Exemplarische Mensch-Maschine-Interaktionsszenarien und deren Komfort-, Safety- und Security-Implikationen am Beispiel von Gesicht und Sprache

Andrey Makrushin, Jana Dittmann, Stefan Kiltz, Tobias Hoppe

Arbeitsgruppe Advanced Multimedia and Security
Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2
39106 Magdeburg
{makrushin, jana.dittmann, kiltz, t.hoppe}@iti.cs.uni-magdeburg.de

Abstract: Personalisierung, sprachbasierte Bedienung von Fahrzeugsystemen und permanente Beobachtung des Fahrerzustandes gehören zu den am stärksten angestrebten Funktionalitäten eines modernen Fahrzeugs. Mit heute erhältlichen Systemen sind diese Funktionen schwer realisierbar. Die Einführung biometrischer Sensoren könnte diese Funktionalitäten unterstützen. In diesem Beitrag werden Mensch-Maschine-Interaktionsszenarien entwickelt, die auf einer biometrischen Authentifizierung des Fahrers anhand Gesicht und Sprache basieren und das Ziel haben, das Fahrzeug komfortabler und sicherer zu machen. Um die Authentifizierung möglichst zuverlässig zu gestalten, wird eine adaptive dynamische Fusion der biometrischen Merkmale unter Berücksichtigung der automotiven Umgebung vorgestellt. Anhand von Szenarien werden sowohl der erzielbare Nutzen eines solchen Systems demonstriert als auch möglicherweise dadurch neu eingeführte Einschränkungen von Komfort, Funktions- oder Informationssicherheit analysiert. Zudem werden zwei ausgewählte Angriffe auf neue Schnittstellen im Rahmen einer Risikobetrachtung exemplarisch diskutiert, um den Bedarf an Designempfehlungen zu motivieren.

Keywords: Eingebettete Rechensysteme, Automotive, funktionale Sicherheit, Risikobetrachtung, HCI, Fahrerauthentifizierung, Sensordatenfusion

1 Motivation

Um die Ansprüche der Nutzer an Komfort, Safety und Security eines modernen Fahrzeugs zu erfüllen, nimmt die Integration von IT-Technik in einem Auto beständig zu. Zur Erhöhung des Komforts werden als zukünftig potenziell relevante Anwendungen bereits verschiedene Mensch-Maschine-Interaktionsmöglichkeiten erforscht wie z.B. biometrische Fahrererkennungssysteme [LS07,BS07]. Derartige Interaktion als aktive oder passive Fahrer-Assistenz (Maschine zu Mensch) könnte prinzipiell auch die Kommunikation des Fahrers zum Fahrzeug (Mensch zu Maschine) vereinfachen und verbessern. Neue automotive IT-Systeme zur Steigerung des Komforts dürfen jedoch nicht zur Einschränkung der funktionellen Sicherheit (Safety) führen. Auch die Sicherheit gegen beabsichtigte Angriffe (Security) muss angesichts gezielter Angriffe auf gegenwärtige

und zukünftige automotive Kommunikationsnetze [HK07,LD07] im automotiven Sektor zunehmend Berücksichtigung finden. In diesem Beitrag wollen wir Interaktionsparadigmen für Mensch-Maschine- und Maschine-Mensch-Aktionen am Beispiel einer Kamera für potenzielle Gesichts-Erkennung und eines Mikrofons zur Sprach- und Sprechererkennung untersuchen, um das Potential für die Erhöhung des Komforts, der Safety und Security sowie daraus ggf. resultierende Wechselwirkungen zu erforschen. Zur Ermöglichung der Mensch-Maschine-Kommunikation betrachten wir zwei Sensoren, eine low-quality Innenraum-Kamera und ein Mikrofon. Wir erwägen dabei eine Kamera, die auf der Front-Verkleidung oder am Rückspiegel verbaut ist. Der wesentlichste Vorteil einer solchen low-quality Kamera ist, dass sie neben dem niedrigen Preis vielseitig einsetzbar ist. Mikrofone sind in den heute gängigen Automobil-Reihen bereits häufig Bestandteil (z.B. dem Multimedia-Bus angegliedert) und somit kostenneutral. Abbildung 1 stellt schematisch ein solches Fahrzeug mit grob skizzierten Bussystemen dar, wobei neben herkömmlichen Bussystemen auch ein potenzieller (eventuell zukünftig einzuführender) Biometriebus enthalten ist, der aktiv die Vorteile der Kamera und des Mikrofons nutzt.

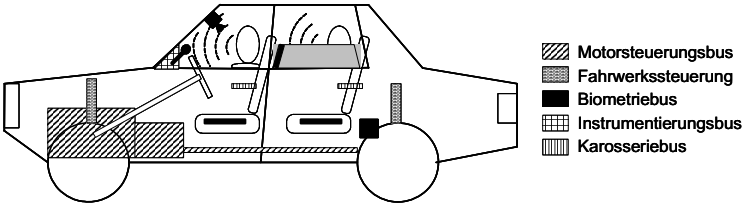

Abbildung 1. Pauschalisiertes Fahrzeug.

Die Nutzung von Kameras und Mikrofonen für das Lösen von Aufgaben aus dem Mustererkennungsbereich (in unserem Beispiel die biometrische Identifikation und die Erkennung von Sprachbefehlen) bringt heute noch gewisse Schwierigkeiten mit sich. Diese werden hauptsächlich durch nicht-konstante Lichtverhältnisse und wechselnden Hintergrund für eine Kamera sowie durch Innenraumgeräusche wegen verschiedener interner und externer Störgeräusche für ein Mikrofon verursacht (siehe z.B. interne und externe Motor- oder Hupgeräusche, Alarmsignale, Radio- oder Mobiltelefongeräusche, mitfahrende Insassen). Um eine bessere Identifikation des Fahrers zu erreichen, sollten alle Sensordaten im Auto in den Identifikationsprozess einbezogen werden, z.B. Fensterpositionen oder die Geschwindigkeit, um die aktuelle Geräuschkulisse erklärbar zu machen und eine angepasste Erkennung zu ermöglichen. Wir schlagen deshalb eine **adaptive dynamische Fusion** vor, die wir in diesem Beitrag weiter ausführen und exemplarisch für Gesicht und Sprache diskutieren. Von nicht-biometrischen Sensoren erhaltene Signale stellen dabei Softbiometriken [JDN04] dar, die bei der Bestimmung der Identität bzw. des Zustandes des Fahrers mit Ausgaben der biometrischen Sensoren (Kamera, Mikrofon) fusioniert werden [RJ03].

