

Anhalten unkooperativer Autos: Ein interaktives Bezugssystem

Robert Altschaffel · Mario Hildebrandt · Falko Rassek
Stefan Kiltz · Jana Dittmann

Otto-von-Guericke Universität Magdeburg
{robert.altschaffel | mario.hildebrandt | falko.rassek
stefan.kiltz | jana.dittmann}@iti.cs.uni-magdeburg.de

Zusammenfassung

Häufig ist es notwendig kurzfristig Entscheidungen über den Einsatz von Technologien selbst und die Art und Weise des Einsatzes zu treffen. Vor allem wenn der Einsatz dieser Technologie potentiell gefährliche Folgen mit sich bringen kann, ist eine solche Abwägung häufig schwierig. Problematisch sind sowohl der Komplexitätsgrad der zu bescheidenen Technologie, als auch deren interaktive Effekte in der praktischen Anwendung. Eine vollständige experimentelle Erprobung in allen denkbaren Szenarien ist eher die Ausnahme denn die Regel. Im Rahmen dieses Beitrages wird diskutiert, inwiefern Ontologien genutzt werden können, notwendige Faktoren für eine solche Abwägung zu ermitteln und darzustellen. Aus diesen Faktoren können sich im Einsatzszenario neben technischen ebenfalls weitere Implikationen ergeben. Hierbei muss auf die Diskriminierungsfreiheit und die Einhaltung der UN-Menschenrechtscharta nach der jeweiligen aktuellen Rechtslage geachtet werden. Ein solches Modell sollte dabei semi-automatisch realisiert sein, um Faktoren und Rahmenparameter automatisiert aufzunehmen und als Ergebnis die entscheidungstreffenden Instanzen sowie die potentiellen Anwender über die zu erwarteten Implikationen bedarfsabhängig zu informieren. Die Aufgabe einer Ontologie ist dabei, die Komplexität zu reduzieren, um eine schnelle und angemessene Entscheidung zu ermöglichen. In diesem Beitrag wird ein solches Modell am Beispiel von Technologien zum Anhalten von unkooperativen Straßenfahrzeugen (PKW) unter verschiedenen Zielstellungen vorgestellt, diskutiert und in Hinblick auf die Anwendbarkeit kritisch bewertet.

1 Einleitung

In zeitkritischen Situationen wird die Entscheidungsfindung dadurch erschwert, dass die Sammlung von Informationen und auch die Identifizierung von zu betrachtenden Faktoren in einem kurzen Zeitraum unzureichend sein können. Hinzu kommt, dass es in einem kurzen Zeitraum meistens nicht möglich ist alle Risiken und Implikation durch die Auswahl einer bestimmten Problemlösungsstrategie zu erfassen. Ein prominentes Beispiel, welches auch die potentiellen Folgen einer Fehlhandlung verdeutlicht, ist die Kubakrise [Piou01]. Vor allen wenn der Einsatz einer Technologie Einfluss auf die körperliche Unversehrtheit haben kann, müssen diese Faktoren jedoch beachtet werden, um eine fundierte Risikoabschätzung durchführen zu können. Ein Ansatz um die Entscheidungsfindung in einer solchen Situation zu verbessern, ist die Triage (vgl. Kapitel 2.2). Wir stellen jedoch fest, dass ein Teil der Entscheidungsfindung bereits vor dem Eintreten eines konkreten Ereignisses, in dem eine solche Entscheidung not-

wendig ist, durchgeführt werden sollte, um die Reaktionszeit zu minimieren ohne wichtige Faktoren zu übersehen. Zu diesem Zweck werden die jeweiligen Faktoren, die einen Einfluss auf den Einsatz einer spezifischen Technologie haben können, bereits im Vorfeld ermittelt. Diese Vorbereitungsphase ist analog zu einer strategischen Vorbereitung innerhalb eines forensischen Prozesses zu sehen [KiHD09]. Als Werkzeug werden hierfür Ontologien vorgeschlagen, da diese dazu geeignet sind, komplexe Zusammenhänge in einem Modell zusammenzufassen. Im Rahmen dieses Beitrags wird aufgezeigt, wie solche Ontologien zu erzeugen sind und wie sie dafür genutzt werden können, semi-automatisiert Implikationen eines bestimmten Technologieeinsatzes zu ermitteln. Dabei kann das in diesem Beitrag vorgestellte Vorgehen keine Entscheidungen treffen – dies obliegt einem menschlichen Verantwortlichen, der jedoch durch das hier vorgestellte Werkzeug die Möglichkeit zur Abschätzung von Folgen und Implikationen hat. Diese Implikationen finden sich auch im ethischen oder rechtlichen Bereich, weshalb die Modellierung eine regelmäßige Überprüfung hinsichtlich der aktuellen Rechtslage benötigt, um im Einsatzfall kurzfristig eine (menschen-)rechtskonforme Entscheidung hinsichtlich der anzuwendenden Technik treffen zu können. Im Rahmen dieses Beitrags wird eine solche Vorgehensweise am Beispiel von Technologien zum Anhalten von unkooperativen Straßenfahrzeugen demonstriert. Dieses komplexe Anwendungsfeld erfordert schnelle Entscheidungen über den Einsatz von Technologien und bringt eine mögliche Gefährdung von Menschen, Tieren und Material mit sich.

Dieser Beitrag gliedert sich wie folgt: Im ersten Kapitel wird das exemplarische Themenfeld aufgezeigt. Das zweite Kapitel diskutiert Modelle zur Verbesserung von Entscheidungsprozessen unter Zeitdruck und gibt sowohl eine Übersicht über Ontologien als auch über Technologien zum Anhalten von unkooperativen Straßenfahrzeugen. Das dritte Kapitel stellt unser Vorgehen zur Verwendung von Ontologien zur verbesserten Entscheidungsfindung und die Übertragung dieses Konzeptes auf Technologien zum Anhalten unkooperativer Straßenfahrzeuge dar. Das vierte Kapitel gibt eine Zusammenfassung und einen Ausblick.

