Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Abschlussarbeit

Anastasios Palatiou

Konzept für die Integration eines Autos als Angriffsziel in einer CTF-Umgebung

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Anastasios Palatiou

Konzept für die Integration eines Autos als Angriffsziel in einer CTF-Umgebung

Bachelorthesis eingereicht im Rahmen der Bachelorprüfung

im Studiengang Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter : Prof. Dr. Franz-Josef Korf

Abgegeben am 20.11.2020

Anastasios Palatiou

Thema der Arbeit

Konzept für die Integration eines Autos als Angriffsziel in einer CTF-Umgebung

Stichworte

Capture-The-Flag, Wettbewerb, Hacking, Automobil

Kurzzusammenfassung

An der Hochschule für Angewandte Wissenschaften Hamburg soll künftig ein wählbares Capture-The-Flag (CTF) Projekt an ein Automobil durchgeführt werden. Ein Automobil stellt in dieser Beziehung allerdings eine besondere Ressource dar, welche nicht ohne weiteres durch mehrere Gruppen gleichzeitig angreifbar ist und Sicherheitskonzepte vorhält, welche nicht beschädigt werden dürfen. Am Beispiel der Integration eines Automobils in eine CTF-Umgebung wurde in dieser Arbeit ein Leitfaden entwickelt, wie diese und ähnliche Ressourcen sinnvoll für ein CTF behandelt werden können. In diesem Bezug wurde das Automobil analysiert und es wurden entsprechende Anforderungen und Randbedingungen entwickelt. Basierend auf die ausgewählte CTF Art Jeopardy wurden Aufgabenstellungen (Challenges) erarbeitet welche die besondere Ressource Automobil und die damit verbundenen empfindlichen Systeme und die geringe Erfahrungsstufe der Teilnehmenden berücksichtigen. Zur Vermeidung von Kollisionen zwischen unterschiedlichen Teams während der Arbeiten wurde eine Lösung zu dieser Ressourcen Problematik entwickelt. Um das Event für Teilnehmende zugänglicher sowie interessanter zu gestalten wurde ein Story-basierter Handlungsstrang entworfen, welcher ebenso den inhaltlichen Ablauf des CTF Events vorgibt.

Anastasios Palatiou

Title of the paper

Concept for the integration of a car as an attack target in a CTF environment

Keywords

Capture-The-Flag, Contest, Hacking, Automotive

Abstract

At the Hamburg University of Applied Sciences, a selectable Capture-The-Flag (CTF) project is to be carried out on an automobile in the future. However, an automobile represents a special resource in this respect, which is not easily attacked by several groups at the same time and which provides security concepts that must not be damaged. Using the example of the integration of an automobile into a CTF environment, this thesis developed a guideline how these and similar resources can be handled in a meaningful way for a CTF. In this respect the automobile was

analysed, and corresponding requirements and boundary conditions were developed. Based on the selected CTF type Jeopardy, challenges were developed which consider the special resource of the automobile and the associated sensitive systems and the low level of experience of the participants. To avoid collisions between different teams during the work, a solution to this resource problem was developed. In order to make the event more accessible and interesting for participants, a story-based storyline was designed, which also defines the content of the CTF event.

Inhaltsverzeichnis

1 Einführung

1.1 Motivation

In der Lehre der Informationssicherheit kann ein wichtiger Punkt durch Capture-The-Flag (CTF) Veranstaltungen abgedeckt werden. In gewöhnlichen Informationssicherheits-Veranstaltungen wird anhand von Vorlesungen, Büchern und kleinen praktischen Aufgaben den Lernenden bezügliches Wissen vermittelt. Durch Vorlesungen und Bücher werden ihnen Konzepte auf einem theoretischen Level nähergebracht. Diese werden dann in praktischen Aufgaben von den Lernenden umgesetzt, wodurch sie diese Konzepte korrekt und konkret anwenden. Es werden dadurch zwar praktische Fertigkeiten ausgebaut, es schult sie jedoch nicht darin Konzepte auf neue Situationen anzuwenden, in denen der Erfolg vom Einfallsreichtum abhängig ist (Mirkovic und Peterson, 2014). Dieser Lerneffekt ist bei einem CTF gegeben, denn dort haben die Teilnehmenden die Freiheit zum Experimentieren und können so ihre Fertigkeiten verbessern (Eagle und Clark, 2004).

An der Hochschule für Angewandte Wissenschaften (HAW) Hamburg existiert ein wählbares Capture-the-Flag Projekt, bei dem die Studierenden ihre Fertigkeiten verfeinern können. Für die Zukunft ist angedacht, ein CTF im Automobil abzuhalten. Dies soll in Kooperation mit einem Forschungsprojekt zur Sicherheit in autonomen Fahrzeugen an der HAW Hamburg stattfinden. Das Forschungsprojekt kann so wertvolle Daten zur Untersuchung der Sicherheit in autonomen Fahrzeugen sammeln, während die Studierenden anhand eines aktuellen Themas ihre Fertigkeiten verbessern.

Damit das CTF Projekt in dieser Form stattfinden kann, wird ein Konzept für ein CTF im Automobil benötigt und es müssen die dabei aufkommenden technischen Hürden überwunden werden.

1.2 Zielsetzung

Ein Automobil ist nicht unbedingt ein typisches Angriffsziel in einer CTF-Umgebung, allerdings stellt es den Teilnehmenden einen aktuellen und interessanten Kontext zur Verfügung. Dabei kommt jedoch eine Ressourcen-Problematik auf, wenn mehrere Teams zur selben Zeit auf dieselbe Hardware des Automobils zugreifen müssen. Hierdurch kommt es regelmäßig zu Kollisionen, wenn sich Angriffe gegenseitig behindern oder befördern, oder bestimmte Flaggen nur einmal erworben werden können. Diese Ressourcen-Problematik stellt sich nicht nur bei einem Auto, sondern auch bei anderen Angriffszielen wie beispielsweise einer Fabrik, einem Flugzeug oder einem Zug. Alle haben diese Gemeinsamkeiten, dass sie eine besondere Ressource darstellen: Sehr interessant aber nicht ohne weiteres durch mehrere Gruppen gleichzeitig angreifbar. D.h. aber auch, dass diese Besonderheit, in einer CTF-Umgebung geeignet berücksichtigt werden muss.

In dieser Arbeit soll am Beispiel der Integration eines Automobils in eine CTF-Umgebung, ein Leitfaden erarbeitet werden, wie CTFs mit solchen besonderen Ressourcen sinnvoll behandelt werden können. Hierbei werden die besonderen Anforderungen, die sich hinsichtlich des Ablaufs und der Gestaltung eines CTFs ergeben untersucht und auf der Basis der Ergebnisse und allgemeinen Anforderungen an CTFs ein Konzept entwickelt. Dieses Konzept soll auf die Möglichkeiten eines Autos als Angriffsziel eingehen, aber auch auf die dafür besonderen Randbedingungen. In diesem Konzept soll besonders herausgearbeitet werden, welche Art von CTF sinnvoll ist, wie ein interessanter und praktisch umsetzbarer Ablauf gestaltet werden kann, wo Flaggen platziert und verschiedene Challenges gestaltet werden können und wie das CTF insgesamt didaktisch sinnvoll gestaltet werden kann.

Dadurch kann diese Arbeit auch herangezogen werden, um eigene CTFs mit weiteren Angriffszielen, die besondere Ressourcen darstellen, zu planen und aufzubauen.

1.3 Aufbau der Arbeit

Grundlagen

Im zweiten Kapitel werden relevante Themen für diese Arbeit erläutert. Da es sich um ein CTF im Automobil handelt, werden moderne Fahrzeugnetzwerkarchitekturen vorgestellt, welche in einem im CTF genutzten Automobil vorhanden sein würden. Des Weiteren werden im Automobil enthaltene Systeme sowie das Thema CTF vorgestellt. Dabei werden die verschiedenen Arten von CTFs und der gewöhnliche Aufbau, bzw. Ablauf beschrieben.

Anforderungsanalyse

Im dritten Kapitel werden das Anwendungsszenario und das Automobil als besondere Ressource beschrieben. Es wird bestimmt, welche (nicht-) funktionalen Anforderungen und welche weiteren Randbedingungen gelten.

Entwurf

Im vierten Kapitel wird zunächst das CTF Event aus einem organisatorischen Blickwinkel anhand Automobil- und CTF spezifischer Anforderungen geplant. Dazu wird der inhaltliche Ablauf mithilfe einer interessanten Storyline entwickelt, welche eine umzusetzende CTF Art miteinbezieht und die Anordnung der Aufgabenstellungen bestimmt. Des Weiteren wird konzipiert, wie der Zugriff auf das Auto als besondere Ressource behandelt werden kann. Zuletzt wird der Umgang mit Aufgabenstellungen des CTFs betrachtet.

Fazit & Ausblick

Im letzten Kapitel wird die Arbeit zusammengefasst und die erlangten Erkenntnisse, sowie das Konzept für die Integration eines Autos in eine CTF-Umgebung, dargelegt. Außerdem wird ein kurzer Ausblick für mögliche Verbesserungen anhand des erlangten Wissens beschrieben.

2 Grundlagen

2.1 Capture-The-Flag

Bei einem CTF handelt es sich um einen speziellen Wettbewerb, der im Kontext der Informationssicherheit angesiedelt ist. In diesem Wettbewerb werden Teams gebildet, welche eine Reihe von Problemen zur Verfügung gestellt bekommen, welche diese lösen sollen. Diese Probleme werden Challenges genannt und beinhalten eine auszunutzende Sicherheitslücke oder eine Aufgabe im Sicherheits-Kontext. Wird eine dieser Challenges gelöst, erhält das jeweilige Team entweder höhere Zugriffsprivilegien für ein bestimmtes System oder es bekommt eine Art Antwort, welche als Flag bezeichnet wird. Diese beweist, dass das Team die Challenge gelöst hat oder wird in einem Bewertungssystem gegen Punkte eingelöst, die zur Bewertung der Teams dienen (Chung und CTFd LLC, 2017).

Folgend werden die verschiedenen Arten von CTFs beschrieben. Anschließend wird jeweils erläutert, welchen Stellenwert ein CTF als Lern- und Forschungsplattform haben kann. Außerdem werden die Herausforderungen bei Einsatz eines CTFs, für die Teilnehmenden und die Organisierenden erklärt. Zuletzt werden aktuelle CTF Frameworks vorgestellt und in ihren allgemeinen Funktionen beschrieben.

2.1.1 Capture-The-Flag Arten

Nachfolgend werden unterschiedliche CTF Arten beschrieben.

Jeopardy: Hierbei handelt es sich um die meist genutzte Art, welche für gewöhnlich übers Internet stattfindet. Der Name Jeopardy stammt von der gleichnamigen Fernseh-Quizshow, an welche die Darstellung der Challenges bei dieser CTF Art erinnert. Die Challenges werden von den Organisierenden kreiert und auf ihren eigenen Servern zur Verfügung gestellt. Jede Challenge wird einer Kategorie zugeordnet und wird in Form eines Jeopardy Boards dargestellt (Nighswander, 2016). Eine mögliche Visualisierung der Kategorien und Challenges wird in Abbildung 1-1 veranschaulicht. Es werden in diesem Beispiel zwei Kategorien gezeigt: Reverse Engineering und Misc. Den Kategorien sind jeweils mehrere Challenges

untergeordnet, welche in dieser Ebene jeweils einen Namen und eine, je nach Schwierigkeitsgrad, auszuschüttende Punktzahl besitzen.

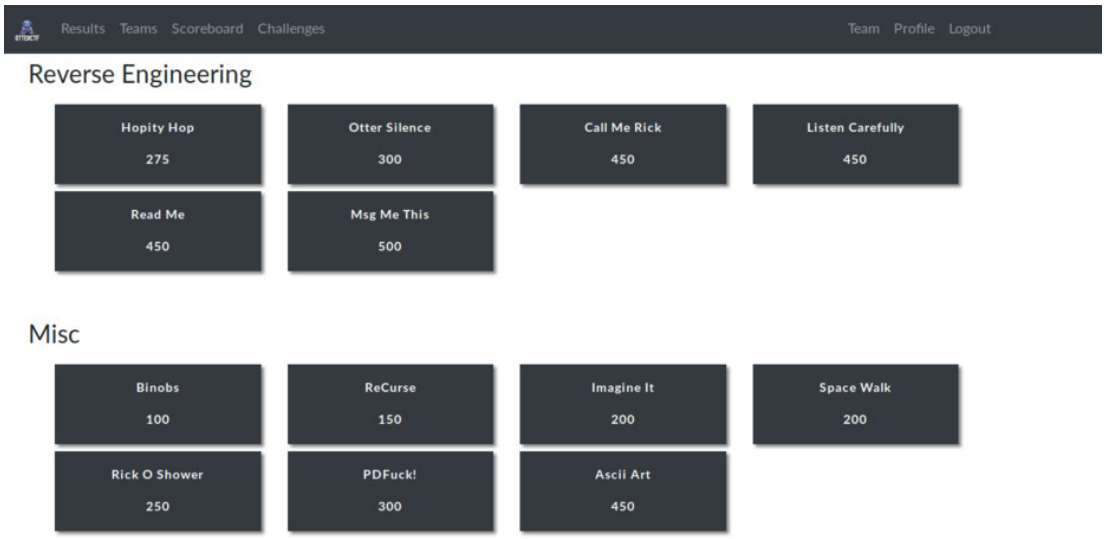

Abb. 1-1: Challenge Übersicht (Beispiel zur Verdeutlichung)

Die Teilnehmenden können frei darüber entscheiden, welche der zur Verfügung stehenden Challenges als nächste bearbeitet werden soll. Es können dabei weitere Challenges freigeschaltet werden, sobald ein Team bestimmte Challenges gelöst hat. Es existieren bei einem Jeopardy CTF mehrere Kategorien, wobei diese jeweils einen Aspekt der Informationssicherheit behandeln. Weitere mögliche Kategorien sind: Cryptography, Stegonographie, Binary Exploitation, Mobile Security, Forensic und Weitere. Für jede gelöste Challenge bekommt das jeweilige Team eine Flag. Diese kann beim Punktesystem eingereicht werden, wodurch das Team Punkte bekommt (CTFTime.org, o.J.). Für gewöhnlich erhalten die ersten drei Teams, welche eine bestimmte Challenge absolvieren eine erhöhte Punktzahl gutgeschrieben (CTF Wiki, o.J.). Am Ende gewinnt das Team mit den meisten Punkten.

Attack-Defense: Im Gegensatz zu Jeopardy geht es hier darum, Flags von anderen Teams zu stehlen und die eigenen zu verteidigen. Ein solches Event findet in der Regel nicht wie Jeopardy übers Internet statt, sondern vor Ort und für gewöhnlich in Verbindung mit Konferenzen. Die Challenges werden von den Organisierenden kreiert und werden jeweils von jedem Team auf ihren eigenen Servern zur Verfügung gestellt (Nighswander, 2016). Für gewöhnlich wird den Teams Zeit gegeben, die Schwachstellen in den eigenen Challenges zu finden. Wenn ein Team eine Schwachstelle findet, sollte diese gepatched werden, damit sie später nicht von einem anderen Team angegriffen werden kann. Wenn die Zeit um ist, werden die Systeme der Teams miteinander verbunden. Die Teams werden dann versuchen, die eigenen Challenges zu verteidigen und versuchen die gefundenen Schwachstellen bei den Systemen der anderen Teams anzugreifen (CTFTime.org, o.J.). Wenn ein Team eine

Schwachstelle erfolgreich angreift, kann es von dieser Challenge eine Flag erhalten und somit Punkte sammeln. Allerdings kann ein Team auch effektiv Punkte sammeln, wenn die eigenen Challenges durch eine gute Verteidigung eine geringe Downtime haben (Genovese, 2016). Für gewöhnlich ist bei dieser CTF Art die einzige relevante Challenge Kategorie Binary-Exploitation (Nighswander, 2016).

King-of-the-Hill: Diese Art von CTF ähnelt Attack-Defense. Sie unterscheiden sich dadurch, dass bei King-of-the-Hill von den Teams zunächst keine eigenen Server bearbeitet und verteidigt werden müssen. Das Ziel der Teams ist, die von den Organisierenden zu Verfügung gestellten vorkonfigurierten Systeme zu erobern. Dadurch kann das jeweilige Team ein Token auf einem System platzieren und muss dieses fortan vor Angriffen anderer Teams schützen. Für jedes System, auf welches ein bestimmtes Team ihr Token hinterlegt hat, können Punkte gesammelt werden. Zur Berechnung der Punkte existiert für gewöhnlich ein eigener Dienst auf dem System, welcher das aktuelle Token an ein Bewertungssystem übermittelt. Während des Wettbewerbs können bereits eroberte Systeme von anderen Teams angegriffen werden, wodurch ein Team mit einem erfolgreichen Angriff das ehemalige Token auf dem System mit ihrem eigenen ersetzen kann (Bansal, 2019).

Collegiate-Cyber-Defense-Challenge: Bei einer Collegiate-Cyber-Defense-Challenge existiert ein Netzwerk, welches durch ein studentisches Team (Blue-Team) gegen professionelle Angreifer (Red-Team) verteidigt wird. Der Fokus dieser Art liegt bei der Vermittlung der administrativen Aspekte der Verteidigung eines fiktiven Unternehmens. Dabei werden etliche technische Aspekte der Informationssicherheit vernachlässigt (Chung und Cohan, 2014).

Wargames: Das Konzept von Wargames differenziert sich von den bereits vorgestellten CTFs dadurch, dass es stets fortlaufend ist. Ein Wargame besteht aus mehreren Levels, welche nacheinander vollendet werden, um ein jeweiliges nächstes freizuschalten. Bei den Levels handelt es sich um einzelne Challenges welche am Schwierigkeitsgrad zunehmen, je weiter ihre Lösung voranschreitet. Das Angebot solcher Wargames ist meist stetig und es können nach einer beliebigen Zeit weitere Levels hinzugefügt werden, wodurch der Aspekt der Fortläufigkeit entsteht (OverTheWire, o.J.).

Hack-Quest: Ein Hack-Quest CTF ist ein Wettbewerb, welcher über einen bestimmten Zeitraum mit einem zeitlichen Abstand einzelne Challenges zur Verfügung stellt. Ein CTF könnte sich beispielsweise über eine ganze Woche hinziehen, wobei jeden Tag eine neue Challenge veröffentlicht wird. Die jeweiligen Challenges haben ebenfalls ein Zeitlimit in welcher sie bearbeitet werden müssen (ZeroNights, 2019) (Sudo Null, o.J.).

2.1.2 Capture-The-Flag als Lernplattform

CTFs sind nicht nur Wettbewerbe zur Bewertung von Fähigkeiten, sie erfahren zusätzlich eine starke Akzeptanz durch die Community als Lernplattform (Chung und Cohan, 2014). In Bezug zur Lehre ergeben sich nach Leune und Petrilli (2017) mit einem angemessen ausgearbeiteten CTF, folgende Punkte:

- Die Teilnahme an einem CTF ermöglicht es den Lernenden potenziell gefährliche Techniken in einer geschützten Umgebung zu trainieren. Dies soll das Vertrauen in die eigenen Fähigkeiten, Angriffe durchzuführen, sie zu erkennen und diese abzuwehren festigen

- An einem CTF teilzunehmen bereitet den Lernenden Freude. Dabei haben sie eine große Motivation bei dem Versuch die Challenges zu lösen und verbringen so insgesamt mehr Zeit damit. Dadurch wird effektiv ein besseres Lernergebnis erzielt

- Durch ein CTF verbessern die Lernenden tatsächlich ihre praktischen Fertigkeiten. Angriffs-Szenarien werden durch die eigene Umsetzung in einem CTF besser verstanden

Wie Leunes und Petrillis ersten beiden Punkte beschreiben, wird den Lernenden die Möglichkeit gegeben, in einer geschützten Umgebung zu trainieren und sie haben eine große Motivation dabei. Anzumerken ist, dass es ein üblicher und wichtiger Aspekt von CTFs ist, dass es keine Teilpunkte für einzelne Challenges gibt. Dadurch sind die Teilnehmenden dazu gezwungen ihre Ansätze solange anzupassen, bis die Challenges gelöst werden können. So ergeben sich zahlreiche Gelegenheiten, etwas über eine bestimmte Technologie zu lernen. Dies ermöglicht es den Organisierenden ein CTF zu nutzen, um den Teilnehmenden Teilbereiche der Informationssicherheit näher zu bringen (Chung und Cohan, 2014).

Daraus ergibt sich für die Lernenden, wie bereits in Abschnitt 1.1 beschrieben, die Möglichkeit zum Experimentieren. Damit geht der Lerneffekt eines CTFs noch über den dritten Punkt von Leune, das Aneignen von praktischen Fertigkeiten, hinaus. Es wird gelernt Konzepte zu verstehen, in der Praxis zu erkennen, zwischen verschiedenen Lösungsansätzen abzuwägen und das jeweilige Konzept korrekt anzuwenden (Mirkovic und Peterson, 2014).

2.1.3 Capture-The-Flag als Forschungsplattform

Ein Aspekt, welcher durch ein CTF erforscht werden kann, ist die Entdeckung von neuen und realen Sicherheitsschwachstellen. Nighswander (2016) betrachtet den Bezug von in CTF genutzten Schwachstellen zu realen Problemen. Dabei beschreibt er unteranderem, dass CTF Schwachstellen und reale Probleme gleicher Wesensart sind. Bei der Bearbeitung von CTF Schwachstellen werden die gleichen Fertigkeiten genutzt und es werden über die gleichen Probleme nachgedacht wie bei realen.

Diese Aussagen stützt er anhand verschiedener Beispiele von CTFs, in welchen neue, reale Sicherheitslücken gefunden worden sind. Bei der Vorbereitung dieser CTFs wurden einzelne Challenges entworfen, welche sich als reale Sicherheitslücken herausgestellt haben. Darüber hinaus erwähnt er Challenges, bei denen Teams bei der Bearbeitung ein nicht vorgesehenes reales Sicherheitsproblem gefunden haben und die Challenge mit diesem alternativen Weg lösten. Zudem erwähnt er eine häufig genutzte Strategie für das Attack-Defense CTF: DEFCON CTF. In der Vergangenheit haben Teams neue Sicherheitslücken in Anwendungen, die von anderen Teilnehmenden häufig genutzt werden, gesucht. Mit diesen realen Sicherheitslücken wollen die Teams dann während des Wettbewerbs die Konkurrenz angreifen.

Es ist zu beachten, dass diese Beispiele einzelne Fälle beschreiben. Damit ist gemeint, dass solche neuen Sicherheitslücken nicht in jedem CTF auftauchen werden. Allerdings zeigt es den Bezug der Challenges zur Realität.