Die Hauptidee und Zielsetzung dieses Beitrags ist es, Kommunikationsparadigmen basierend auf Gesicht und Sprache anhand existierender und neuer Sensoren für potenziell sinnvolle Mensch-Maschine-Interaktionsszenarien mittels der diskutierten adaptiven dynamischen Fusion zu analysieren, um exemplarisch aufzuzeigen, wie der Komfort, die Safety und Security des Fahrzeuges erhöht werden können und welche potenziellen neuen Bedrohungen solche Szenarien bergen. Dabei soll keine Vollständigkeit der Szenarien erreicht werden, vielmehr sollen diese Beispiele einer Diskussion dienen, um

zukünftigen Gestaltungsbedarf als auch Gestaltungsmöglichkeiten zu motivieren. Folgende Szenarien werden betrachtet: Fahreridentifizierung für die Vornahme individueller Einstellungen, Identifizierung des Fahrers für den Motorstart, fahrerabhängige Abgrenzung der Fahrzeugfunktionalität, permanente Beobachtung und Verifizierung des Fahrers und Ausführung von Sprachbefehlen. In unseren folgenden Szenarien begrenzen wir uns auf vordefinierte Sprachbefehle, wobei für die Zukunft eine Erkennung beliebiger Texte nicht ausgeschlossen wird.

Nachfolgend stellt Kapitel 2 allgemeine Definitionen zu Komfort, Safety und Security zusammen und führt die von uns benutzten Bewertungsmaße ein. In Kapitel 3 werden die exemplarisch ausgewählten Szenarien zur Mensch-Maschine-Interaktion präsentiert und bezüglich ihres Einflusses auf Komfort, Safety und Security eines Fahrzeuges bewertet. Mögliche Gefahren durch die Einführung von neuen Interaktionsparadigmen im Fahrzeug werden in Kapitel 4 diskutiert. Abschließend werden in Kapitel 5 Schlussfolgerungen über die entworfenen Szenarien gezogen und zukünftige Visionen zur Integration biometrischer Authentifizierungsverfahren in Fahrzeugen diskutiert.

2 Begriffe und Definitionen

In diesem Kapitel werden die Begriffe, Definitionen und Messkriterien eingeführt, die in diesem Beitrag verwendet werden, um den Komfort, die Safety und Security eines Fahrzeuges und seiner Komponenten einzuschätzen.

Generell kann **Komfort** als Bequemlichkeit interpretiert werden, die auf dem Vorhandensein bestimmter Geräte oder Gegenstände beruht. Eine Einrichtung ist komfortabel, wenn sie dem Menschen Aufwand abnimmt und/oder ihm ein Wohlgefühl bietet. Formal wird der Komfort eines Fahrzeuges durch die Summe der integrierten Komponenten und deren Bequemlichkeit bestimmt. Die Bedienung solcher Komponenten wie Fahrassistenz- (Servolenkung) oder Infotainment-Systemen (Radio, TV) ist somit desto komfortabler, je weniger Mühe der Fahrer sich geben muss, ein bestimmtes Ziel zu erreichen. Parallel dazu kann auch der Ablenkungsfaktor betrachtet werden. Wird der Fahrer bei der Bedienung weniger vom eigentlichen Fahren abgelenkt, dann besitzt das System höheren Komfort, da die Bedienung bequemer wird. Zur Klassifizierung des Komforts einzelner Komponenten schlagen wir eine Skala mit zunächst drei Komfortstufen vor (Tabelle 1), die bei Bedarf zukünftig verfeinert werden könnte. Dabei konzentrieren wir uns vor allem auf den Ablenkungsfaktor, da dieser auch die größten Safety- und Security-Implikationen haben kann. Ein Beispiel für manuelle Bedienung (Komfortstufe KS0) ist die Konfiguration und Betätigung herkömmlicher Navigations-Systeme. Um eine Route zu bestimmen, muss der Fahrer anhalten und das Ziel manuell eingeben. Eine Steuerung mit Sprachbefehlen könnte den Komfort der Navigation auf KS1 erhöhen. Um KS2 zu erreichen, muss das Fahrzeug gewisse Vorkenntnisse über den Fahrer (z.B. Gewohnheiten oder physiologische und verhaltensbasierte Charakteristiken / Biometriken) oder die Insassen allgemein haben, d.h. sich komplett an sie anpassen. Daher sollte ihr Verhalten ständig beobachtet werden, um zu lernen, den momentanen Zustand (z.B. Laune, Müdigkeit) zu bestimmen und darauf aufbauend entsprechende Dienste leisten zu

können. Ein Beispiel für die höchste Komfortstufe 2 ist eine automatische Einstellung des Sitzes und der Spiegel beim Einsteigen.

KS0	Manuelle Bedienung des Systems	volle Ablenkung des Fahrers
KS1	halbautomatische Bedienung des Systems	teilweise Ablenkung des Fahrers
KS2	vollautomatische Bedienung des Systems	keine Ablenkung des Fahrers

Tabelle 1. Komfortstufen (KS) bei der Mensch-Maschine-Interaktion.

Um die **funktionale Sicherheit (Safety)** eines Systems abzuschätzen, existieren nach IEC/EN 61508 [IEE07] vier diskrete Stufen, so genannte Sicherheits-Integritätslevels (SILs). Jede Stufe entspricht einem Bereich für die Ausfallwahrscheinlichkeit einer Sicherheitsfunktion. Wir beziehen uns auf eine Interpretation von SILs nach [IE04], die in Tabelle 2 dargestellt ist. Für uns ist die Ausfallwahrscheinlichkeit der technischen Komponenten weniger von Bedeutung als vielmehr die Beeinträchtigung der Safety durch den menschlichen Faktor. Zum Beispiel kann es durch Müdigkeit oder Ablenkung des Fahrers zu einem Unfall kommen. Zudem können Störungen, die durch Mitfahrer unabsichtlich entstehen, den Fahrer oder die Fahrt an sich beeinträchtigen und zu einem Unfall führen. In einer Mensch-Maschine-Interaktion sollten deshalb das Verhalten des Fahrers und als auch der Mitfahrer als safety-bezogener Faktor in Betracht gezogen werden. Im Kontext unserer Untersuchungen sehen wir Safety als a) Sicherheit für Leib und Leben und b) Sicherheit vor unbeabsichtigten Bedrohungen und Gefährdungen.

SIL 1	Stellt die erforderliche Integrität dar, um geringfügige Unfälle zu vermeiden, was in der Regel bereits durch ein ausreichend fehlertolerantes Design gemäß sorgfältiger, gängiger Praxis erreicht werden kann.
SIL 2	Stellt die erforderliche Integrität dar, um ernsthaftere, aber im Ausmaß limitierte, Vorfälle zu vermeiden, von denen in einigen Fällen schwere Verletzungen oder Todesfälle einer oder mehrerer Personen auftreten können.
SIL 3	Stellt die erforderliche Integrität dar, um ernsthafte Unfälle zu vermeiden, die zahlreiche Todesopfer oder schwere Verletzungen nach sich ziehen.
SIL 4	Stellt die erforderliche Integrität dar, um katastrophale Unfälle zu vermeiden.

Tabelle 2. Sicherheits-Integritätslevels (SILs).

