Die Aufgabe und Arbeitsziele von SATiSFy liegen darin, die komplexe Verbindung von Security und Safety-Anforderungen für den Kontext eines SAF (System zum autonomen Fahren) als heterogenes Mehrkomponentensystem frühzeitig beherrschbar (mittels der Erfassung geeigneter Sicherheitsanforderungen und -komponenten im Designprozess) und nachvollziehbar (mittels geeigneter Verifikations- und Validationsmethoden) zu machen. Hinsichtlich eines definierten Angreifer- bzw. Fehlermodells sind dabei grundlegende Designstrategien und Schutzmethoden für viele Safety- und Security-Anforderungen bekannt. Viele davon sind als „Building Block“ bzw. Strukturelement aus Vorarbeiten verfügbar. Es gilt diese jedoch in den Gesamtkontext eines SAF so einzubetten, dass durch formale Argumente und Komposition eine hinreichende Aussage über die erreichte Sicherheit und Resilienz bzw. das Restrisiko gegenüber (I) absichtlichen Angriffen und (II) unabsichtlichen Einwirkungen getroffen werden kann. Bislang ist exakt dies nur fragmentarisch möglich und kann nur durch stringente formale Vorgaben bei den Komponentenschnittstellen zur Komposition und Verifikation von Sicherheitseigenschaften realisiert werden. Bei komplexen SAF ist dies jedoch zwingend in einer gesamtheitlichen Art und Weise erforderlich um ein jegliches Fehlverhalten hinsichtlich (I) und (II) ausschließen zu können. Dabei kann in SATiSFy das Konzept virtueller Prototypen (d.h. eine Simulationsumgebung für die frühzeitige Verifikation von Komponenteneigenschaften) zum Einsatz kommen, um Einzelkomponenten sowie Subsysteme in einem hierarchischen Prozess separat zu verifizieren und abschließend deren Komposition in eine gesamtheitliche Verifikationsaussage zu überführen. Dies kann gleichzeitig auch einen allgemeinen Ansatz als neue Ingenieursdisziplin bereitstellen, um die Sicherheit im Sinne vom Security und Safety gesamtheitlich zu verbessern.

2.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Im Rahmen der Tätigkeiten innerhalb des Projektes ist es eine Herausforderung, Disziplinübergreifend Expertisen zu sammeln und diese in den erarbeiteten Modellen zusammenzuführen. Um dies zu gewährleisten, wurde als Unterauftragnehmer das Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH gewählt. Dieses ist ein Experte auf dem Bereich der

quantitativen Sicherheits- und Zuverlässigkeitsanalyse sowie im Bereich der Funktionalen Sicherheit, wodurch innerhalb des Projektes die Safety-Aspekte abgedeckt werden. Security-Aspekte und die Expertise im Bereich automatisiertes Fahren werden hauptsächlich durch die Mitarbeiter der Volkswagen AG, insbesondere Ingenieure aus der Konzernforschung, sowie im Rahmen vom regelmäßigen Austausch mit den Projektpartnern, insbesondere dem DFKI, abgedeckt.
Die inhaltliche Projektleitung des Teilvorhabens wurde von Herr Dr. Julian-Steffen Müller übernommen.

2.3 Planung und Ablauf des Vorhabens

Das Vorhaben folgt dem in Abbildung 1 dargestellten Zeitverlaufsplan. Hierbei ist zu beachten, dass regelhafte Rückkopplungen zwischen den Arbeitspaketen implementiert werden, die durch grüne Pfeile gekennzeichnet sind. Daher wird kein klassisches Wasserfallmodell, sondern vielmehr ein Feedback-basierter Entwicklungsansatz im Vorhaben SATiSFy verfolgt. Aufgrund der vorgesehenen Rückkopplungsschleifen sind daher auch längere Bearbeitungszeiträume für die Arbeitspakete AP2 bis AP6 vorgesehen.

Paket	Titel	Monate	Projektmonate 1-12	Projektmonate 13-24	Projektmonate 25-35
AP 0	Projektmanagement	M01-M36			
AP 1	Sicherheits- & Anforderungsanalyse	M01-M24			
AP 2	Framework für sichere SAF-Architekturen	M06-M30			
AP 3	Statische Sicherheitseigenschaften	M06-M30			
AP 4	Dynamische Sicherheitseigenschaften	M12-M30			
AP 5	Werkzeugentwicklung	M12-M30			
AP 6	Evaluation und Sicherheitsanalyse	M09-M36			
AP 7	Demonstration und Dissemination	M15-M36			

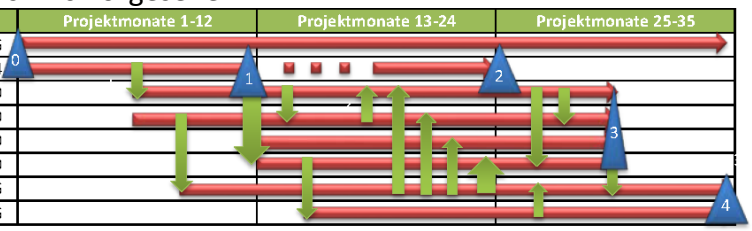

Abbildung 1: Zeitlicher Ablauf des Projektes

Meilensteine sind als blaue Dreiecke markiert. Diese sind im Detail:

- Meilenstein M0: Projekt Kick-off.
- Meilenstein M1: Analyse der Bedrohungen und Anforderungen erfolgt, Ergebnisse liegen als Bericht vor.
- Meilenstein M2: Zwischenevaluation nach Verfeinerung der Anforderungen **(Abbruchmeilenstein).**
- Meilenstein M3: Abschluss der Implementierungen und vorläufige Evaluationsergebnisse liegen vor.
- Meilenstein M4: Projektabschluss: Demonstratoren vorhanden.

2.4 Wissenschaftlicher und technischer Stand zu Beginn des Vorhabens

Vergangene Forschungsprojekte wie SHE oder EVITA haben die Einführung von grundlegenden kryptographischen Methoden zur Steigerung der Security im Fahrzeug bewirkt. Ebenso hat die verpflichtende Umsetzung der ISO 26262 zu einer erheblichen Steigerung der Safety in modernen Fahrzeugen geführt. Weiterhin gibt es viele kleinere Technologien und Methoden, welche diese Aspekte behandeln und die allgemeine Sicherheit von Fahrzeugen verbessert haben.
Jedoch haben all diese Methoden und Technologien meist einen Fokus auf spezifische Fahrzeugfunktionen. Dies bedeutet, dass die Sicherheit der einzelnen Funktion betrachtet und verbessert wird, was auch zu einer Steigerung der ganzheitlichen Sicherheit führt. Jedoch wird dadurch nicht eine Untersuchung der gesamten Fahrzeugarchitektur vorgenommen, womit

insbesondere komplexe Systeme wie ein automatisch fahrendes Fahrzeug nicht direkt bewertet werden können. Ebenso ist die Bewertung dynamisch redundanter Systeme (Systeme mit redundant begrenzten Kapazitäten mit der Möglichkeit mehrere andere Funktionen zu übernehmen, jedoch nicht alle gleichzeitig) mit diesen klassischen Methoden nicht möglich. Unter dem Ziel „Vision Zero“ werden aber die zu entwickelnden Systeme noch geringere Fehlerwahrscheinlichkeiten aufweisen müssen, welche voraussichtlich nur über Redundanz zu erreichen sind. Hierzu existieren aber heutzutage keine etablierten Methoden, um Redundanz oder dynamische Rekonfiguration in eine Fahrzeugarchitektur zu integrieren und zu bewerten.
Weiterhin lassen sich existierende Methoden und Techniken aus anderen Branchen nicht direkt im Fahrzeug anwenden. Beispielsweise hat die Luft- und Raumfahrt sehr mächtige Technologien zum Berechnen und Verwenden redundanter Komponenten entwickelt, jedoch sind diese sowohl von der Entwicklungszeit zu langwierig als auch von der Verwendung zu kostspielig um in der Automobilbranche verwendet werden zu können. Um beide Punkte zu adressieren, bietet sich eine Zusammenarbeit mit Experten aus den entsprechenden Bereichen an um eine Anpassung an die spezifischen Zielanforderungen der Automobilbranche zu ermöglichen.

2.5 Zusammenarbeit mit anderen Stellen

Im Rahmen des Projektes SATiSFy erfolgte ein intensiver Austausch zum Themenkomplex Anforderungen an die Sicherheitsarchitektur sowie mögliche Methoden zur Validierung von Sicherheitseigenschaften. Um eine enge Kooperation der Projektpartner zu ermöglichen, damit die Projektziele erreicht werden, fanden Projekttreffen sowie regelmäßige Telefonkonferenzen statt.
Darüber hinaus wurde, wie in Abschnitt 2.2 das Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH als Unterauftragnehmer durch die Volkswagen AG beauftragt, um die Expertise im Bereich Safety sicherzustellen.