2 Stand der Technik

In diesem Kapitel werden die für das Verständnis dieses Beitrags benötigten Grundlagen vorgestellt. Nach einer Übersicht zum Thema unkooperativer Fahrzeuge und einer Auswahl von Technologien/Techniken, um diese anzuhalten, wird auf Modelle und Ansätze zur Vorbereitung von Entscheidungsfindungen unter Zeitdruck eingegangen. Abschließend werden Grundlagen von Ontologien erläutert.

Unkooperative Fahrzeuge: Es existieren eine Vielzahl von Gründen, weshalb ein Fahrzeug aus der Entfernung angehalten werden soll, z.B. absichtliches Fehlverhalten eines Fahrers (Flucht), Kontrollverlust durch technische Defekte, medizinische Zwischenfälle (Zusammenbruch eines Fahrers) oder autonome Fahrzeuge, bei denen der Autopilot die Rolle des Fahrers einnimmt und auf Grund eines Soft-/Hardwarefehlers ein Fehlverhalten zeigt. Verschiedene Entitäten mit unterschiedlichen Motivationen und unterschiedlichste, verfügbare Techniken ergeben hierbei eine fast unendliche Anzahl an möglichen Szenarien. In diesem Beitrag liegt der Fokus jedoch ausschließlich auf Szenarien mit unkooperativen Fahrzeugen, z.B. Flucht vor der Polizei. Lum und Fachner [LuFa08] haben Verfolgungsjagden der Polizei in den USA analysiert und fanden dabei heraus, dass trotz aktueller Überwachungstrends hin zu proaktiver und informationsgetriebener Vorgehensweisen Hochgeschwindigkeitsverfolgungsjagden weiterhin eine führende Rolle einnehmen. In diesem Bericht zeigen Lum und Fachner sehr detaillierte

Statistiken über in den USA angehaltene Fahrzeuge, welche die aktuelle Situation gut reflektieren. Diese Erkenntnisse können zwar nicht direkt auf Deutschland bzw. die EU übertragen werden, jedoch scheinen solche detaillierten Daten für europäische Länder nicht verfügbar zu sein.

In den Vereinigten Staaten wurden von 23 Behörden 6133 Fälle im Zeitraum von 2003 bis 2006 gemeldet (im Durchschnitt 1533 Fälle pro Jahr bzw. 4 Fälle pro Tag) [LuFa08]. Die Gründe für eine Verfolgung reichen hierbei von Verkehrsverstößen (42%), Verdacht eines gestohlenen Fahrzeuges (18%) und Fahrern unter Betäubungsmiteleinfluss (15%) bis hin zu Straftaten (gewalttätig: 8,6% und nicht-gewalttätig: 7,5%). In 79% aller Fälle kam es zu keinem Schaden; in 14,5% aller Fälle kam es zu Sachschäden und in 9% wurde über Verletzte berichtet. Betrachtet man die Fälle mit Verletzten genauer, ergibt sich folgende Aufteilung: Polizeibeamte – 14% (meistens leichte Verletzungen), Unbeteiligte – 21% (meist nur leichte Verletzungen), Verdächtige – 52% mit leichten Verletzungen, 11% mit schwereren Verletzungen und 2% mit schwersten Verletzungen. Dies zeigt, dass nicht nur die Fahrer von unkooperativen Fahrzeugen bei Verfolgungsjagden gefährdet sind, sondern ebenso die Polizeibeamten und unbeteiligte Personen. Der Hauptgrund kann hier im physischen Kontakt (z.B. Straßenblockaden, taktisches Rammen, Nagelbänder) gesehen werden, welcher derzeitig nötig ist, um ein unkooperatives Fahrzeug abzubremsen bzw. anzuhalten. In 94% aller Fälle wurde keine der traditionellen Methoden zum Anhalten von Fahrzeugen verwendet. In 3,4% der Fälle wurden Nagelbänder, in 0,7% ein taktisches Rammen und in 0,4% stationäre bzw. in 0,3% rollende Straßenblockaden verwendet. Bereits das Schadenspotential und der Umstand, dass nur in 6% aller Fälle eine passende Technik zum Einsatz kam, zeigen bzw. motivieren, dass alternative Anhaltetechniken benötigt werden.

Betrachtet man nur die Verfolgungen kann zusammenfassend gesagt werden, dass bessere Möglichkeiten benötigt werden, z.B. die Möglichkeit über einen Fernzugriff oder einer anderen sicheren Möglichkeit zum Anhalten von Fahrzeugen. In gerade einmal 35% aller Fälle haben die Verdächtigen angehalten (diese Prozentzahl berücksichtigt ebenso das Anhalten auf Grund technischer Defekte oder leeren Tanks). In 18% der Fälle waren die Verdächtigen in Unfälle verwickelt, in 18% der Fälle entkamen die Verdächtigen der Polizei, während in nur 2,6% der Fälle das Fahrzeug unbrauchbar gemacht wurde.

2.1 Beispiele zum Anhalten unkooperativer Fahrzeuge

In [BoSa00] werden drei verbreitete passive Techniken zum Anhalten von flüchtenden Fahrzeugen beschrieben: rollende Straßenblockaden, stationäre Straßenblockaden und sogenannte "Stop Sticks" (Nagelbänder). Weitere Methoden werden in [Stev09] aufgezeigt. Zusätzlich besteht in modernen, vernetzten Fahrzeugen die Möglichkeit, mittels Fernzugriff die Zündung zu blockieren oder das Fahrzeug abzubremsen. Die zuvor genannten Methoden und Techniken werden in den nachfolgenden Abschnitten näher erläutert.

Rollende und stationäre Straßenblockaden: Eine Beschreibung über die Anwendung von rollenden und stationären Straßenblockaden findet sich in [BoSa00]. Mit Hilfe von stationären Straßenblockaden werden Teile einer Straße blockiert. Diese Blockaden werden nicht zwangsläufig dazu verwendet, um die komplette Straße zu blockieren, sondern eher um ein flüchtendes Fahrzeug dazu zu zwingen abzubremsen. Stationäre Blockaden müssen im Voraus aufgebaut werden. Eine rollende Blockade wird als ein Manöver beschrieben, in welchem Polizeifahrzeuge das unkooperative Fahrzeug umgeben und abbremsen.