Man findet in der Literatur verschiedene Definitionen der IT-Sicherheit. In diesem Beitrag verstehen wir unter dem Begriff **IT-Sicherheit (IT-Security)** alle Maßnahmen, die das Ziel verfolgen, die Vertraulichkeit ($\mathcal{C}$), Integrität ($\mathcal{I}$), Verfügbarkeit ($\mathcal{A}$), Nicht-Abstreitbarkeit ($\mathcal{N}$) und Authentizität ($\mathcal{U}$) von Informationen im IT-Bereich sicherzustellen [HK07]. Sie dient vor allem dem Schutz vor beabsichtigten Gefahren, um Schäden zu vermeiden und Risiken zu minimieren. In Bezug auf automotive Systeme soll Security im Folgenden als a) Sicherheit immaterieller Güter wie im Auto gespeicherter Informationen/Daten und b) Sicherheit vor einer Bedrohung durch absichtliche Angriffe gesehen werden. Dazu könnten biometrische Mechanismen zur Authentifizierung und Autorisierung ergänzend zu bestehenden Sicherheitsmechanismen wie Fahrzeugschlüsseln oder Wegfahrsperren eingesetzt werden.

Wir definieren Mensch-Maschine-Interaktion für die von uns im Weiteren betrachteten Szenarien[1] wie folgt: Über eine **Mensch zu Maschine Schnittstelle** werden Informatio-

[1] Hinweis: Andere Definitionen sind durchaus denkbar und sinnvoll. Die hier aufgeführten Schnittstellen sollen vor allem im Kontext der betrachteten Szenarien stehen und diese fokussieren.

nen von einem Menschen zu einer Maschine übertragen. Ein Mensch ist somit der Sender und eine Maschine ist der Empfänger. Dabei unterscheiden wir zwischen bewussten Aktionen (bei denen der Mensch eine aktive Handlung ausführt) und unbewussten Aktionen (bei denen der Mensch unbewusste Informationen an die Maschine aussendet, die diese erkennen und auswerten muss ohne eine explizite Aktion seitens des Menschen zu erhalten). In den Szenarien verstehen wir den Sprachbefehl als ein Beispiel für eine bewusste Aktion und die Aufnahme des Gesichts als ein Beispiel einer unbewussten Aktion. Der Fahrer zeigt in unserem Beispiel sein Gesicht, ohne bewusst eine spezielle Aktion auszulösen. Dagegen werden über eine **Maschine zu Mensch Schnittstelle** Informationen von der Maschine zum Menschen übertragen oder personanhängige Einstellungen der Maschine getätigt. Eine Maschine ist somit der Sender/Anbieter von Informationen/Einstellungen und ein Mensch ist der Empfänger/Nutzer. Die übertragenen Informationen können z.B. Navigationshilfen oder Warnsignale sein. Unter personabhängigen Einstellungen werden z.B. Einstellungen für Sitze, Spiegel, Klimaanlage usw. oder fahrerabhängige Fahrassistenz / Freischaltung bestimmter Funktionalität verstanden. Abbildung 2 zeigt schematisch und beispielhaft die beiden beschriebenen Mensch-Maschine-Interaktionen. Als Mensch verstehen wir im Folgenden Fahrer oder Insassen, als Maschine verstehen wir das Fahrzeug (Automobil) als Ganzes.

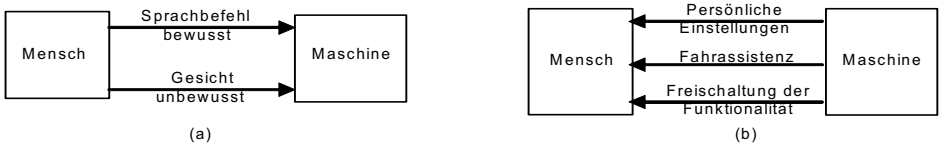

Abbildung 2. Mensch zu Maschine (a) und Maschine zu Mensch (b) Schnittstellen.

3 Beschreibung der Mensch-Maschine-Interaktionsszenarien

In diesem Kapitel entwickeln wir einige ausgewählte Mensch-Maschine-Interaktionsszenarien, die bezüglich ihres Einflusses auf Komfort, Safety und Security klassifiziert und analysiert werden. Diese Szenarien sind: Fahreridentifizierung für Umsetzung individueller Einstellungen (SZ1), Fahreridentifizierung für den Motorstart (SZ2), Fahreridentifizierung für fahrerabhängige dynamische Abgrenzung der Fahrzeugsfunktionalität einschließlich fahrerabhängiger Motorisierung (SZ3), permanente Beobachtung und Verifizierung des Fahrers (Erkennung der Müdigkeit, Emotionen, Ablenken) (SZ4) und Fahrerverifizierung zur anschließenden Ausführung von Sprachbefehlen (SZ5). In Tabelle 3 werden die Szenarien zusammengefasst und bezüglich der erzielten Verbesserungen von Komfort, Safety und Security klassifiziert. Der zusätzliche Wert SIL0 bei den Safety-Betrachtungen repräsentiert dabei das Nicht-Vorliegen der betrachteten Safety-Eigenschaft in aktuellen Systemen.

Im Weiteren beschreiben wir ein generelles Kommunikationsschema, wobei einige bestimmte Aktionen genauer definiert und formalisiert werden. Eine Vollständigkeit, gerade auch vor dem Hintergrund der variierenden Technik im Automobil, soll an dieser Stelle nicht erreicht werden. Vielmehr soll das prinzipielle Konzept einer adaptiven und dynamischen Unterstützung von Komfort, Safety und Security gezeigt werden. Unter **adaptiv und dynamisch** verstehen wir die Fusion von gesichts- und sprachbasierten

Merkmalen mit Merkmalen aus der automotiven Umgebung (z.B. Daten nichtbiometrischer, automotiver Sensoren).

	Komfort	Safety	Security
SZ1	Fahreridentifizierung für Umsetzung individueller Einstellungen, wie Sitze, Spiegel usw.; KS0 zu KS2;		
SZ2			Fahreridentifizierung für Start des Motors. Authentizität des Fahrers ist gewährleistet ($\mathcal{U}$).
SZ3		Fahreridentifizierung für adaptierte Motorisierung und erzwungene dynamische Einschaltung der Fahrassistenzsysteme; SIL0 zu SIL1;	
SZ4		Permanente Beobachtung Beobachtung bzgl. Müdigkeit, Emotionen und Ablenkung des Fahrers. Informationen an den Fahrer zu unvorhergesehenen Ereignissen oder Ausfällen und Risiken; SIL0 zu SIL2;	Verifizierung der Fahreridentität. Vermeidung eines Fahrertausches bei laufendem Motor. Authentizität des Fahrers ist gewährleistet ($\mathcal{U}$).
SZ5	Vereinfachung der Kommunikation, Reduzierung der Ablenkung vom Fahren; KS0 zu KS1	Sprachbefehle zur Bedienung von Fahrzeugkomponenten. Individualisierung der Spracherkennung durch Fahreridentifizierung, um zufällige, safetyrelevante Ereignisse durch Insassen oder externe Kommunikation auszuschließen bzw. zu verhindern; SIL0 zu SIL1	Individualisierung der Spracherkennung durch Fahreridentifizierung, um gezielte Angriffe durch Insassen oder externe Kommunikation auszuschließen bzw. zu verhindern. Authentizität der Sprachbefehle ist gewährleistet ($\mathcal{U}$).