2018

Datum	Thema	Ort	Beteiligte
04.06.2018-05.06.2018	Kickoff	Bremen	alle
22.08.2018-23.08.2018	Anforderungsworkshop bei Volkswagen: Sicherheits und Anforderungsanalyse	Wolfsburg	Alle
17.09.2018	SATiSFy-Architektur	Telefonkonferenz	alle
12.10.2018	SATiSFy-Architektur	Telefonkonferenz	VW, Bosch
15.10.2018	Verfeinerung der SATiSFy-Architektur	Telefonkonferenz	alle
26.10.2018	SATiSFy-Architektur	Telefonkonferenz	VW, Bosch
07.11.2018	SATiSFY-Architektur	Telefonkonferenz	VW, Bosch
19.11.2018	Verfeinerung der SATiSFy-Architektur	Telefonkonferenz	alle

03.12.2018- 04.12.2018	Workshop bei Bosch: SATiSFy-Architektur Safety-Anforderungen Security-Anforderungen	Reutlingen	alle

2019

Datum	Thema	Ort	Beteiligte
21.01.2019	Status Updates	Telefonkonferenz	Alle
18.02.2019	Vorbereitung Treffen Hamburg	Telefonkonferenz	Alle
18.03.2019	Planung Statustreffen	Telefonkonferenz	Alle
31.03.2019	Security Angreifer	Telefonkonferenz	Alle
02.04.2019	„Security“ Angreifer und Angriffe Problem- und Technischer- Scope Safety & Security auf OSI-Layer 2 Constraint Korridore Zuverlässigkeit beim Autonomen Fahren Datenflusskontrolle im Sinne der Vertraulichkeit	Hamburg	Alle
20.05.2019	Vorbereitung Statustreffen	Telefonkonferenz	Alle
17.06.2019	Architektur	Telefonkonferenz	Alle
25.06.2019- 26.06.2019	Statustreffen	Bremen	Alle
15.07.2019	Nachbesprechung Statustreffen	Telefonkonferenz	Alle
16.09.2019	Planung TelKos und Projekttreffen	Telefonkonferenz	Alle
17.10.2019	Projekttreffen und Themenfindung	Telefonkonferenz	Alle
21.11.2019	SATiSFy Szenario	Telefonkonferenz	Alle
12.12.2019- 13.12.2019	SATiSFy Szenario	Tübingen	Alle
19.12.2019	SATiSFy Szenario	Telefonkonferenz	Alle

2020

Datum	Thema	Ort	Beteiligte
16.01.2020	Monatliche Telko; Besprechung des VDI Vortrags	Telefonkonferenz	Alle
20.02.2020	Monatliche Telko;	Telefonkonferenz	Alle

19.03.2020	Monatliche Telko; Besprechung und Organisation des Projektreffens in Freiburg. Weitere Besprechung des VDI Vortrags	Telefonkonferenz	Alle
09.04.2020	Monatliche Telko; Finalisierung der Präsentation für VDI Vortrag (Cybersecurity for Vehicles), Foliensätze der Partner	Telefonkonferenz	Alle
29.04.2020	Projekttreffen, Corona-bedingt virtuell	Telefonkonferenz	Alle
06.05.2020	Zusammenarbeit; Verknüpfung der beiden Methodiken und Tools (Analyse + Simulation)	Telefonkonferenz	DFKI, IQZ, VW
28.05.2020	Monatliche Telko; Agenda für Statustreffen	Telefonkonferenz	Alle
18.06.2020	Monatliche Telko; Finale Besprechung des Statustreffens	Telefonkonferenz	Alle
23.06.2020	Statustreffen mit Projektträger	Telefonkonferenz	Alle
20.08.2020	Monatliche Telko; Abstimmung von Arbeiten in der verbleibenden Projektlaufzeit, Demonstratoren	Telefonkonferenz	Alle
20.08.2020	Hybrides-Modell; Erste Vorstellung in kleiner Runde	Telefonkonferenz	DFKI, IQZ, VW
17.09.2020	Monatliche Telko	Telefonkonferenz	Alle
15.10.2020	Monatliche Telko; Kostenneutrale Verlängerung	Telefonkonferenz	Alle
19.11.2020	Monatliche Telko	Telefonkonferenz	Alle
03.12.2020	Projekttreffen; Demonstratoren, Hybrid-Modell	Telefonkonferenz	Alle
17.12.2020	Monatliche Telko	Telefonkonferenz	Alle

2021

Datum	Thema	Ort	Beteiligte
21.01.2021	Monatliche Telko	Telefonkonferenz	Alle
18.02.2021	Monatliche Telko	Telefonkonferenz	Alle
18.03.2021	Monatliche Telko	Telefonkonferenz	Alle
15.04.2021	Monatliche Telko	Telefonkonferenz	Alle
20.05.2021	Monatliche Telko	Telefonkonferenz	Alle
14.06.2021	Besprechung Abschlusspräsentation	Telefonkonferenz	DFKI, VW, IQZ
17.06.2021	Monatliche Telko	Telefonkonferenz	Alle
24.06.2021	Monatliche Telko	Telefonkonferenz	Alle

3 Eingehende Darstellung

Die folgenden Abschnitte beschreiben eingehend die vorgenommenen Arbeiten und Untersuchungen im Vorhaben SATiSFy sowie deren Ergebnisse.

3.1 Verwendung der Zuwendung

Arbeitspaket 1: Sicherheits- und Anforderungsanalyse

Innerhalb von Arbeitspaket 1 wurden folgende Recherchen hinsichtlich Literatur und Normen zur Aufarbeitung des Standes der Forschung und Technik für Safety-Methoden durchgeführt.

Literaturrecherche zum Thema Architekturen für Entscheidungs-/Votingmechanismen bei redundanten E/E/PE-Systemen

Das Ergebnis der Recherche zeigen, dass unterschiedliche Mechanismen zu berücksichtigen und aus Safety-Sicht nicht alle Bereiche bereits mit Methoden abgedeckt sind. Für den Bereich der Hardwareeigenschaften eignen sich Simulationsmethoden, während für mathematische Entscheidungsmechanismen Optimierungsmethoden angewendet werden können. Erkenntnisse hinsichtlich der Anwendung von Entscheidermechanismen sowie Straßenverkehrskenngrößen konnten nicht errungen werden. Bei den Kenngrößen für den Straßenverkehr stoßen aktuelle Vorgaben bei der Anwendung auf das autonome Fahren schnell an ihre Grenzen. So bietet beispielsweise die ISO 26262 „Road vehicles – Functional safety“ zwar ein generisches Vorgehen für den Produktentwicklungsprozess, jedoch müssen bei autonomen Fahrzeugen im Vergleich zu konventionellen, aktuell verfügbaren Fahrzeugen zusätzliche Aspekte berücksichtigt werden müssten, welche in der ISO 26262 adressiert werden. Hierzu ist anzumerken, dass sich viele Standards zu diesem Bereich aktuell in der Entstehung befinden, beispielsweise die ISO 21448 „Safety of the intended functionality“. Eine Zusammenfassung ist in Abbildung 2 gezeigt.

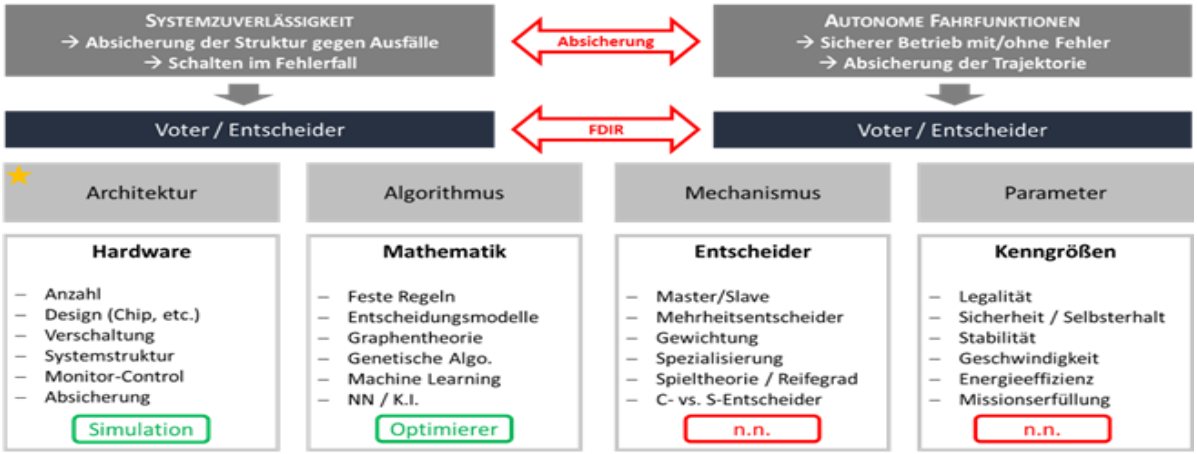

Abbildung 2: Literaturrecherche zum Thema Entscheidungsmechanismen

Literaturrecherche zum Thema Optimierungsalgorithmen für Netzstrukturen

Grundsätzlich sind Optimierungsmethoden des ILP (Integer-Linear-Programming) und LP (Linear-Programming) am besten für die im Forschungsprojekt vorhandenen Optimierungsaufgaben geeignet.

Unterschieden wird zwischen ganzzahligen Optimierungsvariablen und nicht-ganzzahligen Optimierungsvariablen. Die Lösungsmenge der ganzzahligen Optimierungsmethoden ist deutlich geringer, allerdings ist es im ganzzahligen Bereich deutlich schwieriger optimale Lösungen zu errechnen, da nicht im realen Zahlenbereich optimiert werden kann.
Innerhalb des SATiSFy-Projektes geht es um die Optimierung von Systemzuständen in einem endlichen Parameterraum mit einer endlichen Lösungsmenge. Physikalische Zwischenzustände können von Hardware-/Softwarestacks nicht eingenommen werden. Aus diesem Grund werden die Methoden des ILP für die weiteren Arbeiten fokussiert. Ein exemplarisches Beispiel befindet sich in Abbildung 3.