Taktisches Rammen: Das taktische Rammen (PIT Manöver – Präzisions-Immobilisierungstechnik) wird bei Verfolgungen verwendet. Hierbei verursacht ein verfolgendes Fahrzeug eine kontrollierte Kollision in das seitliche Heck (von links oder rechts) des flüchtenden Fahrzeuges, so dass sich dieses seitwärts dreht, der Fahrer hierdurch die Kontrolle über das Fahrzeug verliert und zum Stehen kommt. Da eine Konsequenz dieses Manövers der Verlust der Kontrolle über das Fahrzeug ist, ergibt sich ein erhöhtes Risiko, dass das Manöver in einem Unfall/Zusammenstoß endet.

Nagelbänder: Nagelbänder, auch bekannt als "Stop Sticks" und Reifenluft-Ablass-Instrument, sind Vorrichtungen, welche zum Abbremsen oder Anhalten von flüchtenden Fahrzeugen genutzt werden. Diese Vorrichtungen durchlöchern hierzu den Reifen mittels hohler, löchriger und mit stahlverstärkten Spitzen versehenen Stacheln, um aus diesen innerhalb von 5-10 Sekunden die Luft abzulassen [BoSa00]. Hierdurch wird die Geschwindigkeit des Fahrzeuges reduziert, welches jedoch weiterhin fahrbar ist. Die Kontrollierbarkeit des Fahrzeuges ist im Allgemeinen weiterhin gegeben und platzende Reifen sollen aktiv vermieden werden.

Schusswaffen: In jüngerer Vergangenheit wurden Schusswaffen zum Anhalten von flüchtigen Fahrzeugen verwendet. Eine Reihe von Vorfällen, bei denen Fahrzeuginsassen durch die Schüsse getötet wurden, führte zu einer Überarbeitung der Richtlinien für den Beschuss bewegter Fahrzeuge. Die US Richtlinien für den Einsatz von Schusswaffen gegen sich bewegende Fahrzeuge wurden in der Hinsicht überarbeitet, dass ein Schusswaffeneinsatz nur dann erlaubt ist, wenn die Insassen des flüchtenden Fahrzeuges tödliche Gewalt gegenüber anderen Personen ausüben [Brot99]. Daher untersagen die US Richtlinien den Einsatz von Schusswaffen gegen flüchtige Fahrzeuge, die keine direkte Gefahr für andere Personen darstellen.

Anhalten über Fernzugriff: Das Anhalten eines Fahrzeuges mittels Fernzugriff basiert auf einer in ein Fahrzeug eingebauten Technologie, welche zur Kommunikation mit einem Service-Center vorgesehen ist. Der Vorteil dieses Verfahrens soll in einem kontrollierten Abbremsen (z.B. durch Reduzierung der Motorleistung) oder Abschalten des Fahrzeuges liegen, solange dieses noch brems- und lenkbar bleibt. Beispiele für diese Ansätze sind ENLETS (z.B. [BBC14]) und ONSTAR [ONST15]. ENLETS ist Teil der Gesetzesvollstreckungs-Arbeitsgruppe des EU Rats, welches für Polizeikräfte im Kampf gegen schwere und organisierte Kriminalität gedacht ist. ONSTAR ist eine Ausstattung für Fahrzeuge von General Motors weltweit, welche verschiedene Online-Angebote zur Verfügung stellt. Eines dieser Angebote ist u.a. der „Diebstahl-Notfallservice“, über welchen ein Service-Mitarbeiter in der Lage ist, den Motor eines als gestohlen gemeldeten Fahrzeuges dauerhaft auszuschalten. Da diese Technik, sowohl eine in einem Fahrzeug verbaute Komponente als auch eine aktive Kommunikation benötigt, ist es möglich, dass die entsprechende Komponente vor einer Verfolgung ausgebaut oder deaktiviert bzw. die Kommunikation beispielsweise mittels eines entsprechenden Jammers gestört wird.

EM-basierte Techniken: Ein Vertreter der elektromagnetischen (EM) Technologie ist ein Ansatz, welcher im Rahmen des SAVELEC Projektes untersucht wird [SAVE12]. Dieses Projekt hat zum Ziel eine Pulsconfiguration zu finden, welche Sensoren, Aktoren und Steuergeräte eines Fahrzeuges stört, ohne diese oder andere Teile des Fahrzeuges zu zerstören. Diesem Ansatz folgend soll der Motor des Fahrzeuges, mit nur sehr geringen bis keinen Auswirkungen auf den Menschen, ausgeschaltet werden, so dass das Fahrzeug langsam und sicher, bis hin zum vollständigen Stopp, ausrollt. Weitere Ziele im Rahmen dieses Projektes sind, dass keine gefährdenden Auswirkungen auf den Treibstoff, die Airbags oder Batterien innerhalb des Fahrzeuges erkennbar sind.

Auf Grund eines speziellen Antennendesigns kann der Abstrahlwinkel der Vorrichtung gut definiert werden, wodurch eine Bestimmung des bestrahlten Gebietes und eine genauere Berechnung der abgegebenen EM Strahlung erfolgen kann. Verschiedene Simulationen zur Untersuchung der Belastung des Menschen wurden durchgeführt, unter Berücksichtigung der von der Internationalen Kommission für nicht-ionisierenden Strahlen-Schutz (ICNIRP) vorgegebenen maximalen Grenzwerte und der spezifischen Absorptionsrate (SAR). Entgegen der traditionellen Techniken benötigt ein elektromagnetischer Impuls (EMP) keinen physikalischen Kontakt zum unkooperativen Fahrzeug. Zudem wird bisher davon ausgegangen, dass die Lenk- und Bremsbarkeit des Fahrzeuges durch den EMP nicht beeinflusst wird, zum Beispiel wird angenommen, dass das Fahrzeug auch ohne Servolenkung weiterhin lenkbar ist. Diese Annahme gilt ebenso für Bremsen mit Bremskraftverstärker. Für beide Situationen wird davon ausgegangen, dass ein höherer, jedoch überschaubarer Kraftaufwand für den Fahrer entsteht, um das Fahrzeug zu kontrollieren. Zukünftige autonome Fahrzeuge sind jedoch kritischer, da hier einerseits manuelle Eingriffsmöglichkeiten fehlen könnten, andererseits die Übernahmezeit für die manuelle Bedienung zu lang sein kann. Der vorgeschlagene Ansatz muss jedoch zukünftig weiter im Detail an verschiedenen Fahrzeugen evaluiert werden, um ungewollte Ereignisse im Fahrzeug zu vermeiden. Weiterhin müssen die Ergebnisse der ersten Tests in umfangreichen Versuchen überprüft werden.

