Hochschule Reutlingen
Reutlingen University

INF
Informatik

Uwe Kloos, Natividad Martínez, Gabriela Tullius (Hrsg.)

Tagungsband

Hochschule Reutlingen

17 Informatics Inside

www.infoinside.reutlingen-university.de
infoinside@reutlingen-university.de

Hochschule Reutlingen
Reutlingen University

INF
Informatik

Uwe Kloos, Natividad Martínez, Gabriela Tullius (Hrsg.)

Informatics Inside
Digital Future

Informatik-Konferenz an der Hochschule Reutlingen
10. Mai 2017

ISBN 978-3-00-056455-0

Impressum

Anschrift:
Hochschule Reutlingen / Reutlingen University
Fakultät Informatik
Human-Centered Computing
Alteburgstraße 150
D-72762 Reutlingen

Telefon: +49 7121 / 271-4002
Telefax: +49 7121 / 271-4042

E-Mail: infoinside@reutlingen-university.de
Internet: http://www.infoinside.reutlingen-university.de

Organisationskomitee:
Prof. Dr. Gabriela Tullius, Hochschule Reutlingen
Prof. Dr. Natividad Martínez, Hochschule Reutlingen
Prof. Dr. Uwe Kloos, Hochschule Reutlingen

Lukas Brand
Heiko Brumme
Tobias Fleischer
Gamze Gök
Isabel Hagen
Denise Junger
Mücahit Karabulut
Dina Kurbanismailova
Arjana Mehmeti
Armin Müller
Iana Preuß
Marc Roswag
Anastasia Schmieder
David Schneider
Oliver Streicher
Benjamin Weinert

Hochschule Reutlingen
Reutlingen University

Herstellung und Verlag: Hochschule Reutlingen
ISBN 978-3-00-056455-0

Vorwort

Zur neunten Informatics Inside Konferenz unter dem Motto „Digital Future“ darf ich Sie herzlich willkommen heißen! Jedes Jahr organisieren Studentinnen und Studenten des Masterprogramms „Human-Centered Computing“ die Konferenz mit äußerst hohem Engagement, um Ihnen ihre wissenschaftlichen Arbeiten ihres jeweiligen Vertiefungsgebiets vorzustellen. Dabei stellen sich die Studierenden nicht nur der Herausforderung Neues zu erforschen, sondern verantworten auch die Organisation und Durchführung des Konferenztags. Neben den Vorträgen der Master-Studenten erwarten Sie auch eine Vielzahl von Posterbeiträgen von Studierenden anderer Programme sowie von Schülerinnen und Schülern der Ferdinand-von-Steinbeis-Schule und der Kerschensteinerschule aus Reutlingen.

Die digitale Zukunft zu definieren und zu gestalten ist in aller Munde – in der Industrie, der Lehre und so auch im Fokus der diesjährigen Informatics Inside Konferenz. Dazu gehören einerseits die Möglichkeiten, die die Digitalisierung mit sich bringt, z.B. beschrieben im Umfeld Krankenhaus oder in der Pferdezucht, andererseits die Schnittstelle zwischen realer und virtueller Welt, ausgeführt an Beispielen der Gesichts- und Bewegungserkennung. Auffällig ist, dass auch die Studierenden sich immer stärker auf die Sicherheit und Privatsphäre persönlicher Daten in einer digitalen Welt fokussieren. Dazu gehören fundamentale Sicherheitsuntersuchungen für ausgewählte Domänen, z.B. Industrie 4.0 oder Smart Home, wie auch die Betrachtung konkreter Einsatzszenarien, wie das autonome Fahren, die Kommunikation zwischen Fahrzeugen und dem neuen Personalausweis. Darüber hinaus stellen die Studierenden ihre Master-Projekte in Kurzbeiträgen vor.

Die Teilnehmer erfüllen nicht nur den Anspruch, die Ergebnisse ihrer Arbeit in schriftlicher Form anschaulich auszuarbeiten, sondern auch interaktiv vor ihrem Publikum zu verteidigen und zu diskutieren. Die Informatics Inside bietet somit ein Forum für Studierende, um während des Studiums, zum einen die Ergebnisse ihrer Arbeit professionell einem interessierten Publikum zugänglich zu machen und zum anderen Anregungen anderer Vertiefungsgebiete aufzunehmen, aber auch die Arbeiten anderer kritisch zu hinterfragen. Diese wertvolle Erfahrung bereichert das Kompetenz-Portfolio aller Beteiligten maßgeblich.

Ich wünsche allen Besuchern und Vortragenden viel Spaß und hoffe auf intensive Diskussionen, neue Ideen und einige Erkenntnisse wie unserer digitale Zukunft gestaltet werden kann.

Prof. Dr.-Ing. Marcus Schöller

Inhaltsverzeichnis

Longpaper

Shortpaper

Schülerbeiträge

Analyse von 3D-Controllern zur Steuerung der Echtzeit-MRT

Vanessa Zurawka
Reutlingen University
Vanessa.Zurawka@Student.Reutlingen-University.DE

Abstract

Die Arbeit stellt die Möglichkeiten von 3D-Controllern für den Einsatz in der interventionellen Radiologie und insbesondere für die Steuerung der Echtzeit-Magnetresonanztomographie (MRT) dar. Dies ist interessant in Bezug auf die kontrollierte Navigation in ein Zielgewebe. Dabei kann der Interventionalist durch Echtzeit-Bildgebung den Verlauf des Eingriffs verfolgen, allerdings kann er bisher das MRT während der Durchführung des Eingriffs nicht selbst steuern, da dies durch den Assistenten im Nebenraum erfolgt. Die Kommunikation ist bei dem hohen Geräuschpegel aber sehr schwer. Diese Arbeit setzt an dieser Stelle an und analysiert 3D-Controller auf die Eignung für die Echtzeit-Steuerung eines MRTs. Dabei wurden trackingbasierte und trackinglose Geräte betrachtet. Als Ergebnis ließ sich festhalten, dass trackingbasierte Verfahren weniger geeignet sind, aufgrund der nicht ausreichenden Interpretation der Eingaben. Die trackinglosen Geräte hingegen sind aufgrund der korrekten Interpretation aller Eingaben und der intuitiven Bedienung geeignet.

Betreuer Hochschule: Prof. Dr. Oliver Burgert
Hochschule Reutlingen
Oliver.Burgert@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

Schlüsselwörter

Intervention, MRT, Echtzeit, 3D-Controller

CR-Kategorien

I.3 Computer Graphics, I.3.6 Methodology and Techniques: Interaction techniques

1 Einleitung

In der interventionellen Radiologie werden Instrumente in das Zielgewebe eines Patienten eingeführt und mit intraoperativer Bildgebung kann sich der Chirurg im Körper orientieren. [1, S.467] Somit kann der Eingriff konstant überwacht und entsprechend unmittelbar korrigiert werden, [2, S.872] MRT-Systeme sind besonders interessant aufgrund des hohen Weichteilkontrasts, der Multiplanarität und der nicht vorhandenen Strahlung. [3, S.14] Des Weiteren haben viele Hersteller bereits Interfaces für Interventionen, welche multiplanare Bildebenen darstellen können. Bisher werden zwar die Bilder auf Monitoren im MR-Raum für den Chirurgen dargestellt, aber die Steuerung des MRTs erfolgt im Nebenraum durch die Assistenten. Insbesondere beim Echtzeit-MRT wird die Kommunikation durch die zusätzlichen lauten Geräusche stark erschwert. [4] Aufgrund dessen wäre es sinnvoll, wenn der Chirurg während des Eingriffs die MRT-Geräteparameter selbst einstellen könnte, zum einen um die Kommunikation zum Nebenraum zu ersetzen und zum anderen um Zeit zu gewinnen. In dieser Arbeit werden deshalb 3D-Controller analysiert und verglichen, um die Eignung für diesen Anwendungsfall zu prüfen.

2 Interventionelle Radiologie

In diesem Bereich der Radiologie werden therapeutische Leistungen für den Patienten angeboten. Unter Bildgebung werden Sonden für die Biopsie oder Thermotherapie auf dem günstigsten Weg ins Zielgewebe eingeführt. Des Weiteren gehören Tumorbehandlungen mit Röntgen- oder Ionenstrahlen in diesen Bereich. [1, S.467]

Allgemein gehören zu den bildgebenden Systemen die Röntgentechnik, die Computertomographie, die Magnetresonanztomographie (MRT) und der Ultraschall. Diese Arbeit fokussiert sich allerdings auf die Unterstützung von MRT-basierten Eingriffen, sodass die MRT im Folgenden näher beschrieben wird.