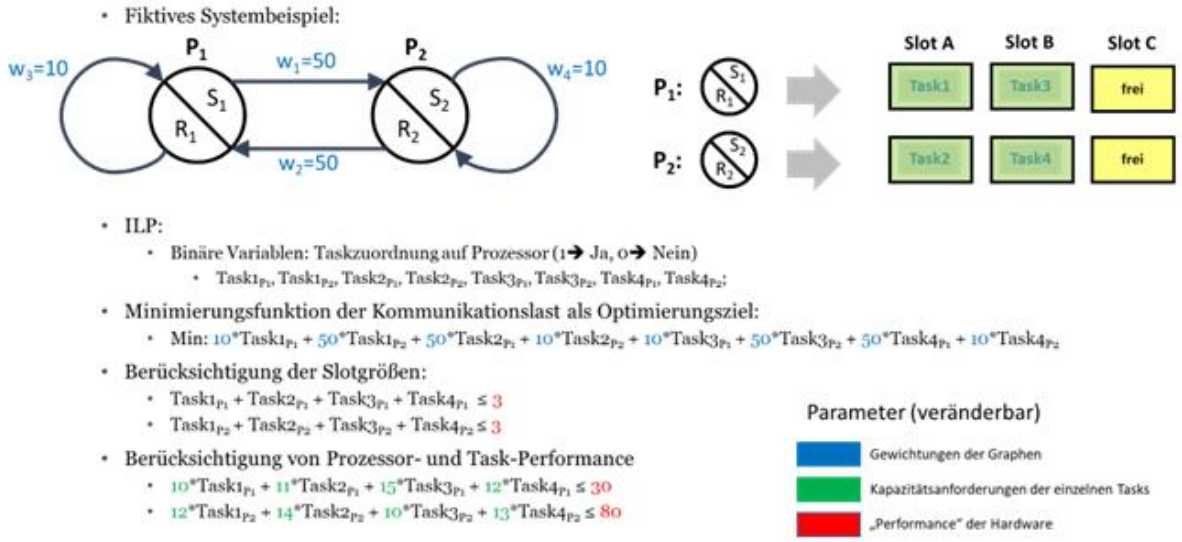

Abbildung 3: Optimierungsansatz nach ILP-Methodik

Arbeitspaket 2: Framework für sichere SAF-Architekturen/ Arbeitspaket 3: Statische Sicherheitseigenschaften (Designzeit)

Im Rahmen von Arbeitspaket 2 und 3, der Erstellung der Sicherheitsanforderungen auf unterschiedlichen Leveln, wurde ein Ebenenmodell entwickelt, welches unterschiedliche Awarenessebenen definiert, welche die Sicherheitsanforderungen in den Gesamtkontext des hochautomatisierten/autonomen Fahrens bringt.
Definiert wurden folgende Ebenen:

- Umweltebene (dynamisch/Umgebungsabhängig)
- Fahrzeugebene (statisch/Vernetzung im Fahrzeug)
- Umsetzungsebene (Operations-Zentrale)
- Systemebene (Apps/Komponenten)
- Optionale Ebenen (Lastkollektive, Ausfallmechanismen)

Die Umweltebene setzt sich aus dem Missionsziel und der Kontextebene zusammen, welche die Context Awareness beinhaltet. In der Context Awareness befinden sich alle Parameter, die den aktuellen Missionszustand unter Berücksichtigung der Umgebungs- und Missionsbedingungen beinhalten. Dies führt in Summe zu Sicherheitsanforderungen, die auf die Umsetzungsebene projiziert werden. Als Pendant dazu werden auf der Fahrzeugebene die technischen Möglichkeiten abgebildet, welche das Fahrzeug in Form von Assistenzebenen (Software) und Funktionspfaden (Soft- und Hardware) umsetzen kann.

Hieraus entsteht ein endlicher Pool an Funktionspfaden für einzelne Applikationen, auf welchen die Fahrfunktionen (samt Sensorik und Aktuatoren) ausgeführt werden können.
In der Umsetzungsebene findet nun, als zentrale Operationsinstanz (OPS), die Systemkonfiguration und – im Fehlerfall – das Dynamic Safety Management statt.
Die OPS überwacht und steuert den aktuellen Status und die einzelnen Funktionspfade jeder Applikation und moderiert die unterschiedlichen Betriebsmodi. Im Fehlerfall wird hier ein FDIRO-Prozess (siehe AP 4) ausgelöst, der die Rekonfiguration der Funktionspfade, eine Systemdegradierung oder einen Notmodus auslöst.
Auf dieser Ebene wird die Safety Awareness gebildet, abhängig von den Sicherheitsanforderungen, den technischen Möglichkeiten und dem aktuellen Status der einzelnen Funktionspfade.
Aus der OPS wird die Softwareallokation auf den Steuergeräten bestimmt (Systemebene mit Apps/Komponenten). Auf der Systemebene werden die Funktionen real ausgeführt. Das heißt, dass auf dieser Ebene, über die in SATiSFy verwendeten Simulationsmethoden Ausfälle- und Wiederherstellungszeitpunkte simuliert werden, die dann wiederum auf der OPS mit dem FDIRO-Prozess verarbeitet werden.
Somit entstehen eindeutig getrennte virtuelle und physische Ebenen, die das Gesamtmodell des hochautomatisierten Fahrens abbilden. Abbildung 4 skizziert das beschriebene Ebenenmodell kurz.

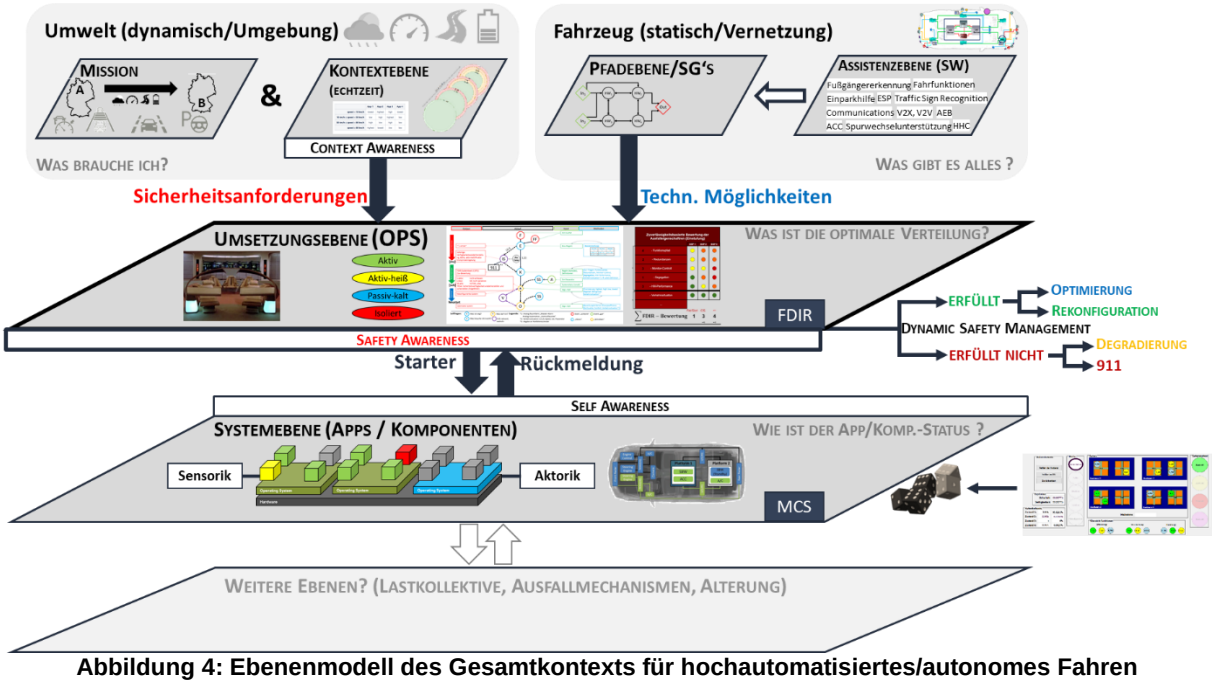

Abbildung 4: Ebenenmodell des Gesamtkontexts für hochautomatisiertes/autonomes Fahren

Arbeitspaket 4: Dynamische Sicherheitseigenschaften (Laufzeit)

Autonome Fahrzeuge müssen bei einer ausgefallenen sicherheitskritischen Anwendung diese eigenständig lösen können, ohne dass die Passagiere handeln müssen. Aus diesem Grund muss das verantwortliche System des autonomen Fahrzeugs die Ausfälle selbst erkennen und behandeln, um die Sicherheit der Passagiere und anderer Verkehrsteilnehmer zu gewährleisten. Aus diesem Grund wurde FDIRO („**F**ehler **D**etektion, **I**solation, **R**ückgewinnung und **O**ptimierung“) entwickelt. Dieses Vorgehen beruht auf dem FDIR-Prinzip (Abbildung 5), welches

aus der Luft- und Raumfahrt bekannt ist. Im Vergleich zur Automobilindustrie besteht in diesem Industriezweig die Herausforderung der Abwesenheit eines Menschen als Rückfallebene schon länger.

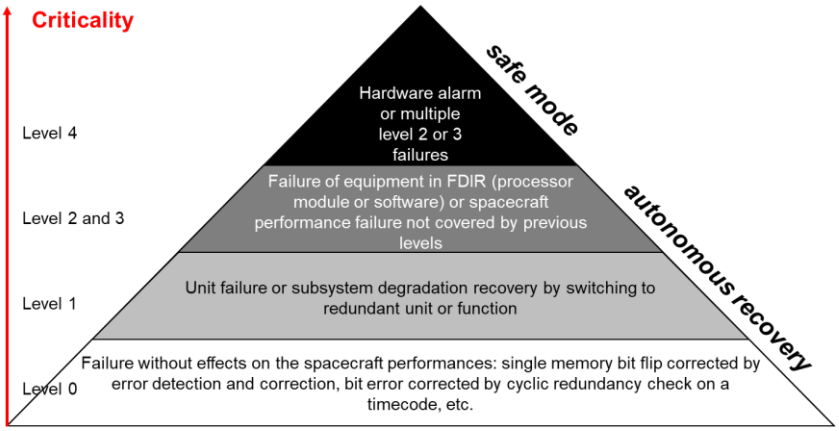

Abbildung 5: Fehler Diagnose und Management Architektur für Satelliten und Raumschiffe[1]

Der auf diesem FDIR-Prozess basierende FDIRO Prozess zum Management von Fehlern in automatisierten und autonomen Fahrzeugen ist in Abbildung 6 dargestellt.