Ein weiterer Ansatz von EM-basierten Techniken beschreibt eine Vorrichtung, die einen Impuls von Mikrowellenergie auf ein flüchtendes Fahrzeug abfeuert und so einen Ausfall der Elektronik des flüchtenden Fahrzeuges verursacht [Stev09].

2.2 Modelle für Entscheidungsfindungen unter Zeitdruck

Dieser Abschnitt beinhaltet eine kurze Vorstellung von Modellen zur Vorbereitung von Entscheidungsfindungen in zeitkritischen Szenarien. Dabei wird auf die Triage [RGMW06] eingegangen und die Vor- und Nachteile einer solchen Vorgehensweise aufgezeigt.

Triage: Um den derzeitigen, anspruchsvollen Vorstellungen in der IT Forensik gerecht zu werden, wird das Konzept der Triage diskutiert [RGMW06]. Der traditionelle Ansatz (z.B. [Case11]) zum Auffinden und Sichern von Beweisen sieht das Erstellen eines Images des Massenspeichers und die Durchführung der Untersuchungen an diesen Images in einem Labor vor. Dieser Ansatz benötigt jedoch viel Zeit und Aufwand. Der Ansatz der Triage hingegen eignet sich für Situationen, in welcher die Zeit eine äußerst wichtige Rolle spielt (z.B. Entführungen, vermisste Personen, etc.). Wie in [RGMW06] angedeutet, wird in der Triage ein anderer Ansatz zum Einsparen von Zeit genutzt (im Vergleich zu unserem Vorschlag des vor-untersuchten, halb-automatisierten Entscheidungsbaums). Triage in Bezug auf die IT Forensik wird definiert als Prozess, in dem Sachen anhand ihrer Bedeutung und Dringlichkeit eingestuft werden. Im Wesentlichen müssen die wichtigsten bzw. unbeständigsten Objekte, Beweisstücke oder potentielle Behälter mit Beweisen, zuerst berücksichtigt werden. Durch die möglichst starke Nutzung von Vorwissen, können potentielle Behälter mit Beweisen (z.B. Geräte mit Spuren) nach forensischen Prinzipien (z.B. Nur-Lese-Zugriff auf die Quelldaten, um die Integrität des Behälters so gut wie möglich aufrechtzuerhalten) identifiziert und gesammelt, sowie vor Ort untersucht werden. Dieser Beitrag schlägt eine statische, vordefinierte Vorgehensweise (z.B. Nutzerordner, Dateieigenschaften, Registrierungseinträge, Verlauf, Internet-Artefakte) unter Einbeziehung von Vorfalls-spezifischen Kenntnissen vor. Mit unserem in diesem Beitrag vorgestellten Ansatz für ähnliche Situationen, z.B. die Zeit ist das Wesentliche und es steht nur eine begrenzte

Zeit zur Entscheidungsfindung zur Verfügung, versuchen wir einen ersten halb-automatisierten Ansatz aufzuzeigen.

Ontologien: Bei einer Ontologie handelt es sich um eine Methode zur Strukturierung von Entitäten [Grub93], die Begrifflichkeit stammt aus der Philosophie [Oxfo16]. In der Informatik versteht man unter einer Ontologie eine Spezifikation eines repräsentativen Vokabulars für eine bestimmte Domäne [Grub93]. Sie besteht aus Modellierungsobjekten wie Klassen, Relationen, Funktionen und weiteren Objekten. Ontologien stellen statisches Domänenwissen dar, während problemlösende Methoden in den Bereich dynamischer Schlussfolgerungen (dynamic reasoning knowledge [GoBe99]) fallen. Ontologien können verwendet werden, um strukturierte Informationen weiterzugeben und die Komplexität von Anwendungsfeldern zu beherrschen.

Angriffsbäume: Angriffsbäume stellen eine Methodik dar, welche zur Beschreibung von Sicherheitsszenarios verwendet wird. Die Modellierung basiert auf gerichteten, nicht-zyklischen Graphen. Wie in [KoPS14] aufgezeigt, existieren derzeit mehr als 30 Ansätze von DAG-basierten Angriffsbäumen mit unterschiedlichen Eigenschaften und Zielen. Diese umfassende Anzahl zeigt die Vorzüge dieser Ansätze bezüglich ihrer Nutzerfreundlichkeit, intuitive Nutzung und Möglichkeit der Aufspaltung komplexer Szenarien auf. Demzufolge scheinen Angriffsbäume eine passende Technik zu sein, um Entscheidungsfindungsprozesse zu unterstützen.

3 Ontologiegestützte Technikfolgenabschätzung

Unser Ansatz kombiniert die Modellierung von statischem Domänenwissen mit dynamischer Schlussfolgerung zur „Strategischen onTologie zur technikfOlgenabschätzung für den Polizeigebrauch“ (STOP). Als erster Schritt wird entsprechend das Domänenwissen in Form einer Ontologie modelliert. Dabei werden Klassen und Relationen zwischen diesen Klassen verwendet. Im Fokus der Modellierung stehen einerseits das anzuhaltende Fahrzeug sowie seine unmittelbare Umgebung und andererseits die Techniken zum Anhalten unkooperativer Fahrzeuge. Die Modellierung des Fahrzeugs und seiner Umgebung fixiert sich dabei auf die jeweiligen Eigenschaften (Geschwindigkeit des Fahrzeugs, Stromleitungen in der Nähe, etc.) während die Modellierung der Techniken sich auf die Implikationen ihres Einsatzes bezieht. Mit diesem Wissen wird ein Entscheidungsbaum basierend auf dem Konzept von Angriffsbäumen [KoPS14] erstellt. Diese Entscheidungsbäume können dann Experten, wie zum Beispiel Polizisten, bei der Entscheidung, ob eine Methode zum Anhalten eines Fahrzeugs geeignet ist, unterstützen indem die Folgen des Einsatzes der jeweiligen Techniken dargestellt und aus technischen, ethischen oder rechtlichen Gründen nicht anwendbare Techniken bereits automatisch aus der Liste der Optionen entfernt werden, womit der Entscheidungsprozess weiter vereinfacht wird. Die Erstellung der Ontologie und die Ableitung des Entscheidungsbaums ist dabei ein manueller Prozess. Die Abarbeitung des Entscheidungsbaums kann dann teilautomatisiert erfolgen. Die nachfolgende Abbildung 1 zeigt unser vorgeschlagenes Gesamtkonzept, welches erweiterbar ist. Dabei können potentiell verschiedene Anhaltetechniken evaluiert werden. Diese nutzen ihrerseits Schwachstellen im unkooperativen Fahrzeug aus, können aber auch selbst Schwachstellen aufweisen, welche zu einem Missbrauch oder Fehlverhalten der Technik führen können. Gegenstand dieses Beitrags ist die Evaluation des SAVELEC-Geräts, welches als Demonstrator existiert, und dessen erste Anwendung auf die vorgeschlagene Eignungsabschätzung. Grundlegend müssen aber verschiedene Techniken und die Angemessenheit des erzwungenen Anhaltens evaluiert werden (Proportionalitätsprinzip). Letzteres erfolgt nach der Evalu-