2.1 MRT

Die Magnetresonanztomographie (engl.: magnetic resonance imaging, Abk.: MRT, MRI), die auch Kernspintomographie genannt wird, erzeugt überlagerungsfreie Schichtbilder unterschiedlicher Körperschichten, die einen hohen Weichteilkontrast aufweisen. [3. S.14] Im menschlichen Körper kommen Atomkerne vor, was die Magnetresonanztomographie zur Bildgebung nutzt. In den meisten Fällen werden Wasserstoffkerne, also einfache Protonen, verwendet. Die Protonen haben einen Spin und bewegen sich wie magnetische Kreisel, die in einem stärkeren äußeren Magnetfeld eine Präzessionsbewegung ausführen. Die Kerne selbst werden kurzzeitig zum Sender, indem kurze Impulse von elektromagnetischen Wellen im Frequenzbereich der Radiowellen eingestrahlt werden. [5, S.185] Die Intensität der Signale hängt dabei von vielen messtechnischen und gewebespezifischen Einflüssen ab. Die hohe Bandbreite an Darstellungsmöglichkeiten von Gewebestrukturen ist durch die Beeinflussung der gemessenen Bildsignale im Gewebe durch mehrere sich überlagernde Relaxationsprozesse zu begründen. Zusammenfassend stellen die generierten Bilder „[…] die Verteilung der zum Messzeitpunkt in jedem Volumenelement einer Körperschicht vorliegenden Magnetisierung durch Verwendung von Grauwertskalen […]“ dar. [3, S.14] Der Aufbau eines MRTs ist in Abbildung 1 dargestellt.

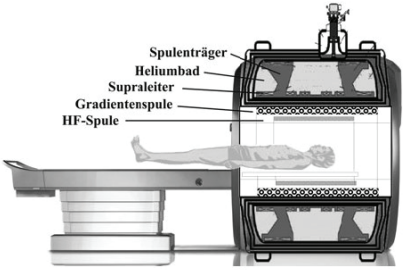

Abbildung 1: Prinzipaufbau eines MRT [6, S.342]

2.2 Minimalinvasive Tumortherapie

Das Interesse an der Entwicklung von minimalinvasiven Therapieverfahren in der Medizin hat stark zugenommen. Dabei ist bei der lokalen Zerstörung von Tumoren das Applizieren von thermischer Energie eine viel versprechende Möglichkeit. Zu den thermoablativen Verfahren gehören die Elektroporation, Laser-, Mikrowellen-, Kryo-, und Radiofrequenzablation (RFA). [7, S.1] Dabei kommt die RFA am häufigsten zum Einsatz, da diese eine relativ einfache Anwendung mit guten Ergebnissen bei der Tumorzerstörung und zudem niedrige Komplikationsraten aufweist. Bei der RFA wird unter Bildgebung eine Nadelelektrode im Tumorgewebe positioniert. Um die Nadel möglichst genau und sicher zu positionieren, muss eine konstante Bildkontrolle erfolgen. Dies ist mit Ultraschall, Computertomographie oder MRT möglich. Dabei hat die MRT einige Vorteile gegenüber den anderen Bildgebungen: die multiplanare Schichtführung, einen besseren Weichteilkontrast, die Abgrenzung von Gefäßen ohne Kontrastmittel und die Temperaturdarstellung des Gewebes. Die größten Nachteile bisher sind allerdings der hohe Zeitaufwand und dadurch auch die hohen Kosten. [8]

3 State-of-the-Art

Ein Großteil der Hersteller von MRT-Systemen bietet integrierte Benutzeroberflächen für Interventionen an. Diese haben die Möglichkeit multiplanare Bildebenen zur interaktiven Lokalisierung, Planung und Überwachung des Eingriffs darzustellen. [9, 10] Des Weiteren können sie auf Bildschirmen innerhalb des MR-Raumes dargestellt werden, wobei die Bedienung über die MR-Konsole im Vorraum durch den Assistenten erfolgt. Um allerdings einen unmittelbaren Nutzen aus der Multiplanarität zu gewinnen, wäre die selbständige Einstellung der Ebenen und Bildparameter vom Interventionalist selbst sinnvoll. Hinzu kommt die schwierige Kommunikation zwischen Interventionalist und Assistenten bei Eingriffen mit Echtzeit-MRT, da hier die lauten Gradientengeräusche hinzukommen und die Kommunikation zusätzlich erschweren. [4] In diesem Zusammenhang wurde in [11] eine MR-taugliche PC-Maus in das MRT-System integriert. In dieser Studie waren die Ziele die Steuerung der Bildauswahl, sowie weitere Einstellungen, wie die Fensterung, der Sequenzstart und -wechsel. Damit konnte der Interventionalist komfortabel, sicher und unabhängig von der technischen Assistenz arbeiten. Allerdings wurde die PC-Maus nur zur Steuerung der Benutzeroberfläche der Software verwendet. Des Weiteren wäre diese nicht zur Steuerung im 3D-Raum geeignet, da nicht genügend Schaltflächen bereitstehen. Diese Arbeit setzt bei der Steuerung des MRTs in Echtzeit an. Da hier bei Sichtverlust der Instrumentenspitze der Vorteil wäre, sofort reagieren zu können und nicht die Echtzeit-Bildgebung unterbrechen zu müssen.

4 3D-Controller

In diesem Kapitel werden verschiedene 3D-Controller beschrieben. Hierfür wurde eine Vorauswahl getroffen, bei der folgendes Kriterium ausschlaggebend war: Die einhändige Benutzung, da der Interventionalist in der anderen Hand sein Instrument hält.

4.1 Trackingbasiert

Bei trackingbasierten Verfahren werden entweder Bewegungen des Menschen oder eines Eingabegerätes mit Hilfe von Methoden der Bildrekonstruktion verfolgt und anschließend die Position und Orientierung im Raum rekonstruiert. Die Geräte werden frei bewegt. [12, S.293]

4.1.1 Microsoft Kinect

Bei diesem Verfahren benötigt der Benutzer kein weiteres Eingabegerät, da die Kopf-, Hand- und Fingerbewegungen erfasst werden. Der größte Nachteil dabei ist allerdings die Genauigkeit und Robustheit der Eingabe. Tiefenkameras können nicht nur Bilder aufnehmen, sondern auch den Abstand vom Objekt zur Kamera erfassen. Meist wird Infrarotlicht eingesetzt und mit Tiefensensoren gemessen, wie lange der Lichtstrahl bis zu einer Oberfläche benötigt. Die verschiedenen Längen des Lichtstrahls werden zu einer Tiefenkarte zusammengefasst. Diese Art an Kameras war lange Zeit sehr teuer, bis zur Markteinführung der Microsoft Kinect. Diese erzeugen ein Signal, das allerdings in der Auflösung und Qualität begrenzt ist. In vielen Fällen wird das Signal deshalb mit Filtermethoden und Bildrekonstruktion verbessert. Der Anwender muss sich immer innerhalb eines definierten Bereichs befinden und die Position und Orientierung wird dann mit Hilfe eines Skeletts dargestellt. Aufgrund der vorhandenen Software Development Kits kann ein breiter Einsatz erfolgen. Die Tiefenkamera hat eine Auflösung von 640 x 480 Pixeln und ermöglicht eine Bildrate von 30 Hz, was allerdings bedeutet, dass sehr schnelle Bewegungen meist nicht erfolgreich erfasst werden und kleine Details im Bild verloren gehen. Die Tiefenauflösung liegt bei 11 Bit und demnach können 2048 Tiefenwerte erfasst werden. [12, S.302f]

4.1.2 Leap Motion

Der Leap Motion 3D-Controller basiert auf zwei Kameras und Infrarot-Bildgebung zur Detektion von Händen. Der Controller befindet sich für gewöhnlich zwischen den

Händen und dem Bildschirm und kann einen Bereich von 60 Zentimetern in alle Raumrichtungen detektieren. Dabei können fünf Bilder pro Sekunde analysiert werden und entsprechend gering fällt die Latenz aus. Aufgrund der Interpretierung der Fingerbewegungen als Gesten kann Zoomen, Pannen und Scrollen als natürliche Bewegung realisiert werden. [12, S.299]

4.1.3 Wiimote

Die Wii Remote (Abk.: WIIMOTE) wurde ursprünglich als Eingabegerät für Computerspiele entwickelt, aber wird inzwischen auch darüber hinaus eingesetzt. Durch einen Beschleunigungssensor ist die Steuerung mit Armbewegungen im Raum möglich. Des Weiteren können mit den Bedienelementen Modi und Kommandos ausgeführt werden. Dafür gibt es ein Digitalsteuerkreuz und zudem sieben weitere Tasten. Das Gerät basiert auf Bluetooth mit dem kabellos bis zu vier Infrarot-Hotspots getrackt werden können. Bereits 2009 wurde die Wii Motion Plus eingeführt, die eine genauere Positionsbestimmung und Bewegungserfassung bietet. Die Anwendung ist insbesondere für die Interaktion mit 3D-Darstellungen auf großen Bildschirmen geeignet. Das Gerät wird wie ein Laserpointer zur Auswahl von Objekten verwendet. [12, S.301f]

4.1.4 Datenhandschuh

Die Beweglichkeit einer menschlichen Hand kann durch die Menge an möglichen Handlungen für die 3D-Interaktion genutzt werden. Dafür müssen Finger, Daumen und Handgelenk erfasst werden, was mit Hilfe mehrerer Kameras und der daraus resultierenden 3D-Rekonstruktion passieren kann. Eine andere Möglichkeit wäre die Übermittlung von Daten über Sensoren am Benutzer, was die Hand zuverlässiger und genauer erfasst. Die ursprüngliche Idee des Einwebens von Sensoren in einen Handschuh ist relativ alt (erster Prototyp 1970). Dabei wurden Dehnmessstreifen zur Krümmungsmessung einzelner Finger verwendet und zudem ein Tracking der Handposition und -orientierung mit beispielsweise reflektierenden Markern am Datenhandschuh, um die Hand im Ganzen zu erfassen. Seither wurden einige Datenhandschuhe entwickelt, unter anderem der Power Glove, der für Nintendo-Spiele vermarktet wurde. Die Meisten sind heutzutage zudem drahtlos, was zu einer starken Verbesserung der Ergonomie führt. Der große Nachteil an solchen Geräten ist die große Variation der Hände von Mensch zu Mensch, wodurch eine Kalibrierung nötig ist bei der der Benutzer verschiedene Gesten ausführen muss. Systeme die darauf verzichten sind demnach weniger genau. Der Datenhandschuh erfasst zwar alle Freiheitsgrade der Hand, ist allerdings dabei unbequem, bewegungseingeschränkt und kann nicht schnell beiseitegelegt werden. [12, S.297]

4.2 Trackinglos

Im Folgenden werden trackinglose Eingabegeräte vorgestellt. Diese basieren auf der mechanischen Eingabe des Benutzers.