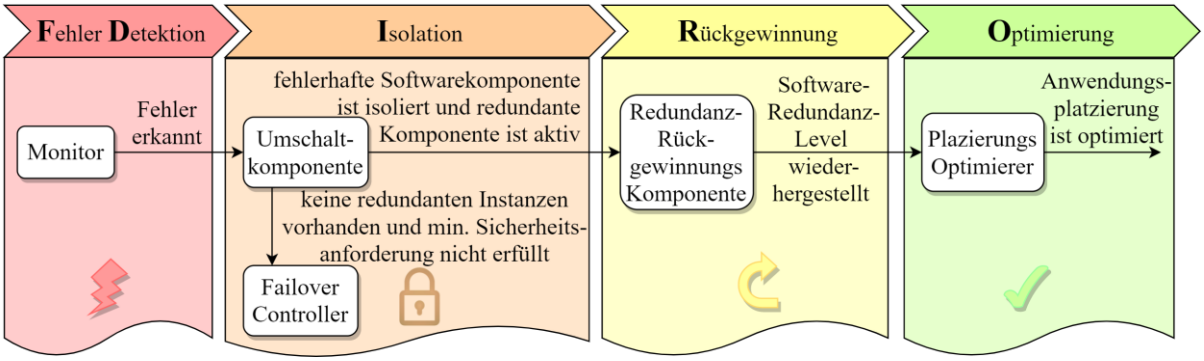

Abbildung 6: Zusammenfassung des FDIRO Prozess

Der erste Schritt definiert die Erkennung des Fehlers. Dazu beobachten sogenannte Monitore die Hardware- und Software-Anwendungen des selbstfahrenden Systems. Stellt ein Monitor einen Fehler fest, meldet er diesen an die Umschaltkomponente. Diese Komponente isoliert den Fehler indem sie die fehlerhaften Software-Applikationen deaktiviert. Als nächstes aktiviert die Umschaltkomponente redundante Softwareanwendungen, die die Aufgaben der ausgefallenen Anwendungen übernehmen. Wenn solche redundanten Anwendungen nicht vorhanden sind, müssen die Folgen des Fehlers bewertet werden. Falls diese Bewertung schwerwiegende Folgen vorhersagt, übernimmt der Failover-Controller die Steuerung des Systems und bringt das Fahrzeug zum Stillstand. Nach der Isolierung der fehlerhaften Komponente und der Aktivierung einer redundanten Komponente hat die Redundanz-Rückgewinnungs-Kompo-

[1] Zolghadri, A., Henry, D.; Cieslak, J.; Efimov, D; Goupil, P.: Fault Diagnosis and Fault-Tolerant Control and Guidance for Aerospace Vehicles – From Theory to Application. Springer-Verlag London, 2014, ISBN: 978-1-4471-5312-2.

nente das Ziel, das Software-Redundanzlevel wiederherzustellen. Dazu versucht die Redundanz-Wiederherstellungs-Komponente, Hardware-Komponenten zu finden, die genügend freie Ressourcen bieten, um redundante Anwendungen auszuführen. Im letzten Schritt versucht der Platzierung-Optimierer, eine optimierte Applikationsplatzierung zu finden, die zur aktuellen Fahrsituation passt.
Der detaillierte Verlauf des FDIRO Prozesses ist im folgenden Aktivitätsdiagramm (Abbildung 7) dargestellt.

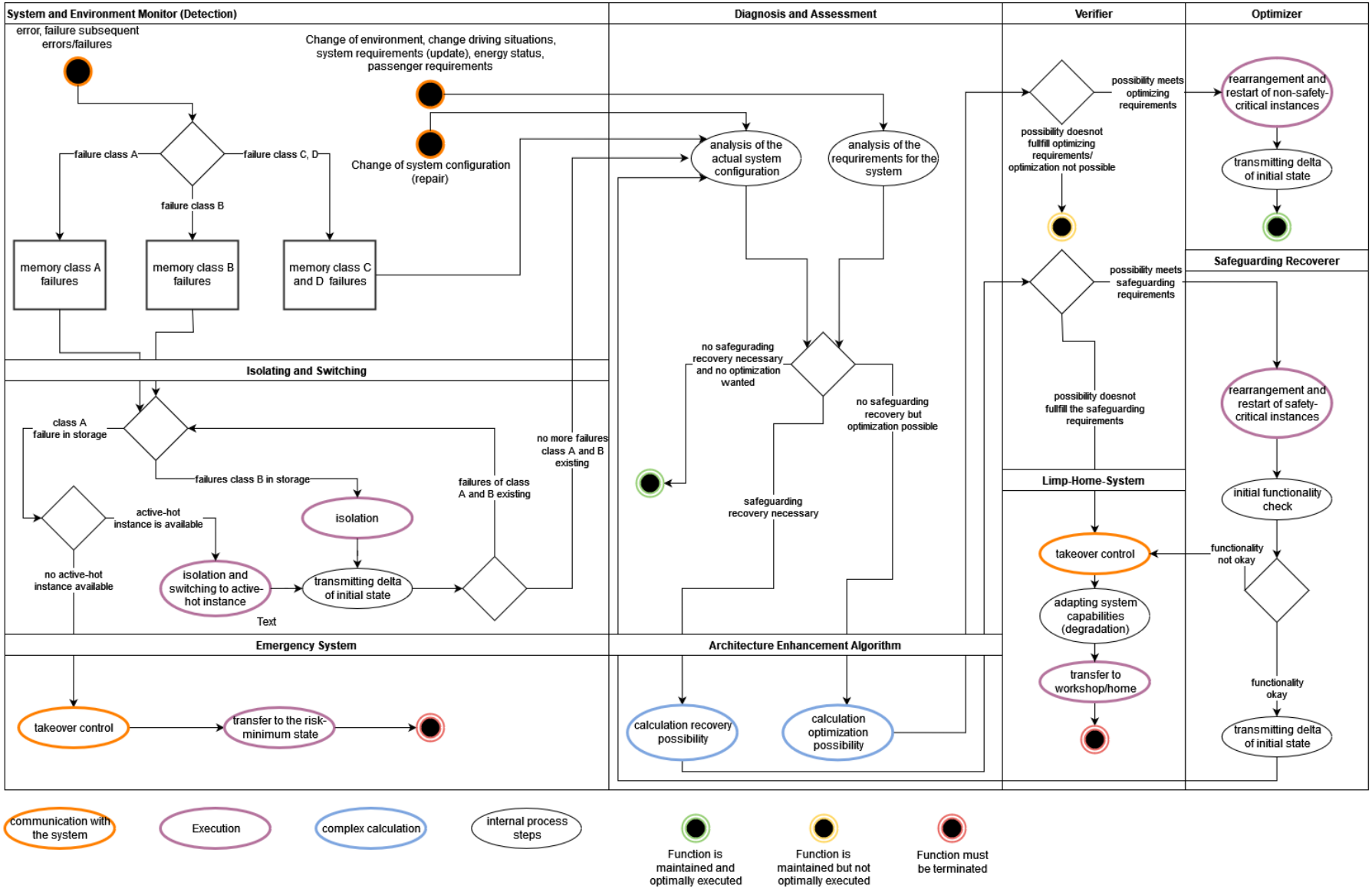

Abbildung 7: Aktivitätsdiagramm FDIRO Prozess

Arbeitspaket 5: Werkzeugentwicklung

Autonome Fahrzeuge sind komplex verteilte Systeme, die aus mehreren Softwareanwendungen und Rechenknoten bestehen. Die Bestimmung der Zuordnung zwischen diesen Softwareanwendungen und Rechenknoten wird als Application-Placement-Problem bezeichnet. Das Optimierungsziel für das Application-Placement-Problem ist jedoch nicht statisch, sondern muss entsprechend dem aktuellen Kontext, in dem sich das Fahrzeug befindet, angepasst werden. Daher wird ein Ansatz für eine kontextbasierte Bestimmung des Optimierungsziels für eine gegebene Instanz eines Applikationsplatzierungsproblems benötigt. Der Ansatz C-PO (**C**ontext-based **P**lacement **O**ptimization) adressiert genau diese Problemstellung. C-PO stellt sicher, dass bei einem Absinken des Sicherheitsniveaus eines Systems aufgrund eines auftretenden Fehlers das Optimierungsziel für die sukzessive ausgeführte Applikationsplatzierung darauf abzielt, das Sicherheitsniveau wieder herzustellen. Sobald das höchste Sicherheitsniveau erreicht ist, optimiert C-PO die Applikationsplatzierung entsprechend der aktuellen Fahrsituation.

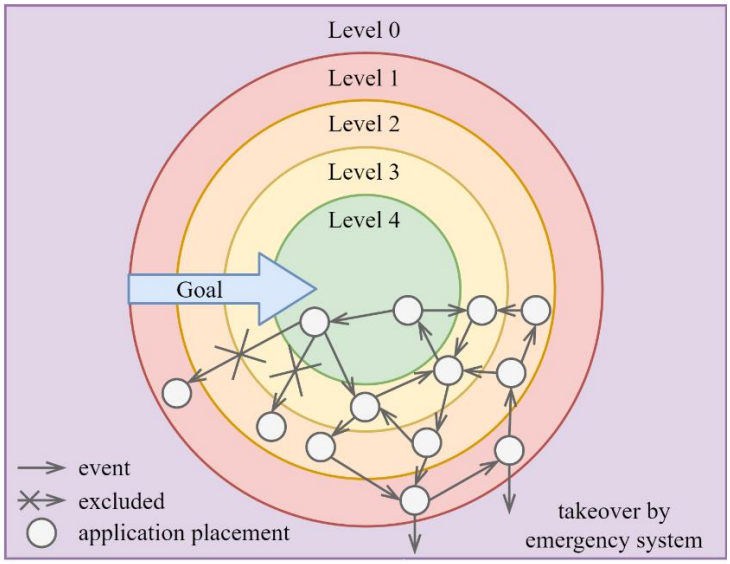

Abbildung 8: Visualisierung des Konfigurationsgraphen und der von C-PO hinzugefügten Ebenen. Die Ebenen über dem Konfigurationsgraphen unterteilen den Graphen in N Ebenen, wobei in diesem Beispiel N=4.