ation der jeweiligen Technik durch eine Beurteilung der Konsequenzen. Wird eine Anhaltetechnik als ungeeignet oder unwirksam beurteilt, können andere Anhaltetechniken evaluiert werden. Erst wenn keine weiteren Optionen mehr zur Verfügung stehen oder das Anhalten nicht notwendig/rechtfertigbar ist, wird die Bewertung der Techniken beendet.

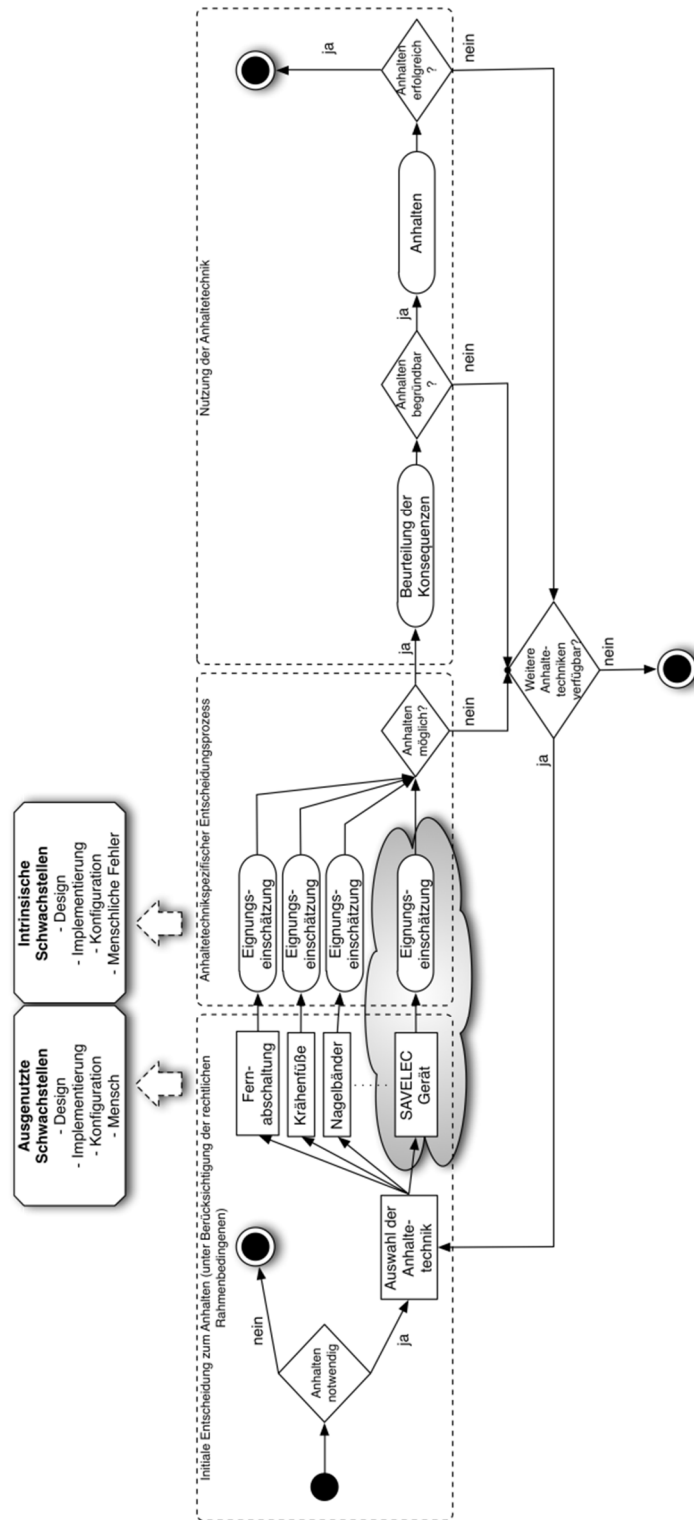


Abb. 1: Konzeptanwendungsbereich – Bewertung allgemeiner Anwendbarkeit und Risiken/Folgen

3.1 Modellierung des statischen Domänenwissens

Um die Eignungseinschätzung zukünftig zu konkretisieren ist eine erste Modellierung des statischen Domänenwissens erfolgt, welche eine Vielzahl verschiedener Faktoren des komplexen Anwendungsfelds berücksichtigt. Die Ausformulierung der Faktoren im Detail ist noch nicht erfolgt, was in zukünftigen Arbeiten sowie auch in weiteren Tests zur Bewertung und Einschätzung erfolgen muss. Die folgenden Darlegungen stellen einen ersten Ansatz dar und können erweitert bzw. angepasst werden.