4.2.1 Haptische Ein-/Ausgabegeräte

Für haptische Interaktionen in virtuellen Simulationsumgebungen gibt es spezielle Hard- und Softwarelösungen. Diese Geräte haben einen 3D-Arbeitsraum, sodass die Bewegungen direkt auf die virtuelle Szene übertragen werden können. Somit wird eine intuitive Interaktion und Manipulation von Objekten im 3D-Raum möglich. Die wichtigsten Merkmale sind die Anzahl der Freiheitsgrade, die Größe des Arbeitsbereichs, die räumliche Auflösung und die maximale Kraftrückgabe. Die Geräte können auch werkzeugbasiert sein, sodass der Benutzer einen Stift in der Hand hält. Diese sind besonders für den medizinischen Bereich geeignet, um beispielsweise Skalpelle, Punktionsnadeln und endoskopische Instrumente zu simulieren und mit diesen im virtuellen Raum zu interagieren. [3, S.338] Mechanische Eingabegeräte können die Bewegungen eines Anwenders über eine Mechanik aufnehmen, wie beispielsweise über ein Gestänge oder einen Seilzug. Die Vorteile sind die hohe Genauigkeit und die

gute Eignung für haptisches Feedback. Die Nachteile sind die Gebundenheit an das Gerät und die teilweise störende Mechanik. Bei einem Stift ist der Anwender bereits daran gewöhnt und insofern kann die Anwendung intuitiv gesteuert werden. Die Messung erfolgt mit Winkelmessungen an den Gelenken oder Rollen und Abstandsmessungen zwischen den Gelenken. Eine hohe Messgenauigkeit wird dabei durch Zahnräder, Potentiometer oder Dehnmessstreifen erreicht. Aufgrund der direkten Messung ist die Latenz sehr gering. Die Leichtgängigkeit ist bei solchen Geräten sehr wichtig, da der Benutzer so nicht eingeschränkt wird und das Gerät nicht als störend erachtet. Als zusätzliche Komponente kann dem mechanischen Eingabegerät ein haptisches Feedback hinzugefügt werden, sodass es gleichzeitig zum Ausgabegerät wird. [13, S.110f] Die Abbildung 3 stellt das haptische Gerät Phantom Omni dar.

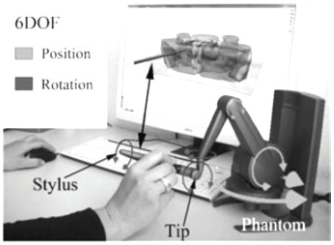

Abbildung 2: Haptisches Gerät Phantom Omni [12, S.320]

4.2.2 3D-Mäuse

3D-Mäuse wurden zur Steuerung von 3D-Positionen und Orientierungen entwickelt. [12, S.289] Sie sind eine der einfachsten Eingabegeräte und verfügen meist zusätzlich über frei belegbare Buttons. [13, S.110] Von der 2D-Maus können wichtige Merkmale übernommen werden, wie das Aufsetzen auf eine Unterlage, das Greifen und Loslassen, das keine Aufmerksamkeit erfordert und das kontrollierte Bewegen des Cursors. Diese Vorteile wurden versucht auf die entwickelten 3D-Mäuse zu übertragen. [12, S.289] Ein Nachteil ist aber die Gebundenheit an den Desktop, allerdings werden viele VR-Anwendungen im Raum ausgeführt, sodass oft die Verwendung von Zeigegeräten erfolgt, die in der Hand gehalten und frei im Raum bewegt werden können. [14, S.33f] Der Vorteil wiederrum ist die sehr hohe Genauigkeit. [13, S.110] Die SpaceMouse und der SpaceNavigator wurden von dem Hersteller 3DConnexion entwickelt und bieten eine freie 3D-Eingabe. Rotationen, Translationen und Zoomen werden durch Drücken, Drehen, Kippen und Ziehen der Kappe ermöglicht. Der SpaceNavigator ist auf diese Funktionalität beschränkt, sodass eine Taste das 3D-Modell in der Mitte des Bildschirms ausrichtet und die andere Taste Navigationseinstellungen zugänglich macht. Die SpaceMouse hingegen bietet mit vier Funktionstasten, sowie Tasten für Control, Shift, Alt und Escape weitere Möglichkeiten. [12, S.290f]

4.2.3 Fußschalter

Steute Meditec entwickelt Hand- und Fußschalter für den medizinischen Bereich und insbesondere für die Bildgebung. Dabei kann zwischen den Produktlinien „Classic“ und „Custom“ gewählt werden. Ersteres bietet Standardkomponenten, die mit Gehäuse, Aktoren und Schalteinsätzen konfiguriert werden können. Das „Custom“-Programm liefert User Interfaces, die individuell für den Anwender entwickelt werden. Des Weiteren lassen sich die Geräte einfach reinigen und die Kommunikation erfolgt über Funk, durch einen selbst entwickelten Funkstandard, der den Anforderungen der Medizintechnik entsprechen soll. [15] In Abbildung 4 ist eine Möglichkeit eines Fußschalters dargestellt.

Abbildung 3: Beispiel eines Fußschalters von steute [18]

5 Bewertung der Eingabegeräte

Im Nachfolgenden werden Anforderungen an die vorgestellten 3D-Controller definiert. Anschließend werden diese mit den Geräten verglichen und ausgewertet.

5.1 Anforderungen

Bei der interventionellen Radiologie mit Echtzeit-Bildgebung gibt es Anwendungsszenarien, die in Kapitel 3 und 4 beschrieben werden, aus welchen sich bestimmte Anforderungen ableiten lassen, die nachfolgend aufgelistet sind:

- Intuitive Bedienung
- Korrekte Interpretation aller Eingaben
- schnelle Integration und Entfernung
- Sterilität
- MR-Kompatibilität
- Einhändige Bedienung

Die *intuitive Bedienung* ergibt sich daraus, dass meist verschiedene Ärzte den gleichen Eingriff praktizieren und entsprechend meist keine Zeit bleibt neue Interaktionsformen zu erlernen, insbesondere da der Arzt sich während des Eingriffs auf das Vorschieben des Instruments konzentriert und von dem Steuergerät nicht abgelenkt werden darf. Dies wird in dieser Arbeit durch eigene Erfahrungen und Studien aus der Literatur bewertet.

Die *korrekte Interpretation aller Eingaben* muss gegeben sein, da der Arzt sonst vom Eingriff abgelenkt werden könnte oder im schlimmsten Fall das Instrument falsch führt, wenn sich die Bildebene spontan anders verändert als zu erwarten war. Die Bewegungen des Anwenders müssen also immer exakt und konstant korrekt übertragen und interpretiert werden. Diese Anforderung wird mit einem Testaufbau bewertet.

Die *schnelle Integration und Entfernung* muss möglich sein, da gegebenenfalls das 3D-Steuergerät für andere Eingriffe vom MRT entfernt werden muss. Des Weiteren darf keine zusätzliche Zeit für das Einrichten des Geräts notwendig sein, da das Ziel eine Zeiteinsparung beim Eingriff sein soll. Das Gerät sollte entsprechend nur an den richtigen Platz gestellt und an das System angeschlossen werden und gleich funktionieren. Dies wird mit einem Testaufbau bewertet.

Die *Sterilität* ergibt sich aus den Bedingungen bei Interventionen. Dabei ist der Interventionalist steril und die zu behandelnde Körperstelle des Patienten. Das heißt für die 3D-Controller, dass sie entweder nicht berührt werden, oder steril abgedeckt oder eingepackt werden müssen.

Die *MR-Kompatibilität* ergibt sich aus den Gegebenheiten des MRTs. Aufgrund des Magnetfeldes dürfen die Geräte keine magnetischen Teile enthalten, da es sonst zu starken Bildbeeinträchtigungen kommen kann. Diese Anforderung kann allerdings im Rahmen dieser Arbeit nicht getestet werden, da kein MRT-Gerät zur Evaluation zur Verfügung steht.