Abbildung 8 veranschaulicht die Idee der kontextbasierten Application-Placement-Optimierung. Der Ansatz von C-PO, ein Optimierungsziel für das aktuelle Application-Placement zu bestimmen, besteht darin, eine Schicht über den Konfigurationsgraphen zu legen. Diese Schicht unterteilt den Konfigurationsgraphen in mehrere Ebenen, wobei eine Ebenennummer (Level), $x \in \mathbb{N}$, für die $0 \leq x \leq N$ gilt, jede Ebene identifiziert, wobei $N \in \mathbb{N}$ die Anzahl der Ebenen ist. Je mehr Redundanzen es von einer Anwendung gibt, desto höher wird die Ebene klassifiziert, wobei ebenfalls die Anwendungspriorität betrachtet wird. Für die dynamische Anpassung der Anzahl der Ebenen und der Prioritäten wurden zwei Ansätze entwickelt: Der „Dynamische-Ebenen-Ansatz“ passt die Anzahl der Ebenen basierend auf dem aktuellen Kontext an und der „Dynamische-Priorisierungs-Ansatz“ passt die Priorität der Anwendungen entsprechend der aktuellen Situation an.

Arbeitspaket 6: Evaluation und Sicherheitsanalyse

Die Entwicklung von Systemarchitekturen, die eine Vielzahl von technischen und wirtschaftlichen Anforderungen erfüllen, ist bekanntlich eine anspruchsvolle Aufgabe bei der Konzeption eines neuen Fahrzeugs. Die Anforderungen, insbesondere an die Zuverlässigkeit, Verfügbarkeit und Sicherheit des Systems, steigen jedoch mit Blick auf die vollständige Autonomie (SAE Level 5) des Fahrzeugs deutlich an, da dieser Automatisierungsgrad jegliche Übernahmeaktionen durch die Fahrgäste ausschließt. Um den Anforderungen gerecht zu werden, ist ein ausfallsicheres Systemdesign erforderlich, das mehrere Rückfallpfade beinhaltet. Das Problem ist jedoch, dass die Systeme, die aus der Anwendung dieser Konzepte resultieren, sehr komplex sind und mit den heute verwendeten Werkzeugen und Methoden nicht ausreichend hinsichtlich der Verfügbarkeit, Sicherheit und Zuverlässigkeit des Systems analysiert werden können. Daher wurde AT-CARS „Analyzing Tool for Complex, Autonomous, and Reliable Systems“ entwickelt - ein Werkzeug, das in der Lage ist, verschiedene komplexe Systemarchitekturen, die für autonome Fahrzeuge entwickelt wurden, zu analysieren. Das Werkzeug zielt darauf ab, Systemingenieure zu unterstützen, die für die Bestimmung geeigneter Systemarchitekturen verantwortlich sind, die die erwarteten Sicherheitsanforderungen erfüllen und gleichzeitig die monetären Bedingungen einhalten indem es Messungen bezüglich Verfügbarkeit, Sicherheit und Zuverlässigkeit bereitstellt. Diese Parameter werden durch eine zustandsbasierte Monte-Carlo-Simulation ermittelt welche dynamische Fehlermanagementverfahren wie z.B. FDIRO unterstützt.

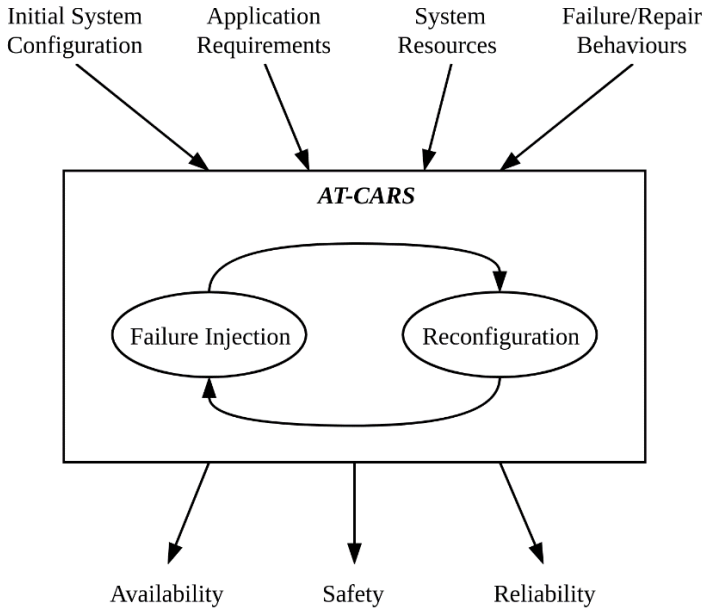

Abbildung 9: Systemübersicht von AT-CARS

Die Grundidee von AT-CARS, wie in Abbildung 9 dargestellt, besteht darin, dass der Benutzer die anfängliche Systemkonfiguration sowie einen Satz von Anwendungsanforderungen, Systemressourcen und Fehler-/Reparaturverhalten bereitstellt. AT-CARS simuliert dann das Systemverhalten durch Injektion von Fehlern, gefolgt von einer anschließenden Systemrekonfiguration. Basierend auf dieser Simulation bestimmt AT-CARS die Verfügbarkeit, Sicherheit und Zuverlässigkeit des gegebenen Systems.
Ein Wirksamkeitsnachweis hinsichtlich der Zuverlässigkeit des Systems ist in der folgenden Abbildung 10 sichtbar. Es werden hier Systeme mit und ohne FDIRO, sowie mit guten und zuverlässigen sowie schlechten und weniger zuverlässigen Komponenten verglichen. An der

blauen und violetten Linie, welche bei ~50% und ~55% Zuverlässigkeit nach 8760 Betriebsstunden liegen, ist zu erkennen, dass die Implementierung eines Fehlermanagementsystems wie FDIRO in ein System mit schlechten Komponenten die Verwendung von guter und zuverlässiger Hardware egalisieren kann. Auf diese Weise können Kosten eingespart werden.

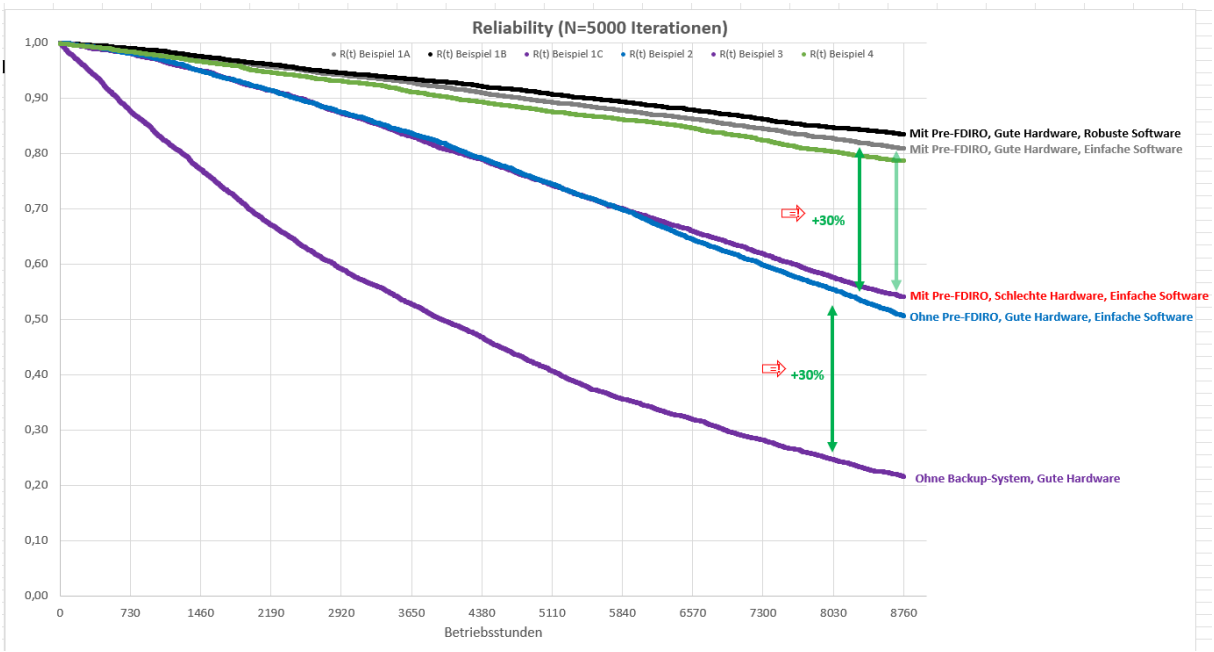

Abbildung 10: Beispielhafter Vergleich von Architekturen mit und ohne FDIRO

Ein weitere Problematik ist, dass autonome Fahrzeuge per Definition jegliche Übernahmeaktionen von Passagieren ausschließen. Daher müssen solche Fahrzeuge nicht nur die Fahraufgabe autonom erfüllen, sondern auch in der Lage sein, auftretende Hard- und Softwarefehler zu erkennen und zu behandeln. Viele Fehler erfordern jedoch Informationen über den aktuellen Kontext, in dem sich das Fahrzeug befindet, um sie zu erkennen. Daher werden Fehlererkennungsverfahren benötigt, die den aktuellen Kontext mit einbeziehen. Um dieses Problem entgegenzuwirken wurde ein kontextbasierter Ansatz zur Fehlererkennung erarbeitet, der für den Einsatz in autonomen Fahrzeugen entwickelt wurde. Die Idee ist, den Fehlererkennungsprozess in zwei aufeinanderfolgende Aufgaben aufzuteilen: Die erste Aufgabe überwacht kontinuierlich die Verfügbarkeit und Integrität der Systemkomponenten, während die zweite Aufgabe einen Fehler verifiziert, wenn eine potenziell fehlerhafte Komponente mit homogenen und heterogenen Komponenten erkannt wird. Der kontextbasierte Fehlererkennungsansatz wurde in einem experimentellen Aufbau. Dazu wurde der Open-Source-Simulator CARLA verwendet. Darüber hinaus implementiert die vorgeschlagene kontextbasierte Fehlererkennung die Schnittstellen, wie sie von FDIRO definiert werden. Der Ablauf dieser Fehlererkennung ist in den folgenden Aktivitätsdiagrammen (Abbildung 11, Abbildung 12, Abbildung 13 und Abbildung 14) dargestellt.