Ein weiterer erforschbarer Aspekt ist, das Verhalten der Teilnehmenden bei einem CTF und die Herangehensweise an die Challenges. Beispielsweise wurde in einem Experiment von Vigna (2003) anhand eines Jeopardy ähnlichen CTFs, die Durchführung eines CTFs als Lehrplattform und die Arbeitsweise der Teilnehmenden beobachtet. Es gab neun Challenges, welche nacheinander bewältigt werden mussten und jeweils verschiedene Fertigkeiten abverlangten. Wurde eine Challenge innerhalb eines bestimmten Zeitlimits gelöst, wurde für das jeweilige Team eine erhöhte Punktzahl gutgeschrieben. Ein Team, welches die Challenge nicht innerhalb des Zeitlimits lösen konnte, bekam einen Hinweis, konnte aber für diese Challenge keine Punkte mehr sammeln. Es konnte beobachtet werden, dass die einzelnen Teams sich möglichst effizient in Sub-Teams organisiert haben, weil eine erhöhte Belohnung in Aussicht gestellt wurde. Allerdings wurden die Teilnehmenden anhand des Alphabets in Teams aufgeteilt und nicht anhand ihrer Fertigkeiten. Dadurch hat sich ein bemerkbarer Unterschied in den Fertigkeiten der jeweiligen Teams gezeigt, da die Erfahrenen zufälligerweise demselben Team zugelost wurden.

Ein Beispiel zu der CTF Art Attack-Defense beschreibt Genovese (2016). Er geht auf das von den Teilnehmenden praktizierte Meta-Gaming ein. Dabei geht es darum, dass die Teilnehmenden sich klar machen wie das Spiel gespielt wird und wo Lücken in den Regeln gefunden werden können. Dabei geht er auf eine Situation ein, in welcher ein Team eine Challenge offline genommen hat, damit ein bestimmtes erfolgreiches Team keine Flagge von ihnen stehlen konnte. Dafür wurde das Team zwar in ihrer Punktzahl bestraft, allerdings wurde die kleine Strafe in Kauf genommen. Eine weitere beobachtete Praxis von einigen Teams, war die Technik: Reflection. Dabei werden die eigenen Challenges als Honeypot genutzt. Dadurch können eingehende Angriffe betrachtet, analysiert und gegen andere Teams verwendet werden. Durch dieses zurückwerfen eines Angriffes, kann unteranderem eine erstmalige Lösung einer Challenge von einem Team gestohlen werden.

2.1.4 Herausforderungen beim Einsatz von Capture-The-Flag

Bei dem Einsatz von CTFs kann es zu verschiedenen Herausforderungen kommen. Darunter zählen die Schwierigkeit für Neueinsteigende, das Design von Challenges und die allgemeine Konfiguration der Infrastruktur sowie der Challenges (Chung und Cohan, 2014).

Für Neueinsteigende kann es schwierig sein in ein CTF Wettbewerb einzutauchen. Denn falls sie dabei die Aufgaben nicht selbst lösen können verlieren sie die Motivation steigen womöglich aus. Um dies zu verhindern, können CTFs so aufgebaut werden, dass sie Neueinsteigende motivieren und ein Belohnungssystem bereitstellen, welches ihr Engagement fördert. Allerdings schließt die Zielgruppe vieler CTFs Neueinsteigende nicht mit ein. Bei diesen CTFs werden für Challenges oft komplexe und hoch technische Fähigkeiten benötigt, wobei diese Challenges als Herausforderung für CTF-Erfahrene designet werden. Da der erste Schritt für Neueinsteigende bei CTFs auch oft der Schwierigste ist, werden sie bei solchen nicht weit kommen und wahrscheinlich aufgeben. Damit sowohl Neueinsteigende als auch Erfahrene das erwünschte Erlebnis aus einem CTF mitnehmen, muss eine Zielgruppe bei der Entwicklung definiert und nach außen kommuniziert werden.

Um ein gutes Challenge Design zu erreichen, können verschiedene Aspekte von Challenges betrachtet werden. Zunächst existieren in einem CTF Challenges mit verschiedenen Schwierigkeitsgraden. Zu simple Challenges haben einen geringen Lerneffekt, werden aber wahrscheinlich schnell gelöst. Schwere Challenges haben die Chance den Teilnehmenden etwas beizubringen, können sie aber auch frustrieren. Da einzelne Teilnehmende in der Regel selbst herausfinden müssen, wie mit einzelnen Challenges umzugehen ist, sollten sie digitale Brotkrümel hinterlassen. Diese stellen kleine Hinweise dar, welche während der Bearbeitung einer Challenge gefunden werden können. Sie sollen auf den Lösungweg der jeweiligen Challenge hindeuten und somit frustrierten Teilnehmenden den Pfad zur finalen Lösung erleichtern.

Als nächstes soll betrachtet werden, dass sich Erschwerungen durch Verkomplizierungen oder künstliche Beschränkungen, meist negativ auf die Challenge auswirken. Diese Praxis würde eine Frustration unter den Teilnehmenden bewirken, da bei diesen Challenges oft Glück der wichtigste Faktor ist. Ein Beispiel dafür wären Brute-Force Komponenten. Es bedarf entweder Glück oder einer für ein CTF zu langer Zeit, durch Brute-Force an die richtige Lösung zu gelangen.

Daneben ist es von Bedeutung, dass das Format der Flags bekannt ist und nicht selbst eine weitere Challenge darstellt. Wenn das Format den Teilnehmenden nicht bekannt ist, könnte ein Team zwar die Flag gefunden haben, erkennt diese aber nicht als solche und sucht vergebens nach ihr. Die meisten CTFs nutzen dasselbe Flag Format: key{*flag*} wobei *flag* den Inhalt darstellt, welcher bei dem Belohnungssystem als Austausch für die Punkte eingegeben werden muss.

Für das Challenge Design muss abschließend noch betrachtet werden, dass die Challenge-Beschreibungen und Hinweise sehr wichtig sind und mit Bedacht gewählt werden sollten. Damit die Teilnehmenden motiviert an dem CTF weiterarbeiten, sollte das CTF ein Thema oder eine Storyline besitzen. Darauf können sich die Challenges beziehen und haben somit eine Verbindung zueinander. Challenge Beschreibungen können ferner in die Challenge selbst eingebunden werden, indem beispielsweise versteckte Hinweise darin platziert werden.

Die Konfiguration der Infrastruktur und der Challenges ist ebenfalls sehr wichtig. Die Punktzahl bei Lösung von Challenges wird von den Teilnehmenden oft als Indiz für die Schwierigkeit dieser verstanden. Daraus resultiert, dass Challenges mit niedriger Punktzahl eher angegangen werden, als welche mit hoher Punktzahl, obwohl beide ggf. den gleichen Schwierigkeitsgrad aufweisen. Um dem entgegenzuwirken ist eine geeignete Wahl der Punktzahlen notwendig. Wenn Punktzahlen von den Organisierenden falsch eingeschätzt werden oder wenn Challenges nicht den erwarteten Lösungsweg für die Teilnehmenden offenbaren, kann es zu viel Frustration auf der Seite der Teilnehmenden führen. Um dies zu verhindern, kann es sinnvoll sein, die Challenges vor dem Start des CTFs von Dritten begutachten zu lassen. Diese können die Challenges ohne Vorwissen testen und so überprüfen, ob diese korrekt konfiguriert wurden. Sollte dabei etwas auffallen, können jene Challenges durch eine weitere Entwicklungs-Iteration verfeinert werden.

Bezüglich der Infrastruktur eines CTFs stellt die Wettbewerbs-Webseite einen sehr wichtigen Aspekt dar. In den meisten Fällen können die Teilnehmenden über diese mit dem Bewertungssystem kommunizieren. Die Webseite und das Bewertungssystem sollten für die Teilnehmenden so verständlich wie möglich gestaltet werden, da die Infrastruktur bei einem CTF nicht hinderlich bei der Bearbeitung sein sollte. Wenn die Teilnehmenden die Webseite leicht verstehen, können sie sich auf die komplexen oder schwierigen Challenges konzentrieren (Fuzyll und Psifertex, 2015). Abgesehen davon, dass die Webseite verständlich gestaltet werden soll, muss sie auch funktionieren und darf keine Fehler während des CTFs zulassen. Damit ist gemeint, dass die Webseite beispielsweise keine Fehler beim Laden oder beim Verhindern von Flag Brute-Force Attacken haben sollte. Um das zu verhindern, sollte die Webseite ausgiebig getestet werden. Außerdem sollten alle Teams einer festen IP-Adresse zugeordnet sein und es sollten Logs gesammelt werden, wodurch alle Aktionen einem Team zuordbar gemacht werden. Diese Schutzmaßnahmen sollten ebenfalls für den Server gelten, welcher die Challenges hostet.

2.1.5 Capture-The-Flag Frameworks

Wie in Abschnitt 2.1.4 beschrieben, ergeben sich beim Einsatz eines CTFs unter anderem infrastrukturelle Herausforderungen. Diese können durch den Einsatz eines geeigneten CTF Frameworks behandelt werden. Es wird eine Auswahl verschiedener CTF Plattformen von

Apsdehal (2019) vorgestellt, worunter sich die in Tabelle 1-1 beschriebenen Open-Source-Frameworks befinden.

Name	URL	Lizenz
CTFd	https://ctfd.io/	Apache-2.0 License
FBCTF	https://github.com/facebookarchive/fbctf	CC BY-NC 4.0
Mellivora	https://github.com/Nakiami/mellivora	GPL-3.0 License
NightShade	https://github.com/UnrealAkama/NightShade	-
RootTheBox	https://github.com/moloch--/RootTheBox	Apache-2.0 License
picoCTF	https://github.com/picoCTF/picoCTF	MIT License

Tabelle 1 – 1: Unterschiedliche CTF Frameworks

Diese verschiedenen Frameworks überschneiden sich in ihren grundlegenden Funktionen, welche aber jeweils unterschiedlich umgesetzt sind. Darunter zählen, am Beispiel des in der Programmiersprache PHP geschriebenen CTF Frameworks Mellivora (2020), die Bereitstellung eines Administrations- und Nutzer-Interface. Dabei beinhaltet das Nutzer-Interface ein Scoreboard und eine Challenge Übersicht, während das Administrations-Interface ein Challenge- und Team Management anbietet. Zusätzlich kann über das Administrations-Interface die Infrastruktur konfiguriert werden und es können beispielsweise Logs eingesehen werden.

In Abbildung 1-2 ist die Challenge Übersicht, vom Nutzer-Interface des CTF Frameworks Mellivora, exemplarisch dargestellt. Im oberen Bereich der Webseite wurde der Reiter Challenges ausgewählt, wodurch eine Auswahl weiterer Reiter verschiedener Challenge Kategorien angeboten wird. Einige dieser Reiter sind noch ausgegraut, wobei eine darüber liegende Maus darauf hindeutet, dass diese Kategorien erst in der Zukunft freigeschaltet werden. Unter jedem Kategorie-Reiter befinden sich die jeweiligen Challenges, welche untereinander angeordnet sind. Sie enthalten einen Titel, eine Punktzahl, eine Beschreibung, eine herunterladbare Datei und ein Feld, in welches eine Flag eingefügt werden kann.

In Abbildung 1-3 kann im selben Kontext ein potenzielles Scoreboard betrachtet werden. Hier wurde im oberen Bereich der Webseite der Reiter Scores ausgewählt. Dadurch wird eine Liste der Teamnamen, ihrer aktuellen Platzierung und ihrer Punktezahl angezeigt. Dabei werden die Teams mit den meisten Punkten, und somit auch den besten Platzierungen, in der Liste weiter oben platziert. Ferner wurden die Teams in eine Gruppe eingeordnet, sodass

nur Teams aus Universitäten miteinander verglichen wurden. Neben dieser Liste existiert eine zweite, in welcher alle Kategorien und deren zugehörigen Challenges angezeigt werden. Für jede einzelne Challenge wird angezeigt, welche drei Teams die jeweilige Challenge zuerst gelöst haben.

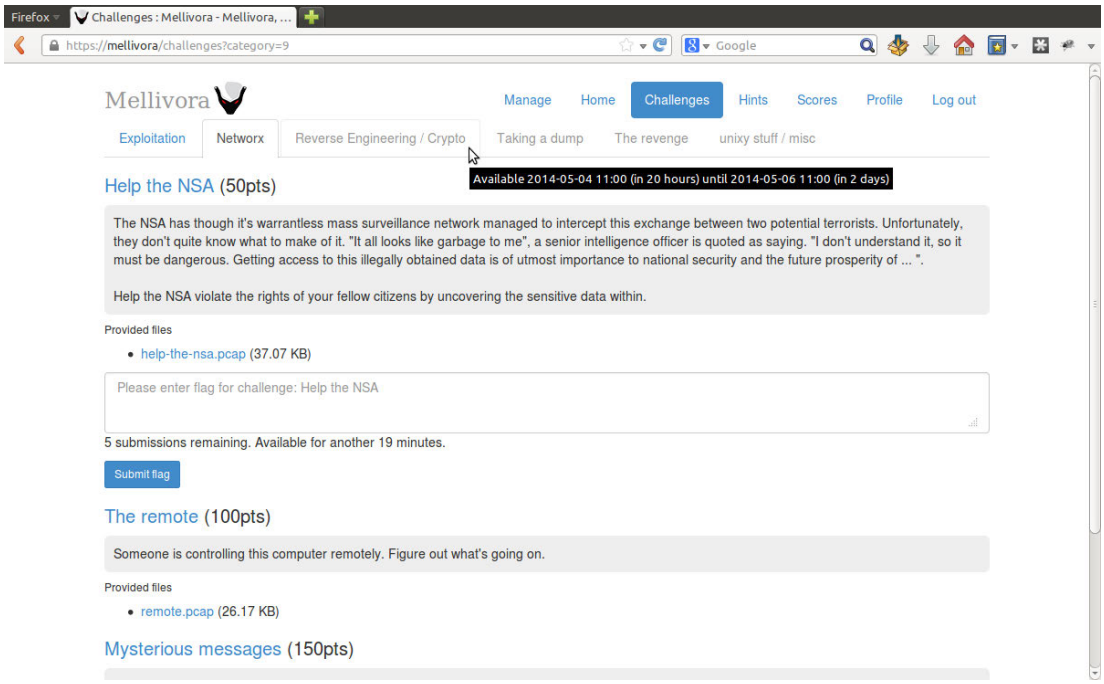

Abb. 1-2: Mellivora Challenge Übersicht

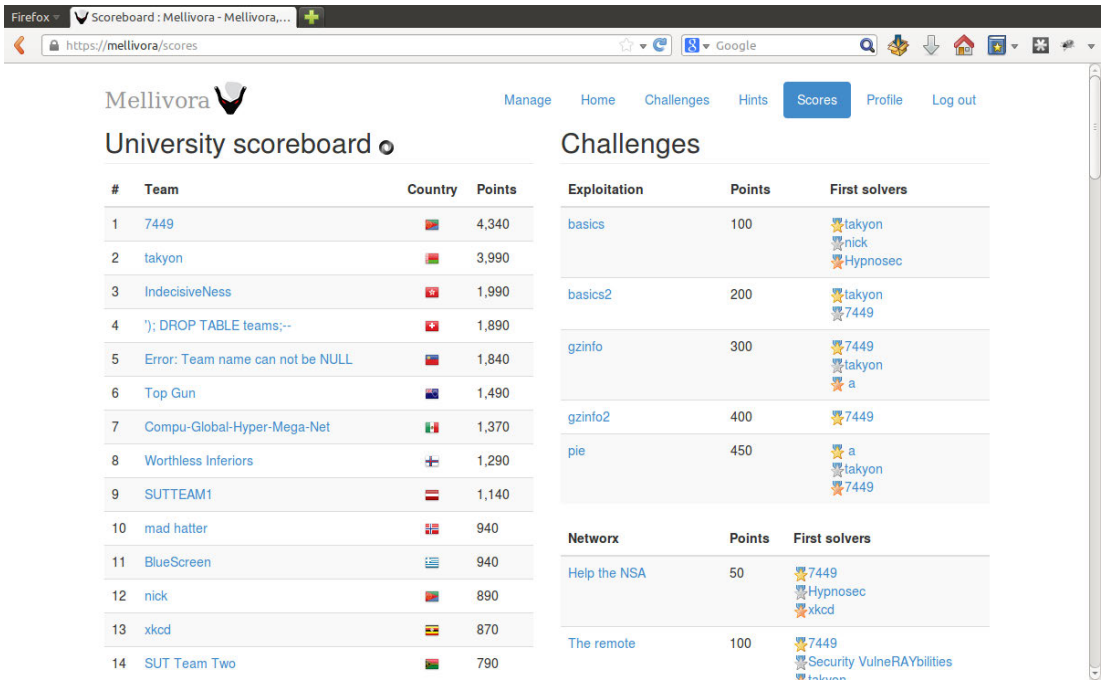

Abb. 1-3: Mellivora Scoreboard

Das in der Programmiersprache Python geschriebene CTF Framework CTFd (2020), verfügt wie alle genannten Frameworks über die beschriebenen grundlegenden Funktionen. Allerdings besitzt es als einziges ein Plugin- und Theme Interface. Damit lässt sich das Layout der Webseite individuell gestalten und es können eigene Funktionen hinzugefügt werden. Da solche Erweiterungen durch ein Interface an das Framework angebunden werden, muss der Source Code des Frameworks nicht modifiziert werden. Dadurch ergibt sich der Vorteil, dass die erstellten Plugins und Themes sehr einfach mit Dritten geteilt werden können und dass das Framework ohne Probleme auf eine neuere Version aktualisiert werden kann.

Ein weiteres Framework mit speziellen Funktionen ist das FBCTF (2018), welches von Facebook stammt und in dessen PHP Dialekt Hack geschrieben ist. Die vorherigen vorgestellten Frameworks waren für Jeopardy CTFs ausgerichtet, während FBCTF zusätzlich die CTF Art King-of-the-Hill unterstützt. Die FBCTF Plattform verfügt über drei verschiedene Challenge Formate: Quiz, Flag-basiert und Basis-basiert. Quizze sind einfache Frage-Antwort Aufgaben, Flag-basierte Challenges sind gewöhnliche Jeopardy Aufgaben und Basis-basierte Challenges sind King-of-the-Hill Aufgaben. Es lassen sich Challenges in Kategorien einordnen, welche als klassisches Jeopardy Board dargestellt werden können. Des Weiteren existiert eine alternative Darstellung für Challenges, bei welcher diese auf einer interaktiven Weltkarte dargestellt werden.

In der Regel wurden all diese Frameworks schon häufiger genutzt und getestet, wodurch sie immer wieder angepasst und somit sicherer gemacht wurden. So wurde das CTFd Framework in einem mehrjährigen CTF genutzt (Chung und CTFd LLC, 2017). Durch die erwähnten und die zahlreichen weiteren Funktionen der einzelnen Frameworks, wird der Fokus der CTF Entwicklung von der Infrastruktur weg in Richtung der Konfiguration dieser, der Erstellung von Challenges und des allgemeinen Ablaufs des Events verschoben.

2.2 Fahrzeug-Domänen

Bis hierhin wurden CTFs beschrieben. Allerdings soll in dieser Arbeit ein Automobil als Angriffsziel innerhalb eines CTFs dienen. Um dafür Automobilspezifische Flags zu entwickeln, werden folgend unterschiedliche Systeme innerhalb eines Automobils herangezogen.

Es lassen sich häufig die gleichen Designprinzipien bei den elektronischen Bordnetzen unterschiedlicher Hersteller erkennen. Das Gesamtsystem wird in Teilsysteme aufgeteilt, in sogenannte Domänen. Dabei erfolgt die Aufteilung nach deren Anwendungszeck (Adam, 2016). Dies lässt sich bei Broschüren von Continental (2015) und Bosch (o.J. a) wiedererkennen. Beide Male wird das Gesamtsystem in Domänen aufgeteilt, wobei diese sich in der genauen Anordnung und Benennung der Domänen leicht differenzieren. Die Gleichheit des Designprinzips lässt sich dennoch durch etliche parallelen wiedererkennen. Einen tieferen Einblick wurde in die Domänen nicht geboten.

Da also bei unterschiedlichen Herstellern, von den gleichen Designprinzipien ausgegangen werden kann, wird in Abbildung 2-1 eine schematische Darstellung der Fahrzeug-Domänen präsentiert, dessen Benennung an die vorherigen Namen angelehnt wird. Zum einfacheren Verständnis wurden die von den Herstellern angewandten Benennungen allerdings leicht angepasst.

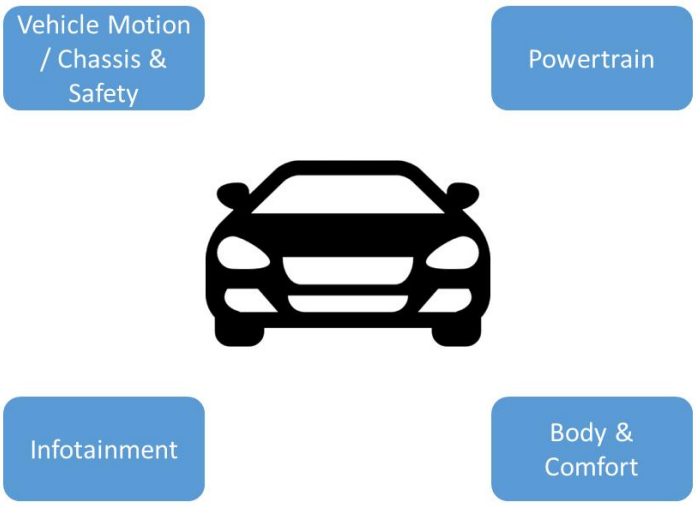

Abb. 2-1: Schematische Darstellung der Fahrzeug-Domänen

In der Abbildung werden folgende Domänen dargestellt:

- Vehicle Motion / Chassis & Safety
- Infotainment
- Powertrain
- Body & Comfort

Um den Umfang der Systeme im Fahrzeug darzustellen, werden nachfolgend den jeweiligen Domänen Systeme zugeordnet und verwandte- und aufeinander aufbauende Systeme in Kategorien eingeordnet. Diese Kategorien werden in ihren enthaltenen grundlegenden Funktionen beschrieben.

2.2.1 Powertrain

Die Systeme der Domäne Powertrain sind maßgeblich an den grundlegendsten Funktionalitäten eines Fahrzeugs beteiligt. Sie sorgen dafür, dass das Fahrzeug gestartet,

beschleunigt sowie abgebremst werden kann. In Abbildung 2-2 werden diese Systeme dargestellt und anschließend beschrieben.

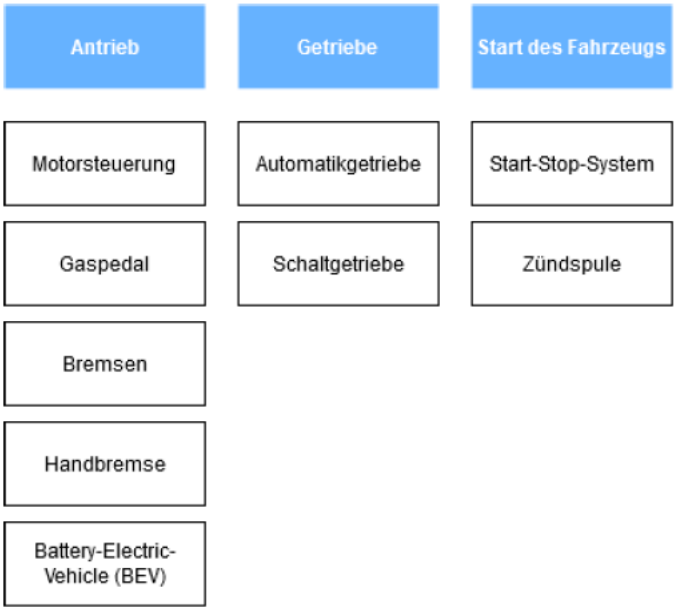

Abb. 2-2: Kategorisierte Systeme der Fahrzeug-Domäne Powertrain

Antrieb: Ein wichtiger Aspekt des Antriebs eines Fahrzeugs stellt die Motorsteuerung dar. Sie beschreibt alle Bausteine, die an dem Zustrom der Frischgase und an der Abfuhr der Abgase beteiligt sind (Mein-autolexikon.de, o.J.). Daneben existieren die vom Fahrenden genutzten Elemente wie das elektronische Gaspedal und die (Hand-) Bremse (SEAT, o.J.).