Tabelle 3. Mensch-Maschine-Interaktionsszenarien bezüglich der Verbesserung von Komfort, Safety und Security.

Zielsetzung ist es dabei, einerseits (a) bei Ausfall eines Merkmals adhoc weitere Eigenschaften zu nutzen, um eine erfolgreiche Auswertung entsprechend des Szenarios zu erzielen (Adaptivität) und andererseits (b) die biometrische Authentifizierung vor dem Hintergrund sich dynamisch ändernder Umgebungseinflüsse entsprechend anzupassen (dynamisch oder adaptiv). Die Idee ist dabei für (a) so genannte Softbiometriken (Soft Biometrics) zu erfassen, die aus automotiven Sensoren bestimmt werden. Im Folgenden werden wir als Softbiometrik **exemplarisch** das Gewicht des Fahrers nutzen, um den Ansatz zu verdeutlichen. Zur Erfassung der Umgebungseinflüsse für (b) definieren wir relevante Umweltereignisse und dazugehörige Sensortechnik zur Erfassung, um aufgrund der aufgenommen Größen eine entsprechende Wichtung vorzunehmen. Exemplarisch werden sechs Sensoren ausgewählt, um das Konzept zu verdeutlichen. Die Kommunikation beginnt mit einer Aktion (siehe $AktX_i$ in Abbildung 3) von Seiten des Fahrers (Mensch) in Form des Bereitstellens biometrischer Modalitäten (Gesicht, Sprache) – Aktion 1. Das Fahrzeug (Maschine) bekommt biometrische Daten und verwendet diese z.B. zur Authentifizierung des Fahrers – Aktion 2. Sollte der Fahrer als zugelassen authentifiziert werden, so erfolgt z.B. eine Aktivierung des Motors – Aktion 3. Sollte er nicht authentifiziert werden, wird er abgewiesen oder eine Information wie Warnhinweise an den Halter gesendet – Aktion 4. Wir benutzen ein Sequenzdiagramm (siehe Abbildung 3) zur grafischen Darstellung des Interaktionsablaufs. Die Aktionen werden als Bestandteile für die Mensch-Maschine-Interaktionsszenarien verwendet.

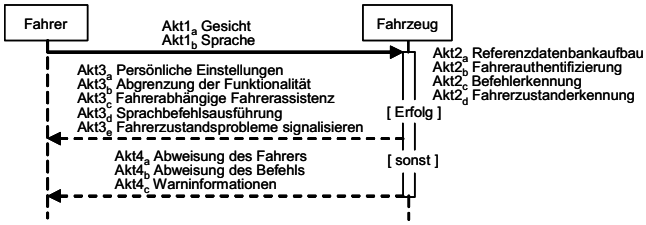

Abbildung 3. Sequenzdiagramm des Mensch-Maschine-Interaktionsablaufs.

Für die formale Beschreibung der Szenarien definieren wir die folgenden Komponenten: F sei eine Menge aller Fahrzeuge f_i: $f_i \in F$ und P eine Menge von Personen (potenzielle Fahrer, Insassen oder Angreifer) p_i: $p_i \in P$. Zu jeder Person p_i betrachten wir drei Modalitäten m_{i1}, m_{i2}, m_{i3}, die wobei m_{i1} dem Gesicht, m_{i2} der Sprache und m_{i3} dem Gewicht (exemplarisch für eine mögliche Softbiometric, andere Betrachtungen sind hier natürlich denkbar) der Person p_i entsprechen, die zu einem Messungszeitpunkt t aufgenommen werden ($m_{ij}= m_{ij}(t)$, j=1,2,3).

Da wir in der Folge nur elementare Szenarien mit nur einem Fahrzeug betrachten, werden wir den Index bei f in der Folge weglassen. Ein bestimmtes Fahrzeug f sei gegeben. Für dieses Fahrzeug bestimmen wir eine Menge Z als Untermenge von P: $Z \subset P$ zugelassener Fahrer z_i: $z_i \in Z$. Ebenfalls definieren wir eine weitere Untermenge A: $A \subset P$ als Menge potenzieller Angreifer[2] a_i: $a_i \in A$ und eine Menge I: $I \subset P$ von Auto-Insassen i_i: $i_i \in I$. Jede Person kann unter Umständen jede dieser Rollen annehmen, z.B. könnte ein Beifahrer (Insasse) ebenfalls ein zulässiger Fahrer desselben Fahrzeugs sein. Außerdem führen wir verschiedene Umgebungsgrößen u_k , k=1,2,... ein. In diesem Beitrag betrachten wir **exemplarisch fünf Größen** u_1, u_2, u_3, u_4, u_5, wobei u_1 der Geräuschkulisse, u_2 den Lichtverhältnissen, u_3 der Sitzbelegung, u_4 den Fensterpositionen und u_5 der Geschwindigkeit entsprechen, die ebenfalls zum Messungszeitpunkt t erfasst werden ($u_k= u_k(t)$, k=1,...,5). Zudem definieren wir für ein Fahrzeug f biometrische und nicht biometrische Sensoren, die benutzt werden um die biometrischen Modalitäten und die Umgebungsverhältnisse zu erfassen. Wir wählen exemplarisch sechs Sensoren aus, deren Messdaten wir als s_1, s_2, s_3, s_4, s_5 und s_6 bezeichnen, wobei s_1 das Kamerabild, s_2 die Mikrofonaufnahme, s_3 die Sitzbelegungswerte, s_4 die Innenraumhelligkeit, s_5 die Fensterpositionen und s_6 die Geschwindigkeit repräsentieren, die zum Zeitpunkt t aufgenommen wurden ($s_l= s_l(t)$, l=1,...,6).

Für jeden im gegebenen Fahrzeug f zugelassenen Fahrer z_i definieren wir eine Menge K_i der nur für ihn gültigen Sprachkommandos $k_{i1,} \ldots, k_{i|Ki|} \in K_i$., wobei $|K_i|$ die Anzahl der für den Fahrer z_i individuell hinterlegten Spachbefehle ist. Zudem definieren wir die Referenzdatenbildung als eine Abbildung R_f: $P \rightarrow Z$, und gehen weiter davon aus, dass R_f schon durchgeführt und eine Datenbank aller registrierter Fahrer $z_1...z_n$ und dementsprechende Mengen zulässiger Sprachkommandos $K_1...K_n$ im Automobil f gespeichert wurde. Eine adaptive Aufbewahrung von Referenzdaten [URJ04] wird von uns vorgesehen, wird aber im Rahmen dieses Beitrags nicht im Detail betrachtet.