Die *einhändige Bedienung* muss möglich sein, da der Interventionalist in einer Hand die Nadel in den Körper führt. Entsprechend hat er zeitgleich nur eine Hand frei für die Steuerung der Bildgebung. Da diese Anforderung zwingend erforderlich ist, wird diese zur Vorauswahl der 3D-Controller verwendet. Entsprechend sind alle Controller, die im Nachfolgenden beschrieben werden, einhändig bedienbar.

5.2 Vergleich 3D-Controller

Im Nachfolgenden wird nun diskutiert, ob die vorgestellten 3D-Controller die zuvor angeführten Anforderungen erfüllen können.

5.2.1 Microsoft Kinect

Die *intuitive Bedienung* ist hier stark abhängig von der Implementation der Gestenerkennung. Für den Anwendungsfall kommen entweder Hand- oder Fingerbewegungen in Frage, da Kopfbewegungen für 3D-Eingaben sehr ungünstig sind. Allerdings ist bei Gestenerkennungen generell die Robustheit die größte Schwierigkeit. Des Weiteren

müssten Gesten zum Starten und Beenden der Verschiebung der Ebene erlernt werden, da sonst nicht klar differenziert werden kann. Ohne diese Gesten müsste die Hand immer in der gleichen Position gehalten werden, was aber nicht möglich wäre bei gleichzeitiger Führung eines Instruments.

Eine *korrekte Interpretation aller Eingaben* kann eine kamerabasierte Lösung meist nicht bieten, da die Erkennung nicht immer eine korrekte Interpretation der Gesten gewährleisten kann. Zwar können Gesten bei einer nicht eindeutigen Identifikation ignoriert werden, was im Anwendungsfall für den Arzt aber sehr störend sein kann.

Die *schnelle Integration und Entfernung* wäre größtenteils erfüllt, da die Kamera auf einen günstigen Platz gestellt und schnell angeschlossen werden kann. Allerdings muss das Sichtfeld der Kamera entsprechend gut ausgerichtet sein, sodass der Arzt die Gesten immer im Sichtfeld ausführt.

Die *Sterilität* ist sehr einfach möglich, da der Arzt hier im Raum agiert und das Gerät nicht anfassen muss, um es zu bedienen. Somit ist die Sterilität vollkommen gewährleistet.

5.2.2 Leap Motion

Bei diesem 3D-Controller sind die gleichen Vorteile, als auch Nachteile wie bei der Kinect zu nennen. Der einzige Unterschied ist, dass die Leap Motion ausschließlich für die Detektion der Hand entwickelt wurde. Somit kann davon ausgegangen werden, dass die Erkennung von Gesten eine etwas höhere Detektionsrate aufweist.

5.2.3 Wiimote

Die *intuitive Bedienung* ist bei der Wiimote deutlich besser, als bei der Microsoft Kinect und dem Leap Motion Controller. Das liegt insbesondere an dem zusätzlichen Eingabegerät, das wie ein Laserpointer funktioniert. Entsprechend müssen keine Gesten erlernt werden, sondern das Gerät kann intuitiv im Raum bewegt werden und die Buttons am Gerät können als Start- oder Endsignal für die Veränderung der Ebene genutzt werden. Dies ist ein deutlicher Vorteil gegenüber den anderen beiden kamerabasierten Geräten.

Eine *korrekte Interpretation aller Eingaben* ist wahrscheinlich in den meisten Fällen möglich, aber aufgrund der Kamera nicht immer gewährleistet. Im Gegensatz zu den anderen kamerabasierten Systemen aber deutlich besser.

Eine *schnelle Integration und Entfernung* wäre wie auch bei der Kinect und dem Leap Motion Controller gegeben. Ein Nachteil ist aber die Notwendigkeit von Batterien, sodass entweder für jeden Eingriff aus Sicherheitsgründen neue Batterien verwendet werden, oder diese gegebenenfalls während dem Eingriff ausgetauscht werden müssen, was allerdings zusätzliche Zeit beansprucht.

Die *Sterilität* ist bei der Wiimote schwieriger zu gewährleisten, da das Eingabegerät vom Anwender in der Hand gehalten werden muss und dieses nicht steril ist. Ritter et al. [16] haben allerdings gezeigt, dass die Wiimote eingeschweißt werden kann und die Erkennung trotzdem gut genug funktioniert.

5.2.4 Datenhandschuh

Bei diesem Gerät ist die *intuitive Bedienung* in etwa wie bei anderen kamerabasierten Systemen, mit dem zusätzlichen Nachteil, dass der Anwender den Handschuh immer tragen und dieser zusätzlich auf den Anwender kalibriert werden muss.

Eine wirklich *korrekte Interpretation aller Eingaben* kann der Datenhandschuh meist auch nicht bieten, allerdings befindet sich die Präzision etwa bei der gleichen Genauigkeit wie die Wiimote, da auch hier ein zusätzliches Gerät zur Kamera vorhanden ist.

Eine *schnelle Integration und Entfernung* ist bedingt gegeben, da zwar die Positionierung der Kamera einfach zu bewerkstelligen ist, allerdings der Handschuh selbst kalibriert werden muss, was Zeit benötigt.

Die *Sterilität* ist sehr schwer umsetzbar, da der Datenhandschuh selbst nicht steril ist und nicht eingeschweißt werden kann, wie

die Wiimote. Eine sterile Haube kann auch nicht über den Datenhandschuh gezogen werden, da sonst die Erkennung nichtmehr funktionieren würde. Entsprechend kann der Datenhandschuh nicht für intraoperative Eingriffe verwendet werden, außer er wird aus Materialien gefertigt, die sterilisiert werden können.

5.2.5 Phantom Omni

Eine *intuitive Bedienung* ist gewährleistet, da der Anwender haptisch das Gerät in der Hand halten kann und die Ebene intuitiv verändern kann.

Eine *korrekte Interpretation aller Eingaben* kann erreicht werden, da durch die Mechanik die Position sehr genau berechnet und übertragen werden kann.

Eine *schnelle Integration und Entfernung* kann erfolgen, da nur ein Gerät angeschlossen und für den Arzt zugänglich platziert werden muss und keine zusätzlichen Einstellungen notwendig sind.

Die *Sterilität* ist nicht vom Gerät selbst gewährleistet, sodass eine Haube oder sterile Abdeckung notwendig ist. Diese muss entweder über das komplette Gerät gestülpt werden, was allerdings die Bewegungsfreiheit beeinflussen kann, oder nur über das Teilstück, welches der Arzt in der Hand hält.

5.2.6 SpaceMouse

Alle Anforderungen werden wie beim haptischen Gerät Phantom Omni erfüllt, da auch die SpaceMouse ein haptisches Gerät ist und die gleichen Gegebenheiten aufweist. Ein Unterschied ist allerdings, dass der Anwender die Maus einfach loslassen kann, wenn er seine Interaktion beendet hat. Beim Phantom Omni hingegen muss er den Stift ablegen oder in einer anderen Weise seine Aktion beenden. Der haptische Bewegungsraum hingegen ist bei der 3D-Maus deutlich kleiner.

5.2.7 Fußschalter

Bei diesem Gerät hängt die *intuitive Bedienung* stark von den Schaltflächen ab und müsste mit den Anwendern evaluiert werden. Allerdings ist klar, dass mindestens sechs Schaltflächen verfügbar sein müssen für die Veränderung der Translation in alle Raumrichtungen und gegebenenfalls weitere Schalter für die Rotation, falls dies zusätzlich gefordert ist. Je nach Aufbau des Geräts kann die Bedienung also mehr oder weniger intuitiv sein.

Eine *korrekte Interpretation aller Eingaben* wird möglich sein, da die Geräte medizinischen Standards gerecht werden und die Schalter so positioniert sein sollten, dass keine fehlerhafte Eingabe möglich ist und entsprechend kann das System auch alle Eingaben korrekt interpretieren.

Eine *schnelle Integration und Entfernung* ist gewährleistet, da das Gerät über Funk kommuniziert und entsprechend zu jeder Zeit einfach weggelegt werden kann. Zudem muss das Gerät nicht eingerichtet werden, sondern kann einfach eingesteckt und verwendet werden.

Die *Sterilität* ist sehr gut gewährleistet, da das Gerät bereits für medizinische Anwendungen konzipiert wurde und entsprechend die Hygiene-Vorschriften einhält.