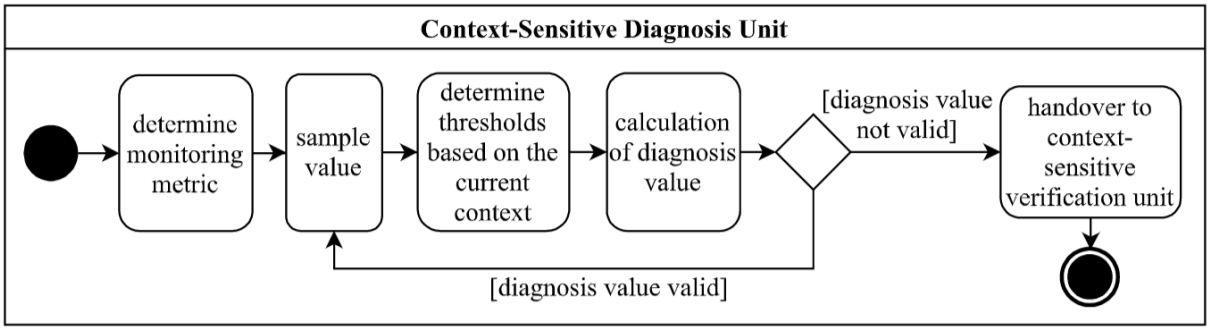

Abbildung 11: Das Aktivitätsdiagramm der kontextsensitiven Diagnoseeinheit zeigt den Ablauf während des Erkennungsschritts des vorgeschlagenen Überwachungskonzepts

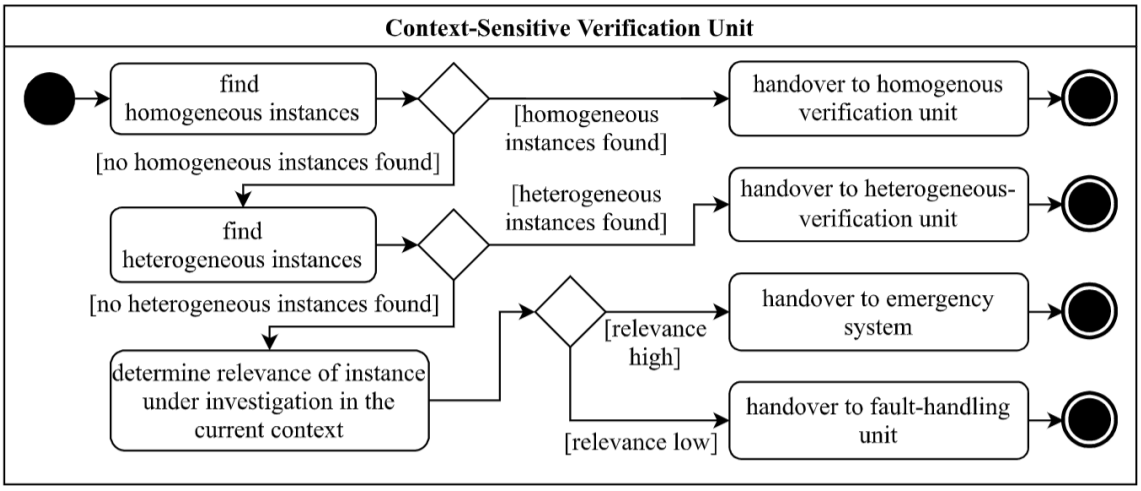

Abbildung 12: Das Aktivitätsdiagramm der kontextsensitiven Prüfeinheit

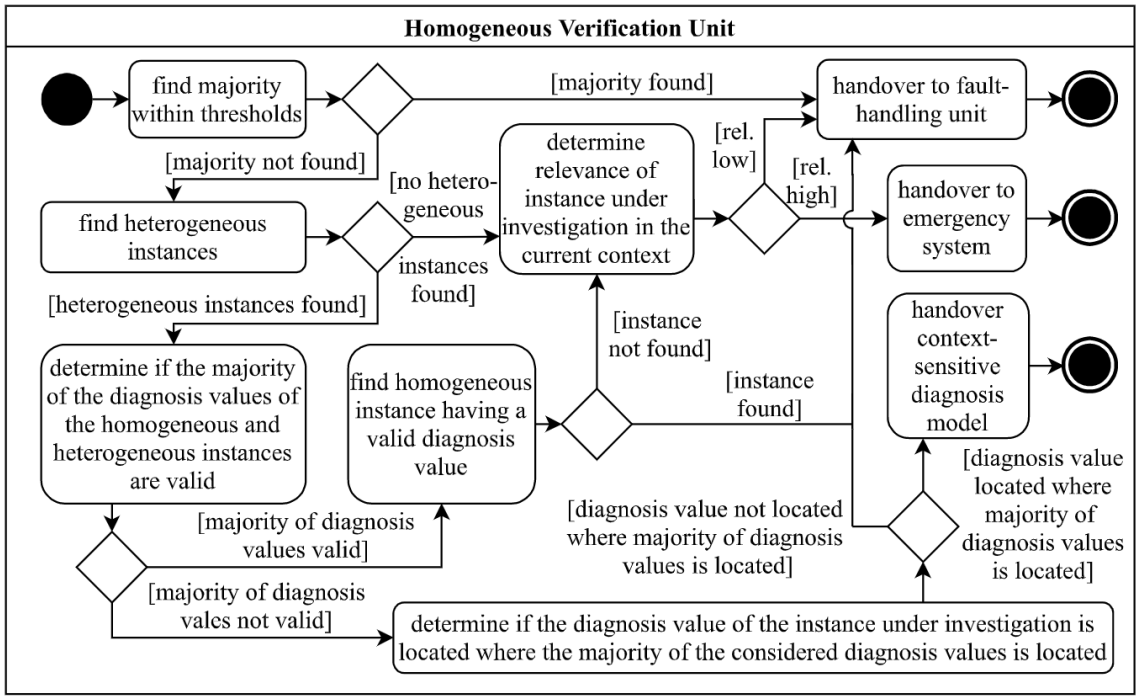

Abbildung 13: Das Aktivitätsdiagramm der homogenen Prüfeinheit

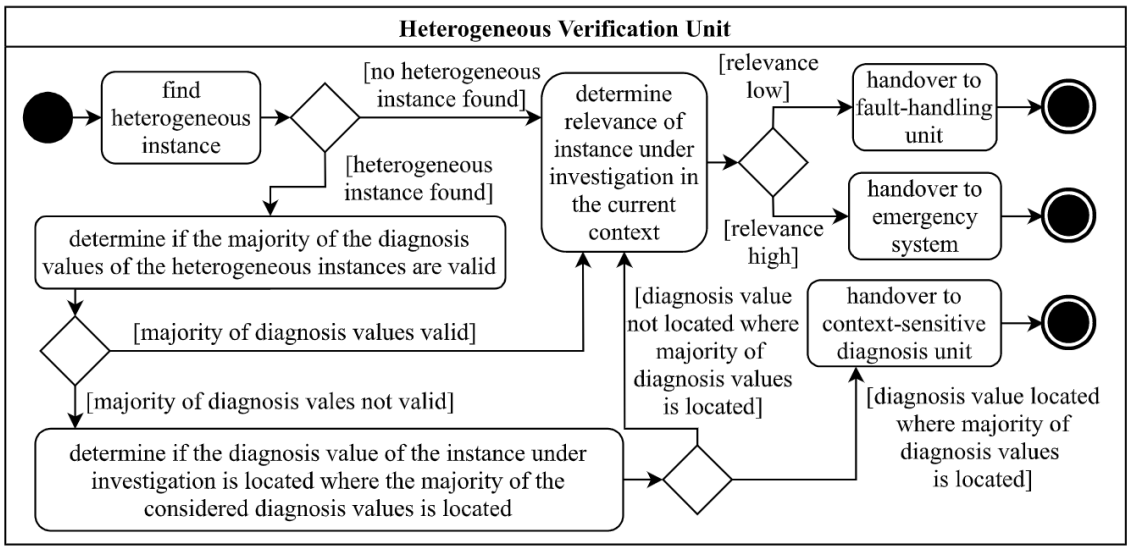

Abbildung 14: Das Aktivitätsdiagramm der heterogenen Prüfeinheit

.