Da wir in allen weiteren Szenarien eine **biometrische Authentifizierung** des Fahrers vorsehen, definieren wir zuerst generell, um daraufhin die Identifizierung/Verifizierung in den Einzelfällen zu betrachten. Abbildung 4 zeigt dazu das generelle Authentifizierungsschema. Ein potenzieller Fahrer p_i steigt ein und gibt einen Sprach-Befehl k_{im}. Sowohl biometrische Modalitäten m_{ij}, j=1,...,3 des Fahrers als auch Umgebungsverhältnisse u_k, k=1,...,5 werden in Form von Sensorwerten s_l, l=1,...,6 aufgenommen. Weiterhin wird ein Vertrauensfaktor V_j, j=1,...,3 für jede der verwendeten Modalitäten zum Messzeitpunkt t als Funktion der Sensorausgaben berechnet. V_1 bestimmt den Vertrauensfaktor der Kameraaufnahme angesichts von Beleuchtungsvariationen. Er hängt von der Innen-

[2] Dies schließt nicht aus, dass in einem Notfall auch nicht-autorisierte Personen die Rolle des Fahrers einnehmen können, sofern sie ein anderes Autorisierungsmerkmal vorweisen können (beispielsweise den bei erfolgreicher Identifizierung durch das biometrische System aus Komfortgründen nicht benötigten Schlüssel)

raum-Helligkeit s_4 und den Fensterpositionen s_5 ab: $V_1=V_1(t,s_4,s_5)$. V_2 bestimmt den Vertrauensfaktor für das Sprachsignal angesichts von Fahrgeräuschen oder Zugluft. Er hängt von den Fensterpositionen s_5 und der Geschwindigkeit s_6 ab: $V_2=V_2(t,s_5,s_6)$. Für V_3 verwenden wir eine vordefinierte Konstante. Generell kann man einen Vertrauensfaktor als eine reelle Funktion zum Messzeitpunkt von Sensorausgaben mit dem Wertebereich [0,1] definieren: $V_j=V_j(t,s_1,...,s_h)$, $V_j \in R_{[0,1]}$, wobei h die Anzahl der Sensoren ist, im Beispiel h=6. Je größer V_j ist, desto mehr wird der Modalität vertraut.

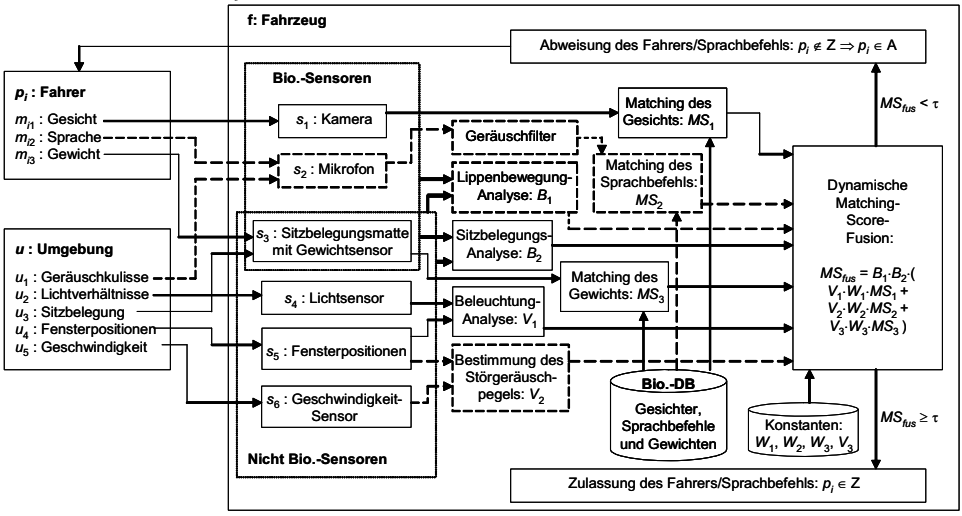

Abbildung 4. Biometrische Authentifizierung des Fahrers. Punktierte Elemente werden nur bei einer kombinierten Authentifizierung anhand Gesicht und Sprachbefehl aktiv.

Die konstanten reellen Gewichte W_1, W_2 und W_3 mit dem Wertebereich [0,1] sind motiviert nach [SVD05] vorbestimmt und stellen standardmäßige Beiträge der einzelnen Modalitäten für die Fusionsentscheidung dar. Die Berechnung der Gewichte basiert auf einer Schätzung der Equal Error Rate (EER). Die Ähnlichkeitswerte, im folgenden engl. Matching-Scores genannt, für Gesicht MS_1, Sprache MS_2 und Gewicht MS_3 entstehen durch den Abgleich der zum Messzeitpunkt t erfassten biometrischen Sensordaten s_1, s_2 bzw. s_3 mit der Datenbank: $MS_j=MS_j(t,s_j)$. Um das System angriffresistenter zu machen, werden exemplarisch **binäre** Zusatzbedingungen in Form von Funktionen $B_1=B_1(t,s_1,\ldots,s_6)$ als Lippenbewegungsflag und $B_2=B_2(t, s_1,\ldots,s_6)$ als Sitzbelegungsflag eingeführt. Es wird geprüft, ob der Fahrer p_i auf seinem Platz sitzt (B_2=1) und ob der Sprachbefehl wirklich vom Fahrer p_i ausgesprochen wurde (B_1=1). Die Ermittlung/Verifikation der Identität und dementsprechende Akzeptanz oder Abweisung des Fahrers p_i wird mittels einer adaptiven dynamischen Fusion vorgenommen. Dabei wird ein mutual Matching-Score MS_{fus} als eine lineare Kombination der Matching-Scores der einzelnen Modalitäten mit den zusammengesetzten Gewichten $V_j \cdot W_j$ gebildet und mit den binären Zusatzbedingungen multipliziert:

$$MS_{fus} = \prod_{j=1}^{2} B_j(t, s_1, ..., s_6) \cdot \sum_{j=1}^{3} V_j(t, s_3, ..., s_6) \cdot W_j \cdot MS_j(t, s_j) \quad wobei \quad \sum_{j=1}^{3} V_j \cdot W_j = 1$$

Der Einfachheit halber verwenden wir motiviert aus den Ergebnissen aus [SVD05] eine lineare Verknüpfung der Matching-Scores, wobei zukünftig jedoch auch andere Lösun-

gen untersucht werden müssten. Die Adaptivität der vorgeschlagenen Fusion äußert sich in den umgebungsabhängigen Gewichten V_j, die die Qualität bzw. den Vertrauensfaktor für das jeweilige Signal ermitteln. Sollte einer der Vertrauensfaktoren klein sein, werden dadurch die anderen automatisch größer, indem man die Summe der Gewichte auf 1 normiert. Dadurch wird außerdem erreicht, dass der mutual Matching-Score MS_{fus} im Intervall [0,1] liegt. Zusätzlich können weitere Charakteristika der Geräuschkulisse u_1 (z.B. Alarmsirenen oder Äußerungen von Mitfahrern) über ein Geräuschfilter auch direkt aus dem Mikrofonsignal s_2 ermittelt werden sowie im Idealfall per Trennung (Fission) aus der Eingabe für den Sprachbefehlsabgleich (Matching) entfernt werden. Je nachdem, ob in einem der folgenden Szenarien die Fahrerauthentifizierung nur anhand von Gesicht oder in Kombination mit einem Sprachbefehl geschieht, sind bestimmte Blöcke aus Abb.4 aktiv oder passiv, wodurch eine **adaptive und dynamische Anpassung** erfolgt.