5.2.8 Auswertung

In der nachfolgenden Tabelle 2 werden die einzelnen 3D-Controller mit dem jeweiligen Erfüllungsgrad der Anforderungen zur besseren Übersicht dargestellt. Daraus lässt sich schließen, dass die kamerabasierten Systeme mit Microsoft Kinect und Leap Motion die besten Ergebnisse im Bereich Sterilität liefern, wohin gegen die beiden haptischen Geräte Phantom Omni und SpaceMouse die intuitive Bedienung und die korrekte Interpretation aller Eingaben bereitstellen. Zudem wäre der Fußschalter mit einer entsprechenden Ausstattung geeignet, sodass er auch die Anforderung der intuitiven Bedienung erfüllen kann. Entsprechend lässt sich folgern, dass die beiden

haptischen Geräte und der Fußschalter für den Anwendungsfall in der interventionellen Radiologie zur Steuerung der Echtzeit-MRT geeignet sind. Die kamerabasierten Systeme Microsoft Kinect, Leap Motion und Wiimote könnten trotz allem für andere Bereiche in der Medizin geeignet sein, wenn geringere Anforderungen an die Interpretation der Eingaben gefordert wird und der Anwender mehr Konzentration auf die Ausführung von Gesten aufwenden kann. Der Datenhandschuh wird in nächster Zukunft für medizinische Anwendungen nicht verwendet werden können, aufgrund der zeitaufwändigen Integration und schlechten Sterilisierbarkeit.

6 Zusammenfassung und Ausblick

Innerhalb dieser Arbeit wurde im Zusammenhang der interventionellen Radiologie zunächst auf bildgebende Verfahren eingegangen. Darauffolgend wurde die interventionelle Bildgebung dargestellt und Studien in diesem Bereich vorgestellt. Im nächsten Schritt wurden gängige 3D-Controller beschrieben. Des Weiteren wurden Anforderungen herausgearbeitet, die es bei der Auswahl eines 3D-Controllers zu beachten gilt. Diese wurden mit den Gegebenheiten der Geräte verglichen und abschließend ausgewertet. Dabei ergab sich, dass die beiden haptischen Geräte Phantom Omni und SpaceMouse und zudem der Fußschalter am besten geeignet sind für die Steuerung von Echtzeit-MRTs. Die konkrete Entscheidung für ein Gerät muss allerdings in einer Nutzeranalyse zusammen mit Interventionalisten für die jeweilige Radiologie einer Klinik erfolgen. Des Weiteren müssen die 3D-Controller für die medizinische Nutzung zugelassen werden, da die Geräte ursprünglich für den Spielebereich entwickelt wurden.

In zukünftigen Entwicklungen könnten die 3D-Controller aber definitiv einen großen Mehrwert erzielen, da diese relativ einfach in ein bestehendes System integriert werden können. Insbesondere im Vergleich zu kompletten Systemen von MRT-Herstellern, die integrierte Steuergeräte liefern, wäre die Alternative mit 3D-Controllern deutlich kostengünstiger und mit weniger Aufwand verbunden.

Tabelle 1: Übersicht Vergleich 3D-Controller,

Legende: +++: sehr gut, ++: gut, +: eher gut, -: eher schlecht, --: schlecht, ---: sehr schlecht

	Intuitive Bedienung	**Korrekte Interpretation aller Eingaben**	**Schnelle Integration und Entfernung**	**Sterilität**
Kinect	--	--	++	+++
Leap Motion	--	--	++	+++
Wiimote	-	+	++	+
Datenhandschuh	--	+	---	---
Phantom Omni	+++	+++	+++	+
SpaceMouse	+++	+++	+++	+
Fußschalter	+	+++	+++	+++

7 Literaturverzeichnis

[1] T. M. Lehmann: Handbuch der Medizinischen Informatik, Carl Hanser Verlag München Wien, 2005. ISBN: 3-446-22701-6

[2] R. Kramme: Medizintechnik, Springer-Verlag, 2017. ISBN: 978-3-662-48770-9

[3] H. Handels: Medizinische Bildverarbeitung – Bildanalyse, Mustererkennung und Visualisierung für die computergestützte ärztliche Diagnostik und Therapie. Vieweg + Teubner, Wiesbaden, 2009. ISBN: 978-3-8351-0077-0

[4] M. Bock, K. Wacker: MR-guided Intravascular Interventions: Techniques and Applications, Journal of Magnetic Resonance Imaging, 2008. DOI: 10.1002/jmri.21271

[5] O. Dössel: Bildgebende Verfahren in der Medizin – Von der Technik zur medizinischen Anwendung. Springer-Verlag, Berlin Heidelberg, 2016. ISBN: 978-3-642-54406-4

[6] R. Kramme: Medizintechnik. Springer-Verlag, Berlin Heidelberg, 2011. ISBN: 978-3-642-16186-5

[7] T.J. Vogl, B. Panahi, S. Fischer, N. Naguib, N.-E.A. Nour-Eldin, T. Gruber, J. Trojan, W. Bechstein, S. Zangos, K. Eichler: Interventionelle Therapie von Lungen- und Lebermetastasen. Der Onkologe. 2014, DOI: 10.1007/s00761-014-2669-3

[8] Pereira PL, Trubenbach J, Schmidt D: Radiofrequenzablation: Grundlagen, Techniken und Herausforderungen. Fortschr Röntgenstr 175: 20-27, 2003, DOI: 10.1055/s-2003-36612

[9] S. Morikawa, T. Inubushi, Y. Kurumi, et al.: Advanced computer assistance for magnetic resonance-guided microwave thermocoagulation of liver tumors, 2003. DOI: 10.1016/S1076-6332(03)00508-7

[10] A. Nabavi, D.T. Gering, D.F. Kacher, et al.: Surgical navigation in the open MRI, 2003. DOI: 10.1007/978-3-7091-6043-5_17

[11] J.G. Pinkernelle, F. Streitparth, J. Rump, U. Teichgräber: Adaptation of a Wireless PC Mouse for Modification of GUI during Intervention in an Open Highfield MRI at 1.0T, 2010. DOI: 10.1055/s-0028-1109895

[12] B. Preim, R. Dachselt: Interaktive Systeme Band 2. Springer-Verlag, Berlin Heidelberg, 2015. ISBN: 978-3-642-45246-8

[13] R. Dörner, W. Broll, P. Grimm, B. Jung: Virtual und Augmented Reality. Springer-Verlag, Berlin Heidelberg, 2013. ISBN: 978-3-642-28902-6

[14] M. Brill: Virtuelle Realität. Springer-Verlag, Berlin Heidelberg, 2009. ISBN: 978-3-540-85117-2

[15] Steute Schaltgeräte GmbH & Co. KG: Im Trend: Spezifische User Interfaces, in MEDengineering Ausgabe 7-8/2015, S.28-30, letzter Aufruf: 27.03.2017: http://archiv.med-eng.de/fileadmin/user_upload/archiv_2015/MED_7-8_2015_APP.compressed.pdf

[16] F. Ritter, C. Hansen, K. Wilkens, A. Köhn, H.-O. Peitgen: Benutzungsschnittstellen für den direkten Zugriff auf 3D-Planungsdaten im OP, 2009. DOI: 10.1524/icom.2009.0005

Analyse von Reifegradmodellen zur Unterstützung der Digitalisierung von Krankenhäusern

Denise Junger
Reutlingen University
Denise.Junger@Student.
Reutlingen-University.DE

Abstract

In der Medizin existieren verschiedene Reifegradmodelle, die die Digitalisierung von Krankenhäusern unterstützen können. Die Anforderungen an ein Reifegradmodell für diesen Zweck umfassen Aspekte aus allgemeinen und spezifischen Bereichen des Krankenhauses. Die Analyse der Reifegradmodelle HIN, CCMM, EMRAM und O-EMRAM zeigt große Lücken im Bereich des OP sowie fehlende Aspekte in der Notaufnahme auf. Ein umfassendes Reifegradmodell wurde nicht gefunden. Durch eine Kombination aus HIN und CCMM könnten fast alle Bereiche ausreichend abgedeckt werden. Zusätzliche Ergänzungen durch spezialisierte Reifegradmodelle oder sogar die Entwicklung eines umfassenden Reifegradmodells wären sinnvoll.

Schlüsselwörter

Reifegradmodell, Digitalisierung, Klinische Aspekte, IT-Fähigkeiten, Krankenhaus

CR-Kategorien

I.6.4 [**Model Validation and Analysis**]

Betreuer Hochschule: Prof. Dr.-Ing. Oliver Burgert
Hochschule Reutlingen
Oliver.Burgert@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1 Einleitung

Reifegradmodelle bewerten die Reife von Organisationen, indem verschiedene Aspekte wie beispielsweise spezifische Prozesse oder Technologien untersucht werden [3]. Auch im medizinischen Bereich haben sich Reifegradmodelle entwickelt, die Teilaspekte einer Klinik beschreiben [4], mit dem Ziel, die Digitalisierung von Krankenhäusern in unterschiedlichen Bereichen zu unterstützen.

Die Digitalisierung betrifft hierbei Informationen, Geräte und andere Objekte [13] und beschreibt im klinischen Kontext ein papierloses Krankenhaus [1]. Bisher ist nicht bekannt, welche Reifegradmodelle eine umfassende Bewertung der Fähigkeiten einer gesamten Krankenhaus-IT ermöglichen, um dadurch die Digitalisierung von Krankenhäusern zu unterstützen.

Ziel dieser Arbeit ist die Identifizierung und Analyse verschiedener Reifegradmodelle im medizinischen Bereich. Zuerst werden Digitalisierungsaspekte für Kliniken definiert. Eine Auswahl an Reifegradmodellen wird auf diese Anforderungen verglichen, um die Abdeckung und den Fokus sowie Überschneidungen und Lücken der Modelle zu identifizieren. Als Ergebnis wird die Identifizierung eines umfassenden Reifegradmodells für alle Krankenhausbereiche erhofft, welches zur Unterstützung der Digitalisierung genutzt werden kann.