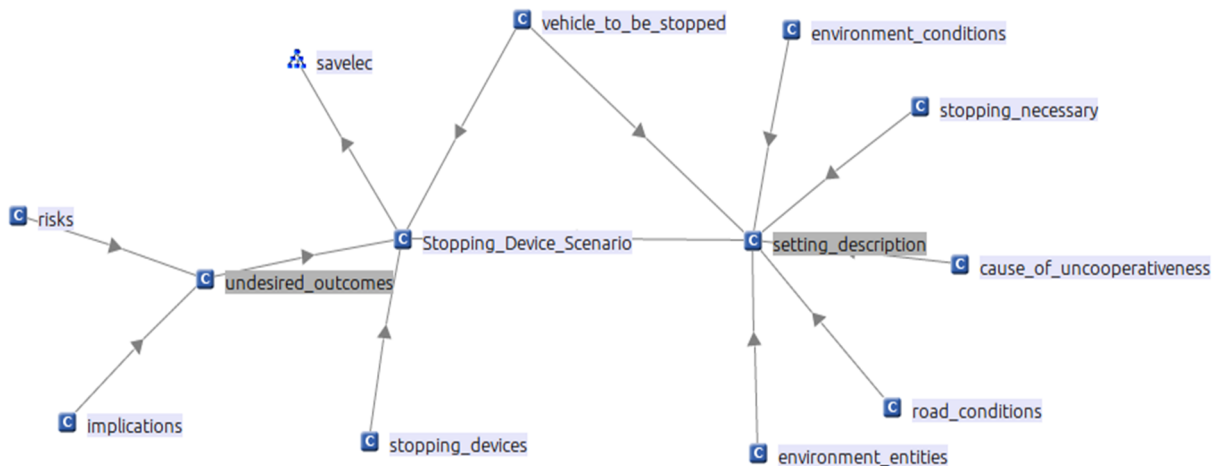


Abb. 2: Übersicht der obersten Klassen des statischen Domänenwissens

Auf den obersten Stufen der in Abbildung 2 dargestellten Ontologie ergeben sich die Klassen der Faktoren zur Berücksichtigung der Eignungsprüfung und Konsequenzabschätzung für STOP wie folgt:

- **Vehicle_to_be_stopped** (Anzuhaltendes Fahrzeug): Das unkooperative Fahrzeug inklusive des Fahrers, Insassen und der Fracht
- **Stopping_devices** (Technik zum Anhalten): Die zur Verfügung stehenden Vorgehensweisen zum Anhalten von unkooperativen Fahrzeugen
- **Stopping_necessary** (Anhalten notwendig): Abwägungen hinsichtlich der Notwendigkeit des Anhaltens des Fahrzeuges, z.B. um weitere Gefahren abzuwenden
- **Cause_of_uncooperativeness** (Grund der Nichtkooperation): Die grundlegende Ursache für den Grund der Nichtkooperation. Momentan umfasst dieser Punkt lediglich absichtliches Fehlverhalten, aber Erweiterungen hinsichtlich medizinischer Auslöser oder Funktionsstörungen sind möglich, weitere müssen definiert werden
- **Road_conditions** (Straßenbedingungen): Beschreibung der Straßenverhältnisse
- **Environment_conditions** (Umgebungsbedingungen): Faktoren, die nicht direkt mit dem Fahrzeug oder seinem Pfad zusammenhängen, aber einen Einfluss auf den Entscheidungsprozess haben können
- **Environment_entities** (Umgebungsentitäten): Externe Entitäten. Diese umfassen sowohl Lebewesen als auch leblose Objekte, die durch den Einsatz einer Anhaltetechnik beeinflusst sein können. Dies umfasst sowohl die Infrastruktur als auch zahlreiche elektronische Geräte (z.B. medizinische Geräte, Laptops, Mobiltelefone)
- **Undesired_outcomes** (ungewollte Resultate): Risiken und Implikationen beim Anhalten des Fahrzeuges

- Risks (Risiken): Eine Abschätzung potentieller, unerwünschter Ergebnisse aus dem Einsatz einer Anhaltetechnik
- Implications (Implikationen): Konsequenzen aus dem Einsatz einer Anhaltetechnik. Das Verhältnis von Risiken und Implikationen ist dabei zyklisch: Risiken bringen Implikationen mit sich, die weitere Risiken hervorrufen können. Eine Herausforderung des Rahmenwerks ist es die Iteration an geeigneter Stelle zu unterbrechen.

Diese Kategorien werden auf verschiedenen Ebenen müssen zukünftig im Detail definiert und gegebenenfalls erweitert werden, um die gesamten Faktoren abzubilden, die eine Rolle bei dem Ansatz einer Anhaltetechnik spielen können. Insbesondere die Risiken und Implikationen müssen ständig auf Basis von Testergebnissen hinsichtlich rechtlicher, technischer, organisatorischer und ethischer Aspekte erweitert werden.

In Abbildung 3 werden die Beteiligten des Anhalteszenarios dargestellt. Dabei werden Lebewesen (Menschen wie auch Tiere), materielle und immaterielle Güter innerhalb des Fahrzeuges und in dessen Umgebung betrachtet. Hierbei ist vor einem Einsatz einer Anhaltetechnik zwingend zu evaluieren, ob eventuelle Auswirkungen auf diese Beteiligten zu rechtfertigen sind. Daneben werden auch verschiedene Einflüsse der Umgebung berücksichtigt, welche eine zusätzliche Gefährdung darstellen können.