Eine alternative Methode zum Fahrzeug mit fossilen Brennstoffen stellt das Battery-Electric-Vehicle (BEV) dar. Wie bereits der Name offenbart, werden Fahrzeuge dieser Art durch einen elektrischen Motor betrieben, welcher durch die verbauten Batterien bzw. Akkus mit Energie versorgt wird. Aufgeladen werden die Batterien bzw. Akkus durch externe Quellen oder durch Rekuperation, welche beim Bremsvorgang die daraus gewonnene Energie zurückführt und speichert (SEAT, o.J.).

Getriebe: Fahrzeugmotoren arbeiten in bestimmten Drehzahlbereichen welche durch die Leer- und Maximaldrehzahl (Drehzahlband) begrenzt sind. Die maximale Leistung wie das maximale Drehmoment sind allerdings nur in Teilbereichen des Drehzahlbandes optimal genutzt weshalb ein Wechsel des Ganges notwendig ist. Im Automobil kann dies mit einem Schaltgetriebe umgesetzt werden, wobei der Wechsel der Schaltstufe durch die Betätigung der Kupplung erfolgt. Im Gegensatz dazu sorgt das Automatikgetriebe selbstständig für die Auswahl der Übersetzungen wie den Wechsel zwischen den Schaltstufen. Wann ein

Schaltvorgang notwendig wird, wird von Sensoren an das Automatikgetriebe gemeldet (SEAT, o.J.).

Start des Fahrzeugs: Die Zündspule sorgt für eine Hochspannung, welche an die Zündkerze weitergegeben wird, um das Starten eines Verbrennungsmotors zu ermöglichen (HELLA, o.J. c). Des Weiteren kann während der Fahrt ein Start-Stop-System eingesetzt werden, welches dafür sorgt, dass der Motor bei Stillstand und eingelegtem Leerlauf (bei Schaltgetriebe) abgeschaltet wird. Mit einem Tritt auf die Kupplung wird der Motor wieder gestartet (SEAT, o.J.).

2.2.2 Vehicle-Motion / Chassis & Safety

Bei den Systemen der Domäne Vehicle-Motion / Chassis & Safety, handelt es sich um Fahrassistenzsysteme und solchen, die der Sicherheit aller Beteiligten im Straßenverkehr dienen. In Abbildung 2-3 werden diese Systeme dargestellt und anschließend beschrieben.

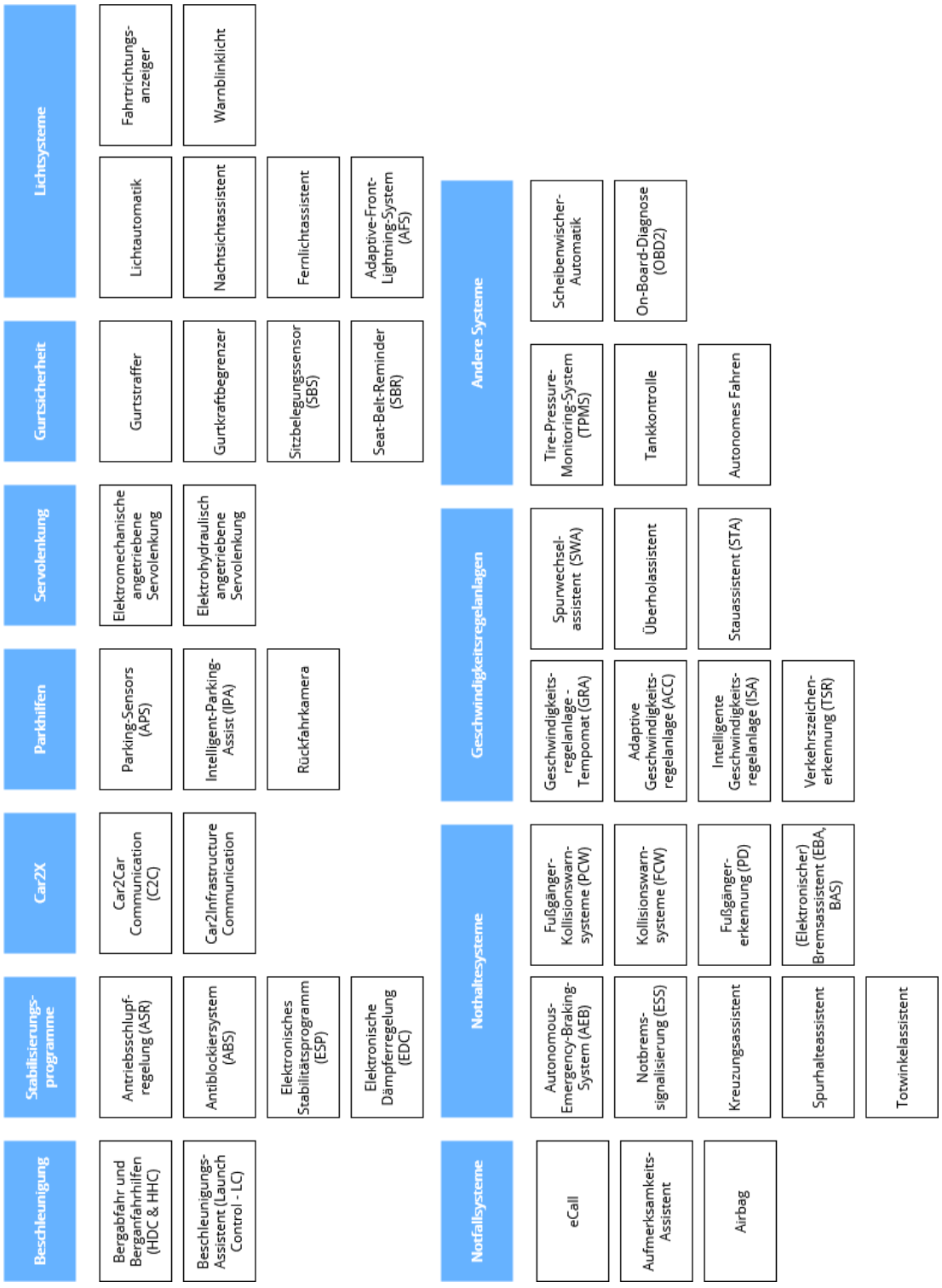

Abb. 2-3: Kategorisierte Systeme der Fahrzeug-Domäne Vehicle-Motion / Chassis & Safety

Beschleunigung: Unter dieser Kategorie befinden sich zwei Systeme: Bergabfahr- / Berganfahrhilfen (HDC & HHC) (Toyota, 2016) und der Beschleunigungs-Assistent (LC) (Hyundai, 2019). Bei den Systemen wird der Anfahr-Vorgang bei Schräglagen, durch die Verhinderung des Wegrollens unterstützt und es kann eine Anfahrt mit maximaler Anfahrtsgeschwindigkeit kontrolliert durchgeführt werden.

Stabilisierungsprogramme: Die vier Systeme, welche sich in diese Kategorie einordnen lassen, sorgen dafür, dass das Fahrzeug während der Fahrt, trotz kritischer Fahrsituationen, in einem stabilen Zustand bleibt. Es wird verhindert, dass das Auto schleudert, umkippt, übersteuert, aus der Fahrbahn ausbricht oder blockiert (SEAT, o.J.)

Car2X: Die Car2X Systeme ermöglichen eine Echtzeit-Kommunikation zwischen verschiedenen Fahrzeugen oder zwischen einem Fahrzeug und verkehrstechnischer Infrastruktur. Der Informationsaustausch mit der Umgebung soll dazu beitragen, gefährliche Situationen zu verhindern und den Verkehrsfluss in Städten und auf Autobahnen besser zu steuern. Es gibt bereits Teilbereiche, in denen solche Systeme zum Einsatz kommen. Um diese Ziele allerdings vollständig erreichen zu können, bedarf es einem einheitlichen Kommunikationsstandard (ADAC, 2018).

Parkhilfen: Die Systeme der Parkhilfen sind dazu gedacht, den Vorgang des Parkens sicherer zu gestalten. Sie ermitteln den Abstand des Fahrzeugs zu anderen Objekten, wodurch akustische und visuelle Warnungen gegeben werden können. Durch eine Kamera kann der Bereich hinterm Fahrzeug auf dem Display betrachtet werden, wobei zusätzliche Informationen zum Einpark-Vorgang dargestellt werden. Zusätzlich kann der Intelligent-Parking-Assist (IPA) aktiviert werden, wodurch sich das Fahrzeug selbsttätig in eine Parklücke manövriert (Toyota, o.J. a).

Servolenkung: Eine Servolenkung sorgt beim Stand des Fahrzeugs oder bei niedrigen Geschwindigkeiten für eine leichtgängige Lenkung. Bei hohen Geschwindigkeiten sorgt sie hingegen für Stabilität. Die technische Umsetzung kann variieren, wodurch zusätzliche Komfort- und Sicherheitsfunktionen geboten werden können (SEAT, o.J.).

Gurtsicherheit: Der analoge Dreipunktgurt ist die wichtigste Sicherheitsausstattung im Fahrzeug. Bei einer Kollision wird der Gurt binnen weniger Millisekunden gestrafft, wodurch der Passagier früh abgebremst und in einer Position gehalten wird, in welcher der Airbag und die Kopfstütze optimalen Schutz bieten. Die Straffung wird während des Vorgangs auf eine bestimmte Stärke beschränkt, sodass der Passagier dadurch nicht verletzt wird. Zusätzlich kommen Sensoren zum Einsatz, welche feststellen welche Sitze im Fahrzeug belegt sind. Dies kann für weitere Systeme genutzt werden, wie beispielsweise einem Warnsystem, welches die Passagiere bei nicht angeschnalltem Zustand an den Sicherheitsgurt erinnert (Continental, 2018a) (Mayser, o.J.) (SEAT, o.J.).

Lichtsysteme: Die Beleuchtung des Fahrzeugs kann automatisiert werden. So kann je nach Tagesverhältnis das Abblendlicht reguliert, bei Kurvenfahrten das Kurvenfahrlicht aktiviert und bei aktiviertem Fernlicht kann dieses bei entgegenkommendem Verkehr aus und wieder eingeschalten werden. Des Weiteren kann zur Unterstützung bei einer sehr dunklen Umgebung im Fahrerbereich eine frontale Nachtsichtaufnahme eingeblendet werden (SEAT, o.J.) (Bussgeldkatalog.org, 2020a). Zudem sind in jedem Fahrzeug Fahrtrichtungsanzeiger integriert, welche den Vorgang des Abbiegens signalisieren (Bussgeldkatalog.org, 2020b). Zur Signalisierung einer Gefahr und um die Aufmerksamkeit Dritter zu erhöhen gehören ebenso Warnblinklichter zum Standardrepertoire eines Fahrzeugs (Bussgeldkatalog.org, 2020c).

Notfallsysteme: Der Aufmerksamkeitsassistent warnt den Fahrenden haptisch und akustisch sobald Ermüdungserscheinungen zu erkennen sind (ITWissen.info, 2015a). Sollte es zu einem Unfall kommen, kann das Notrufsystem eCall eingesetzt werden. Dieses stellt einen schwerwiegenden Unfall fest und baut automatisch eine Telefonverbindung zur nächstgelegenen Rettungsleitstelle auf. Es werden zusätzlich der Standort und Informationen zu den Umständen des Unfalls übertragen (ADAC, 2019a). Im Falle eines Unfalls sind Airbags neben den Sicherheitsgurten maßgeblich für die Sicherheit in einem Fahrzeug verantwortlich (SEAT, o.J.)
Nothaltesysteme: Sollte das Fahrzeug bei einer zu drohenden Kollision nicht manuell vom Fahrenden gebremst werden oder sollte der Bremsvorgang nicht stark genug durchgeführt werden, kann ein Autonomous-Emergency-Braking-System (AEB) eingreifen. Es kann eine Notbremsung unterstützen, selbständig agieren und auf intelligente Weise Kollisionen vermeiden oder zuletzt eine maximale Reduzierung der Aufprallgeschwindigkeit erreichen (Continental, 2018b). Zusätzlich lässt sich dieses System durch viele weitere Funktionen erweitern. Bei den Erweiterungen handelt es sich um Systeme, welche auf spezifische Situationen spezialisiert sind (ADAC, 2006) (Audi, 2018) (Bosch, o.J. b) (Bosch, 2013) (ITWissen.info, 2015b) (ITWissen.info, 2015c) (MAN, o.J.) (Volkswagen, o.J.).

Geschwindigkeitsregelanlagen: Durch eine Geschwindigkeitsregelanlage (GRA) kann die Geschwindigkeit des Fahrzeugs gewählt werden, welche folglich vom Fahrzeug konstant beibehalten wird. Somit müssen Fahrende nicht selbst das Gaspedal bedienen. Die Adaptive- (ACC) und Intelligente-Geschwindigkeitsregelanlage (ISA) sind beide Erweiterungen der GRA, welche zum einen bei einem erscheinenden Hindernis den Abstand zum Hindernis und die eigene Geschwindigkeit anpassen und zum anderen die Geschwindigkeit des Fahrzeugs der Geschwindigkeitsbegrenzung der aktuellen Straße angleichen (Ford, 2018a) (Ford, 2018b) (Ford, 2019a) (Volkswagen, 2016a). Geschwindigkeitsbegrenzungen und weitere Verkehrszeichen können erfasst werden und den Fahrenden unabhängig einer GRA angezeigt werden (Volkswagen, 2016b). Daneben gibt es den Spurwechselassistent (SWA), welcher bei einem Überholmanöver die Fahrenden unterstützt und bei drohender Kollision warnt oder in das Lenkmanöver eingreift. Es existiert eine erweiterte Form dieses Systems, welches das Überholmanöver selbstständig durchführt, sofern die Umstände dies erlauben (ITWissen.info, 2017a) (Mercedes-Benz, 2017).

Andere Systeme: Trotz der zuvor definierten Kategorien existieren Systeme, die keiner dieser direkt zuordbar waren. Diese werden nachfolgend beschrieben:

- **Tire-Pressure-Monitoring-System (TPMS):** Durch das TPMS können während der Fahrt Druckabfälle im Fahrzeugreifen erkannt werden (ITWissen.info, 2019).

- **Scheibenwischerautomatik:** Die Scheibenwischer des Fahrzeugs können durch den Regensensor das Aufprallen und die Menge des Niederschlags messen und die Scheibenwischer dementsprechend einstellen. Der Regensensor regelt so das Ein- und Ausschalten der Scheibenwischer ohne Einwirkung des Fahrenden (HELLA, o.J. a).

- **Tankkontrolle:** Damit überprüft werden kann wie viel Tank noch im Fahrzeug enthalten ist, existiert die Tankkontrolle. In der Regel zeigt sie weniger an, als tatsächlich noch vorhanden ist (ADAC, 2019c).

- **On-Board-Diagnose-2 (OBD-2):** Mit der Bezeichnung OBD-2 ist das im Fahrzeug integrierte Diagnosesystem gemeint. Es überwacht Systeme im Fahrzeug, speichert Daten bei aufgetretenen Fehlern, zeigt Fehlfunktionen mithilfe der Motorkontrollleuchte an und bietet eine Schnittstelle zum Auslesen der gespeicherten Daten und laufender Betriebsdaten (obd-2.de, o.J.).

- **Autonomes Fahren:** Durch die Systeme, welche innerhalb dieser Domäne vorgestellt wurden, wird das automatisierte Fahrzeug definiert. Die Assistenzsysteme übernehmen dabei allerdings nur einen kleinen Teil der Steuerung und sind lediglich zur Unterstützung des Fahrenden konzipiert. Daher muss noch immer der Mensch jederzeit dazu bereit sein die Steuerung zu übernehmen. Beim autonomen Fahren würden die Menschen lediglich als Passagiere mitfahren, während das Fahrzeug komplett fahrerlos zuverlässig agiert (Toyota, o.J. b).

2.2.3 Infotainment

Das Infotainment beschreibt ein Angebot von Funktionalitäten im Automobil, welche der Unterhaltung, Information, Kommunikation und Fahrassistenz dienen (ITWissen.info, 2017b). In Abbildung 2-4 werden die dafür zuständigen Systeme dargestellt und anschließend beschrieben.

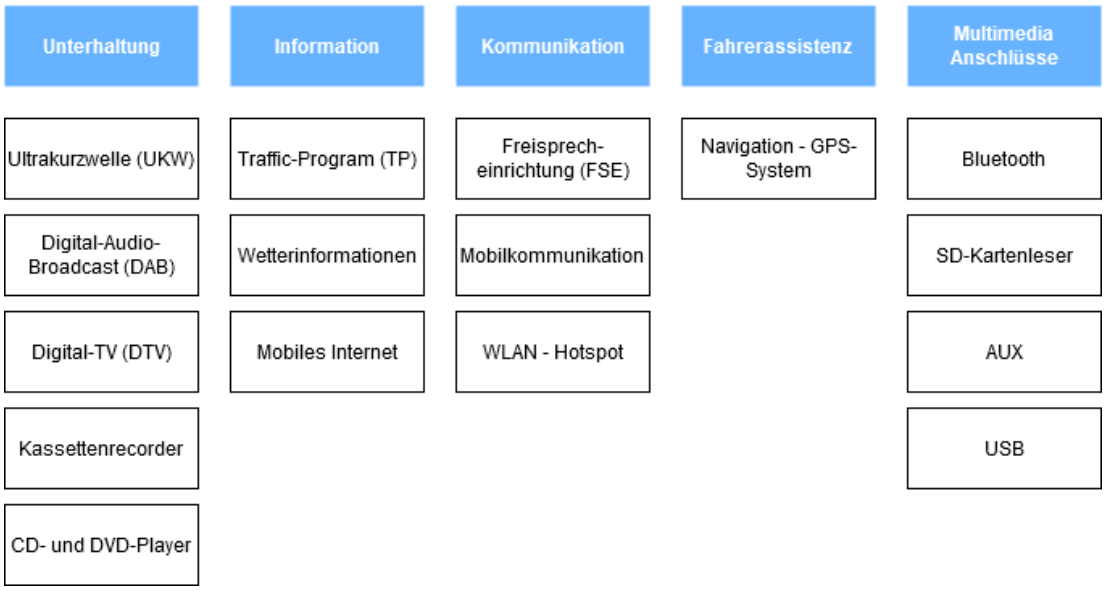

Abb. 2-4: Kategorisierte Systeme der Fahrzeug-Domäne Infotainment

Unterhaltung: Im Bereich der Unterhaltung wird Rundfunk in traditioneller und digitaler Technik angeboten. Dies wird Angeboten als Ultrakurzwelle (UKW) (NRD, o.J.), Digital-Audio-Broadcasting (DAB) (SEAT, o.J.) und Digital-TV (DTV) (ITWissen.info, 2014). Des Weiteren umfasst dieser Bereich ebenso den Einsatz von Kassettenrekordern und CD- und DVD-Player.

Information: Bei den Informationen, die ein Automobil von außen beziehen kann, handelt es sich beispielsweise um Verkehrsinformationen durch ein Traffic-Program (TP) (ITWissen.info, 2012), um Wetterinformationen (ITWissen.info, 2017b) und um allgemeine Datenübertragung aus dem Internet durch die Bereitstellung eines Mobilen Internets (ITWissen.info, 2013).

Kommunikation: Die Kommunikation im Automobil kann beispielsweise in Form einer klassischen Freisprecheinrichtung umgesetzt werden (ITWissen.info, 2015d). Diese kann umgesetzt werden mithilfe der Mobilkommunikation (Curved, 2019). Die Mobilkommunikation bietet durch die Anbindung ans Infotainment neben der Möglichkeit einer Freisprechanlage weitere Funktionalitäten eines Smartphones wie die Übertragung von Musik oder die Darstellung von Textnachrichten in vorgelesener Form. Des Weiteren kann das Automobil selbst einen WLAN-Hotspot bereitstellen, welcher Zugang zum Mobilen Internet bietet (ITWissen.info, 2013).
Fahrassistenz: Eine weitere Standard Funktionalität des Infotainments ist ein Navigation – GPS – System (ITWissen.info, 2018). Dies kann alternativ auch durch die Mobilkommunikation bereitgestellt werden (Curved, 2019).

Multimedia Anschlüsse: Für die Umsetzung der beschriebenen Infotainment Funktionalitäten sind im Automobil mehrere Multimedia Anschlüsse vorhanden wie das Bluetooth, ein SD-Kartenleser, eine AUX-Schnittstelle oder eine USB-Schnittstelle.

2.2.4 Body & Comfort

Die Body & Comfort Domäne bietet Systeme, die dem Komfort des Fahrenden und weiteren mitfahrenden Personen dienen. Viele dieser Systeme finden während der aktiven Nutzung des Fahrzeugs Anwendung. Es werden aber auch solche vorgestellt, die sich auf Vorgänge wie das Abstellen oder auf den Start des Fahrzeugs beziehen. In Abbildung 2-5 werden diese Systeme dargestellt und anschließend beschrieben.

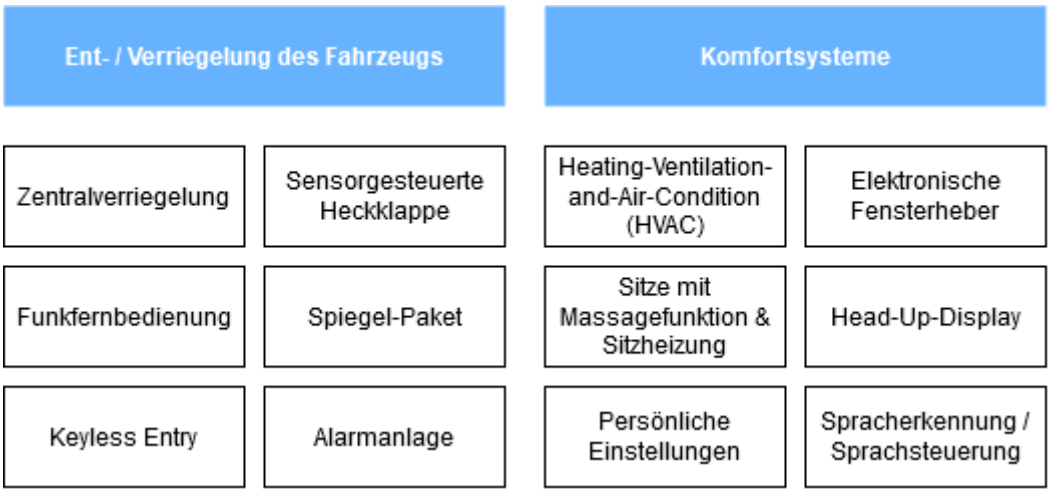

Abb. 2-5: Kategorisierte Systeme der Fahrzeug-Domäne Body & Comfort

Ent- / Verriegelung des Fahrzeugs: Die Zentralverriegelung stellt die Grundlage für die Ent- / Verriegelung des Fahrzeugs dar. Durch sie werden alle Türen und ggf. das Gepäckraumschloss und die Tankdeckelklappe zuverlässig gesperrt. Dazu existiert eine Funktionstaste im Fahrzeug und eine Funkfernbedienung durch welche die Zentralverriegelung bedient werden kann (SEAT, o.J.). Mithilfe eines Keyless-Entry Systems (HELLA, o.J. b) ist lediglich die Mitführung des Fahrzeugschlüssels notwendig, um das Automobil zu Entriegeln und den Motor zu starten. Dabei wird der Fahrzeugschlüssel nicht aktiv genutzt. Weitere Komfortsysteme sind in diesem Kontext die sensorgesteuerte Heckklappe (Ford, o.J.) und ein Spiegel-Paket, welches die Außenspiegel automatisch einklappt beim Parken (Mercedes-Benz, o.J.). Zur Sicherheit des geparkten Automobils existieren Alarmsysteme, welche Erschütterungen, Glasbruch, Neigungsänderung oder Spannungsabfall wahrnehmen und Alarm schlagen in diesen Situationen (ADAC, 2019b).