Arbeitspaket 7: Demonstration und Dissemination

Um das Prinzip von FDIRO in AT-CARS zu veranschaulichen, wurde der Tabletop-Demonstrator aus dem Berichtsjahr 2019 auf einer neuen Plattform weiterentwickelt und stellt nun die wichtigsten Funktionen in einem Anwendungsfall dar. Der Demonstrator zeigt ein Systembeispiel anhand einer Hardwarekomponente mit vier verschiedenen Computing Nodes (CN), die durch vier Raspberry Pis repräsentiert werden. Jeder CN kann maximal zwei Anwendungen ausführen. Es wurden vier verschiedene Anwendungen implementiert: ein Szenenverständnis, einen Trajektorienplaner, einen Musikplayer und eine AC-Steuerung. Eine beispielhafte Darstellung zweier Anwendungen ist in Abbildung 15 zu sehen.

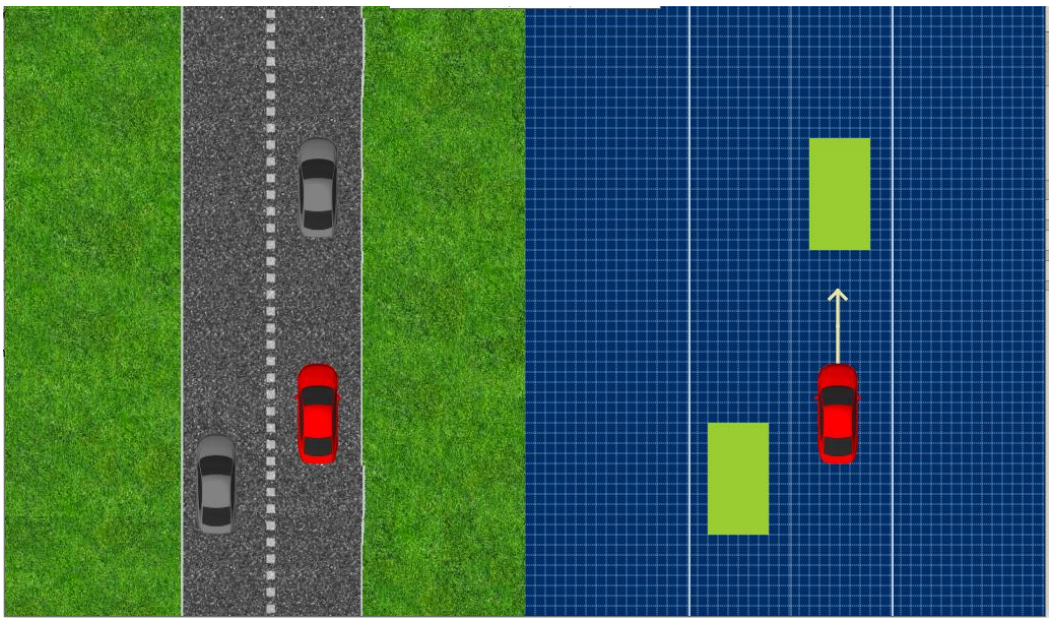

Abbildung 15: Darstellung der Anwendungen Szenenverständnis (links) und Trajektorienplaner (rechts) auf einem Raspberry Pi

Diese Anwendungen imitieren die Funktionalitäten und werden nur zu Präsentationszwecken verwendet. Es werden also keine echten Ein- oder Ausgabedaten verarbeitet. Die Anwendung

Szenenverständnis simuliert die Informationsverarbeitung von den Sensoren zur Modellierung der Umgebung des Fahrzeugs. Der Trajektorienplaner errechnet mögliche Fahrtrajektorien. Der Musikplayer und die Klimaanlagensteuerung sind Anwendungen, die die Komfortfunktionalitäten des Fahrzeugs darstellen. Der Trajektorienplaner und die Anwendung zum Verstehen der Szene sind für die Funktionalität des autonomen Fahrzeugs notwendig und sicherheitskritisch. Daher werden für das initiale Mapping mehrere redundante Instanzen beider Applikationen angenommen. Darüber hinaus ist es möglich die Komfortfunktionalitäten im Rahmen des FDIRO-Prozesses durch die sicherheitskritischen Anwendungen zu ersetzen, damit möglichst schnell ein verfügbarer und abgesicherter Systemzustand eingenommen werden kann.
Das Graphical User Interface (GUI) des Demonstrators wird über ein, mit den Raspberry Pis verbundenen, Tablet realisiert, welches einerseits die Architektur den Systems mit den CN und den Anwendungen darstellt, andererseits auch den aktuellen Zustand des Systems in einem zeitlichen Verlauf und den aktuellen Schritt des FDIRO-Prozesses abbildet (Abbildung 16).

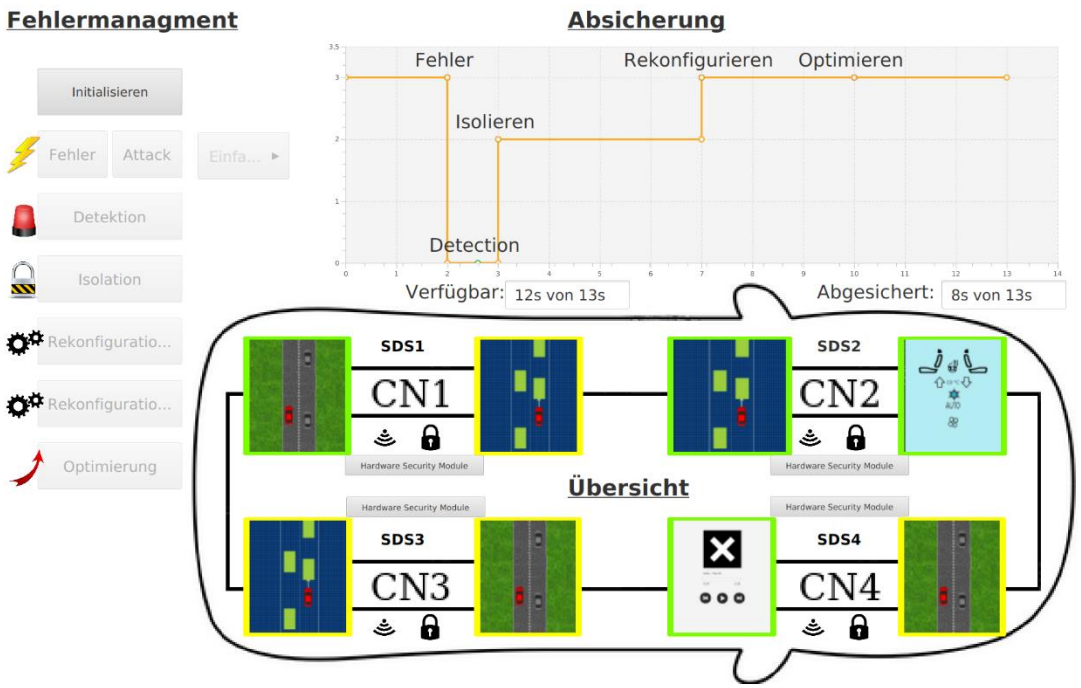

Abbildung 16: GUI des Demonstrators

Über diese GUI kann der Anwender auch Ausfälle in das System initiieren. Das System reagiert im Anschluss an einen Fehler eigenständig auf diesen und führt den FDIRO-Prozess durch. Außerdem zeigt die GUI einen Graphen an, der den aktuellen Zustand des Systems anzeigt. Basierend auf den Informationen aus diesem Graph wird die Dauer des Systems in einem verfügbaren und gesicherten Zustand berechnet und in der GUI angezeigt. Das System wird dabei als verfügbar angenommen, solange mindestens eine aktive Funktion des Szenenverständnisses und des Trajektorienplaners läuft. Darüber hinaus wird angenommen, dass das System abgesichert ist, solange eine aktive und eine heiße Instanz des Szenenverständnisses und des Trajektorienplaners läuft. So können alle wesentlichen Merkmale dargestellt werden. Es muss jedoch erwähnt werden, dass die dargestellten Anwendungen nur eine Auswahl und eine Vereinfachung eines tatsächlichen Software-Stacks sind.

3.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die größten Ausgaben im Rahmen des Projektes beliefen sich einerseits auf die angefallenen Personalkosten bei der Volkswagen AG, sowie auf die Kosten für den Unterauftrag an das Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH.

3.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Thematik des automatisierten Fahrens hat sich in den letzten Jahren neben der Elektromobilität zu einem der primären Forschungs- und Entwicklungsbereiche in der Automobilindustrie entwickelt. Neben den am Markt etablierten Automobilherstellern und Zulieferern sind auch neue Firmen außerhalb von Europa gegründet worden, die diese Thematik adressieren. Um neben diesen Akteuren konkurrenzfähig zu bleiben ist es notwendig, die Thematik des automatisierten Fahrens in Form von Forschungsprojekten zu behandeln und konkrete Aspekte, wie die Safety- und Security-Betrachtung, zu bearbeiten.

3.4 Verwertbarkeit

Sicherheitsprobleme und erfolgreiche Hackerangriffe der letzten Jahre mit kriminellem, terroristischem, oder geheimdienstlichem Hintergrund haben zu der auf breiter Basis akzeptierten Erkenntnis geführt, dass sich die Chancen der weiteren Digitalisierung nur nutzen lassen, wenn Lösungen für die IT-Sicherheit gefunden werden. Die dargestellten Verwertungsabsichten werden dabei wie unten angegeben verfolgt.

3.4.1 Wirtschaftliche Erfolgsaussichten

Die vom SATiSFY -Projekt erarbeiteten technologischen Lösungsmöglichkeiten und Konzepte stellen für einen Automobilhersteller einen darstellbaren Kundenvorteil dar, welcher verkaufsfördernd wirken kann. Durch eine Schaffung etablierter Standards besteht zusätzlich die Chance Entwicklungskosten zu senken und die enorme Komplexität moderner Fahrzeuge besser zu beherrschen.
Insbesondere im Wettbewerb mit internationalen Anbietern stellt ein ausgeprägtes Sicherheitskonzept einen Wettbewerbsvorteil dar. Es ist generell zu erwarten das die Anforderungen an Safety und Security Anforderungen mit dem Einführungsprozess von autonomen Fahrzeugen rasant steigen. Lösungen für diesen Anstieg bieten die Ergebnisse des SATiSFY Projekt.