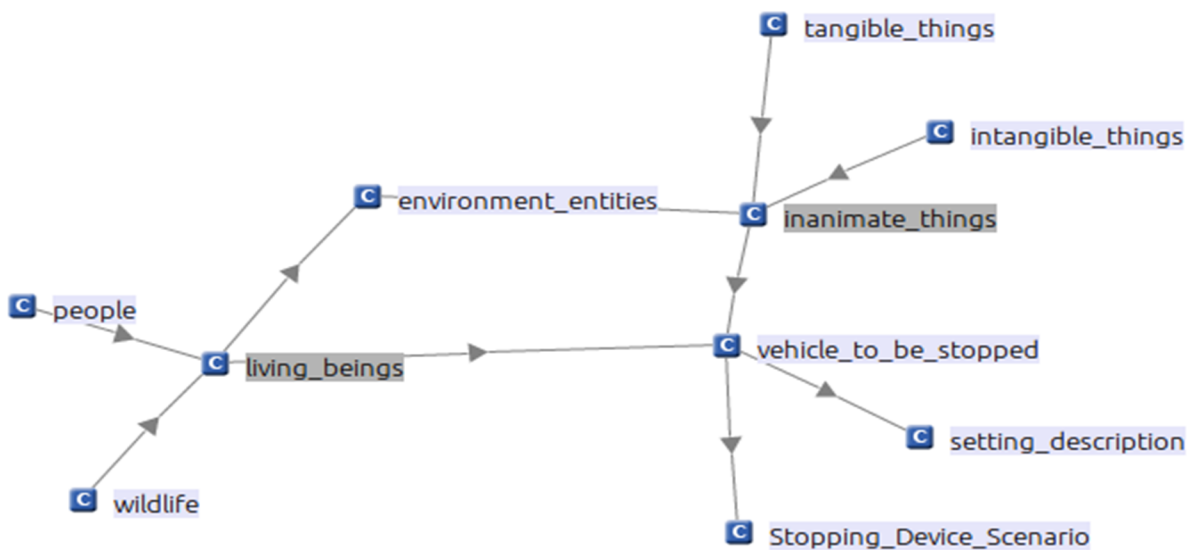


Abb. 3: Übersicht der Beteiligten in einem Anhalteszenario

Im nachfolgenden Abschnitt werden die Relationen zwischen den einzelnen Klassen dargestellt. Beispielsweise hat der Einsatz von Nagelbändern einen Einfluss auf die Reifen des Fahrzeuges, welches gestoppt werden soll, aber auch auf die Reifen anderer Fahrzeuge (siehe Abbildung 4).

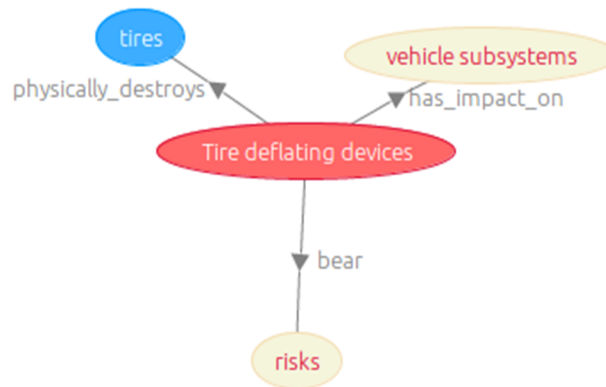


Abb. 4: Relation zur Wirkung von Nagelbändern

Im Kontext von elektromagnetischen Anhaltetechniken ergibt sich eine Wirkung auf die Fahrzeugelektronik.

In Anlehnung an die in Abbildung 5 dargestellten Auswirkungen einer Anhaltetechnik erlauben die Relationen eine Evaluation von verschiedenen Techniken, um abzuschätzen ob der Einsatz einer Methode möglich bzw. zu begründen ist. Aus dieser Basis lassen sich dann Entscheidungsbäume ableiten, welche eine computerunterstützte Anhaltetechnikauswahl ermöglichen, ohne dabei potentielle Risiken aufgrund des Zeitdrucks zu vernachlässigen.

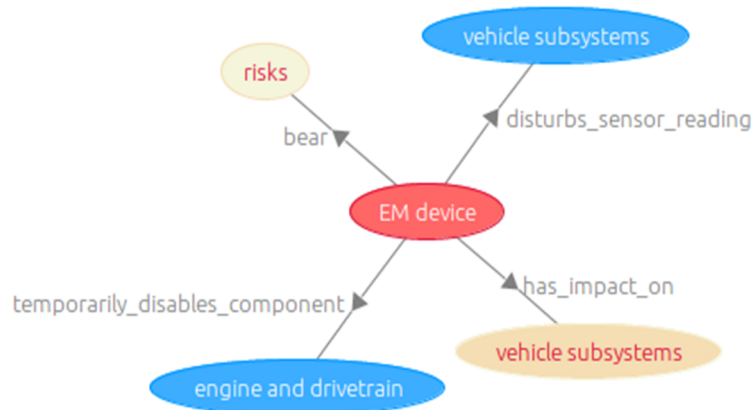


Abb. 5: Wirkung von EM-Geräten auf Fahrzeuge

3.2 Ableitung von Entscheidungsbäumen aus Ontologien

Entscheidungsbäume können anhand der Relationen der Ontologie abgeleitet werden. Unser Ansatz ist eine Abwandlung des Konzeptes von Angriffsbäumen, da sich der erzwungene Anhaltvorgang als Angriff auf das unkooperative Fahrzeug auffassen lässt. Die Wurzel des Baumes ist dabei das Anhalten des Fahrzeuges. Durch die Verwendung von „und“ oder „oder“ Beziehungen zu den jeweiligen Kindknoten kann die Notwendigkeit eine oder alle Bedingungen zu erfüllen, verdeutlicht werden. Für unseren Fall ist insbesondere die Und-Beziehung sinnvoll, da im Zuge der Beurteilung einer Anhaltetechnik eine binäre Entscheidung über deren Einsatz bzw. deren Einsetzbarkeit getroffen werden soll. Die konkreten Implikationen des Einsatzes der Anhaltetechnik müssen nach der initialen Beurteilung anhand des Entscheidungsbaumes evaluiert werden. Der entsprechende Pfad im Entscheidungsbaum, bzw. dessen verwendete Teilbäume geben hierzu jedoch Aufschluss über die zu erwartenden Risiken und Implikationen anhand der Relationen der Ontologie.

Um den Entscheidungsbaum zu erstellen werden unterhalb der Wurzel zwei Kindknoten eingefügt: „Fahrzeug kann gestoppt werden“ und „Implikationen für Entitäten in der Umgebung sind zu rechtfertigen“. Die folgenden Ebenen werden anhand der Ontologie abgeleitet. Hierzu wird im linken Teilbaum evaluiert, ob die untersuchte Anhaltetechnik die gewünschte Wirkung erzielt. Dazu werden, wie in Abbildung 5 dargestellt, die jeweiligen Relationen hinsichtlich der Technik und deren Auswirkung auf Fahrzeugs subsysteme entgegen der Richtung der Relation in die Baumstruktur aufgenommen. Hierbei muss berücksichtigt werden, ob für den jeweiligen Fahrzeugtyp die antriebsrelevanten Funktionen gestört werden. Im rechten Teilbaum werden die restlichen Auswirkungen der Anhaltetechnik sowie potentielle unerwünschte Effekte auf das Fahrzeug abgebildet. Die konkrete Tiefe der Teilbäume hängt stark vom Detailgrad der Ontologie und der Vielfältigkeit der Auswirkungen der Anhaltetechnik ab.