SZ1 (Umsetzung individueller Einstellungen): Ein potenzieller Fahrer p_i steigt in das Fahrzeug *f* ein. Sein Gesicht m_{i1} wird sofort aufgenommen und daraufhin seine Identität mittels Identifizierung festgestellt (siehe Abbildung 4). Sollte die Identität einem der bekannten Fahrer, z.B. z_1, entsprechen, werden Fahrersitz, Spiegel, Lenksäule, Radio, Klimaanlage und weitere Fahrzeugsysteme vollautomatisch an den Fahrer p_i angepasst (siehe Abbildung 5). Sollte der Fahrer p_i nicht erkannt werden, bleiben die Einstellungen unverändert. Da Sprache und Lippenbewegung hier nicht berücksichtigt werden (B_1=1, MS_2=0), gilt für die Fusionsformel: $MS_{fus\_SZ1} = B_2 \cdot \left(V_1 W_1 MS_1 + V_3 W_3 MS_3\right)$

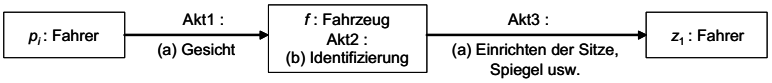

Abbildung 5. Szenario SZ1= { $Akt1_a$, $Akt2_b$, $Akt3_a$ }.

SZ2 (Start des Motors): Ein potenzieller Fahrer p_i steigt in das Auto ein und sagt z.B.: „Motor starten". Vorraussetzung dafür ist insbesondere, dass bei ihm dabei Lippenbewegung B_1 und Sitzbelegung B_2 detektiert werden und die aus den Lichtverhältnissen sowie dem Störgeräuschpegel gewonnenen Vertrauensfaktoren V_1 bzw. V_2 eine Erkennung ermöglichen. Entspricht die ermittelte Identität (siehe Abb. 4) einem zugelassenen Fahrer, z.B. z_1, so wird der Motor gestartet (Abbildung 6), andernfalls erfolgt kein Start und/oder können andere Aktionen eingeleitet werden. Die Fusions-Formel lautet $MS_{fus\_SZ2} = B_1 \cdot B_2 \cdot \left(V_1 W_1 MS_1 + V_2 W_2 MS_2 + V_3 W_3 MS_3\right)$.

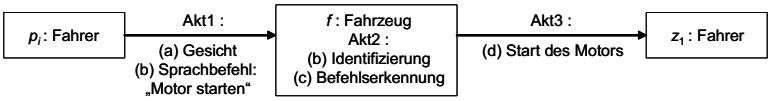

Abbildung 6. Szenario SZ2 = { $Akt1_a$, $Akt1_b$, $Akt2_b$, $Akt2_c$, $Akt3_d$ }.

SZ3 (Fahrerabhängige dynamische Abgrenzung der Fahrzeugsfunktionalität): Ein potenzieller Fahrer p_i steigt ein und spricht einen angezeigten Text, der zufällig vom Automobil generiert wird. Wird durch die dazu direkt auf den Fahrer gerichtete Kamera Lippenbewegung B_1 detektiert und entspricht die ermittelte Identität des Fahrers p_i (siehe Abb. 4) einem der zugelassenen Fahrer, z.B. z_1, werden besondere, für den Fahrer z_1 relevante, Komponenten freigeschaltet. Im Weiteren werden für z_1 (wenn nötig) die Motorleistung begrenzt und Fahrassistenz-Systeme aktiviert. Sollte die Person p_i nicht erkannt werden, bleiben die zusätzlichen Funktionen inaktiv. Dies kann beispielsweise eintreten, wenn ein anderer Insasse den Befehl spricht. In diesem Fall kann beim Fahrer keine passende Lippenbewegung detektiert werden oder der tatsächliche Sprecher wird

vom Geräuschfilter als Teil der Geräuschkulisse u_1 erkannt und herausgefiltert. Szenario SZ3 wird in Abb. 7 dargestellt. Für das vorliegende SZ3 lautet die zugehörige Fusionsformel: $MS_{fus\_SZ3} = B_1 \cdot B_2 \cdot \left(V_1 W_1 MS_1 + V_2 W_2 MS_2 + V_3 W_3 MS_3\right)$.

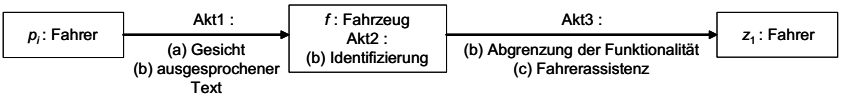

Abbildung 7. Szenario SZ3 = { Akt1_a, Akt1_b, Akt2_b, Akt3_b, Akt3_c }.

SZ4 (Permanente Beobachtung des Fahrers): Bei diesem Szenario wird ein laufendes Fahrzeug betrachtet. Es wird davon ausgegangen, dass der Fahrer p_i bereits als ein zugelassener Fahrer z_1 erkannt wurde (z.B. durch das Szenario SZ2) und seine Identität dem Auto bekannt ist. Nach dem Start des Motors wird die Kamera in den Beobachtungsmodus umschaltet. Sie wird so auf den Fahrer z_1 gerichtet, dass der Kopf des Fahrers immer vom Kameraobjektiv erfasst wird. Funktionen zur Gesichts- und Augendetektion sowie zur Augenverfolgung sind in der Kamera vorhanden. Durch die Beobachtung der Häufigkeit des Blinzelns kann versucht werden, eine Übermüdung des Fahrers zu erkennen. Sollte dies eintreten, so wird ein Signal an den Fahrer gesendet oder ihm angezeigt, eine Fahrpause einzulegen (siehe Abbildung 8). Neben Müdigkeit kann auch der emotionale Zustand des Fahrers beobachtet werden, indem Gesichtsmerkmale abgeschätzt werden [CG00]. Über den ausgewerteten emotionalen Zustand wird der Fahrer informiert und darauf hingewiesen, z.B. eine Pause einzulegen. Der dritte beobachtete Faktor kann der Ablenkungsgrad des Fahrers sein, welcher durch eine Kontrolle der Kopfposition und des Blickwinkels erkannt werden kann. Sollte der Fahrer z.B. zu lange Zeit nicht geradeaus schauen, können akustische Warnsignale gegeben werden. Die Identität des Fahrers z_1 wird während der Beobachtung regelmäßig verifiziert (siehe Abb. 4). Sprache und Lippenbewegung spielen für dieses Szenario keine Rolle (B_1=1, MS_2=0), die Fusionsformel lautet $MS_{fus\_SZ4} = B_2 \cdot \left(V_1 W_1 MS_1 + V_3 W_3 MS_3\right)$.