Komfortsysteme: Im Automobil sind mehrere Komfortsysteme enthalten, welche die Fahrt allgemein angenehmer gestalten. Darunter zählt das Heating-Ventilation-and-Air-Condition (HVAC) System, welches die Temperatur im Innenraum des Fahrzeugs steuert und auch bestimmte Bereiche des Innenraums anpassen kann (EDN, 2012). Des Weiteren sind Sitze mit Massagefunktion und Sitzheizung enthalten, sowie elektronisch gesteuerte Fensterheber (SEAT, o.J.). Für Automobile, welche von mehreren Personen genutzt werden, können Persönliche Einstellungen (Porsche, 2015) eingepflegt werden. Beim Start des Fahrzeugs besteht eine Auswahl an Nutzerprofilen, welche Einstellungen des Außenspiegels, des Innenspiegels, der Sitzeinstellung und des Displays speichern und bei Aktivierung anwenden. Ferner können durch ein Head-up-Display Informationen der aktuellen Fahrt, wie beispielsweise der Navigation oder der Höchstgeschwindigkeit, in Höhe der Windschutzscheibe angezeigt werden (Ford, 2019b). Letztlich kann in das Fahrzeug eine Sprachsteuerung eingebettet werden, welche Funktionen des Infotainments sowie der Body & Comfort Domäne per Spracherkennung umsetzen kann (Mercedes-Benz, 2019).

2.3 Moderne Fahrzeugnetzwerkarchitekturen

In welcher Art sich die Struktur des Fahrzeugbordnetzes bis hin zur heutigen gewandelt hat, wird durch Steinbach (2018) erläutert. Heutzutage besteht dieses aus etlichen Steuergeräten, welche über verschiedene Feldbus- und Kommunikationstechnologien miteinander verbunden sind. Dabei sind im Automobil Fahrassistenzsysteme integriert, wie zum Beispiel das Elektronische Stabilitätsprogramm, die Antriebsschlupfregelung oder sogenannte Advanced-Driver-Assistance-Systems (ADASs).

Durch die Einführung der fortschrittlichen ADASs, der ansteigenden Anzahl von Funktionen und den neuen Anforderungen welche sich aus dem Bereich des hochautomatisierten und autonomen Fahrens ergeben, werden deutlich größere Datenmengen erzeugt und es wird daher eine höhere Bandbreite im Kommunikationsbordnetz benötigt als zuvor. Für die Einführung der benannten Anwendungen steigt die Anzahl von Sensoren im Automobil, welche ebenfalls im Einzelnen mehr Daten erzeugen als vorherige. Außerdem müssen zur Realisierung neuer Funktionen die Systeme immer enger miteinander vermascht werden. Die zuvor in einer bestimmten Funktionsdomäne isolierten Daten werden zukünftig auch in zunächst unverwandten Domänen benötigt, in jenen die Daten gesammelt und dann zur Realisierung von Funktionen zusammengesetzt werden. Aus diesen Gründen bedarf es an leistungsfähigeren Kommunikationsverbindungen.

Um den Engpässen der Feldbusarchitektur aus dem Weg zu gehen, stellt die Ethernet-Technologie für die Automobilindustrie einen Hoffnungsträger dar. Diese wird schon heute als zusätzliche Kommunikationstechnologie in der aktuellen Fahrzeuggeneration eingesetzt. Dadurch wird allerdings die Anzahl unterschiedlicher Kommunikationstechnologien innerhalb eines Automobils erhöht, was die Kontrolle der Architektur erschwert. Aus diesem Grund wird eine Fahrzeugarchitektur benötigt, welche künftig ein homogenes Kommunikationsbordnetz im Automobil darstellt.

Eine solche Fahrzeugnetzwerkarchitektur ist der Echtzeit-Ethernet-Backbone. Durch ihn ist ein zentrale Kommunikationsinfrastruktur gegeben, welche eine hohe Bandbreite besitzt und flexibel die verschiedenen Anforderungen des Automobils erfüllen kann.

Er stellt eine leistungsfähige zentrale Kommunikationsinfrastruktur mit hoher Bandbreite dar, welche sich flexibel auf die Anforderungen der Anwendungen im Fahrzeug anpassen lässt.

2.3.1 Netzwerk-Topologien für Fahrzeuge

Die elektrische/elektronische- (E/E) Architektur beschreibt die Kraftfahrzeugelektrik und die Kraftfahrzeugelektronik. Ferner beschreibt sie die Vernetzung, die Schnittstellen sowie die optimale Strom-, Signal- und Datenverteilung zwischen den E/E-Komponenten (ITWissen.info, 2020). Ein wichtiger Bestandteil der E/E-Architektur ist die Vernetzung und somit die Netzwerk-Topologie eines Fahrzeugs.

Für die Umsetzung eines Echtzeit-Ethernet-Backbones, wie zuvor erwähnt, bedarf es einer angepassten Fahrzeugnetzwerkarchitektur in zukünftigen Fahrzeugen. Daher betrachten Steinbach (2018) und Brunner (2017) die heutige Netzwerk-Topologie in Serienfahrzeugen und wie diese den Anforderungen eines Echtzeit-Ethernet-Backbones entsprechend angepasst werden kann. Dazu beschreibt Steinbach die Evolutionsschritte einer busbasierten- hinzu einer Switch-basierten-Topologie. Hingegen hält Brunner zunächst den Fokus auf der Architektur und geht vom Einsatz verschiedener Feldbus- und Kommunikationstechnologien aus, wobei er ebenfalls die Entwicklung hin zum Einsatz von Ethernet empfiehlt. Im Endeffekt beschreiben beide dasselbe Konzept, wobei sie den Fokus unterschiedlich verlagern.

Die Grundlage für die Entwicklung möglicher Topologien wird von der physikalischen Verteilung der Steuergeräte gebildet. Steuergeräte verschiedener Domänen sind über das gesamte Fahrzeug verteilt, wobei drei Bereiche besonders viele beinhalten: Der Motorraum (Steuergeräte der Domäne Powertrain), das Armaturenbrett (Steuergeräte der Domänen Powertrain und Body & Comfort) sowie des Infotainmentsystems.

Heutige Architektur

Heutzutage werden in Serienfahrzeugen für die Steuergeräte der verschiedenen Anwendungsdomänen separate Feldbus- und Kommunikationstechnologien eingesetzt. Dabei wird die domänenübergreifende Kommunikation mit einem zentralen Gateway realisiert, welches für diagnostizierende Funktionen, die Weiterleitung der Kommunikation und die Übersetzung heterogener Kommunikationstechnologien zuständig ist. Im Automobil werden vermehrt Feldbusse eingesetzt, welche aufgrund der Verteilung von Steuergeräten innerhalb einer Anwendungsdomäne durch das gesamte Fahrzeug gezogen sein können. Dabei können auch von bereits am Gateway angebundenen Steuergeräten weitere private Kommunikationskanäle ausgehen, welche nicht mit dem zentralen Gateway verbunden sind. Dies wird zwischen Steuergeräten mit hohen Bandbreitenbedarf genutzt, um die Anwendungsdomänen zu entlasten. Abgesehen davon werden für die Einhaltung der Echtzeitfähigkeit die peripheren Sensoren und Aktoren mit solchen Anforderungen direkt mit den verarbeitenden Steuergeräten verbunden. Diese Topologie bringt aus der Sicht der heutigen Entwicklung einige Nachteile mit sich:

- Wenn ein neues Steuergerät in einem Feldbus integriert werden soll, muss entweder ein freier Platz im Bus existieren oder es muss der gesamte Bus neu verlegt werden

- Die gleichzeitige Nutzung gesammelter Steuergeräts-Daten ist aufgrund der Auslastung des Fahrzeugnetzwerks schwierig umsetzbar

- Das Einspielen neuer Software-Updates benötigt aufgrund der Steuergeräte, welche nur mithilfe separater privater Busse erreichbar sind, ungleich mehr Zeit

- In einer Anwendungsdomäne wird derselbe Kanal für die interne- und die domänenübergreifende Kommunikation genutzt, wodurch das zentrale Gateway die gesamte Kommunikation bearbeiten muss. Dies führt zu einem Bottleneck beim zentralen Gateway, welches die zunehmende Kommunikation durch neue Funktionen nicht bewältigen kann

- Insgesamt ergibt sich durch die mögliche Integrierung vieler heterogener Kommunikationstechnologien eine zu hohe Komplexität

Domänen-basierte-Architektur
Um diesen Problemen entgegenzuwirken, kann eine Domänen-basierte Topologie herangezogen werden, welche folglich als Domänen-basierte-Architektur bezeichnet wird. Jede Anwendungsdomäne erhält einen Domänen-Controller, welche wiederum mit dem ehemaligen zentralen Gateway verbunden sind. Die Domänen-Controller stellen die Kommunikation innerhalb einer Anwendungsdomäne zur Verfügung und stellen das einzige Interface zum zentralen Gateway dar.

Dadurch wird die interne Anwendungsdomänen-Kommunikation vom zentralen Gateway getrennt und die domänenübergreifende Kommunikation wird vom Backbone, den Domänen-Controllern und dem Gateway abgewickelt, wodurch sich die Komplexität im zentralen Gateway reduziert und eine bessere Skalierbarkeit für die Architektur erreicht, weil neue Funktionen oft nur den jeweiligen Anwendungsdomänen angepasst werden.

Für den Backbone könnten hohe Anforderungen in Bezug auf die Kommunikation gelten, weshalb leistungsstarke Kommunikationstechnologien in Betracht gezogen werden sollten. Diese Anforderungen könnten beispielsweise durch einen Ethernet-Backbone erfüllt werden, wodurch ein erster Schritt zur Umsetzung eines Echtzeit-Ethernet-Backbones unternommen wird. Dabei wird das zentrale Gateway durch einen Ethernet-Switch realisiert und die domänenübergreifende Kommunikation findet direkt zwischen den Domänen-Controllern – oder in diesem Kontext nach Steinbach den Domänen-Gateways – statt. Durch diese Topologie ergeben sich mehrere Vorteile:

- Durch einen Ethernet-Switch, welcher die Anwendungsdomänen miteinander verbindet, kann ein erster Ethernet-Backbone eingesetzt werden

- Eine Anbindung der Anwendungsdomänen mit höherer Bandbreite, kann die Übertragungsdauer von Software deutlich reduzieren

- Mithilfe eines Ethernet-Backbones könnten Sensoren mit hohen Bandbreitenbedarf – wie zum Beispiel Kameras – in das Fahrzeugnetzwerk eingebunden werden

- Der Bottleneck des zentralen Gateways wird aufgelöst

Allerdings löst diese Topologie nicht das Problem, dass Feldbusse durch das gesamte Auto gezogen werden müssen. Zudem rücken die Funktionalitäten des Fahrzeugs immer weiter zusammen, beispielsweise durch den sich ergebenden Anforderungen des autonomen Fahrens. Dadurch würde sich ein höheres Vorkommen von domänenübergreifender Kommunikation ergeben, wodurch die Auslastung erneut steigt.

Zonal-Architektur
Die Domänen-basierte-Architektur kann weiterentwickelt werden, indem die Steuergeräte aufgrund ihres physikalischen Standorts gruppiert werden. Dazu wird das Fahrzeug in Zonen aufgeteilt, wobei nahbeieinander liegende Steuergeräte einer Zone zugeordnet werden. Daher wird diese Topologie folglich als Zonal-Architektur bezeichnet. Die vorherige Notwendigkeit, alle verteilten Steuergeräte einer Anwendungsdomäne direkt miteinander zu verbinden entfällt, und die das Fahrzeug durchziehenden Feldbusse können in die Zonen zerteilt werden. Jede Zone besitzt einen Zonen-Controller, welche analog zur Domänen-basierten-Architektur miteinander verbunden sind und einen Backbone darstellen. Die verschiedenen Anwendungsdomänen teilen sich so dieselbe physikalische Infrastruktur, über dessen ihre Kommunikation abgewickelt wird.

Ferner wird der Standort aufgrund der Probleme der Domänen-basierten-Architektur der Datenverarbeitung angepasst. Da die Funktionalitäten des Fahrzeugs immer weiter zusammenrücken und die dadurch domänenübergreifende Kommunikation steigt, würde eine lokale Verarbeitung zu einem enormen Kommunikationsaufwand führen. Daher soll jegliche Datenverarbeitung in einer zentralen Instanz im Backbone erfolgen, welche folglich als Server bezeichnet wird. Der Server kann zudem als Datenverarbeitungs-Cluster realisiert werden, wodurch eine Flexibilität hinsichtlich der erforderlichen Rechenleistung auf der Grundlage des Fahrzeugmodells und der verbauten Ausrüstung geboten werden kann.

Durch diese Topologie können neue Funktionen sehr einfach eingebunden werden, da Peripherie-Komponenten direkt an einen Zonen-Controller angeschlossen und neue Software direkt im Server implementiert wird. Aufgrund der Struktur dieser Topologie, den steigenden Anforderungen an die Kommunikationskanäle und für die Umsetzung eines Echtzeit-Ethernet-Backbones, sollte, wie auch bei der Domänen-basierten-Architektur, ein Ethernet-Backbone in Betracht gezogen werden.

Mit der Zonal-Architektur, welche einen Ethernet-Backbone einbinden kann, ist es bereits möglich einen Echtzeit-Ethernet-Backbone umzusetzen. Allerdings nutzt diese Topologie neben Ethernet weitere Feldbus- und Kommunikationstechnologien. Bei der theoretischen Endstufe eines Ethernet-Backbones würde für jegliche Kommunikation Ethernet genutzt werden, wodurch eine physikalische Infrastruktur entsteht, welche von allen Komponenten geteilt wird.

2.3.2 AUTOSAR

Bei der Automotive-Open-System-Architecture (AUTOSAR) handelt es sich um eine weltweite Entwicklungspartnerschaft von Automobilherstellern, Zulieferern und anderen Unternehmen der Elektronik-, Halbleiter- und Softwareindustrie (AUTOSAR, 2020).

Durch AUTOSAR soll das Komplexitätsmanagement der im Automobil integrierten E/E-Architekturen verbessert werden. Um dies zu erreichen, zielt AUTOSAR darauf ab die Softwarearchitektur von Steuergeräten im Automobil zu standardisieren. Es sollen so Softwaremodule entstehen, die zwischen verschiedenen Automobilherstellern und Zulieferern austauschbar und wiederverwendbar sind. So zeichnet sich die von AUTOSAR entwickelte Softwarearchitektur durch eine weitgehende Unabhängigkeit zwischen Hard- und Software, sowie einer Unterteilung innerhalb der Software durch weitere horizontale Schichten aus. Somit stellen neue Applikationen die höchste Schicht dar und nutzen das zugrunde liegende Gerüst, welches durch die darunter liegenden Schichten gestaltet wird. Dadurch werden Softwaremodule wie beschrieben austauschbar und wiederverwendbar, wodurch an Qualität, (Kosten-) Effizienz und einer schnelleren Entwicklungszeit gewonnen wird (AUTOSAR, 2020).

Für den Einsatz im Automobil hat AUTOSAR zwei Softwareplattformen entwickelt: die AUTOSAR-Classic-Platform und die AUTOSAR-Adaptive-Platform. Die AUTOSAR-Classic-Plattform ist der Standard für tief eingebettete Steuergeräte. Allerdings werden durch neue Trends wie beispielsweise des Autonomen Fahrens tief eingebettete Applikationen eingesetzt, welche einen hohen Bedarf an Rechenleistung haben. Die standardmäßig eingesetzten Steuergeräte werden diesen Anforderungen nicht gerecht, weshalb eine neue Art von Steuergerät mit neuen Eigenschaften benötigt wird. Damit eine Umgebung existiert, welche diesen neuen Eigenschaften und den Anforderungen neuer Trends gerecht wird, wurde die AUTOSAR-Adaptive-Platform entwickelt (Fürst und Bechter, 2016).

Für tief eingebettete Systeme, welche typische Powertrain und Chassis Funktionalitäten realisieren, wird die AUTOSAR-Classic-Platform die erste Wahl bleiben. Sie ist eine erprobte und ausgereifte Softwareplattform, welche den Anforderungen dieser Systeme gerecht wird. In der Fahrzeug-Domäne Infotainment wird hingegen für gewöhnlich Linux oder andere kommerzielle Allzwecks-Betriebssysteme verwendet (Fürst und Bechter, 2016).

3 Anforderungsanalyse

An der HAW Hamburg soll zukünftig für die Studierenden ein wählbares Capture The Flag (CTF) Projekt mit einem Automobil stattfinden. Dies soll in Kooperation mit einem Forschungsprojekt zur Sicherheit in autonomen Fahrzeugen an der HAW Hamburg durchgeführt werden. Somit kann das Forschungsprojekt wertvolle Daten zur Untersuchung der Sicherheit in autonomen Fahrzeugen sammeln, während die Studierenden anhand eines aktuellen Themas ihre Fertigkeiten verbessern.

Um dieses Vorhaben umsetzen zu können wird ein Konzept für ein CTF im Automobil benötigt, welches aufkommende technischen Hürden angemessen behandelt. Die größte Herausforderung hierbei ist, dass das Automobil bei CTFs bisher keine Verwendung fand und sich durch besondere Eigenschaften auszeichnet, die im folgenden Abschnitt erläutert werden.

3.1 Das Automobil als besondere Ressource

Das Automobil als besondere Ressource zeichnet sich für unsere Zwecke im Vergleich zu einem Server durch seine physisch aktiven Faktoren, wie zum Beispiel das Einschalten des Abblendlichts oder die Betätigung der Verkehrsrichtungsanzeiger aus. Damit ist das Auto zwar nicht die einzige Ressource, die über diese Eigenschaften verfügt, sondern diese könnten ebenfalls auf eine Fabrik, ein Elektrizitätswerk, ein Zug oder einem Flugzeug übertragen werden, welche im gleichen Maße eine besondere Ressource mit solchen Eigenschaften darstellen würden. Im Vergleich zu den anderen Angriffszielen ist das Auto allerdings die zugänglichste Wahl.

Ein Automobil ist eine nicht beliebig vervielfältigbare Ressource

Anders als in einem CTF sonst gewohnt, stellt ein Fahrzeug eine nicht beliebig vervielfältigbare Ressource dar. Die Teilnehmenden sind daher darauf angewiesen zeitgleich an derselben Hardware zu arbeiten, wodurch eine Ressourcen-Problematik immer dann

entstehen würde, wenn sich Angriffe gegenseitig behindern oder befördern, oder bestimmte Flaggen nur einmal erworben werden können.

Mögliche, infrage kommende CTF Arten für ein Automobil
Für die Konzipierung eines CTFs kommen verschiedene Arten in Frage, welche in Abschnitt 2.1.1 beschrieben wurden. Bei der Betrachtung der verschiedenen Arten muss darauf geachtet werden, dass das Automobil als Angriffsziel immer im Fokus stehen soll. Die unterschiedlichen Arten werden folgend mit Blick auf diesen Anwendungskontext betrachtet:

- **Jeopardy:** Bei dieser CTF Art lässt sich das Automobil als Hauptangriffsziel modellieren. Es können den Teilnehmenden mehrere Challenges aus unterschiedlichen Bereichen der Informationssicherheit angeboten werden. Die Challenges beziehen sich dabei auf Systeme der Fahrzeug-Domänen, welche in Abschnitt 2.2 vorgestellt wurden. Anhand von fortschreitend gelösten Challenges können weitere Challenges und dazugehörige Systeme, beziehungsweise Bereiche des Automobils freigeschaltet werden

- **Attack-Defense:** Für die CTF Art Attack-Defense kann es kein einzelnes Automobil als Hauptangriffsziel geben, wie zuvor für Jeopardy modelliert. Das Konzept dieser CTF Art erfordert, dass jedes Team ein eigenes System und die enthaltenden Challenges bearbeitet. Üblicherweise erhalten alle Teams Systeme und Challenges gleicher Art, wodurch eine Chancengleichheit bei deren Bearbeitung entsteht. Ferner müssen die Teams die Systeme anderer Teams angreifen und ihr eigenes verteidigen. Um dieses Konzept effektiv auf ein Automobil zu übertragen, kommen drei Szenarien in Frage:

    - Das CTF wird trotz beschriebener Problematik mit einem einzelnen Automobil durchgeführt. Dabei wird ein vorgegebener Zeitplan befolgt, durch welchen immer nur ein Team zur selben Zeit das Automobil vor den anderen Teams verteidigt. Zusätzlich wird vorab eine Vorbereitungsphase durchgeführt, in welcher jedes Team die Möglichkeit hat, die im Automobil enthaltenen Challenges vorzubereiten

    - Jedes Team erhält ein eigenes Automobil, welches sie bearbeiten und zu einem späteren Zeitpunkt gegen Angreifer verteidigen

    - Mehrere Automobile werden virtuell dargestellt und jedes Team erhält lediglich eine virtuelle Version. Durch diese Modellierung gehen allerdings die physischen Aspekte des Automobils verloren, welche dieses so besonders machen. Der weitere Verlauf gestaltet sich wie der eines traditionellen Attack-Defense CTFs

- **King-of-the-Hill:** Wie bereits in Abschnitt 2.1.1 beschrieben, hat diese CTF Art Ähnlichkeiten zu Attack-Defense. Auch hier existieren Systeme, welche von den verschiedenen Teams angegriffen und verteidigt werden. Die beiden CTF Arten unterscheiden sich dadurch, dass die hier zu bearbeitenden Systeme zunächst keinem Team gehören. Diese müssen zunächst von einem Team erobert und anschließend verteidigt werden. Daraus ergeben sich folgende Szenarien:

    - Das CTF findet innerhalb eines einzelnen Automobils statt. Dabei werden allen Teams innerhalb des Automobils mehrere Systeme zur Verfügung gestellt die es zu erobern und anschließend zu verteidigen gilt. Bei den Systemen handelt es sich um die in den Fahrzeug-Domänen enthaltenden, welche in Abschnitt 2.2 vorgestellt wurden

    - Ergänzend zum vorherigen Szenario können anstatt der dort beschriebenen Systeme auch die Fahrzeug-Domänen als Angriffsziel betrachtet werden, welche von den Teams erobert und dann verteidigt werden. Auf die gleiche Weise könnte das Automobil als Ganzes das Angriffsziel darstellen

    - Es werden mehrere Automobile zur Verfügung gestellt, wobei alle Teams versuchen die jeweiligen Automobile anhand dort enthaltener Challenges zu erobern. Sobald ein Team ein Automobil erobert hat, muss es dieses verteidigen

    - In gleicher Art wie bei der CTF Art Attack-Defense, kann mit Virtualisierungen gearbeitet werden, welche auf alle hier vorgestellten Szenarien übertragen werden können. Allerdings kommen dieselbe Problematik und die gleiche Folge zum Tragen

  Das zweite Szenario birgt die Frage, ab wann eine Fahrzeug-Domäne oder ein gesamtes Automobil als erobert gilt. Diese beiden Angriffsziele bestehen aus mehreren untergeordneten Systemen, wobei sich die Herrschaft über diese Systeme definieren lässt:

    - Ein gesamtes Automobil kann für ein CTF als vollständig erobert betrachtet werden, wenn alle enthaltenen Fahrzeug-Domänen beherrscht werden

    - Einzelne Fahrzeug-Domänen können als vollständig erobert betrachtet werden, wenn alle enthaltenen Systeme beherrscht werden

Für die Herrschaft über eine Fahrzeug-Domäne, sowie über ein gesamtes Automobil müssen also dieselben Systeme bearbeitet werden wie im ersten Szenario. Dementsprechend betrifft dies auch das dritte Szenario, da es als eine Erweiterung des zweiten zu betrachten ist.