3.4.2 Wissenschaftliche Erfolgsaussichten

Die Volkswagen AG erhofft sich ein erweitertes Bewusstsein für erhöhte Sicherheitsmaßnahmen, welche für autonome Fahrzeuge essenziell sind, in der Wissenschaft und der Entwicklung. Ereignisse in jüngster Vergangenheit haben gezeigt das im Bereich Safety für automatisierte Fahrzeuge ein erhöhter Forschungsbedarf besteht, um das Vertrauen der Kunden für diese Technologie zu gewinnen. Durch die in SAFTISFY erlangten Erkenntnisse sollen Industrie- und Wissenschaftsstandards initiiert und weitergetrieben werden, um die nötigen Systeme in Serie zu bringen. Hier kann Deutschland eine Vorreiterrolle in Sicherheitsarchitekturen einnehmen und dies mit einem wissenschaftlichen und technischen Vorsprung untermauern, der langfristig die Konkurrenzfähigkeit der entsprechenden Produkte steigert.

Weiterhin steht einer Verwertung der Ergebnisse in anderen Bereichen mit entsprechenden Anpassungen für die spezifische Anwendungsdomäne nichts entgegen.

3.4.3 Wissenschaftlich-wirtschaftliche Anschlussfähigkeit

Auf Basis der Ergebnisse aus SATiSFY werden idealerweise fortführende Projekte gestartet, die den Veränderungen durch die stetig fortschreitende Digitalisierung und Automatisierung Rechnung tragen. Eine stärkere Automatisierung erfordert stetig wachsende Rechenkapazitäten und eine stetig wachsendes Kommunikationsaufkommen in und um das Fahrzeug. Durch die steigende Komplexität entstehen neue Möglichkeiten aber auch Angriffsvektoren, die betrachtet und bewertet werden müssen, um Risiken und Chancen rechtzeitig identifizieren zu können.
Es ist auch zu erwarten, dass öffentliche und etablierte Lösungsmöglichkeiten es kleinen und mittelständischen Unternehmen ermöglicht Produkte in diesem Bereich anzubieten.

3.5 Bekannt gewordener Fortschritt

Der im Rahmen des Projektes gewonnene Fortschritt wurde einerseits auf Tagungen und Konferenzen präsentiert und diskutiert, siehe hierzu Abschnitt 3.6, andererseits wurden neue Kenntnisse als neue Patente angemeldet. Eine Übersicht über diese Patente findet sich in der folgenden Tabelle.

Kennung	Autoren	Titel/Tagung/Zeitung/Verlag/ISBN/Bemerkung
KD28011	Müller, J.-S., Decke, H., Braasch, A., Plinke, F., Horeis, T., Heinrich, J., Kain, T., Wesche, M.	Verfahren zum Betrieb eines selbstfahrenden Fahrzeugs sowie Steuerungssystem zum Durchführen eines solchen Verfahrens
K 29813 DE	M. Wesche, T. Kain, M. Aguirre Mehlhorn, J.-S. Müller	Verfahren zur kontextabhängigen Detektion eines Fehlers einer Fahrzeugkomponente und Fahrzeug
K 29816 DE	M. Wesche, T. Kain, M. Aguirre Mehlhorn, J.-S. Müller	Verfahren eines Fahrzeugs zur kontextanhängigen Verarbeitung eines potenziellen Fehlers einer Fahrzeugkomponente und Fahrzeug
K 29920 DE	M. Wesche, T. Kain, M. Aguirre Mehlhorn, J.-S. Müller	Verfahren eines Fahrzeugs zur kontextabhängigen Fehlerverarbeitung mittels heterogener Verifikation und Fahrzeug
K28266	T. Kain, M. Wesche, H. Decke, J.-S. Müller, F. Plinke, A. Braasch, J. Heinrich, T. Horeis	Verfahren und Vorrichtung zum Rekonfigurieren eines automatisiert fahrenden
K 28266 DE	F. Plinke, J. Heinrich, T. Horeis, J.-S. Müller, H. Decke	Verfahren und Vorrichtung zum Rekonfigurieren eines automatisiert fahrenden Fahrzeugs in einem Fehlerfall

3.6 Veröffentlichungen

Die Ergebnisse des Projektes wurden auf nationalen und internationalen Tagungen veröffentlicht. Die jeweiligen Beiträge sind der folgenden Tabelle zu entnehmen.

Lfd-Nr.	Autoren	Titel/Tagung/Zeitung/Verlag/ISBN/Bemerkung
2019-1	J. Heinrich, J.-S. Müller, F. Plinke T. F. Horeis, H. Decke	State-based availability analysis of hard- and software architectures using Monte Carlo Simulation under consideration of different failure modes and degradation models Conference: 29th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-11-2724-3_0333-cd Date of Conference: 09-2019
2020-1	T. F. Horeis, T. Kain, J.-S. Müller, F. Plinke, J. Heinrich, M. Wesche, H. Decke	A Reliability Engineering Based Approach to Model Complex and Dynamic Autonomous Systems Conference: 2020 International Conference on Connected and Autonomous Driving (MetroCAD) DOI: 10.1109/MetroCAD48866.2020.00020. Date of Conference: 02-2020
2021-1	T. Kain, H. Tompits, J.-S. Müller, P. Mundhenk, M. Wesche, H. Decke	FDIRO: A General Approach for a Fail-Operational System Design Conference: 30th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-14-8593-0_4204-cd Date of Conference: 01-2021
2021-2	T. Kain, H. Tompits, J.-S. Müller, M. Wesche, Y. A. M. Flores, H. Decke	Optimizing the Placement of Applications in Autonomous Vehicles Conference: 30th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-14-8593-0_5803-cd Date of Conference: 01-2021
2021-3	F. Plinke, J. Heinrich, T. Horeis, J.-S. Müller, H. Decke	Reliability methods and procedures for failure and error management and system reconfiguration in safety critical autonomous driving applications. Conference: 30th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-14-8593-0_3933-cd Date of Conference: 01-2021

2021-04	T. F. Horeis, T. Kain, R. C. Rinaldo, A. Blickle	A Modeling Approach to Consider the Effects of Security Attacks on the Safety Assessment of Autonomous Vehicles -- An AT-CARS Extension and Use Case Conference: 31th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-18-2016-8_519-cd Date of Conference: 09-2021
2021-05	T. Kain, M. A. Mehlhorn, H. Tompits, J.-S. Müller	D-DEG: A Dynamic Cooperation-Based Approach for Reducing Resource Consumption in Autonomous Vehicles Conference: 31th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-18-2016-8_631-cd Date of Conference: 09-2021
2021-06	R. C. Rinaldo, T. F. Horeis, T. Kain	Hybrid Modeling for the Assessment of Complex Autonomous Systems -- A Safety and Security Case Study Conference: 31th European Safety and Reliability Conference (ESREL) DOI: 10.3850/978-981-18-2016-8_519-cd Date of Conference: 09-2021

4 Fazit und Ausblick

Die Arbeiten im Rahmen des vorliegenden Forschungsprojektes haben einen Beitrag auf dem Weg zur Markteinführung des automatisierten Fahrens geleistet. Insbesondere der Safety-Aspekt wurde im Rahmen der Forschungsaktivitäten der Volkswagen AG adressiert, woraus neue Modelle und Methoden entstanden sind. Hierbei war insbesondere das überdisziplinäre Arbeiten zwischen den Ingenieuren der Konzernforschung und dem als Unterauftragnehmer beauftragten Institut für Qualitäts- und Zuverlässigkeitsmanagement erfolgsversprechend. Sicherheitsrelevante Methoden aus dem Bereich der Automobiltechnik und auch aus dem Bereich angrenzender Industrien, z.B. der Luft- und Raumfahrt, konnten auf die komplexen Strukturen automatisierter Systeme angewendet werden, um im Anschluss einen Sicherheits- und Zuverlässigkeitsgewinn zu erzielen. Hierbei haben sich insbesondere zwei Ansätze als wesentlich herausgestellt:

- Differenzierte Betrachtung von Hardware- und Software-Elementen bei der Modellierung
- Implementierung eines automatisiert agierenden Fehlermanagement-Prozesses in die automatisierten Systeme.

Die erarbeiteten Methoden wurden im Rahmen des Matlab-Tools AT-CARS implementiert. Mit Hilfe diesen Tools konnte der Vorteil eines intelligenten Fehlermanagementprozesses gegenüber Systemen ohne diesen aufgezeigt werden. Insbesondere konnte verdeutlicht werden, dass auf diese Weise eine Realisierung des automatisierten Fahrens zu günstigeren Konditionen verwirklicht werden kann, so dass diese Technologie einem größeren Kreis an Endverbrauchern zugänglich gemacht werden kann.

Aktuell werden viele Normen aus dem Bereich der Safety und Security erarbeitet. Beispielsweise sei hier die Norm zur Absicherung der Sollfunktion (ISO 21448) genannt. Diese befindet sich aktuell im Stand eines FDIS (Final Draft International Standard). Sie ist somit noch nicht in ihrer finalen Form veröffentlicht und wird noch bearbeitet. Die Volkswagen AG ist Teil des Komitees, welches sich mit der Bearbeitung beschäftigt und ist bestrebt, Ergebnisse aus dem vorliegenden Forschungsprojekt dort mit einfließen zu lassen. Darüber hinaus werden die erzielten Ergebnisse fortlaufend mit neuen Erkenntnissen aus dem Bereich der Forschung und Entwicklung abgeglichen.