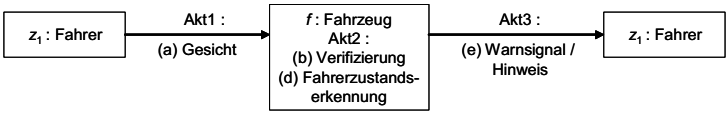

Abbildung 8. Szenario SZ4 = { Akt1_a, Akt2_b, Akt2_d, Akt3_e }.

SZ5 (Ausführung der Sprachbefehle): Bei diesem Szenario wird wie bereits bei SZ4 ein laufendes Fahrzeug betrachtet. Der Fahrer sei z_1 und i_1 ... i_4 weitere Insassen. Die Identität des Fahrers ist dem Auto bekannt. Um eine Komponente bzw. Funktion des Fahrzeugs zu bedienen, spricht der Fahrer z_1 ein Sprachkommando k_{1m} aus. Beim Ausführen des Sprachbefehls wird zunächst der Befehl erkannt. Zweitens wird durch eine Verifizierung geprüft (siehe Abbildung 4), ob der Befehl vom Fahrer und nicht von einem der Insassen stammt (sofern er nicht bereits explizit als Teil der Geräuschkulisse u_1 erkannt wurde) und nur dann ausgeführt. Das Szenario SZ5 wird in Abb. 9 dargestellt. Die Fusionsformel lautet: $MS_{fus\_SZ5} = B_1 \cdot B_2 \cdot \left(V_1 W_1 MS_1 + V_2 W_2 MS_2 + V_3 W_3 MS_3\right)$.

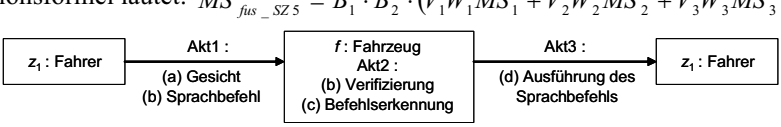

Abbildung 9. Szenario SZ5 = { Akt1_a, Akt1_b, Akt2_b, Akt2_c, Akt3_d }.

4 Mögliche Beeinträchtigung des Komfort, der Safety und Security

Zwei wesentliche Schwachstellen der betrachteten biometriebasierten Interaktions-Paradigmen sollen exemplarisch diskutiert werden, die bei ungeeignetem Design Komfort, Safety und Security beeinträchtigen können. Dies sind die sichere Aufbewahrung biometrischer Daten und unvermeidbare Fehlentscheidungsquoten. In allen beschriebenen Szenarien reduzieren Authentifizierungsfehler den Komfort. In den Szenarien SZ2, SZ3 und SZ5 können sie die Security und in Szenarien SZ3, SZ4 und SZ5 die Safety gefährden. Um die Sicherheitsrisiken durch ein ungeeignetes Design des Sicherheits-Systems zu verdeutlichen, behandeln wir zwei exemplarische Angriffe A1 und A2 - einer bezogen auf das Authentifizierungssystem und einer auf die Fahrzeugbusse.

A1: Verfälschung biometrischer Modalitäten. Sei z_1 ein zugelassener Fahrer, der mit dem Fahrzeug *f* kommuniziert und a_1 ein Angreifer, der das Ziel hat, das Fahrzeug zu stehlen. Während der Aktionen $Akt1_{(a,b)}$ übermittelt der Fahrer z_1 biometrische Modalitäten (Gesicht, Sprachbefehl) zum Fahrzeug *f*. Diese Modalitäten könnten von einem Angreifer ausspioniert werden, indem er z.B. mit einem Rekorder die Sprache und mit einer Kamera Fotos vom Gesicht aufnimmt. Er könnte nun eine Gesichtsmaske herstellen und zusammen mit aufgenommenen Sprachbefehlen im Fahrzeug einspielen, um z.B. den Motor zu starten und das Fahrzeug zu stehlen. Dieses Beispiel entspricht einer Kombination der zwei Basisangriffe [LD07] „Mitlesen" und „Einspielen" (siehe Abbildung 10). Durch diesen Angriff werden Vertraulichkeit (*C*) der biometrischen Merkmale und folglich die Authentizität (*U*) des Fahrers kompromittiert. Nach CERT [HL98] könnte a_1 ein Autodieb (*Angreifer*) sein, der mittels typischer Aufnahmegeräte (*Werkzeuge*) eine *Schwachstelle* in Design ausnutzt, um mittels der *Aktionen* Aufnehmen (Mitlesen) und Einspielen der biometrischen Merkmale das Authentifizierungssystem (*Ziel*) zu betrügen und dadurch Zugriffe auf Fahrzeugkomponenten (*unautorisiertes Resultat*) zu bekommen, was der Realisierung seiner *Absicht* dient, das Fahrzeug zu stehlen.

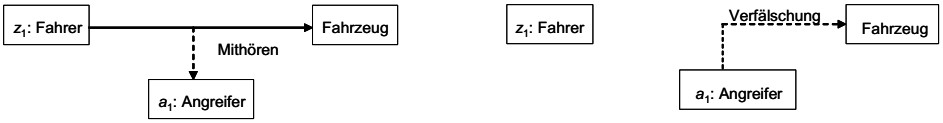

Abbildung 10. Potenzieller Angriff auf Akt1.

A2: Gewinn eines vollständigen Zugriffs zur Fahrzeugfunktionalität. Hier betrachten wir einen Angriff auf den Fahrzeugbus um z.B. die biometrische Authentifizierung oder die Wegfahrsperre zu umgehen und direkt alle Fahrzeugsysteme zu aktivieren. Mit diesem Angriff kompromittiert man die Ziele, die auch in SZ3 angestrebt werden. Eine CERT-Beschreibung dieses Angriffs sieht folgendermaßen aus: Als *Angreifer* a_2 wird ein junger Erwachsener betrachtet, dem nur beschränkte Funktionalität erlaubt ist und der das *Absicht* verfolgt, nicht erlaubte Funktionen einzuschalten (z.B. Freischaltung höherer Motorleistung). Er kauft sich eine von Dritten ausgefertigte Tuning-Platine (*Werkzeug*) und klemmt diese zwischen den Sperrungssystemen (z.B. Wegfahrsperre) und den anliegenden Bussen an. Dabei werden potenzielle *Schwachstellen* im Design bzw. Positionierung des Sicherheitssystems und schwache oder fehlende Verschlüsselung der Bustelegramme ausgenutzt. Als *Aktion* blockiert die Tuning-Platine das Sperrungssignal (Unterbrechung) und sendet ein Zulassungssignal (Erzeugen) an alle Fahrzeugsysteme (*Ziel*). Somit resultiert ein unerlaubter Zugriff zu Fahrzeugkomponenten (*unautorisiertes Resul-*

tat). Der Angriff verletzt die Vertraulichkeit ($\mathcal{C}$), Integrität ($\mathcal{I}$) und Authentizität ($\mathcal{U}$) der Bustelegramme und dadurch letztendlich die Verfügbarkeit ($\mathcal{A}$) der Sperrungssysteme.