Nun könnten diese Szenarien so differenziert werden, dass die Teams nur dann Punkte erhalten, wenn alle untergeordneten Systeme des jeweiligen Angriffsziels erobert wurden. Allerdings würde dies nicht dem Konzept von King-of-the-Hill entsprechen und einen starken Einfluss auf die Spieldynamik haben. So sollten die Teams bei Absolvierung einer Challenge unabhängig der Komplexität des betroffenen Systems belohnt werden, da es sich immer um einen erfolgreichen Angriff handelt.

Daraus folgt, dass sich die ersten drei Szenarien nicht unterscheiden und durch das erste Szenario beschrieben werden

- **Collegiate-Cyber-Defense-Challenge:** Für gewöhnlich wird vom Blue-Team ein fiktives Unternehmen verteidigt. Anhand dessen sollen den Teilnehmenden des Blue-Teams administrative Aspekte der Verteidigung vermittelt werden. Mit einem Automobil kann dies so modelliert werden, dass es das Netzwerk darstellt, welches vom Blue-Team verteidigt wird. Daneben wird ein professionelles Red-Team engagiert, welches das Automobilnetzwerk angreift

- **Wargames:** Bei dieser CTF Art kann in gleicher Art wie bei Jeopardy, den Teilnehmenden Challenges innerhalb eines einzelnen Automobils zur Verfügung gestellt werden. Diese Challenges basieren auf den Systemen der Fahrzeug-Domänen, welche in Abschnitt 2.2 vorgestellt wurden. Dabei steht zu einem beliebigen Zeitpunkt eine einzelne Challenge zur Verfügung, wobei nach Absolvierung die nächste freigeschaltet werden kann. Alternativ können mehrere Informationssicherheitskategorien herangezogen werden, welche jeweils eine unterschiedliche Start-Challenge besitzen und bei Absolvierung weitere freischalten. Es werden dem CTF kontinuierlich neue Challenges hinzugegeben, welche den zuvor bestehenden hinten angefügt werden

- **HackQuest:** Auch bei dieser Art werden den Teilnehmenden Challenges innerhalb eines einzelnen Automobils zur Verfügung gestellt. Diese Challenges basieren auf den Systemen der Fahrzeug-Domänen, welche in Abschnitt 2.2 vorgestellt wurden. Mit einem zeitlichen Abstand werden einzelne Challenges für einen bestimmten Zeitraum zur Verfügung gestellt. Dies wiederholt sich bis zum Ende des Events

Verbindung zwischen physischen und digitalen Vorgängen im Fahrzeug
Im Falle dass, im Vergleich zu einem herkömmlichen CTF Flaggen physisch gesetzt werden, sind Ergebnisse/Flaggen sofort sichtbar. In diesem Zusammenhang muss verstanden werden, dass in einer sonstigen CTF Umgebung die hier physisch aktiven Faktoren nicht vorhanden sind. Die daraus folgende Vermischung von physischer- und digitaler Welt macht das Auto aus diesem Blickwinkel betrachtet besonders.

Besonderheiten und Hürden bei Veränderungen der Fahrzeugsoftware
Herkömmliche CTFs besitzen eine leicht anpassbare Umgebung. So könnte beispielsweise ein wie in Abschnitt 2.1.5 vorgestelltes CTF Framework modifiziert und auf einem beliebigen Server ausgeführt werden.

Mit einem Automobil ist hingegen zu beachten, dass die in Abschnitt 2.2 beschriebenen Fahrzeug-Domänen und die darin enthaltenen Systeme existieren. Viele dieser Systeme vollführen sicherheitskritische Aufgaben, weshalb eine Modifizierung dieser ein Risiko darstellt. Um eine solche Modifizierung vorzunehmen ist eine ausreichende Qualifikation der ausführenden Person notwendig, sowie die dazugehörigen notwendigen Entwicklungswerkzeuge. Solche Systeme sind vor allem innerhalb der Domänen Powertrain und Vehicle-Motion / Chassis & Safety zu finden.

Ferner muss dem Fakt Beachtung geschenkt werden, dass der Großteil der sicherheitskritischen Systeme mit einer AUTOSAR Softwareplattform betrieben wird, wie in Abschnitt 2.3.2 beschrieben. Lediglich in der Fahrzeug-Domäne Infotainment werden für gewöhnlich Linux oder andere kommerzielle Allzwecks-Betriebssysteme verwendet, welche auch in herkömmlichen CTFs fast ausschließlich genutzt werden.

Dennoch gibt es Möglichkeiten trotz des beschriebenen Risikos mit diesen Systemen zu arbeiten. Zum einen kann mithilfe von Linux ein Informationszustand von AUTOSAR Systemen mithilfe des Kommunikationsprotokolls Diagnostics-over-Internet-Protocol (DoIP) abgefragt werden (Mentor, o.J.). Durch das von Gebauer (2018) beschriebene DoIP ist eine flexible und leistungsfähige Diagnose von AUTOSAR Systemen möglich. Eine Diagnose kann durchgeführt werden, insofern das jeweilige System per Ethernet, WLAN oder Mobilfunk einen Kommunikationspfad zum Diagnosetester besitzt und sich dieser zuvor im Automobilnetzwerk authentifizieren konnte. In folgenden Situationen findet DoIP Anwendung:

- **Off-Board:** Die Durchführung der Diagnose erfolgt von außen auf das Fahrzeug. Dies findet beispielsweise in einer Werkstatt statt

- **On-Board:** Während der Fahrt erfolgt die Diagnose durch das integrierte Diagnose-System, welches das Fahrzeug überwacht

- **Remote-Zugriff:** Ebenso kann während der Fahrt per Remote-Zugriff eine Diagnose durchgeführt werden

Für eine effiziente Diagnose und Programmierung moderner Fahrzeugelektronik bietet DoIP folgende Features:

- Datenübertragung
- Suchen und Erkennen von Fahrzeugen
- Aufbauen und Prüfen von Verbindungen
- Flashen von Steuergeräten
- Fehlermanagement
- Firewall-Funktionalitäten

Anhand der in Abschnitt 2.3.1 beschriebenen Evolution der Netzwerk-Topologien für Fahrzeuge kann davon ausgegangen werden, dass durch die zukünftige Entwicklung hinzu zum Echtzeit-Ethernet-Backbones die meisten Steuergeräte per DoIP ansprechbar sind. Bei einer Netzwerk-Topologie, die den Echtzeit-Ethernet-Backbone umsetzen kann wie der Zonal-Architektur, kommt eine zentrale Instanz zur Datenverarbeitung hinzu. Diese wird von allen Steuergeräten für die jeweiligen Berechnungen genutzt. Auch für diese zentrale Instanz kann von einer zukünftigen Entwicklung hin zur DoIP Kompatibilität ausgegangen werden.

Um neben den im Automobil bereits enthaltenen Systemen für ein CTF mehr Spielraum durch modifizierbare Systeme zu schaffen, gibt es die Möglichkeit Linux Systeme einzufügen:

- Eine Methode wie dies umgesetzt werden kann, beschreiben Nett und Schneider (2013). Sie zeigen zunächst unterschiedliche bestehende Ansätze auf und stellen ihren eigenen vor, welcher sich von vorherigen Ansätzen abhebt. Ihr Ansatz unterscheidet sich von den anderen darin, dass eine AUTOSAR Softwareplattform und ein Linux-Betriebssystem durch eine vertikale Partitionierung auf zwei Kernen eines einzelnen ARM-Multiprozessors betrieben werden, wobei die AUTOSAR Softwareplattform vorgeschaltet wird. Dabei werden die Echtzeit-Anwendungen der AUTOSAR Softwareplattform nicht beeinträchtigt

- Als zweite Methode könnte zusätzliche Hardware sehr einfach in ein Ethernet-Backbone eingefügt werden, sofern eine solche Topologie vorhanden ist

Differenzierung von beliebigen Dritten und Personen, die sich im Fahrzeug befinden oder Zugang haben
Mit einem Fahrzeug als Angriffsziel in einem CTF, würden für die Angreifenden unterschiedliche Perspektiven in Frage kommen. Es kann unter folgenden Angreifer-Klassen differenziert werden, wobei diese hier in einem Aufsteigenden Machtverlauf übers Fahrzeug dargestellt werden:

- **Angreifer von außen:** Die Angreifenden haben keinen Zugang zum Fahrzeug und können nur durch externe Kanäle mit dem Fahrzeug kommunizieren

- **Autorisierter Zugang:** Es besteht für die Angreifenden Zugang zum inneren des Fahrzeugs. Die im Fahrzeug existierenden Schnittstellen können genutzt werden, wobei der Schlüssel zur Betätigung der Zündung nicht vorhanden ist

- **Besitzer des Fahrzeugs:** Die Person, welche das Fahrzeug besitzt, hat sowohl Zugang zum inneren des Fahrzeugs, sowie auch den Schlüssel zur Betätigung der Zündung

- **Hersteller & Werkstatt:** Der Hersteller oder eine zuständige Werkstatt hat bei einer Wartung des Fahrzeugs Zugriff auf den Schlüssel zur Betätigung der Zündung. Ferner haben sie die Möglichkeit Software Up- und Downgrades am Fahrzeug durchzuführen

3.2 Funktionale Anforderungen

Nachfolgend werden funktionale Anforderungen definiert, welche bei der Konzipierung des CTFs Beachtung finden sollen.

Mit einer digitalen Aktion soll etwas physisches ausgelöst werden
Wie bereits in Abschnitt 3.1 beschrieben, ist bei einem CTF im Fahrzeug eine Vermischung der physischen- und digitalen Welt realisierbar und erwünscht.

- **Aufgabe für 4.X:** Storyline sowie Challenges

Das Fahrzeug soll über externe Zugänge verfügen
Sollten Angriffsziele auf Personengruppen ohne Zugangsberechtigung zum Fahrzeug zugeschnitten werden, erfordert die Kommunikation mit dem Fahrzeug externe Zugänge, wie zum Beispiel Bluetooth oder WLAN.

Das Fahrzeug soll über interne Schnittstellen verfügen
Sollten Angriffsziele definiert werden, die auf Personengruppen mit autorisiertem Zugriff zum Fahrzeug zugeschnitten sind, ist das Vorhandensein interner Schnittstellen notwendig.

3.3 Nicht-funktionale Anforderungen

Nachfolgend werden nicht-funktionale Anforderungen definiert, welche bei der Konzipierung des CTFs Beachtung finden sollen.

Die Erkenntnis erlangen, dass mit digitalen Aktionen etwas Physisches erreicht werden kann

Wie in Abschnitt 3.1 beschrieben und Abschnitt 3.2 festgelegt, soll im vorliegenden CTF eine Vermischung der physischen- und digitalen Welt konzipiert werden. So sollen mit digitalen Aktionen physische Reaktionen ausgelöst werden, anhand dessen die am CTF Teilnehmenden die Erkenntnis erlangen sollen, dass die zuvor beschriebenen Aktionen möglich sind.

Die Teilnehmenden sollen durch das CTF, Informationssicherheitskonzepte verstehen und laufend neue Erkenntnisse gewinnen

In einem CTF können die eigenen praktischen Fertigkeiten und das Verständnis über Angriffs-Szenarien verbessert werden, wie in Abschnitt 2.1.3 beschrieben. Dies soll den Teilnehmenden im vorliegenden CTF durch eine geeignete Konzipierung möglich gemacht werden.

Durch neues Wissen sowohl Spaß an der Arbeit wie auch Motivationssteigerung erfahren

Die Bearbeitung von CTF Challenges wird von den Teilnehmenden oft als Freude betrachtet. Die daraus resultierende Motivation zur Teilnahme am CTF im Allgemeinen sorgt für einen intensiveren Lerneffekt der Teilnehmenden wie in Abschnitt 2.1.3 beschrieben. Die Wirkung der gesteigerten Motivation sollen die Teilnehmenden des vorliegenden CTFs gleichermaßen erfahren.

Durch gemeinsames Bestreiten des Wettbewerbs die Teamfähigkeit wie den Teamgeist fördern

Ein CTF ist ein spezieller Wettbewerb bei welchem mehrere Teams gegeneinander antreten, wie in Abschnitt 2.1 beschrieben. Um als Team Erfolg zu haben, ist eine gute Zusammenarbeit der Teilnehmenden notwendig. Durch die Arbeiten am CTF sollen die Teilnehmenden auch hier ihre Teamfähigkeiten steigern und ihren Teamgeist fördern.

Relevanz der Zielgruppen für ein CTF

Wie bereits in Abschnitt 2.1.4 beschrieben muss während eines CTF die bereits gemachte Erfahrung einer Zielgruppe berücksichtigt werden. Wird das Konzept eines CTF falsch ausgelegt kann es dazu beitragen, dass sich Erfahrene Teilnehmende unterfordert fühlen, oder dass die Aufgabenstellung neue Teilnehmende überfordert. Daher ist eine Konzeptionierung in Betracht auf beide Teilnehmergruppen nicht zu vernachlässigen.

3.4 Weitere Randbedingungen

Nachdem die (nicht-) funktionalen Anforderungen definiert wurden, sind nun noch die Randbedingungen zu definieren welche für die weitere Planung des Events sowie der Konzipierung des CTF zu befolgen sind.

Das Auto muss unbeschädigt bleiben und die Betriebszulassung beibehalten
Um die Betriebszulassung beizubehalten muss das Auto unbeschädigt bleiben und seine Fahrtüchtigkeit erhalten. Daher gilt bei allen Arbeiten am Fahrzeug vorab zu prüfen, ob währenddessen Beschädigungen an der Software oder am Fahrzeug selbst auftreten könnten.

Das Auto darf keinen Schaden verursachen und keine Person verletzen
Da Risiken an Sach- und Personenschäden bei Arbeiten am Fahrzeug nicht ausgeschlossen sind, ist Vorsicht bei den folgenden Punkten geboten:

- Um Quetschungen bei Öffnen und Schließen der Türen zu vermeiden, sollte darauf gänzlich verzichtet werden. Da bei offenen Türen das Verletzungsrisiko deutlich sinkt, sollten diese während der Arbeiten dauerhaft geöffnet bleiben

- Ein weiteres Risiko ist das Wegrollen des Fahrzeuges. Um dies Effektiv vermeiden zu können, sollten an den Antriebsräder Wegfahrklötze angebracht werden

- Weiterführend muss klargestellt werden, dass das Fahrzeug weder bewusst noch unbewusst in Bewegung versetzt werden darf. Dies könnte unter Umständen zu Verletzungen an Personen oder Sachschäden führen

- Nicht auszuschließen sind Brände und Explosionen deren Auslöser Kurzschlüsse sein könnten. Da Kurzschlüsse allgemein ein hohes Brandrisiko darstellen, sollten mindestens zwei Feuerlöscher bereitgestellt und die Teilnehmenden im Vorwege in dessen Handhabung eingewiesen werden

- Des Weiteren muss sichergestellt werden, dass Betriebsstoffe (gefährliche, umweltschädliche) unter keinen Umständen auslaufen. Aus diesem Grund ist auf alle Maßnahmen, die ein hohes Auslauf-Risiko darstellen zu verzichten

- Bei Elektrofahrzeugen ist von allen Arbeiten, die mit elektrischen Verbindungen zu den Akkus und dessen Stromkreis in Verbindung stehen dringen abzusehen. Auch hier besteht die Gefahr von Bränden und Explosionen, die aufgrund der Beschaffenheit der heutzutage eingesetzten Akkus nur sehr schwer zu löschen sind (Mobile.de, 2020)

Das Auto darf keinen Notruf auslösen
Im Vorfeld der Arbeiten gilt abzuklären wie das Notrufsystem des zu bearbeitenden Fahrzeugs verbunden ist. Wählt das Fahrzeug automatisch eine Notrufnummer muss dessen versehentliche Verwendung oder Auslösung verhindert werden. Dies ist nicht nur aus Grund der Strafbarkeit eines unberechtigten Notrufes (dejure.org, o.J. a), sondern auch um die Notrufzentralen nicht unnötig Kapazitäten zu nehmen.

Der Kilometerstand muss unverändert bleiben
Die Manipulation des Kilometerstandes eines Fahrzeugs ist in Deutschland strafbar (Bussgeldkatalog.org, 2020d) und gilt somit als Betrug. Daher darf der Angezeigte Kilometerstand unter keinen Umständen, weder ausversehen, noch wissentlich geändert werden.

Arbeiten am Fahrzeug sind bei laufendem Motor nicht gestattet
Sollte das Fahrzeug während der Arbeiten doch in Betrieb genommen werden müssen, ist dies mit einer angemessenen Vorlaufzeit anzukündigen, sodass alle Teams Zeit haben die gerade stattfindenden Arbeiten zu Ende zu bringen. Während des Betriebs (laufender Motor) dürfen keine neuen Arbeiten am Auto begonnen werden.

Das Infotainmentsystem darf keine persönlichen Daten beinhalten
Aus Gründen des Datenschutzes darf das Infotainmentsystem des Fahrzeuges keine persönlichen Daten beinhalten (dejure.org, o.J. b). Ferner dürfen von den Teilnehmenden auch keine persönlichen Daten in das System eingebracht werden.

Gefundene Sicherheitslücken sind dem Hersteller zu melden und die allgemeine Veröffentlichung zu unterlassen
Da unsere Arbeit wissenschaftlicher Natur unterliegt, gebietet es die Fairness gefundene Sicherheitslücken oder sonstige in der Software enthaltene Fehler unentgeltlich dem Hersteller zu melden. Daher wird gebeten, alle gefundenen Fehler zu dokumentieren und anschließend dem Projekt zu melden, damit diese geschlossen dem Hersteller zur Verfügung gestellt werden können.

3.5 Festlegung des Anwendungsszenarios

Anhand der Analyse des Automobils als besondere Ressource, sowie den definierten (nicht-) funktionalen Anforderungen und Randbedingungen, wird nachfolgend auf dessen Grundlage das Anwendungsszenario bestimmt.

Chancengleichheit für Teilnehmende trotz Ressourcen-Problematik
Wie in Abschnitt 3.1 beschrieben, entsteht eine Ressourcen-Problematik beim zeitgleichen Arbeiten an derselben Hardware. Bei der Konzipierung des CTF Wettbewerbs soll diese

Problematik behandelt und dadurch eine möglichst hohe Chancengleichheit erlangt werden. Aufgrund der Ressourcen-Problematik soll kein Team bei der Teilnahme benachteiligt sein.

Auswahl der CTF Art
Die in Abschnitt 3.1 beschriebenen CTF Arten im Bezug zu einem Automobil werden nachfolgend aufgegriffen, auf dessen Grundlage eine der möglichen Umsetzungen ausgewählt werden soll.

- **Jeopardy:** Diese Art ist in der beschriebenen Form umsetzbar. Dabei darf dennoch die Ressourcen-Problematik nicht außer Acht gelassen werden, sodass diese den Ablauf des CTFs nicht behindert

- **Attack-Defense:** Für die Umsetzung dieser Art wurden mehrere Szenarien beschrieben. Das erste Szenario sieht die Nutzung eines einzelnen Automobils für alle Teams im laufenden Event vor. Dabei wird das Fahrzeug zur selben Zeit von einem Team verteidigt, während der Bearbeitung der gestellten Aufgaben die anderen Teams das Automobil angreifen. Angreifende Teams sowie das verteidigende Team werden dabei nach einer festgelegten Zeitrotation festgelegt. Zwar nutzt diese Modellierung lediglich ein einzelnes Automobil, allerdings ändert sich die Spieldynamik dadurch enorm. Bei einem weiteren Szenario wird die Zuteilung von mehreren Automobilen herangezogen, wobei jedes Team ein eigenes Fahrzeug erhält. Allerdings würde dies die Ressourcen eines HAW CTF Projekts stark überstrapazieren. Zu beiden beschriebenen Szenarien kommt die Ressourcen-Problematik hinzu, welche traditionelle Attack-Defense CTFs mit ihrer Echtzeit-Spieldynamik fast unmöglich macht.

  Zwar könnte das Event durch ein virtuell dargestelltes Automobil umgesetzt werden, allerdings gehen so alle physischen Aspekte, die es besonders machen verloren. Dies widerspricht den (nicht-) funktionalen Anforderungen aus Abschnitt 3.2 und 3.3, welche explizit physische Aspekte begrüßen

- **King-of-the-Hill:** Für diese CTF Art wurde ein Szenario beschrieben, welches für ein einzelnes Automobil umsetzbar wäre. Dennoch würde die Ressourcen-Problematik ähnlich wie für Attack-Defense die Echtzeit-Spieldynamik verändern. Ein virtuell dargestelltes Automobil hätte denselben Effekt wie für Attack-Defense bereits beschrieben

- **Collegiate-Cyber-Defense-Challenge**: Diese CTF Art wäre zwar für ein Automobil denkbar, allerdings hat sie andere kritisch zu betrachtende Punkte. Sie differenziert sich von den anderen dadurch, dass die Vermittlung administrativer Aspekte der Verteidigung im Fokus steht. In welchem Maß ein Automobil für die Vermittlung solcher Aspekte modelliert werden kann und inwiefern sich dies auf andere Bereiche

übertragen lässt, muss zunächst untersucht werden. Des Weiteren werden von den Teilnehmenden keine technischen Aspekte der Informationssicherheit berührt wodurch sie keine Erkenntnisse in Bezug auf das Zusammenspiel von physischen und digitalen Aktionen erlangen können. Dies widerspricht sich mit den (nicht-) funktionalen Anforderungen aus Abschnitt 3.2 und 3.3. Zuletzt besteht bei dieser Art allerdings die Notwendigkeit, ein professionelles Angreifer Team zu engagieren

- **Wargames:** Ein Wargame besitzt in diesem Kontext Parallelen zu Jeopardy und wäre zunächst umsetzbar. Allerdings ist der Aspekt der Fortläufigkeit in Bezug auf ein HAW CTF Projekt nicht gegeben. Das zu planende Event muss an einem absehbaren Zeitpunkt enden, was die Umsetzung eines traditionellen Wargames behindern würde

- **HackQuest:** Diese CTF Art wäre in der beschriebenen Form umsetzbar. Zudem besitzt sie einen interessanten Blickwinkel auf die Ressourcen-Problematik. Da Challenges einzeln veröffentlicht werden und für einen begrenzten Zeitraum zur Verfügung stehen, könnte jedes Team eigene Zeiträume für die Bearbeitung erhalten. Allerdings könnte ein solch beschriebenes Verhalten ebenso für Jeopardy in Bezug auf die Ressourcen-Problematik adaptiert werden. Somit gestaltet sich diese Art als eine reduzierte Variante von Jeopardy, welche weniger Challenges beinhaltet. Unterscheiden würden sie sich in diesem Fall dadurch, dass bei HackQuest eine Challenge lediglich einmal zu bearbeiten ist

Nach Betrachtung aller zur Verfügung stehender CTF Arten erscheint Jeopardy als die geeignetste. Dabei kann das für HackQuest beschriebene Verhalten in Bezug auf die Ressourcen-Problematik in Betracht gezogen werden.