Aus einem solchen Entscheidungsbaum ergibt sich dann beispielsweise aus der Instanz „vielfahren“ der Klasse „Zustand der Fahrbahnoberfläche“ eine deutliche Einschränkung hinsichtlich der anwendbaren Anhaltetechniken, da Nagelbänder, EM-Techniken oder der Schusswafeneinsatz mit hoher Wahrscheinlichkeit Dritte schädigen können. Somit könnten in dem Fall nur noch andere Anhaltetechniken, wie verschiedene Formen von Straßensperren geeignet sein, welche jedoch auch beurteilt werden müssen.

4 Zusammenfassung und Ausblick

Dieser Beitrag schlägt einen semi-automatisierbaren Ansatz für die Erzeugung von Entscheidungsbäumen vor, die bei dem Treffen von Entscheidungen in zeitkritischen Situationen hilfreich sein können. Dabei wird der Zeitraum vor dem Eintritt einer zeitkritischen Situation genutzt, um ein komplexes Modell der möglichen Faktoren in einer solchen Situation zu erzeugen und daraus Handlungsanweisungen abzuleiten. Dieses Vorgehen ähnelt der strategischen Vorbereitung in der IT-Forensik und verwendet dafür Ontologien. Diese beiden Aspekte wurden im Rahmen dieses Beitrages zur "Strategischen Ontologie zur technikfolgenabschätzung für den Polizeigebrauch" (STOP) zusammengeführt. Im Rahmen dieses Beitrags wurde exemplarisch das komplexe Themenfeld des Anhaltens von unkooperativen Fahrzeugen betrachtet und eine erste Systematisierung vorgenommen.

In zukünftigen Arbeiten ist, vor einem praktischen Einsatz der vorgestellten Methodik, eine ausführliche Evaluation der Anhaltetechniken sowie deren Konsequenzen auf alle Beteiligte (siehe Abbildung 3) in Diskussion und Abstimmung mit Experten und Beteiligten sowie Betroffenen notwendig, um auf dieser Basis die Ontologie zu erweitern. Zusätzlich müssen Sicherungsmaßnahmen erarbeitet und umgesetzt werden, um sicherzustellen, dass der Technikeinsatz nur nach positivem Votum und nur durch berechtigte und legitimierte Anwender erfolgt, die Anwendung des vorgeschlagenen Bezugssystems und der Technik nachvollziehbar protokolliert wird, aktuelle Erkenntnisse in den Bezugsrahmen regelmäßig einfließen und berücksichtigt werden, die genutzten Gerätschaften zertifizierte und geprüfte Funktionalität ausüben und regelmäßig durch unabhängige Stellen (vgl. TÜV) überprüft werden.

Danksagung

Dieser Beitrag wurde durch das European Research Foundation Projekt SAVELEC (FP7 - SEC-2011, Grant Agreement Number 285202) unterstützt. Die Autoren möchten darüber hinaus Sven Kuhlmann für die Diskussion der Inhalte des Beitrags und seine Verbesserungsvorschläge danken.

Literatur

- [BBC14] BBC: EU group mulls 'remote car-stopping device' for police. 2014 [Online] <http://www.bbc.com/news/world-europe-25961096>, letzter Zugriff: 14/12/2015
- [BoSa00] B. Bondurant, E. J. Sanow: Bob Bondurant on Police and Pursuit Driving, MBI Publishing Company, 2000
- [Brot99] P. Brothers: Police adopt new rules on shooting at vehicles. The Cincinnati Enquirer, 1999. http://enquirer.com/editions/1999/10/08/loc_police_adapt_new.html, letzter Zugriff: 11/12/2015
- [Case11] E. Casey: Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet - Third Edition. Academic Press, 2011
- [GoBe99] A. Gomez-Perez, V. R. Benjamins: Applications of Ontologies and Problem-Solving Methods. In: AI Magazine, Vol. 20(1), pp. 119-122, 1999
- [Grub93] T. R. Gruber: A Translation Approach to Portable Ontology Specifications. In: Knowledge Acquisition, Vol. 5(2), pp. 199-220, 1993
- [KiHD09] S. Kiltz, T. Hoppe, J. Dittmann: A new forensic model and its application to the collection, extraction and long term storage of screen content off a memory dump. In: 16th International Conference on Digital Signal Processing (DSP2009), pp. 1-6, 2009
- [KoPS14] B. Kordy, L. Piètre-Cambacédès, P. Schweitzer: DAG-Based Attack and Defense Modelling: Don't Miss the Forest for the Attack Trees. In: Computer Science Review 13–14 (2014), pp. 1-38, 2014
- [LuFa08] C.M. Lum and G. Fachner: Police Pursuits in an Age of Innovation and Reform. Alexandria, VA: International Association of Chiefs of Police, p. 4, 2008
- [ONST15] Onstar: Security. [Online] <https://www.onstar.com/us/en/services/security.html>, letzter Zugriff: 14/12/2015
- [Oxfo16] Oxford Reference: Ontology. [Online] <http://www.oxfordreference.com/10.1093/oi/authority.20110803100250688>, letzter Zugriff: 29/03/2016
- [Piou01] R. M. Pious: The Cuban Missile Crisis and the Limits of Crisis Management. In: Political Science Quarterly, Volume 116(1), 2001
- [RGMW06] M. K. Rogers, J. Goldman, R. Mislán, T. Wedge: Computer Forensics Field Triage Process Model. In Journal of Digital Forensics, Security and Law (JDFSL), Association of Digital Forensics, Security and Law (ADFSL), Vol. 1, Issue 2, pp. 27-40, 2006.
- [Stev09] D. J. Stevens: An Introduction to American Policing, Jones and Bartlett Publishers, 2009
- [SAVE12] EU FP7 Project. SAVELEC (SAfe control of non cooperative Vehicles through ELEctromagnetic means). 2012-01-01 – 2016-06-30. Project reference: 285202. URL: <http://savelec-project.eu/>, letzter Zugriff: 26/05/2016