Beide exemplarische Angriffe motivieren ein gutes Design für ein Mensch-Maschine-Interaktionssystem, um eine sehr zuverlässige Fahrerauthentifizierung vorzusehen, die durch eine adaptive dynamische Fusion sowohl biometrische Daten als auch Informationen über die automotive Umgebung in Betracht zieht. Dadurch wird eine Verfälschung biometrischer Daten zwar nicht ausgeschlossen, jedoch sehr erschwert. Sollte z.B. ein Autodieb ein deutlich anderes Gewicht als alle zulässigen Fahrer haben, wird die Komponente MS_3 in der Fusionsformel klein und dadurch auch der Matchingscore nach der Fusion MS_{fus} für den Angreifer kleiner. Eine zweite unerlässliche Bedingung eines guten Designs sind wirksame Maßnahmen für automotive IT-Security, die in Fällen wie A2 direkte Angriffe auf Hardware-Komponenten und Feldbus-Kommunikation erschweren.

5 Zusammenfassung und Ausblick

Generell können Sprache und Gesicht zwei wesentliche Erweiterungen der Funktionalität eines modernen Fahrzeugs bringen: eine sprachbasierte Bedienung von Fahrzeugsystemen sowie eine Personalisierung des Fahrzeugs durch sichere biometrische Identifizierung des Fahrers. In Kapitel 4 wurden zwei generelle Schwierigkeiten bei der Realisierung der erwähnten Funktionalität identifiziert. Biometrische Authentifizierung im Automobil stellt besondere Anforderungen an das Design der Systeme, die zur Ausführung der vorgeschlagenen Szenarien erforderlich sind. Eine adaptive und dynamische Fusion von Gesicht, Sprache und weiterer Sensordaten, die an die aktuelle Umgebung angepasst ist, kann durch Erkennen von Störungen einerseits die biometrische Erkennung verbessern, aber auch gezielte Angriffe auf das biometrische System durch Konsistenzprüfungen beherrschbar machen. Eine adaptive Umgebung bedeutet in diesem Fall, dass ein Fahrzeug das Verhalten seines Fahrers ständig unter den wechselnden Bedingungen im Automobil lernt und bei der Identifizierung des Fahrers oder der Erkennung der Sprachbefehle Störungsfaktoren berücksichtigt. Desktop-IT-basierter Mustererkennungssysteme nutzen bereits Algorithmen für adaptives Lernen, die technisch gesehen in das automotive Umfeld übertragen werden können. In diesem Beitrag wurden fünf exemplarisch ausgewählte Mensch-Maschine-Interaktionsszenarien vorgestellt um zu zeigen, dass die Einführung von Kameras und Mikrofonen viele neue Funktionalitäten ermöglichen kann. Diese erweitern nicht nur den Komfort des Fahrzeuges, sondern auch seine funktionale Sicherheit und Angriffresistenz. Die Szenarien wurden sowohl bezüglich des Zugewinns als auch potenzieller Einschränkungen an Komfort, Safety und Security analysiert. Die Integration biometrischer Authentifizierung in das Automobil wurde unter Berücksichtigung potenzieller Gefahren angeregt. Zukünftig können die motivierten Ansätze beispielsweise in Richtung einer Erkennung beliebiger Texte noch erweitert werden.

Danksagungen
Diese Veröffentlichung entstand in Kooperation mit dem Verbundprojekt COmpetence in MObility (COMO, EU-Nr.: C-2007-5254). Der Inhalt dieser Veröffentlichung steht in alleiniger Verantwortung der Autoren und widerspiegelt somit in keiner Weise die Meinung der Europäischen Union.

Literaturverzeichnis

[LS07] Mirko Langnickel, Katharina Seifert; Anforderungen und Möglichkeiten - Biometrie im Kontext automobiler Applikationen; In: Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security, Wolfsburg, Germany; 27.-28. November 2007, VDI-Verlag, pp. 111.-129, ISBN 978-3-18-092016-0, 2007

[BS07] Ulrich Büker, Rüdiger Schmidt; Biometrische Fahreridentifikation; In: Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security, Wolfsburg, Germany; 27.-28. November 2007, VDI-Verlag, pp. 95-109, ISBN 978-3-18-092016-0, 2007

[JDN04] A. K. Jain, S. C. Dass and K. Nandakumar, "Soft Biometric Traits for Personal Recognition Systems", Proc. International Conference on Biometric Authentication (ICBA), pp. 731-738, Hong Kong, July 2004.

[RJ03] A. Ross and A.K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, Vol. 24, Issue 13, pp. 2115-2125, September, 2003.

[IEE07] The Institution of Engineering and Technology, “IEC 61508 – The IET”, URL: http://www.iee.org/oncomms/pn/functionalsafety/61508faq_mainupdate.cfm, 2007

[IE04] Innovation Electronics (UK) Ltd, HSL: A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines / Health and Safety Laboratory. 2004. – Forschungsbericht.

[HK07] Tobias Hoppe, Stefan Kiltz, Andreas Lang, Jana Dittmann; Exemplary Automotive Attack Scenarios: Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system; In: Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security, Wolfsburg, Germany; 27.-28. November 2007, VDI-Verlag, pp. 165-183, ISBN 978-3-18-092016-0, 2007

[URJ04] U. Uludag, A. Ross and A.K. Jain: Biometric template selection and update: a case study in Fingerprints, Pattern Recognition 37(7), pp. 1533-1542; 2004

[SVD05] T. Scheidat, C. Vielhauer and J. Dittmann; Distance-Level Fusion Strategies for Online Signature Verification. In Proceedings of the IEEE International Conference on Multimedia and Expo (ICME), Amsterdam, The Netherlands, 2005.

[CG00] I. Cohen, A. Garg and T.S. Huang; Emotion Recognition from Facial Expressions using Multilevel HMM. In Neural Information Processing Systems, 2000.

[LD07] Andreas Lang, Jana Dittmann, Stefan Kiltz, Tobias Hoppe; Future Perspectives: The Car and its IP-Address - A Potential Safety and Security Risk Assessment; In: Computer Safety, Reliability, and Security, Proceedings of the 26th International Conference SAFECOMP 2007, Nuremberg, Germany, September 2007; Springer LNCS 4680; pp. 40-53; Editors: Francesca Saglietti, Norbert Oster; ISBN 978-3-540-75100-7.

[HL98] J.D.Howard and T.A.Longstaff; A Common Language for Computer Security Incidents (SAND98-8667) / Sandia National Laboratories. 1998 (ISBN 0-201-63346-9). – Forschungsbericht.