Modifizierbare Systeme im Fahrzeug
Anhand der in Abschnitt 3.1 beschriebenen Besonderheiten und Hürden bei Veränderung der Fahrzeugsoftware wird nachfolgend betrachtet, welche Systeme für ein CTF modifiziert werden können.

Wie zuvor beschrieben, sind im Automobil sicherheitskritische Systeme enthalten. Die Qualifikation diese zu modifizieren und die dazu notwendigen Entwicklungswerkzeuge sind allerdings nicht vorhanden. Zudem sind die Ressourcen nicht gegeben diese durch Dritte anpassen zu lassen. Daher sind Veränderungen an diesen Systemen praktisch nicht durchführbar.

Ferner wurde der Einsatz von AUTOSAR Softwareplattformen beschrieben. Innerhalb des CTF Events sollen dabei keine Flags innerhalb dieser Softwareplattform eingebettet werden, damit Challenges ausschließlich Schnittstellen und nicht die Software direkt bedienen. Zwar wäre ein Automobilhersteller spezifisches CTF solcher AUTOSAR Challenges sehr interessant,

was allerdings im Rahmen des HAW CTF Projekts eine vollkommen neue Umgebung für die Teilnehmenden schaffen würde.

Die beschriebenen sicherheitskritischen- und AUTOSAR Systeme könnten durch den in Abschnitt 3.1 beschriebenen Einsatz von DoIP in ein CTF eingebettet werden. Wichtig ist hierbei, dass für sicherheitskritische Systeme die Features von DoIP beachtet werden müssen. Durch diese sind potenzielle Modifikationen am Steuergerät möglich, was allerdings in Bezug auf die Randbedingungen aus Abschnitt 3.4 ein Risiko darstellt.

Zuletzt wurden in Abschnitt 3.1 Möglichkeiten beschrieben, weitere Linux Systeme ins Automobil einzubetten. Diese Möglichkeiten sollten für die technischen Umsetzung des CTF Events in Betracht gezogen werden.

Zielgruppe für das CTF
Wie in Abschnitt 3.3 beschrieben, ist die Definition einer Zielgruppe für ein CTF Event erforderlich. Für das hier betrachtete HAW CTF Projekt wird es sich bei den meisten Teilnehmenden um Studierende handeln, welche ggf. keine oder nur geringe CTF Erfahrungen besitzen. Aus diesem Grund gilt es Challenges zu entwickeln, welche den Teilnehmenden einen leichten Einstieg in die Thematik bieten. Dennoch sollten jene Teilnehmende mit bereits vorhandenen CTF Erfahrungen und solche die während des Events große Fortschritte zeigen, gefordert werden. Für beide Arten sollen, die in Abschnitt 3.3 beschriebenen Anforderungen gelten, dass alle Teilnehmenden durch neues Wissen sowohl Spaß und Motivation an der Teilnahme am CTF haben.

Unterschiedliche Angreifer-Klassen
In Abschnitt 3.1 wurden verschiedene Angreifer-Klassen beschrieben, welche jeweils eigene Perspektiven und ein unterschiedliches Maß an Kontrolle über das Fahrzeug verfügen.

- **Angreifer von außen, Autorisierter Zugang:** Dies sind interessante Perspektiven für ein CTF. Ausgehend von beiden kann in das Fahrzeug eingedrungen werden, wobei dies je nach Perspektive auf unterschiedlichen Wegen geschieht

- **Besitzer des Fahrzeuges, Hersteller & Werkstatt:** Bei diesen Perspektiven besitzen die Angreifenden den Schlüssel zum Fahrzeug und haben ferner Zugriff auf Software Down- und Upgrades. Somit besteht bereits erhöhte Kontrolle über das Fahrzeug, was die Anzahl an Angriffen im Kontext eines CTFs beschränkt

Aufgrund der Eigenschaften der beschriebenen Angreifer-Klassen, sind für ein CTF vor allem die des ersten Punktes interessant. Dazu erfüllen die beiden Angreifer-Klassen jeweils die Funktionalen Anforderungen aus Abschnitt 3.2.

Die Angreifer-Klassen des zweiten Punktes sind für das CTF weniger interessant, da die Teilnehmenden keinen Zugriff auf Down- und Upgrades der Fahrzeugsoftware haben werden. Zudem sollten die Teilnehmenden aus Sicherheitsgründen keinen Zugriff auf den Schlüssel des Fahrzeugs verfügen. Sollte Zugriff auf den Schlüssel bestehen, besteht ein Risiko bezogen auf die Randbedingung aus Abschnitt 3.4.

Je nach Anwendungskontext kann eine oder mehrere Angreifer-Klassen ausgewählt werden.

Storyline für das CTF
In Abschnitt 3.3 wurde beschrieben, dass die Teilnehmenden durch die Bearbeitung des CTFs Motivation erfahren sollen, um so einen intensiveren Lerneffekt zu erhalten. Um dies für die Teilnehmenden bei dem CTF zu ermöglichen, soll eine Storyline entwickelt werden, welche den Verlauf des CTF Events begleitet.

Auswahl von Fahrzeugsystemen für ein CTF
Anhand der in Abschnitt 2.2 beschriebenen Fahrzeug-Domänen soll nun eine Auswahl an Systemen, die für ein CTF geeignet sind, getroffen werden. Dabei müssen die entwickelten Randbedingungen aus Abschnitt 3.4 miteinbezogen und eingehalten werden. Um dies umzusetzen wurden die Abbildungen aus Abschnitt 2.2 herangezogen und entsprechend der Anwendbarkeit von Systemen angepasst. Dabei wurden die Systeme anhand folgender Richtlinien markiert:

- Anwendbare Systeme wurden grün markiert
- Nur unter bestimmten Voraussetzungen anwendbare Systeme tragen eine gelbe Markierung
- Nicht infrage kommende Systeme sind rot durchgestrichen

Nachfolgend werden die Fahrzeug-Domänen betrachtet und die Systeme anhand der zuvor beschriebenen Vorgehensweise bewertet.

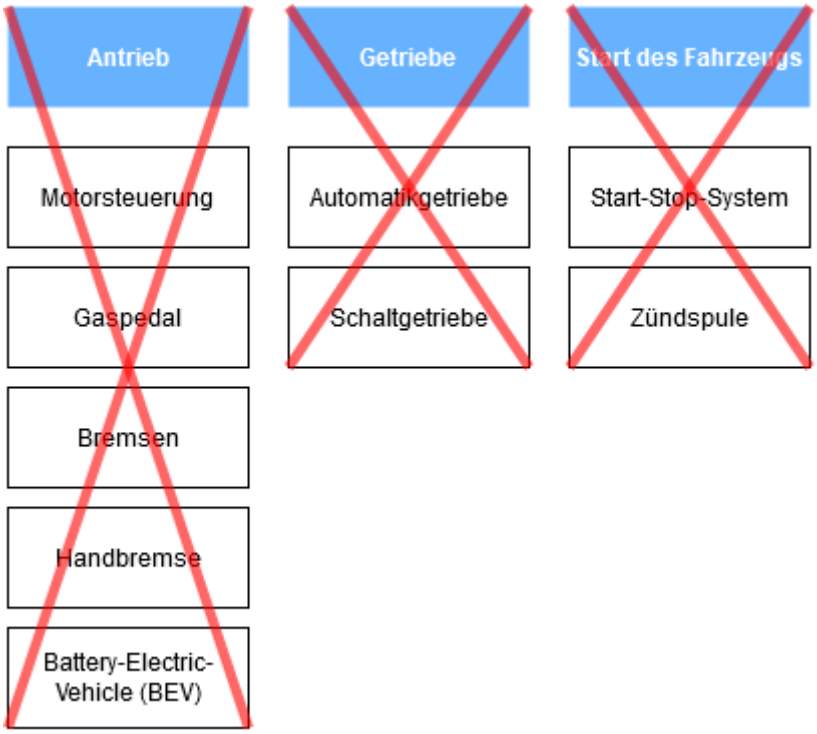

Abb. 3-1: Auswahl von Powertrain Systemen für ein CTF

In Abbildung 3-1 sind die Systeme der Domäne Powertrain dargestellt. Von diesen Systemen kommen für ein CTF keine infrage, da dessen Verwendung in Bezug auf die beschriebenen Randbedingungen ein Risiko bergen. Da diese Domäne sicherheitskritische Systeme beinhaltet, welche unter anderem für den Start des Fahrzeuges zuständig sind, muss sichergestellt sein, dass dieser Vorgang weder aus Versehen noch gewollt möglich wird. Ferner besteht die Möglichkeit, beim Hacken des Akkus oder dessen Stromkreisen einen Brand oder eine Explosion auszulösen die unkontrolliert ausarten und Sach- wie Personenschäden verursachen kann. Diese Risikoquelle zu eliminieren hat oberste Priorität.

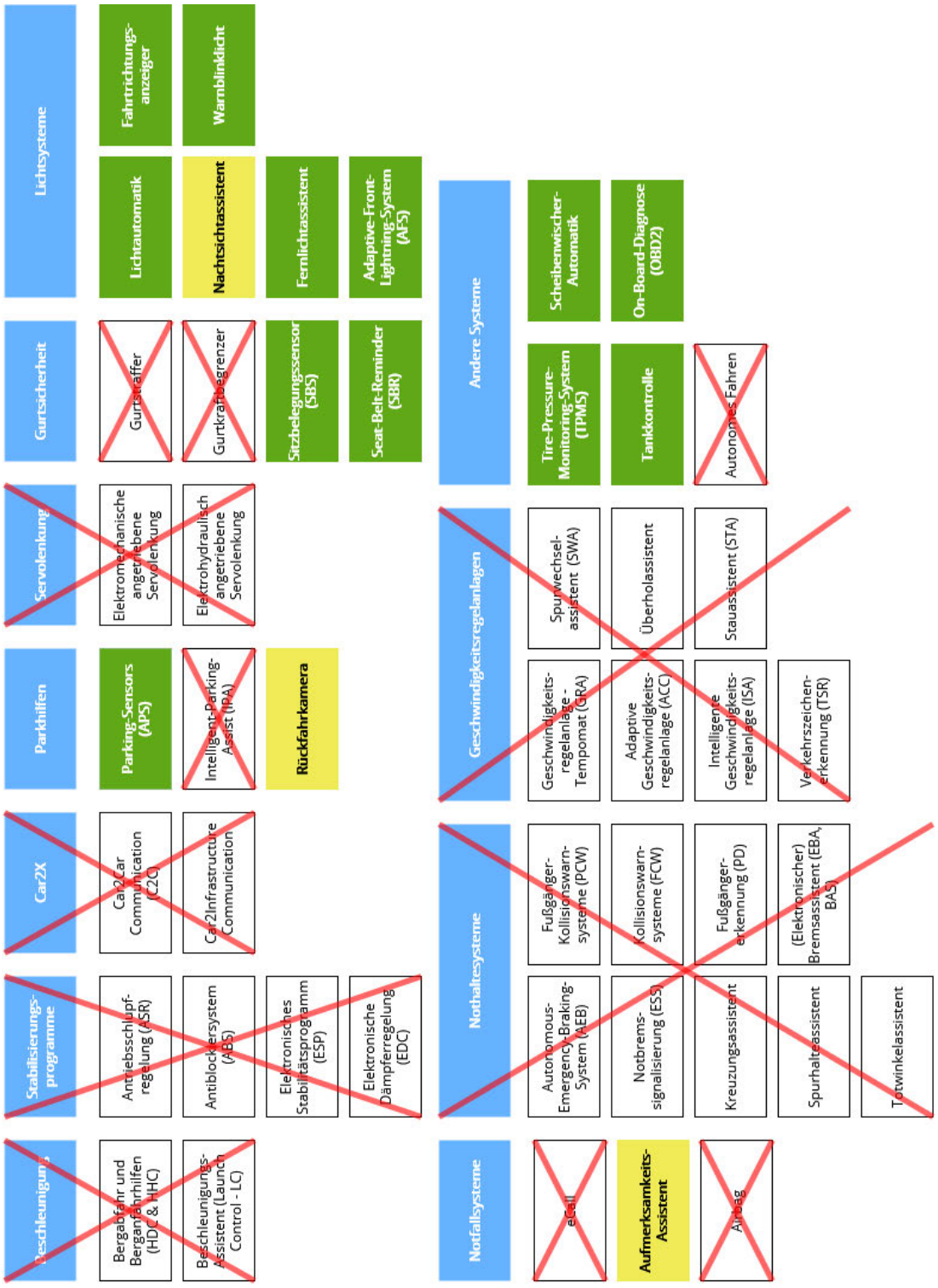

Abb. 3-2: Auswahl von Vehicle-Motion / Chassis & Safety Systemen für ein CTF

In Abbildung 3-2 werden die Systeme der Domäne Vehicle-Motion / Chassis & Safety dargestellt. Auch hier kommen etliche Systeme nicht infrage, da die Verwendung in Bezug auf die Randbedingungen ebenfalls ein Sicherheitsrisiko darstellen. Für die Einbindung der gerade ausgeschlossen Systeme, müsste das bereitgestellte Fahrzeug bereits vom Hersteller oder Forschungspartner nach CTF Vorgaben präpariert werden.

Allerdings bleibt eine kleine Auswahl anwendbarer Systeme bestehen, sowie solcher die nur unter bestimmten Voraussetzungen Anwendung finden können. Jene Systeme, dir nur unter bestimmten Voraussetzungen Anwendbar sind (in der Grafik gelb markiert), sind aufgrund des zur Verfügung gestellten Fahrzeuges mit dem Entwurf eines CTF in Einklang zu bringen.

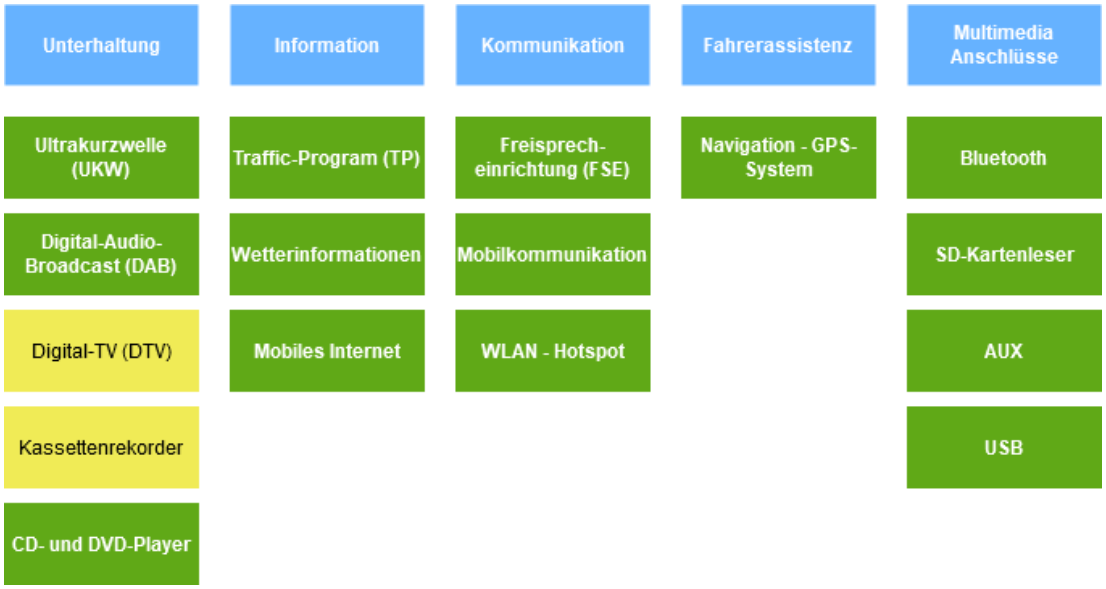

Abb. 3-3: Auswahl von Infotainment Systemen für ein CTF

In Abbildung 3-3 werden Systeme der Domäne Infotainment verdeutlicht. Von diesen sind für ein CTF alle anwendbar. Zwei der zuvor genannten Systeme können nur unter der Vorrausetzung Anwendung finden, dass diese im bereitgestellten Automobil enthalten sind. Es ist davon auszugehen, dass die technische Ausführung des bereitgestellten Automobils keinen Kassettenrekorder oder Digital-TV beinhaltet.

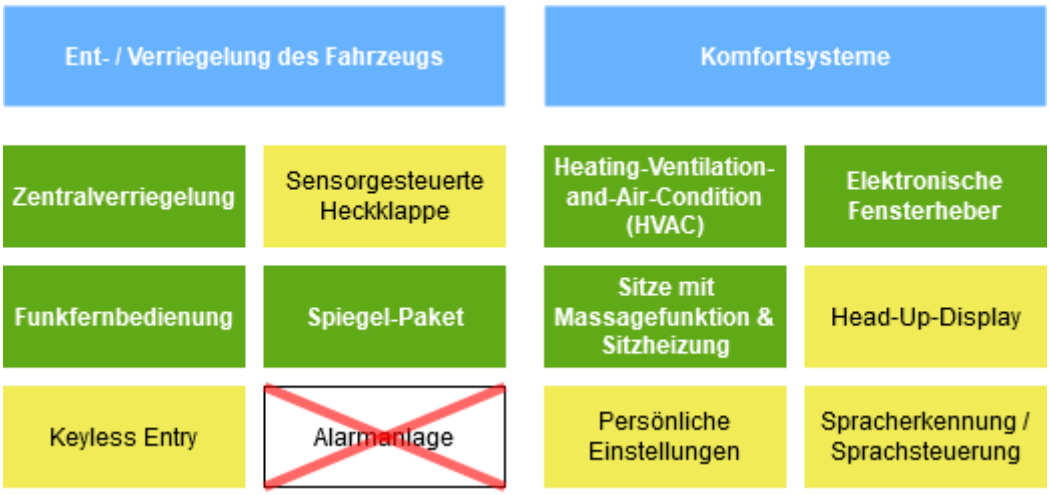

Abb. 3-4: Auswahl von Body & Comfort Systemen für ein CTF

In Abbildung 3-4 werden die Systeme der Domäne Body & Comfort beschrieben. Sollte eine Alarmanlage verbaut sein kann diese nicht zur Anwendung kommen, da sie ein Risiko in Bezug zu den Randbedingungen darstellt. Eine Ausnahme würde auch hier die Präparierung durch den Hersteller oder Forschungspartner ergeben. Alle anderen Systeme können bedenkenlos Anwendung finden, wobei auch hier bei einigen die Voraussetzung erfüllt werden muss, dass das bereitgestellte Automobil diese in der technischen Ausführung enthält.

Letztlich muss der Sachverhalt zu den modifizierbaren Systemen im Fahrzeug aus Abschnitt 3.5 herangezogen werden. Es wurde entschieden, dass sicherheitskritische Systeme im Automobil nicht modifiziert werden sollen. Allerdings könnten einzelne Steuergeräte unter der Prämisse Anwendung finden, dass die dafür benötigte DoIP Schnittstelle vorhanden und betriebsbereit ist. Des Weiteren gilt zu prüfen, ob die Umsetzbarkeit sowie der Umfang der zu verwendenden Systeme im Einklang mit dem geplanten CTF stehen.

4 Entwurf eines CTF Events

4.1 Organisation des CTF Events

Die Organisation des CTF Events wird in den drei Phasen: Vorbereitung, Durchführung und Nachbereitung abgehandelt. In diesen Phasen soll das Event auf der Meta-Ebene anhand Automobil- und CTF spezifischer Anforderungen betrachtet werden.

Vorbereitung
Die Vorbereitung für das CTF Event wird anhand nachfolgender Punkte beschrieben:

- **Das Automobil muss bereitgestellt werden:** Damit das Event stattfinden kann, muss zunächst das physische Automobil zur Verfügung stehen. Zudem muss ein geeigneter Standort gewählt werden

- **Die Flags müssen in das Automobil eingebaut werden:** Sobald das Automobil zur Verfügung steht, muss dieses für das CTF Event vorbereitet werden. Für die technische Umsetzung zur Gestaltung des CTFs können wie in Abschnitt 3.5 beschrieben zusätzliche Systeme in das Automobil eingebettet werden. Der wichtigste Aspekt richtet sich hierbei auf das Einfügen aller erarbeiteten Flags

- **CTF Briefing für Teilnehmende bereitstellen:** Bevor das Event stattfindet muss dieses beworben werden, sodass ausreichend Informationen für mögliche Interessenten zur Verfügung stehen. Dazu sollte im vorherigen Semester der Grundstein gelegt werden. Dies kann in Form einer Webseite für das Projekt, E-Mails im Semesterverteiler sowie durch Erwähnungen oder Kurzpräsentationen während mehrerer Vorlesungen geschehen

- **Entscheidung für eine Angreifer-Klasse:** Um das Lernergebnis zu maximieren sollte die Aufgabenstruktur weniger komplex gestaltet sein, um die Zugänglichkeit für die in Abschnitt 3.5 definierte Zielgruppe zu erhöhen. Dies kann besonders gut bei der Verwendung der Angreifer-Klasse Autorisierter Zugriff umgesetzt werden, da diese

am ehesten eine gewohnte Ausgangsposition darstellt. Da eine solche Modellierung ebenso im Sinne der in Abschnitt 3.3 beschriebenen Nicht-funktionalen Anforderungen ist, ist die Verwendung der Autorisierten Angreifer-Klasse zu empfehlen

- **Der Umgang mit der Ressourcen-Problematik:** Wie in Abschnitt 3.5 beschrieben, muss für unseren Kontext die Entstehung einer Chancengleichheit sichergestellt werden, durch eine Lösung der Ressourcen-Problematik. Diese Lösung muss auf die CTF Art Jeopardy zugeschnitten sein, da sie für die Konzipierung des Events zuvor ausgewählt wurde. Dazu kann ein weiterer Auszug aus Abschnitt 3.5 herangezogen werden welcher beschreibt, dass das für HackQuest beschriebene Verhalten in Bezug auf die Ressourcen-Problematik auch für die Art Jeoapardy adaptiert werden kann. Nachfolgend wird die erarbeitete Lösung beschrieben.