2 Stand der Technik

Im Folgenden werden Reifegradmodelle und ähnliche Arbeiten vorgestellt.

2.1 Reifegradmodelle

Ein Reifegradmodell beschreibt ein Werkzeug zur Entwicklung und Verbesserung von Fähigkeiten, Prozessen, Technologien, Strukturen oder Rahmenbedingungen innerhalb von Organisationen. Dabei kommen Reifegradstufen zum Einsatz, über die der aktuelle Stand der Organisation eingestuft wird. [3]

Im nichtmedizinischen Bereich existieren bekannte Reifegradmodelle wie das Capability Maturity Model (CMM) [10] oder das Capability Maturity Model Integration (CMMI) [26]. CMM und CMMI werden oft als Basis zur Entwicklung von Reifegradmodellen im Gesundheitsbereich verwendet [4].

CMM setzt seinen Fokus auf die Verbesserung von Softwareengineeringprozessen, die in Stufen durchgeführt wird. CMM besteht aus den fünf Reifegraden Initial, Wiederholbar (wiederholen von bereits erledigten Aufgaben), Definiert (charakterisieren und verstehen von Prozessen), Geleitet (gemessener und gelenkter Prozess) und Optimierend (Prozessverbesserung). [10]

CMMI wiederum setzt seinen Fokus auf die Prozessverbesserung von Organisationen im Zusammenhang mit der Entwicklung und Wartung. Es existieren hierbei Ausprägungen für Systemengineering, Einkauf und Serviceentwicklung. CMMI ist ähnlich aufgebaut und besteht aus fünf Reifegraden: Initial, Geführt (grundlegendes Projektmanagement), Definiert (Prozessstandardisierung), Quantitativ geführt (quantitatives Management) und Optimierend (kontinuierliche Prozessverbesserung). [26]

Im medizinischen Bereich existieren Reifegradmodelle, die unterschiedliche Aspekte beschreiben. Diese können in Bezug auf die Digitalisierung im Krankenhaus bedeutend sein, wenn sie beispielsweise die Reife von Informationssystemen betrachten oder Prozesse elektronisch unterstützen. Eine Auswahl an Reifegradmodellen im medizinischen Kontext wird unter 3.2 vorgestellt.

2.2 Verwandte Arbeiten

Eine umfangreiche Vorstellung von verschiedenen Reifegradmodellen für die Medizin stellt [4] dar, dessen Fokus auf Reifegradmodellen für das Management von Informationssystemen liegt. Dabei wurden Modelle vorgestellt, die in einem bestimmten Bereich oder der gesamten Organisation angewandt werden können. Die Analyse der Modelle ergab, dass kein Reifegradmodell alle Areale und Subsysteme abdeckt. Somit fehlt es an einem Modell mit ganzheitlichem Ansatz und umfassendem Satz an Einflussfaktoren. Speziell auf die Digitalisierung von Krankenhäusern wurde hierbei nicht eingegangen. [4]

Eine weitere Reifegradmodellanalyse im medizinischen Bereich wurde in [20] durchgeführt. Hierbei wurden verschiedene Modelle vorgestellt und miteinander verglichen. Das Ergebnis der Analyse zeigt, dass kein perfektes Modell existiert, das alle Aspekte von Patienteninformationssystemen behandelt. Auch diese Arbeit scheint seinen Fokus nicht auf Krankenhäuser und deren Digitalisierung zu legen, sondern betrachtet Modelle für das Management von Patienteninformationen. [20]

3 Materialien und Methoden

Im Folgenden werden die Aspekte der Analyse sowie die Modellauswahl und das Analyseverfahren näher erläutert.

3.1 Anforderungen

Für den Vergleich der Reifegradmodelle wurde ein Anforderungskatalog mit digitalisierungsrelevanten Aspekten erstellt.

Die Digitalisierung im Krankenhaus betrifft viele Bereiche [9]. Der Katalog enthält Anforderungen an die Beurteilungskriterien der Modelle bezüglich der gesamten Kran-

kenhaus-IT [12] sowie der Teilbereiche eines Krankenhauses. Insgesamt wurden 13 Unterbereiche definiert, die über 200 Kriterien beinhalten. Zudem sind allgemeine Anforderungen an die Modelle im Anforderungskatalog enthalten, die weitere 20 Aspekte umfassen. Im Folgenden werden diese Bereiche und Aspekte zusammengefasst wiedergegeben.

Die technische Infrastruktur und das IT-Management sind von großer Bedeutung für die Digitalisierung [13]. Allgemein ist es hier wichtig, Aspekte zu berücksichtigen, die Informations- und Kommunikationstechnik [12] wie auch das gesamte Netzwerk (Einrichtung, Pflege, Aufbau, Betrieb) [24] betreffen. Des Weiteren spielt der Bereich der gesamten Vernetzung [1, 9] inklusive Kommunikation [9, 13] eine Rolle. In diesem Zusammenhang sollten Aspekte, die die Vernetzung mit externen Einrichtungen, aller Beteiligter sowie der Medizintechnik beinhalten, betrachtet werden [9]. Die Patienten- wie auch intersektorale und mobile Kommunikation sollten ebenfalls beinhaltet sein [13].

Ein weiterer wichtiger Bereich ist das Management (Organisation) [13]. Hierbei gibt es verschiedene bedeutende Aspekte wie Belegungs-, Aufgaben-, Wissens- und Ressourcenmanagement sowie Kapazitätssteuerung [13]. Die gesamte Krankenhauslogistik ist hierbei wichtig [12, 13]. Außerdem ist IT-Sicherheitsmanagement von großer Wichtigkeit [27]. Die Modelle sollten ebenfalls medizinische, organisatorische, interne und externe Prozesse wie auch deren Synchronisation betrachten [12]. Des Weiteren sollten technische Prozesse berücksichtigt werden [7].

Zudem sollten wichtige spezifische klinische Bereiche detailliert enthalten sein. Deshalb sollte das Reifegradmodell ebenfalls Behandlungspfade und Workflowmanagement (Pflege, Untersuchung) [13] mit dem gesamten Workflow des Patienten von der Aufnahme bis zur Entlassung [7] abdecken. Dabei spielt die gesamte Gesundheitsversorgung eine große Rolle [1, 9]. Dazu gehört der Überblick über Aufgaben und den Workflow [8] sowie die gesamte Koordination [24]. Hinzu kommen Aspekte wie die Dokumentation [29], analytische Fähigkeiten [1] sowie die Integration von Technik ins Behandlungsnetz [1].

Vor allem sind für die Digitalisierung auch medizinische Informationssysteme und digitale Assistenzsysteme sowie deren Funktionalitäten wichtig [12]. Deshalb sollten ebenfalls Krankenhausinformationssysteme (KIS/HIS) [27] sowie weitere Systeme wie PACS [21] enthalten sein. Für diese Systeme sollten zudem allgemeine Aspekte wie Standardisierung und Datensicherheit [1], Vergleichbarkeit [8] wie auch Revision und Datenzugriff [7] betrachtet werden. In diesem Bereich spielt ebenfalls die elektronische Patientenakte (EPA, engl. Electronic Medical Record EMR) [13, 25] und personenrelevante Daten wie auch deren Verfügbarkeit [7] eine wesentliche Rolle. Zudem sollten erweiternde EPA-Funktionalitäten wie beispielsweise eine Entscheidungsunterstützung [25] enthalten sein.

Weitere Bereiche wie Berichtswesen und Pflege-, Medizin- sowie Finanzcontrolling mit Arztbrief [13], Dokumentation und Klassifikation [11] sollten näher betrachtet werden. Der Bereich Telemedizin mit Aspekten zum Thema Gesundheitsapps und personalisierte Medizin [1] sollte ebenfalls enthalten sein. Zudem sollte der Bereich Radiologie (Diagnostik) [9, 21] mit der Betrachtung des radiologischen Informationssystems [21] und des Laborinformationssystems [14] zur Digitalisierung von Laborwerten [7] abgedeckt werden. Aspekte des Bereichs Notaufnahme [27] sowie der ambulante [18, 19] und stationäre Bereich [1] sollten in der Untersuchung enthalten sein. Des Weiteren spielt auch für den Operationssaal (OP) Digitalisierung eine große Rolle [11, 27]. Hierbei ist das Ziel intelligente Einweisung, Patientenerkennung und Personalerfassung [11]. Auch hier ist Kommunikation und Koordination [8] wie auch

die Unterstützung durch prä-, intra- und postoperative Aspekte [27] wichtig.