  Damit der Ressourcen-Problematik entgangen wird, soll jedes Team bei Arbeiten an der begrenzten Ressource Automobil dies in jeweils reservierten Zeitslots tun. Dabei sollen Reservierungen in Zyklen vergeben werden, sodass jedes Team je Zyklus dieselben Chancen einer Reservierung besitzt. So soll verhindert werden, dass der Vorgang der Reservierung ausnutzbar wird und Teams durch die mehrfache Reservierung innerhalb eines Zyklus andere Teams die Möglichkeit der CTF Bearbeitung nehmen. Beim Reservierungsvorgang soll zudem das First-Come-First-Serve Prinzip Anwendung finden. Nachdem ein Zeitslot beendet wurde müssen die Systeme des Automobils einem Reset unterzogen werden, sodass das nächste Team bei der Bearbeitung dieselben Vorrausetzungen wie das vorherige Team vorfindet.

  So kann die Kollision zwischen verschiedenen Teams verhindert werden, wobei die Frage bleibt, ob Kollisionen ebenso innerhalb desselben Teams auftreten können. Tatsächlich wären solche Kollisionen nicht allzu schwerwiegend. Sollte ein Team mit mehreren Teilnehmenden unwissend an derselben Challenge arbeiten, kann es zu Kollisionen kommen, welche die Arbeiten behindern würden. Dies kann allerdings durch eine geeignete Einführung durch die Organisierenden erklärt und durch eine entsprechende Koordination und Kommunikation innerhalb eines Teams umgesetzt werden.

  In Bezug auf Jeopardy muss noch Betrachtung finden, wie Punkte während des Events berechnet werden. Wie in Abschnitt 2-1 beschrieben, werden den ersten drei Teams, die eine bestimmte Challenge absolvieren erhöhte Punktzahlen angerechnet. Dazu könnte die Eintragung von Punkten ins Score-Board auf das Ende eines Zyklus verschoben werden. Ab Beginn eines Zeitslots soll dazu die Zeit bis zur Einreichung einer Flag aufgezeichnet werden. Am Ende eines Zyklus werden dann die diese Zeiten der verschiedenen Teams verglichen und dementsprechend das Score-Board aktualisiert. Die Motivation eines Echtzeit Score-Boards geht so nicht gänzlich

verloren, sondern wird lediglich an das Ende der jeweiligen Zyklen verschoben. Es würde zudem keinen Sinn ergeben, Punkte bereits während gerade stattfindenden Zyklen ins Score-Board aufzunehmen, denn auf diese Art hätten die Teams bereits die Möglichkeit Ergebnisse von eingetragenen Teams im Score-Board abzugleichen um ihre eigenen Vorgehensweisen zu optimieren.

Durchführung
Die Durchführung für das CTF Event wird anhand nachfolgender Punkte beschrieben:

- **Die Betriebssicherheit des Automobils:** Es muss jederzeit sichergestellt sein, dass die Betriebssicherheit des Automobils bestehen bleibt. Dazu sollte während der CTF spezifischen Arbeiten am Automobil eine verantwortliche Person diese überwachen

- **Startschuss:** Es soll ein klar vorgegebener Start des Events signalisiert werden. Davor darf das Automobil unter keinen Umständen durch die Teilnehmenden genutzt werden

- **Warnsignal:** Es soll eine Art Warnsignal herangezogen werden, welche alle bearbeitenden Teilnehmenden wahrnehmen und aufgrund dessen alle derzeit laufende Arbeiten am Automobil einstellen

- **Schlussschuss:** Sobald das Event endet, muss diese Phase ebenso klar signalisiert werden, sodass alle Arbeit am Automobil sofort zu beenden sind

- **Weitere Sicherheitsmaßnahmen:** Um die Durchführung des Events noch sicherer zu gestalten, können weitere Sicherheitsmaßnahmen herangezogen werden. Ein Beispiel dafür wäre, dass im Falle eines Automobils mit Verbrennungsmotor der Tank vor Start des Events geleert wird

- **Durchführung von Jeopardy:** Die Arbeitsweise dieser CTF Art bleibt so wie sie traditionell beschrieben ist. Die Teilnehmenden können anhand einer Auswahl an Challenges Flags erlangen und diese gegen Punkte einlösen

Nachbereitung
Die Nachbereitung für das CTF Event wird anhand nachfolgender Punkte beschrieben:

- **Lesson Learned:** Nachdem das Event beendet wurde, sollen die umgesetzten Aspekte in Bezug auf die besondere Ressource Automobil reflektiert werden. Dies bezieht sich beispielsweise auf die ausgewählte CTF Art oder allgemeiner auf das Automobil als Angriffsziel

- **Flags wieder ausbauen:** Die ins Automobil eingebrachten Flags müssen wieder entfernt werden

- **Fahrzeugrückführung:** Das Automobil muss in demselben Zustand wie bei Erhalt und betriebsbereit wieder an den Forschungspartner zurückgegeben werden

4.2 Storyline

In Abschnitt 3.5 wurde beschrieben, dass für das CTF Event eine Storyline kreiert werden soll. Anhand dieser Storyline wird das CTF Event ab Beginn durch einen Handlungsstrang begleitet, welcher den Teilnehmenden in Verbindung mit den Challenges einen motivierenden Kontext bietet. Des Weiteren beschreibt die Storyline zu welchen Zeitpunkt Challenges eines bestimmten Charakters und einer bestimmten Schwierigkeit geplant sind. Somit wird der Ablauf des CTF Events durch die Storyline bestimmt. Dabei soll die in Abschnitt 3.5 bestimmte Zielgruppe berücksichtigt werden, sowie das Automobil als die begrenzte Ressource, die es darstellt. Natürlich spielt bei der Kreierung und Strukturierung der Storyline die Auswahl der CTF Art Jeopardy eine übergeordnete Rolle.

Damit die Storyline diesen Anforderungen gerecht wird, wird sie in vier nacheinander folgenden Phasen aufgeteilt. Diese Phasen sollen sich durch die folgenden Punkte auszeichnen:

- Innerhalb einer Phase werden den Teilnehmenden mehrere Challenges aus unterschiedlichen Bereichen der Informationssicherheit zur Verfügung gestellt. Diese werden wie für ein Jeopardy CTF üblich dargestellt. Sobald eine Phase zu 90% absolviert wurde, kann das jeweilige Team mit der nächsten Phase fortfahren

- Challenges einer bestimmten Schwierigkeit werden einer der vier Phasen zugeteilt, wobei sich die Phasen aufsteigend schwieriger gestalten

- Damit die begrenzte Ressource des Automobils anfänglich nicht überlastet wird und sich die Teilnehmenden an die Bearbeitung eines CTFs und an die Umgebung des Automobils langsam gewöhnen, sollen Challenges in der ersten Phase vorwiegend in einer virtuellen Umgebung absolviert werden. Im Laufe der Storyline werden die Challenges zunehmend häufiger im physischen Automobil stattfinden

- Die im Abschnitt 4.1 entschiedene und umzusetzende Angreifer-Klasse „Autorisierter Zugriff“ soll in der Storyline Anwendung finden

Da es sich um ein CTF im Automobil handelt, könnte eine Storyline analog zur US-amerikanischen Fernsehserie Knight-Rider aufgebaut werden. Die Teilnehmenden schlüpfen

in die Rolle von Michael Knight und kämpfen gemeinsam mit dem intelligenten und sprechenden Auto K.I.T.T. für Gerechtigkeit. Auf ihrer Reise wird K.I.T.T.s Software infiltriert, wodurch das Auto „böse“ wird. Die Teilnehmenden müssen aktiv werden und das Auto hacken, um Schaden an der Menschheit zu verhindern.

Natürlich können nicht die originalen Namen der Fernsehserie genutzt werden. Allerdings können diese leicht abgewandelt werden, um so Namensrechtskonflikte zu vermeiden:

- **Michael Knight** ➔ Michelle Day
- **K.I.T.T.** ➔ S.K.I.D. (Side Kick Intelligence by Day)

Nachfolgend werden die einzelnen Phasen beschrieben und die jeweiligen Handlungsstränge dargelegt.

Part_01: Tutorial
„Michelle hat in dieser Woche das intelligente und sprechende Auto S.K.I.D. als neuen Partner zugewiesen bekommen. Damit die beiden miteinander warm werden und Michelle nicht aus Versehen den Schleudersitz mit dem Scheibenwischer verwechselt, muss sie erstmal unter die Haube schauen.“

In dieser Phase ist das Ziel, die Umgebung des Automobils und wichtige Werkzeuge für das CTF kennenzulernen (z. B. CAN, Linux-Basics oder die Netzwerk-Topologie des Automobils). Nachdem die Teilnehmenden eine kurze Einführung zum Handlungsstrang gelesen haben, sollen einfache Challenges gelöst werden. Es werden in dieser Phase keine Angriffe ausgeführt da es lediglich um die Informationsgewinnung geht.

Aufgrund der begrenzten Ressource des Automobils und des Tutorial Charakters der Phase, sollten Challenges dieser Phase innerhalb einer skalierbaren Virtualisierung der Fahrzeugarchitektur stattfinden. Die erste Station für die Teilnehmenden ist somit ein Welcome-Server, auf dem ihnen anhand geeigneter Challenges die Umgebung des Automobils und allgemeine Werkzeuge für die Bearbeitung eines CTFs gezeigt werden. Damit der direkte Bezug zum physischen Automobil hergestellt wird, soll mindestens eine Challenge existieren, welche direkt am Fahrzeug stattfindet aber keine Ressource des Fahrzeugs verbraucht (z. B. ein Kamera Stream). Diese Phase ist an keinen zeitlichen Zyklus gebunden.

Innerhalb dieser Phase können den Teilnehmenden Hinweise für Challenges gegeben werden. In Bezug auf die Handlung werden diese vom sprechenden S.K.I.D. gegeben und beziehen sich auf zu verwendende Tools für die jeweiligen Challenges.

Part_02: Strangerer Things
„Bei dem ersten gemeinsamen Auftrag von Michelle und S.K.I.D. müssen die beiden in Erfahrung bringen was es mit dem Verschwinden von Dr. Itzenplitz auf sich hat. Er war einst ein weltweit bekannter Wissenschaftler und hat im Fachbereich Informatik für einige Durchbrüche gesorgt. Allerdings ist er vor zwei Jahren spurlos verschwunden. Nach den neusten Ermittlungen soll Dr. Itzenplitz in Begleitung von mehreren zwielichtigen Gestalten gesichtet worden sein. Michelle und S.K.I.D. sind diesen zwielichtigen Gestalten bis zu ihrem vermutlichen Stützpunkt gefolgt.

Als Michelle nun vor dem Stützpunkt steht lässt sie S.K.I.D. zurück und schleicht sich in das Gebäude. Nach einiger Zeit ist es ihr gelungen, Dr. Itzenplitz zu finden und versucht ihn aus dem Stützpunkt hinaus zu begleiten. Der Doktor ist zwar sehr geschwächt, kann aber auf dem Weg nach draußen erzählen, dass er aufgrund seines umfangsreichen Wissens entführt wurde, um für den Mafia Boss Mr. Mean zu arbeiten. Kurz bevor sie bei S.K.I.D. ankommen sieht Michelle wie mehrere Personen sich an S.K.I.D. zu schaffen machen. Michelle kann sie zwar in die Flucht schlagen, allerdings antwortet S.K.I.D. ihr nun nicht mehr. Die Monitore im Auto zeigen ebenfalls merkwürdige Dinge und die Lichter spielen verrückt. Nun liegt es an Michelle, mithilfe des geschwächten Doktors und seinen Ratschlägen das Problem zu lösen."

Nachdem die erste Phase absolviert wurde, werden nun anspruchsvollere Challenges zur Verfügung gestellt. Diese finden noch immer innerhalb der Virtualisierung statt, wobei nun Angriffe ausgeführt werden und keine reine Informationsgewinnung betrieben wird. Auch in dieser Phase soll der direkte Bezug zum physischen Automobil beibehalten werden weshalb es hier mindestens zwei Challenges am Fahrzeug geben soll. Während dieser Challenges sollen erstmals Zeitslots und somit eine Ressource des Automobils beansprucht werden.

Den Teilnehmenden können in Bezug auf die Handlung wieder Hinweise geben werden, wobei diesen Part nun Dr. Itzenplitz übernimmt. Er kennt sich gut im Fachbereich aus, ist aber zu geschwächt um selbst zu handeln. Mit seiner Hilfe wird das seltsame Verhalten im Auto lokalisiert und in Form von Angriffen behoben.

Part_03: S.K.I.D. bekämpfen
„Gemeinsam mit dem Doktor hat sich Michelle durch S.K.I.D.s System gearbeitet. Da der Doktor umfangreiches Wissen in diesem Fachbereich aufweist, wurde sie seinerseits immer wieder in die richtige Richtung gelenkt. Als sie die scheinbar letzte Fehlfunktion behoben haben, arbeitet die Anzeige von S.K.I.D. wieder normal. Doch plötzlich beschleunigt das Fahrzeug selbstständig und erhöht stätig die Geschwindigkeit.

Der Doktor fängt zu lachen an und erzählt, wie jeder gute Bösewicht, von seinem Masterplan. Er hatte sein Verschwinden inszeniert und darauf abgezielt S.K.I.D. in seine Hände zu bekommen, um ihn für seine Zwecke umzuprogrammieren.

Michelle kann den Doktor mit einem gezielten Schlag außer Gefecht setzen, allerdings sitzt sie nun in einem umprogrammierten S.K.I.D. welcher noch immer mit steigender Geschwindigkeit seine Irrfahrt fortsetzt. Michelle muss schnell handeln damit sie alles was sie mithilfe des Doktors an S.K.I.D. geändert hat wieder rückgängig machen kann. Damit sie dies bewerkstelligen kann, sollte sie zunächst versuchen S.K.I.D. anzuhalten."

In dieser Phase findet keine Challenge innerhalb der Virtualisierung statt, sondern innerhalb des physischen Automobils. Insofern die Möglichkeit besteht kann parallel zum Fahrzeug ein Tischaufbau in Betracht gezogen werden. Dieser würde es ermöglichen, dass während eines Zeitslot, zwei Teams zur selben Zeit Challenges bearbeiten. Allerdings kann ein Tischaufbau nur Challenges umsetzen, welche einen durchgehend digitalen Charakter besitzen.

In Bezug auf die Handlung können Hinweise für Challenges von S.K.I.D. gegeben werden. Hin und wieder ist er trotz der von Dr. Itzenplitz unterzogenen Manipulierung in der Lage, Nachrichten an Michelle zu senden. Somit unterstützt S.K.I.D. ein wenig und kann versuchen den Blick in die korrekte Richtung zu weisen.

Part_04: Rettung von S.K.I.D.
„Nach einer Weile hat es Michelle geschafft S.K.I.D. anzuhalten. Sofort ruft sie nach Verstärkung, um den Doktor festnehmen zu lassen. Während sie diese Aufgabe der Verstärkung überlässt, muss sie sich um die Bereinigung von S.K.I.D. kümmern."

In dieser Phase wird auch direkt am physischen Automobil gearbeitet. Somit gestaltet sich die Bearbeitung dieser Phase sehr ähnlich wie die vorherige. Lediglich der Schwierigkeitsgrad soll weiter erhöht werden.

4.3 Umgang mit Challenges

Bezüglich der in Abschnitt 3.5 definierten Auswahl der im CTF nutzbaren Systemen und der in Kapitel 4 kreierten Storyline sowie der darin einbezogenen Angreifer-Klasse Autorisierter Zugriff, werden nachfolgend Flags entwickelt. Für diese werden anschließend Challenges beschrieben und den Phasen der Storyline zugeordnet.

4.3.1 Möglichkeiten für Flaggen im „Auto"

Nachfolgend finden sich die Möglichkeiten der Erkennung erfolgreich abgeschlossener Flags:

- Flaggen können bei Erreichung einer physischen Reaktion automatisch dem CTF System übermittelt und eingetragen werden

- Es wird Personal benötigt, welches prüft ob eine Challenge mit physischer Reaktion gelöst wurde und dem Team jeweils die Flags einträgt

- Flags werden den Teilnehmenden in physischer/digitaler Form bei Absolvierung einer Challenge dargestellt

Um den Ablauf des CTF Events für die Teilnehmenden so unkompliziert wie möglich zu gestalten, sollten unterschiedliche Arten der Erkennung von Flags unterlassen werden. In diesem Zusammenhang sind die ersten beiden Punkte lediglich auf die Absolvierung physischer Challenges anzuwenden. In einer digitalen Umgebung wird ein offensichtliches Zeichen benötigt, welches den Teilnehmenden signalisiert, dass sie ihr Ziel erreicht haben. Da die dritt beschriebene Darstellungsart dem entspricht, sollte diese zur Anwendung kommen. In Ausnahmefällen dürfen allerdings auch andere Erkennungsmerkmale herangezogen werden können, falls die dritt beschriebene Darstellungsart Hindernisse aufweist oder aus sonstigen Gründen nicht geeignet scheint. Dies sollte den Teilnehmenden in solch einem Fall kommuniziert werden.

Die Flags benötigen ein einheitliches Format der Darstellung. Dieses kann wie folgt aussehen:

- car{c4r_h4ck7n6_7s_fvn}

Dabei stellt der Inhalt zwischen den geschweiften Klammern die Flag dar, welche für jede Challenge individuell ist. Die restliche Darstellung stellt ausschließlich die Formatierung der Flag Erkennung dar.

Nachfolgend werden Möglichkeiten beschrieben, Flags für Challenges im Automobil einzubetten.

Physische Flags
An dieser Stelle werden die physischen Flags beschrieben, welche im Automobil platziert werden:

- Abblendlicht aktivieren

- Tankdeckel öffnen

- Hupe aktivieren

- Sitzheizung aktivieren

- Kofferraum öffnen

- Klimaanlage auf erforderliche Temperatur manipulieren

- Radio auf eine erforderliche Frequenz stellen

Digitale Flags
An dieser Stelle werden die digitalen Flags beschrieben, welche im Automobil platziert werden:

- Aktivieren des Navigationssystems zu bestimmten Koordinaten
- Routing-Tables: Die vergessene Route
- Per Secure-Shell (SSH) auf den Welcome-Server zugreifen
- Automobil Handbuch als PDF oder E-Book lesen
- Bild der Netzwerk-Topologie des Automobils mit versteckter Flag
- Zugriff auf die im Welcome-Server liegende Datenbank erhalten
- Vom Welcome-Server aus Zugriff auf eine weitere externe Datenbank verschaffen
- CAN-Bus Telemetrie lesen
- CAN-Bus Paket modellieren
- Angesteckten USB-Stick im Automobil ausfindig machen

4.3.2 Einordnung der Challenges in die Storyline

In Bezug auf die in Abschnitt 4.2 beschriebene Storyline des CTF Events werden anbei für die unterschiedlichen Flags Challenges kreiert und den unterschiedlichen Storyline Phasen entsprechend deren Anforderungen zugeordnet.

Part_01

- Per Secure-Shell (SSH) auf den Welcome-Server zugreifen
    - Die Teilnehmenden sollen sich auf den ersten Server per SSH verbinden und bekommen im Terminal bei erfolgreicher Verbindung eine Flag angezeigt
- Automobil Handbuch als PDF oder E-Book lesen
    - Auf dem Welcome-Server der virtuellen Automobilumgebung soll ein Automobil-Handbuch den Teilnehmenden zu Verfügung stehen. Dieses kann

gelesen werden, wobei in dem Dokument in Base64 kodiert eine Flag untergebracht ist

- Bild der Netzwerk-Topologie des Automobils mit versteckter Flag
  - Auf dem Welcome-Server ist ebenso ein digitales Bild der Netzwerk-Topologie des Automobils enthalten. In den EXIF Metadaten ist eine Flag versteckt

- Kofferraum öffnen
  - Die Teilnehmenden können zum Automobil gehen und den Kofferraum manuell öffnen. Im Kofferraum ist eine Flagge physisch versteckt und auf einem Zettel dargestellt. Dieser Zettel befindet sich hinter der Verbandtasche

Part_02

- Zugriff auf die im Welcome-Server liegende Datenbank erhalten
  - Auf dem Welcome-Server ist eine Datenbank enthalten, für deren Abfrage ein Passwort notwendig ist. Der Zugriff auf die Inhalte soll per SQL Injection erfolgen, wobei eine Flag zurückgegeben wird

- Vom Welcome-Server aus Zugriff auf eine weitere externe Datenbank verschaffen
  - Mit einem Brute-Force Angriff soll das Passwort für eine externe Datenbank herausgefunden werden. Das hier genutzte Passwort befindet sich in der Passwort-Sammlung rockyou.txt. In den Tabellen der Datenbank befindet sich ein Eintrag mit einer Flag

- CAN-Bus Telemetrie lesen
  - Ein CAN-Bus muss mithilfe eines bereitgestellten Service ausgelesen werden. Einer der enthaltenen Nachrichten enthält die Flag, welche mit ROT13 verschlüsselt ist

- Angesteckten USB-Stick im Automobil ausfindig machen
  - Im Automobil ist ein USB-Stick versteckt. Dieser muss im Netzwerk ausfindig gemacht werden. Auf ihm ist eine Textdatei mit einer Flag enthalten

- Radio auf eine erforderliche Frequenz stellen
  - Aus unmittelbarer Nähe wird auf einer zuvor definierten Frequenz eine präparierte Nachricht in Morse-Code gesendet. Diese lässt sich in die Karosserienummer übersetzen. Dies soll ein Hinweis darstellen, welcher darauf hindeutet, dass der Motorraum geöffnet werden soll. An der

Innenseite der Motorhaube befindet sich ein Zettel mit einer Flag Beschriftung

Part_03

- CAN-Bus Paket modellieren
  - Es muss ein CAN-Bus Paket selbst modelliert werden, welches mithilfe eines bereitgestellten Service auf einen CAN-Bus gesendet werden kann. Wenn das Paket den korrekten Inhalt hat, wird eine Flag zurückgesendet

- Hupe aktivieren
  - Statt die übliche Signalhupe zu aktivieren erfolgt zur Ausweisung der Flag eine Code-Ansage zur Einlösung von Punkten

- Routing-Tables: Die vergessene Route
  - Im Automobil ist ein Routing-Table enthalten, welcher eine vergessene Route beinhaltet. Diese enthält eine auszulesende Flag

- Aktivieren des Navigationssystems zu bestimmten Koordinaten.
  - Bei Erfolg Weiterleitung eines Codes an das Handy des Teilnehmenden

Part_04

- Tankdeckel öffnen
  - Wenn der Tankdeckel geöffnet wurde, befindet sich im inneren eine Flag in Form eines Zettels mit Beschriftung

- Abblendlicht aktivieren
  - Die Flag Umsetzung in Form eines QR-Codes, welcher durch das Licht an eine Wand gestrahlt wird

- Radio auf eine erforderliche Frequenz stellen
  - Aus unmittelbarer Nähe wird auf einer zuvor definierten Frequenz eine präparierte Nachricht in Morse-Code gesendet. Diese lässt sich in die Karosserienummer übersetzen. Dies soll ein Hinweis darstellen, welcher darauf hindeutet, dass der Motorraum geöffnet werden soll. Daran befindet sich ein Zettel mit einer Flag beschriftet am inneren der Motorhaube

- Klimaanlage auf erforderliche Temperatur manipulieren
  - Die Klimaanlage muss 25° erreichen. Dafür muss das Heating-Ventilation-and-Air-Condition System modifiziert werden, sodass die erforderliche Temperatur erkannt wird und sich auf dem Display die angezeigte Temperatur in eine Flag ändert

- Sitzheizung aktivieren
    - Am Fahrersitz ist ein Zettel befestigt, welcher mit einer hitzeempfindlichen Tinte beschriftet ist. Diese ist bei Raumtemperatur nicht sichtbar, kann aber gelesen werden sobald die Sitzheizung aktiviert wurde. Auf diese Art kann von dem Zettel eine Flag abgelesen werden

5 Fazit & Ausblick

5.1 Zusammenfassung

Damit an der Hochschule für Angewandte Wissenschaften (HAW) Hamburg ein wählbares Capture-the-Flag (CTF) Projekt mit einem Automobil im Fokus veranstaltet werden kann, wurde ein Konzept für dessen Umsetzung benötigt. Dazu wurde die Problematik beschrieben, dass ein Automobil eine besondere Ressource darstellt, welche nicht ohne weiteres durch mehrere Gruppen gleichzeitig angreifbar ist. Um diese Problematik zu lösen, sollte am Beispiel der Integration eines Automobils in eine CTF-Umgebung ein Leitfaden erarbeitet werden, wie diese und ähnliche Ressourcen sinnvoll für ein CTF behandelt werden können.

Nachdem das Automobil in Bezug auf die Integration in eine CTF-Umgebung als besondere Ressource analysiert wurde, wurden Anforderungen und Randbedingungen entwickelt, die für ein solches CTF zu berücksichtigen sind. Weiterhin musste beachtet werden, dass die Systeme eines Fahrzeugs sicherheitskritische Aufgaben erfüllen. Es mussten also Flags gefunden werden, die eine Beschädigung des Fahrzeugs ausschließen sowie die Betriebszulassung erhalten. Für die Konzipierung eines solchen CTFs war es elementar abzustimmen, welche Art für ein Automobil optimal ist. Nach Betrachtung aller zu Verfügung stehender CTF Arten fiel die Entscheidung letztlich auf die CTF Art Jeopardy, da sich das Konfliktpotential im Ablauf am geringsten auswirkt. Anhand dieser Wahl konnte ebenso eine Lösung zu der zuvor beschriebenen Ressourcen-Problematik erarbeitet werden. Die ausgearbeitete Lösung trägt zur Verantwortung bei, die Durchführung von Challenges ohne Kollisionen bezogen zur Ressourcen-Problematik auszuführen. Des Weiteren bietet sie den Teilnehmenden Teams die gleichen Ausgangsbedingungen wodurch Chancengleichheit innerhalb des Wettbewerbs geschaffen wird. Um die nicht vervielfältigbare Ressource Fahrzeug optimal bearbeiten zu können wurden Zeitslots geschaffen, dessen Vergabe in Zyklen stattfindet. Die Teams haben die Möglichkeit innerhalb eines Zyklus einen Zeitslot zu reservieren.

Der organisatorische Ablauf des CTF Events wurde definiert und dessen Ausführung in drei Phasen: Vorbereitung, Durchführung und Nachbereitung geplant. In den jeweiligen Phasen wird das CTF Event auf der Meta-Ebene anhand Automobil- und CTF spezifischer Anforderungen betrachtet.

Der inhaltliche Ablauf des CTF Events wurde basierend auf der Auswahl der CTF Art und der Lösung der Ressourcen-Problematik, anhand einer kreierten Storyline definiert. Diese bietet den Teilnehmenden einen Handlungsstrang, welcher sie bei der Bearbeitung der Challenges begleitet und einen motivierenden Kontext bietet. Des Weiteren bestimmt sie die Anordnung von Challenges anhand ihrer Schwierigkeit und potenzieller physischer Eigenschaften in Bezug auf die begrenzte Ressource Automobil. In Betrachtung der stattfindenden Challenges sowie der Zielgruppe mussten Angreifer Klassen definiert werden, welche im Anschluss auf eine tatsächlich anzuwendende Angreifer Klasse festgelegt wurde. Um die Challenges sowie die Zielgruppe gepaart mit der Schwierigkeit in Einklang zu bringen, wurde die Entscheidung zugunsten der Angreifer Klasse Autorisierter Zugriff getroffen.

Parallel zur Storyline wurden Flags und die dazugehörigen Challenges entwickelt, welche in das Automobil verbaut werden sollen. Deren Erarbeitung orientierte sich an der zuvor definierten Auswahl von Systemen im Automobil, sowie der Angreifer-Klasse Autorisierter Zugriff. Die Flags und deren zugehörige Challenges wurden mit der Storyline abgeglichen.

5.2 Ausblick

Für die beschriebene Ressourcen-Problematik konnte in dieser Arbeit eine Lösung erarbeitet werden. Folglich ist der nächste Schritt die praktische Umsetzung der Lösung in einem CTF. Damit sich der Fokus bei der technischen Umsetzung eines CTFs an der jeweils aufkommenden Herausforderungen ausrichtet, kann eine allgemeine und bis zu einem gewissen Maße sichere Infrastruktur durch ein geeignetes CTF Framework bereitgestellt werden. Einige dieser Frameworks wurden in dieser Arbeit bereits vorgestellt. Bei der Heranziehung eines Frameworks ist es von Bedeutung, dass die erarbeitete Lösung zur Ressourcen-Problematik eingebettet werden kann. Ein Beispiel für ein solches CTF Framework wäre CTFd, da es ein Plugin- und Theme Interface anbietet. Mithilfe dieses Interface können Erweiterungen dem Framework einfacher hinzugefügt oder im Nachhinein mit Dritten geteilt werden. Zudem trägt solch eine Modellierung dazu bei, dass durch einen nicht modifizierten Source-Code ein Framework leichter auf die jeweils neueste Version aktualisiert werden kann. Aus den zuvor genannten Gründen ist die Nutzung von CTFd zu empfehlen.

Abgesehen davon wurde in dieser Arbeit eine Auswahl an Systemen eines Automobils getroffen, welche für ein CTF genutzt sowie modifiziert werden können. Die in dieser Arbeit dafür entwickelten Flags können künftig auf weiterer dieser Systeme ausgeweitet werden. Zudem wäre es denkbar Flags ins Automobil einzubetten, welche als zunächst nicht erreichbar definiert sind. Diese würden zur Prüfung herangezogen ob Teilnehmende trotz dessen eine Möglichkeit zur Lösung finden. Zudem könnte die Auswahl an Systemen künftig durch das in dieser Arbeit bereits vorgestellte Kommunikationsprotokoll DoIP erweitert werden. DoIP ermöglicht die Abfrage des Informationszustandes eines AUTOSAR Systems und ermöglicht unteranderem das Flashen eines Steuergeräts. Für den Einsatz von DoIP in einem CTF müsste die Umsetzbarkeit sowie der Umfang der zu verwendenden Systeme untersucht werden. Für eine künftige Umsetzung der in dieser Arbeit beschriebenen Konzeption wurden modifizierbare Systeme und solche die ins Automobil im Nachhinein hinzugefügt werden können beschrieben. Eine angedachte technische Umsetzung, kann von diesen Erkenntnissen und Empfehlungen Gebrauch machen.

Literaturverzeichnis

ADAC. 2006: *Der Bremsassistent: ADAC-Test*: https://www.adac.de/_mmm/pdf/tuz_fas_iftk_bremsassistent_23946_51202.pdf Stand: 22.07.2020

ADAC. 2018. *Car2X: Wenn Autos mit der Umwelt kommunizieren*: https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/technik-vernetzung/car2x-kommunikation/ Stand: 03.07.2020

ADAC. 2019a. *eCall: Elektronischer Schutzengel im Auto*: https://www.adac.de/rund-ums-fahrzeug/unfall-schaden-panne/unfall/ecall/ Stand: 14.07.2020

ADAC. 2019b: *Systemvergleich: Was schützt vor Autodiebstahl?:* https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/zubehoer/auto-diebstahl-sichern/ Stand: 03.08.2020

ADAC. 2019c: *Tankanzeige: Wie exakt arbeitet sie?*: https://www.adac.de/verkehr/tanken-kraftstoff-antrieb/tipps-zum-tanken/tankanzeige/ Stand: 05.08.2020

Adam, Daniel. 2016. *Konzept einer bionischen E/E-Architektur für Fahrzeuge nach dem Vorbild des menschlichen Körpers*.

Apsdehal. 2019. *Awesome-CTF*: https://apsdehal.in/awesome-ctf/ Stand: 04.03.2020

Audi. 2018: *Audi A8 2018: Kreuzungsassistent (Guided Tour)*: https://www.youtube.com/watch?v=PJ8ef8EG8j4 Stand: 22.07.2020

AUTOSAR. 2020: *AUTOSAR Introduction: The vision, the partnership and current features in a nutshell*: https://www.autosar.org/fileadmin/ABOUT/AUTOSAR_EXP_Introduction.pdf Stand: 15.10.2020

Bansal. 2019. *King of the Hill*: https://medium.com/bugbountywriteup/ctf-are-for-nerds-a-popular-myth-54d6647259eb Stand: 03.03.2020

Bosch. o.J. a: *Systems Engineering Services*: https://www.bosch-engineering.com/de/portfolio/engineering-services/systems-engineering-services/ Stand: 15.06.2020

Bosch. o.J. b: *Totwinkelassistent*: https://www.bosch-mobility-solutions.com/de/produkte-und-services/pkw-und-leichte-nutzfahrzeuge/fahrerassistenzsysteme/totwinkelassistent/ Stand: 22.07.2020

Bosch. 2013: *DE | Bosch Spurhalteassistent*: https://www.youtube.com/watch?v=eSuyXWPGDgI Stand:22.07.2020

Bussgeldkatalog.org. 2020a. *Nachtsichtassistent: Sicher in der Dunkelheit unterwegs*: https://www.bussgeldkatalog.org/nachtsichtassistent/ Stand: 14.07.2020

Bussgeldkatalog.org. 2020b: *Blinker – Alles, was Sie über den Fahrtrichtungsanzeiger wissen müssen*: https://www.bussgeldkatalog.org/blinker/ Stand: 05.08.2020

Bussgeldkatalog.org. 2020c: *Warnblinklicht: Alles Wichtige zum Warnzeichen an Ihrem Auto!*: https://www.bussgeldkatalog.org/warnblinklicht/ Stand: 05.08.2020

Bussgeldkatalog.org. 2020d: Dank Tachojustierung Geschwindigkeitsüberschreitungen entgegentreten: https://www.bussgeldkatalog.org/tachojustierung/ Stand: 19.11.2020

FBCTF. 2018: *FBCTF*: https://github.com/facebookarchive/fbctf Stand: 03.03.2020

Chung, Kevin und Cohan, Julian. 2014: *Learning Obstacles in the Capture The Flag Model*. Genetics Selection Evolution

Chung, Kevin und CTFd LLC. 2017: *Lowering the Barriers to Capture the Flag Administration und Participation*. Berkeley, California, USA. Proceedings of the 2017 USENIX Workshop on Advances in Security Education. Vancouver, British Columbia, Canada

CTFd. 2020: *CTFd – Cyber Security Training made simple*: https://ctfd.io/ Stand: 04.03.2020

CTFTime.org. o.J.: *What is Capture The Flag?*: https://ctftime.org/ctf-wtf/ Stand: 05.07.2020

Continental. 2015. *System architecture advisory services*: https://www.continental-automotive.com/getattachment/ebef9eec-0201-46f5-acbb-

3270da8f7eda/Continental_System-Architecture_Brochure_EN_2015_final.pdf.pdf Stand: 15.06.2020

Continental. 2018a. *Wie funktioniert eigentlich ein Gurtstraffer?*: https://www.continental-reifen.de/autoreifen/ueber-continental/media-services/visionzeroworld/technologie/2018-12-17-gurtstraffer Stand: 09.07.2020

Continental. 2018b: *Wie funktioniert eigentlich der Notbremsassistent?*: https://www.continental-reifen.de/autoreifen/ueber-continental/media-services/visionzeroworld/technologie/2018-09-24-notbremsassistent Stand: 16.07.2020

Curved. 2019: *Handy mit dem Auto verbinden: Diese Möglichkeiten gibt es*: https://curved.de/tipps/handy-mit-dem-auto-verbinden-diese-moeglichkeiten-gibt-es-656168 Stand: 05.08.2020

CTF Wiki. o.J.: *Problem Solving Mode – Jeopardy*: https://ctf-wiki.github.io/ctf-wiki/introduction/mode/ Stand: 20.11.2020

dejure.org. o.J. a: *Strafgesetzbuch – Besonderer Teil (§§ 80 – 358) – 7. Abschnitt – Straftaten gegen die öffentliche Ordnung (§§ 123 – 145d) - § 145 – Missbrauch von Notrufen und Beeinträchtigung von Unfallverhütungs- und Nothilfemitteln*: https://dejure.org/gesetze/StGB/145.html Stand: 19.11.2020

dejure.org. o.J. b: *Datenschutz-Grundverordnung*: https://dejure.org/gesetze/DSGVO Stand: 19.11.2020

Eagle, Chris und Clark, John L.. 2004: *Capture-The-Flag: Learning Computer Security Under Fire.* Monterey, California: Naval Postgraduate School. Proceedings from the Sixth Workshop on Education in Computer Security, Monterey, CA, 12-14, July 2004, pp. 43-49.

EDN. 2012: *Fundamentals of the automotive cabin climate control system*: https://www.edn.com/fundamentals-of-the-automotive-cabin-climate-control-system/ Stand: 03.08.2020

Ford. o.J.: *Sensorgesteuerte Heckklappe*: https://www.ford.de/kaufberatung/informieren/technologien/komfort/sensorgesteuerte-heckklappe Stand: 03.08.2020

Ford. 2018a: *Geschwindigkeitsregelanlage – Tipps zur Bedienung | Ford Deutschland*: https://www.youtube.com/watch?v=YFeLIOqT-I0 Stand: 22.07.2020

Ford. 2018b: *Adaptive Geschwindigkeitsregelanlage – Tipps zur Bedienung | Ford Deutschland*: https://www.youtube.com/watch?v=pnzfLPWBA54 Stand: 22.07.2020

Ford. 2019a: *Intelligente Geschwindigkeitsregelanlage mit Verkehrsschilderkennung – Tipps zur Bedienung*: https://www.youtube.com/watch?v=wvbmK-cUkco Stand: 22.07.2020

Ford. 2019b: *Head-up-Display – Tipps zur Bedienung | Ford Deutschland*: https://www.youtube.com/watch?v=gf28q-eZos8 Stand: 03.08.2020

Fuzyll und Psifertex. 2015: *The Many Maxims of Maximally Effective CTFs*: https://captf.com/maxims.html Stand: 16.05.2020

Fürst, Simon und Bechter, Markus. 2016: *AUTOSAR for Connected and Autonomous Vehicles – The AUTOSAR Adaptive Platform*. 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W). Toulouse, 2016. pp. 215-217

Gebauer, Daniel. 2018: *Diagnosekommunikation für E/E-Systeme effizient entwickeln – Autosar-konforme Fahrzeugdiagnose über DoIP*: https://www.all-electronics.de/autosar-konforme-fahrzeugdiagnose-doip-diagnosekommunikation-entwicklung/ Stand: 12.11.2020

Genovese, Vito. 2016: *Capture the Flag: An Owner's Manual*. San Francisco, CA. {USENIX} Association

HELLA. o.J. a: *Regensensor prüfen und austauschen*: https://www.hella.com/techworld/de/Technik/Elektrik-Elektronik/Regensensor-pruefen-austauschen-42078/ Stand: 23.07.2020

HELLA. o.J. b: *KEYLESS GO*: https://www.hella.com/techworld/de/Technik/Elektrik-Elektronik/Keyless-Go-3195/ Stand: 03.08.2020

HELLA. o.J. c: *Zündspule*: https://www.hella.com/techworld/de/Technik/Elektrik-Elektronik/Zuendspule-2886/ Stand: 05.08.2020

Hyundai Motor Europe GmbH. 2019. *How Launch Control works*: https://www.hyundai.news/eu/model-news/how-launch-control-works/ Stand: 28.06.2020

ITWissen.info. 2012: *Radiotext*: https://www.itwissen.info/Radiotext-radio-data-system-RDS.html Stand: 05.08.2020

ITWissen.info. 2013: *Mobiles Internet*: https://www.itwissen.info/Mobiles-Internet-mobile-Internet.html Stand: 19.11.2013

ITWissen.info. 2014: *Digital-TV*: https://www.itwissen.info/Digital-TV-digital-television-DTV.html Stand: 05.08.2020

ITWissen.info. 2015a. *Aufmerksamkeits-Assistant*: https://www.itwissen.info/Aufmerksamkeits-Assistent-attention-assistance.html Stand: 14.07.2020

ITWissen.info. 2015b: *Fußgänger-Kollisionswarnsysteme*: https://www.itwissen.info/Fussgaenger-Kollisionswarnsystem-pedestrian-forward-collision-warning-PCW.html Stand: 22.07.2020

ITWissen.info. 2015c: *Kollisionswarnsysteme*: https://www.itwissen.info/Kollisionswarnsystem-forward-collision-warning-FCW.html Stand: 22.07.2020

ITWissen.info. 2015d: *FSE (Freisprecheinrichtung)*: https://www.itwissen.info/FSE-Freisprecheinrichtung-hands-free-equipment.html Stand: 05.08.2020

ITWissen.info. 2017a: *SWA (Spurwechselassistent)*: https://www.itwissen.info/Spurwechselassistent-SWA-lane-change-assistant-LCA.html Stand: 22.07.2020

ITWissen.info. 2017b: *IVI (in-vehicle infotainment)*: https://www.itwissen.info/IVI-in-vehicle-infotainment-In-Vehicle-Infotainment.html Stand: 05.08.2020

ITWissen.info. 2018: *Satelliten-Navigation*: https://www.itwissen.info/Satelliten-Navigation-satellite-navigation.html Stand: 05.08.2020

ITWissen.info. 2019: *RDK (Reifendruck-Kontrollsystem)*: https://www.itwissen.info/Reifendruck-Kontrollsystem-RDK-tire-pressure-monitoring-system-TPMS.html Stand: 22.07.2020

ITWissen.info. 2020: *Elektrisch-elektronische Architektur*: https://www.itwissen.info/Elektrisch-elektroniche-Architektur-E-E-architecture-E-E.html Stand: 19.11.2020

Leune, Kees und Petrilli, Salvatore J.. 2017: *Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education*. New York, NY, USA. In Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17). Association for Computing Machinery

Mayser. o.J.: *Sitzbelegungssensor SBS*. Ulm, Germany

MAN. o.J.: *Notbremsassistent (EBA)*: https://www.bus.man.eu/de/de/man-welt/technologie-und-kompetenz/sicherheits-und-assistenzsysteme/notbremsassistent/Notbremsassistent.html Stand: 16.07.2020

Mein-autolexikon.de. o.J.: *Motorsteuerung*: https://www.mein-autolexikon.de/motor/motorsteuerung.html Stand: 05.08.2020

Mellivora. 2020: *Mellivora*: https://github.com/Nakiami/mellivora Stand: 04.03.2020

Mentor. o.J.: *AUTOSAR on Linux and Diagnostics*: https://www.mentor.com/products/electrical-design-software/multimedia/overview/autosar-on-linux-and-diagnostics-3f405db1-cbb8-40c6-9445-dc28cf327d06 Stand: 12.11.2020

Mercedes-Benz. o.J.: *Spiegel-Paket*: https://www.mercedes-benz.de/passengercars/mercedes-benz-cars/models/c-class/saloon-w205/safety.pi.html/mercedes-benz-cars/models/c-class/saloon-w205/safety/safety-packages/mirror-package Stand: 03.08.2020

Mercedes-Benz. 2017: *Mercedes-Benz S-Klasse 2017: Aktiver Spurwechsel-Assistent*: https://www.youtube.com/watch?v=pxtomtGqEys Stand: 22.07.2020

Mercedes. 2019: *Mercedes-Benz How To: "Hey Mercedes".*: https://www.youtube.com/watch?v=2XBFEIBl9ag Stand: 03.08.2020

Mirkovic, Jelena und Peterson, Peter A. H.. 2014: *Class Capture-the-Flag Exercises.* San Diego, CA. Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)

Mobile.de. 2020: *Das ist zu tun, wenn ein Elektroauto brennt*: https://www.mobile.de/magazin/artikel/das-ist-zu-tun-wenn-ein-elektroauto-brennt-20738 Stand: 17.08.2020

NDR. o.J.: *UKW (FM) Der altbewährte Radioempfang*: https://www.ndr.de/der_ndr/empfang_und_technik/ukw/UKW,ukw102.html Stand: 05.08.2020

Nett, Tillmann und Schneider, Jörn. 2013: *Running Linux and AUTOSAR side by side*. Proceedings of the 7th Junior Researcher Workshop on Real-Time Computing.

Nighswander, Tyler. 2016: *Building a Competitive Hacking Team*. San Francisco, CA. {USENIX} Association

obd-2.de. o.J.: *OBD-2 Allgemeines, technische Informationen*: https://www.obd-2.de/obd-2-allgemeine-infos.html Stand: 19.11.2020

OverTheWire. o.J.: *Wargames*: https://overthewire.org/ Stand: 02.11.2020

Porsche. 2015: *Porsche Cayenne - Persönliche Einstellungen*: https://www.youtube.com/watch?v=Jh_nrPGfIrQ Stand: 03.08.2020

SEAT. o.J.: *SEAT Techniklexikon – Alle Details.*: https://www.seat.de/service-zubehoer/technik-lexikon.html Stand: 08.07.2020

Steinbach, Till. 2018. *Ethernet-basierte Fahrzeugnetzwerkarchitekturen für zukünftige Echtzeitsysteme im Automobil*

~ Stücker, Dirk. 2004. *Heterogene Sensordatenfusion zur robusten Objektverfolgung im automobilen Straßenverkehr*

Sudo Null. o.J.: *How I went through the first hack quest CTF Ratazana*: https://sudonull.com/post/98471-How-I-went-through-the-first-hack-quest-CTF-Ratazana Stand: 02.11.2020

Toyota. o.J. a: *Einparkhilfen – Damit Sie leichter in die engen Lücken kommen.*: https://de.toyota.ch/world-of-toyota/safety-technology/parking-aids.json Stand: 08.07.2020

Toyota. o.J. b: *Selbstfahrende Autos: Wie nah sind wir am autonomen Fahren?*: https://www.toyota.de/news/ratgeber/selbstfahrende-autos Stand: 19.11.2020

Toyota. 2016: *Hill Start Assist Control*: https://www.youtube.com/watch?v=nbKlQ4TvBFg Stand: 28.06.2020

Vigna, Giovanni. 2003. *Teaching Network Security Through Live Exercises*. New York, NY. Springer US

Volkswagen. o.J.: *Fußgänger besser schützen. Fußgängererkennung.*: https://www.volkswagen.at/golf-sportsvan/golf-sportsvan/fussgaengererkennung Stand: 03.08.2020

Volkswagen. 2016a: *Fahrassistenzsysteme: Teil 4 – Stauassistent*: https://www.youtube.com/watch?v=hUEQGoy-l0Y Stand: 22.07.2020

Volkswagen. 2016b: *Fahrassistenzsysteme: Teil 5 – Verkehrszeichenerkennung*: https://www.youtube.com/watch?v=uUFbaXvzE7g Stand: 22.07.2020

ZeroNights. 2019: *ZeroNights hackquest*: https://hackquest.zeronights.org/#about Stand: 02.11.2020

Abbildungsverzeichnis

Tabellenverzeichnis

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den __20.11.2020____ [redacted]

Anastasios Palatiou