Zudem sollten für den Vergleich reifegradmodellspezifische Aspekte hinzugezogen werden. Die Analyse sollte sowohl die Reifegradstufen, als auch die Berechnung der Reife beinhalten [15]. Des Weiteren sollte überprüft werden, ob eine Roadmap zur Verbesserung angeboten wird [4]. Sehr wichtig ist zudem, welchen Fokus das Modell hat [5] und ob das Modell prozessorientiert (z.B. Pflegeverfahren) [3], objektorientiert (z.B. Auswertung von Informationssystemen) [3] oder ressourcenorientiert (z.B. technische Ressourcen) [15] ist. Hierbei ist ebenfalls die Art des Modells (Prozess, IT oder Organisation) interessant. Außerdem sollte bewertet werden, ob das System speziell für ein Subsystem oder für die ganze Krankenhaus-IT anwendbar ist [4].

3.2 Auswahl der Modelle

Insgesamt sollte die Analyse Reifegradmodelle enthalten, die unterschiedliche Bereiche des Krankenhauses abdecken und genügend Informationen für die Analyse bereitstellen. Zudem wurde darauf geachtet, dass die Modelle für die Unterstützung der Digitalisierung sinnvoll sind.

Das erste Modell sollte seinen Fokus auf Infrastruktur und Vernetzung legen und verschiedene Bereiche des Krankenhauses abdecken. Hierbei wurde das Health Information Network Maturity Model (HIN) [14] aufgrund der Domänenvielfalt ausgewählt. Modelle wie das NHS Infrastructure Maturity Model (NIMM) [23] oder das Hospital Cooperation Maturity Model (HCMM) [22] wurden deshalb ausgeschlossen. Für die breite Abdeckung weiterer Bereiche wurde das Continuity of Care Maturity Model (CCMM) [17] ausgewählt, da neben allgemeinen Bereichen auch die Pflege fokussiert wird. Das Electronic Healthcare Maturity Model (eHMM) [2] oder das High-Reliability Health Care Maturity Model [6] wurden vergleichsweise als weniger geeignet empfunden.

Da die EPA zudem elementar wichtig für den klinischen Wert sowie die Pflegequalität ist [25], wurde ein Modell ausgewählt, das auf diesen Bereich spezialisiert ist. Das Electronic Medical Record Adoption Model (EMRAM) [18] wurde im Vergleich zu dem PITO Adoption Model [25] aufgrund der verfügbaren Informationen favorisiert. Zusätzlich wurde das Outpatient Electronic Medical Record Adoption Model (O-EMRAM) [19] hinzugezogen, um die Spezialisierung in den Bereichen EPA, Ambulanz und Kommunikation abzudecken.

Weitere Modelle für Bereiche wie beispielsweise Daten und Analyse (AMAM [16]) oder PACS (PMM [28]) wurden als zu speziell für die Analyse angesehen. Speziell für die Digitalisierung von Krankenhäusern gibt es zudem einen Digitalisierungscheck [13], der jedoch kein Reifegradmodell darstellt und demnach weniger formal ist. Deshalb ist auch dieser nicht in der Analyse enthalten.

3.3 Analyseverfahren

Für die Analyse wird der erstellte Anforderungskatalog verwendet. Die Reifegradmodelle werden anhand der Kriterien untersucht. Da die Informationen der Reifegradmodelle allgemein nicht detailliert genug sind, ist eine exakte Beurteilung, um genaue Aussagen über eine Abdeckung bestimmter Anforderungen zu machen, kaum möglich. Für die Aspekte ist somit schwer einzuschätzen, wie umfangreich diese überprüft werden. Es wird jedoch davon ausgegangen, dass die Bewertung des Reifegrades über die vorhandenen Informationen hinaus geht. Deshalb wird die Abdeckung von Aspekten mitunter anhand von Stichworten und Schlussfolgerungen ermittelt.

Die bewerteten Teilaspekte bestimmen die Gesamtbewertung der Bereiche. In den Ergebnissen werden Bereiche als ausreichend abgedeckt definiert, wenn überwiegend alle Teilaspekte des Bereichs erfüllt werden. Als nicht ausreichend abgedeckt werden Bereiche betrachtet, wenn über die

Hälfte der Teilaspekte nicht erfüllt werden. Eine ausgewogene Mischung aus erfüllten, teilweise erfüllten und nicht erfüllten Kriterien eines Bereichs wird als teilweise abgedeckt definiert.

4 Ergebnisse

Im Folgenden werden die Ergebnisse der Analyse der Reifegradmodelle zusammengefasst dargestellt.

4.1 HIN

Die Analyse der Aspekte von HIN wurde anhand von [14] durchgeführt. HIN besteht aus fünf Reifegradstufen und bietet ein Tool zur Beurteilung des Krankenhauses an. Des Weiteren kann mit dessen Hilfe eine Roadmap zur Erreichung eines höheren Reifegrades erstellt werden.

HIN deckt mit zehn Domänen eine Vielzahl an Bereichen ab. Es werden sowohl prozess- als auch objekt- und ressourcenorientierte Aspekte in der Bewertung abgedeckt. Der Fokus von HIN liegt in der Betrachtung des Netzwerkes, der Technologie, Infrastruktur und Systeme. Zudem spielen Data Sharing Prozesse eine Rolle.

Die von HIN fokussierten Beurteilungskriterien sind sehr relevant für die Digitalisierung im Krankenhaus. Es werden viele Bereiche wie die technische Infrastruktur und das IT-Management ausreichend abgedeckt. Auch die Vernetzung, Organisation und Management sowie Prozesse werden hinreichend betrachtet. Somit werden die Anforderungen hinsichtlich der gesamten Krankenhaus-IT abgedeckt. Lediglich im Bereich Kommunikation werden Teilaspekte nicht ausreichend erfüllt.

Spezifische Bereiche im Krankenhaus wie die Radiologie, die Telemedizin wie auch medizinische Informationssysteme werden ebenfalls ausreichend abgedeckt. Auch die Bereiche Berichtswesen und Controlling sowie Behandlungspfade, Workflow Management und der stationäre Bereich werden hinreichend betrachtet. Allerdings werden nicht alle Aspekte der Analyse ausreichend abgedeckt. Es existieren große Lücken innerhalb der Bewertung des OP und der Notaufnahme. Des Weiteren konnten Teilaspekte im ambulanten Bereich sowie bei der Unterstützung des gesamten Workflow des Patienten nicht erfüllt werden. Deshalb wären Ergänzungen der Beurteilungskriterien von HIN innerhalb der nicht ausreichend abgedeckten Bereiche sinnvoll. Insgesamt deckt HIN jedoch sowohl den Bereich Prozesse als auch die Bereiche IT und Organisation ausreichend ab.

4.2 CCMM

Die Analyse der Aspekte von CCMM wurde anhand von [17] durchgeführt. CCMM besteht aus acht Reifegradstufen und bietet ein Expertenteam zur Beurteilung und Dokumentation des Reifegrades. Auch hier kann eine Roadmap zur Erreichung eines höheren Reifegrades erstellt werden.

CCMM deckt verschiedene Bereiche im Krankenhaus ab. Es werden überwiegend prozessorientierte Aspekte in der Bewertung abgedeckt, es sind jedoch auch objekt- und ressourcenorientierte Aspekte enthalten. Der Fokus von CCMM liegt in den Bereichen Governance, Klinik, IT und Pflege.

Diese von CCMM fokussierten Beurteilungskriterien sind relevant für die Digitalisierung im Krankenhaus. Es werden viele Bereiche wie die Vernetzung und Kommunikation sowie Organisation und Management ausreichend abgedeckt, Prozesse jedoch nur teilweise. Anforderungen aus dem Bereich technische Infrastruktur und IT-Management werden nicht ausreichend erfüllt. Somit werden die Anforderungen hinsichtlich der gesamten Krankenhaus-IT nur teilweise abgedeckt.

Spezifische Bereiche in Krankenhäusern wie medizinische Informationssysteme, Berichtswesen und Controlling werden ebenfalls ausreichend abgedeckt. Die Bereiche Behandlungspfade und Workflow Management, die Unterstützung des gesamten

Workflow des Patienten sowie der stationäre und ambulante Bereich werden ebenfalls hinreichend betrachtet. Jedoch sind nicht alle Aspekte der Analyse ausreichend abgedeckt worden. Es existieren große Lücken innerhalb der Bewertung des OP und der Radiologie. Zudem konnten Teilaspekte im Bereich Telemedizin und Notaufnahme nicht erfüllt werden. Aufgrund dessen wären für CCMM ebenfalls Ergänzungen der Beurteilungskriterien innerhalb der nicht ausreichend abgedeckten Bereiche sinnvoll. Insgesamt deckt CCMM jedoch die Bereiche Prozesse und Organisation ausreichend ab und bezieht auch teilweise den Bereich IT mit ein.

4.3 EMRAM

Die Analyse der Aspekte von EMRAM wurde anhand von [18] durchgeführt. EMRAM besteht aus acht Reifegradstufen. Die Überprüfung und Bestätigung des organisatorischen Fortschritts des Krankenhauses wird durch ein Expertenteam durchgeführt. Des Weiteren unterstützt dieses Expertenteam die Erstellung einer Roadmap zur Erreichung eines höheren Reifegrades.

EMRAM deckt verschiedene klinische Bereiche ab. Es werden überwiegend objektorientierte Aspekte in der Bewertung abgedeckt, es sind jedoch auch prozessorientierte Aspekte enthalten. Der Fokus von EMRAM liegt in der Betrachtung der EPA und beteiligter Nebensysteme in Bereichen wie Radiologie, Labor und Pharmazie.

Die von EMRAM fokussierten Beurteilungskriterien sind ebenfalls relevant für die Digitalisierung im Krankenhaus. Es werden verschiedene Bereiche ausreichend abgedeckt. Allerdings werden die Anforderungen hinsichtlich der gesamten Krankenhaus-IT nur bedingt erfüllt. Die Bereiche technische Infrastruktur, IT-Management, Organisation und Management sowie Prozesse werden nicht hinreichend abgedeckt. Nur Aspekte der Vernetzung und der Kommunikation werden teilweise erfüllt.

Spezifische Bereiche im Krankenhaus wie die Radiologie und medizinische Informationssysteme werden ausreichend abgedeckt. Auch der stationäre Bereich sowie Behandlungspfade und Workflow Management werden hinreichend betrachtet. Allerdings sind nicht alle Aspekte der Analyse ausreichend abgedeckt worden. Es existieren große Lücken innerhalb der Bewertung des OP, der Notaufnahme, der Telemedizin und dem ambulanten Bereich. Zudem konnten Teilaspekte in den Bereichen Berichtswesen und Controlling sowie bei der Unterstützung des Patientenworkflow nicht erfüllt werden.

Insgesamt deckt EMRAM die Bereiche Prozesse, IT und Organisation nur teilweise ab. Das auf die EPA spezialisierte Modell deckt Aspekte anderer Bereiche weniger ab, weshalb EMRAM nur in diesem fokussierten Bereich als Ergänzung zu anderen Modellen sinnvoll wäre.

4.4 O-EMRAM

Die Analyse der Aspekte von O-EMRAM wurde anhand von [19] durchgeführt. O-EMRAM besteht aus acht Reifegradstufen. Wie auch bei EMRAM, wird die Reifegradeinstufung und Erstellung einer Roadmap zur Erreichung eines höheren Reifegrades durch ein Expertenteam unterstützt.

O-EMRAM deckt verschiedene Bereiche im Krankenhaus ab. Es werden überwiegend objektorientierte Aspekte in der Bewertung abgedeckt, es sind jedoch auch prozessorientierte Aspekte enthalten. Der Fokus von O-EMRAM liegt in der Betrachtung der EPA im ambulanten Bereich und der Patientenkommunikation.

Diese von O-EMRAM fokussierten Beurteilungskriterien sind relevant für die Digitalisierung im Krankenhaus. Es werden verschiedene Bereiche ausreichend abgedeckt. Allerdings werden die Anforderungen hinsichtlich der gesamten Krankenhaus-IT nur bedingt erfüllt. Die Bereiche technische Infrastruktur, IT-Management, Prozesse sowie Organisation und Management wer-

den nicht hinreichend abgedeckt. Lediglich Aspekte der Vernetzung und der Kommunikation werden ausreichend erfüllt.

Spezifische klinische Bereiche wie die Radiologie sowie die Telemedizin und medizinische Informationssysteme werden ebenfalls hinreichend abgedeckt. Auch der stationäre und ambulante Bereich, die Unterstützung des gesamten Workflow des Patienten wie auch Behandlungspfade und Workflow Management werden ausreichend betrachtet. Allerdings werden nicht alle Aspekte der Analyse abgedeckt. Es existieren auch hier große Lücken innerhalb der Bewertung des OP und der Notaufnahme. Des Weiteren konnten Teilaspekte in den Bereichen Berichtswesen und Controlling nicht erfüllt werden.

Insgesamt deckt auch O-EMRAM die Bereiche Prozesse, IT und Organisation nur teilweise ab. Deshalb wäre O-EMRAM ebenfalls nur in seinem fokussierten Bereich als Ergänzung zu anderen Modellen sinnvoll.

4.5 Vergleich der Modelle

Die Analyse ergab (vgl. Tabelle 1), dass keines der Reifegradmodelle alle Aspekte hinreichend vereint. Insgesamt decken EMRAM und O-EMRAM am wenigsten Bereiche und Aspekte ab, da sie auf einen bestimmten Bereich spezialisiert sind. O-EMRAM kann hierbei vergleichsweise noch etwas mehr bieten als EMRAM. In ihrer Spezialisierung scheinen jedoch beide die Anforderungen gut abzudecken. Allerdings sind alle definierten Bereiche für die Digitalisierung des Krankenhauses wichtig.

HIN deckt hierfür viele relevante klinische Bereiche und Aspekte, für die Digitalisierung eine Rolle spielt, ausreichend ab und scheint am umfangreichsten zu sein. Zudem erfüllt HIN als einziges Modell die Aspekte der Bereiche technische Infrastruktur und IT-Management ausreichend. In den Bereichen OP und Notaufnahme sind jedoch große Lücken vorhanden, die anderweitig gefüllt werden sollten. Für die Bereiche Kommunikation, Ambulanz und gesamter

Tabelle 1: Überblick der Analyseergebnisse (ausreichend erfüllt +, nicht erfüllt -)

	HIN	CCMM	EMRAM	O-EMRAM
Techn. Infrastruktur und IT-Management	+	-	-	-
Vernetzung und Kommunikation	+/-	+	+/-	+
Organisation und Management	+	+	-	-
Prozesse	+	+/-	-	-
Behandlungspfade, Workflow Management, Workflow des Patienten	+/-	+	+/-	+
Medizinische Informationssysteme	+	+	+	+
Berichtswesen und Controlling	+	+	+/-	+/-
Telemedizin	+	+/-	-	+
Radiologie	+	-	+	+
Notaufnahme	-	+/-	-	-
Ambulanter Bereich	+/-	+	-	+
Stationärer Bereich	+	+	+	+
OP	-	-	-	-

Workflow des Patienten sollten noch weitere Aspekte zur Betrachtung hinzugezogen werden. Insgesamt können auch die ausreichend abgedeckten Bereiche von HIN noch weiter ergänzt werden, um eine noch bessere Übereinstimmung mit den Anforderungen zu erzielen.

Auch CCMM deckt viele relevante Krankenhausbereiche ab. Hierbei sind im Vergleich zu HIN die Kommunikationsaspekte sowie der ambulante Bereich und der Workflow des Patienten besser abgedeckt. Vor allem der Bereich Notaufnahme wird hier teilweise erfüllt, den kein anderes Modell aus der Analyse erfüllen konnte. Auch hier wären insgesamt alle Bereiche des Reifegradmodells ausbaufähig, um eine noch bessere Übereinstimmung mit den Anforderungen zu bekommen.

Würde das Reifegradmodell HIN um diese Aspekte von CCMM ergänzt werden, könnten alle Anforderungen bis auf den OP und die Notaufnahme ausreichend erfüllt werden. Lediglich eine Summe von Teilaspekten in den einzelnen Bereichen können nicht abgedeckt werden, wobei auch diese Aspekte wichtig für die Unterstützung der Digitalisierung sind. Deshalb wäre es sinnvoll, für bestimmte Teilbereiche, die in den jeweiligen Krankenhäusern besonders wichtig sind, auf spezialisierte Reifegradmodelle zu verweisen, um eine detailliertere Bewertung zu ermöglichen. Diese könnten potentiell noch mehr Aspekte abdecken. Inwiefern diese jeweils geeignet sind, ist in der Analyse nicht inbegriffen.

Allerdings würde es bei der kompletten Anwendung von HIN in Kombination mit CCMM oder anderen Modellen im Krankenhaus zu starken Überschneidungen kommen. Allein die vier Reifegradmodelle aus dem Vergleich überschneiden sich in mehreren Bereichen, da beispielsweise medizinische Informationssysteme in allen Modellen eine große Rolle spielen. Wie stark die Überschneidungen wirklich sind, ist jedoch anhand der Informationen schlecht einzuschätzen.

Am besten wäre demnach ein einziges Modell, das alle Bereiche und Aspekte beinhaltet. Da es vermutlich nicht möglich ist, das bereits existierende Modell HIN zu erweitern, müsste auf dessen Grundlage ein neues Reifegradmodell entwickelt werden, das zusätzlich alle relevanten Eigenschaften anderer Reifegradmodelle wie CCMM hinsichtlich der Digitalisierung in sich vereint und somit Lücken schließt. Zusätzlich könnten bestimmte Bereiche unabhängig durch spezielle und detailliertere Reifegradmodelle bewertet werden, um die letzten Lücken zu schließen, da der Umfang eines einzigen Modells mit der kompletten Abdeckung aller Aspekte unwahrscheinlich ist. Hierbei muss mit möglichen Überschneidungen gerechnet werden. Dies würde jedoch eine umfangreiche Abdeckung individueller Bereiche ermöglichen.

Im Bereich OP gibt es allerdings keine und in der Notaufnahme nur eine teilweise Abdeckung der Anforderungen. Hier würde es nötig sein, ein extra Reifegradmodell für die Unterstützung der Digitalisierung im OP zu entwerfen. Da hier wenig Wahrscheinlichkeit besteht, dass es zu Überschneidungen mit anderen Modellen in diesem spezifischen Bereich kommt, könnten andere Reifegradmodelle gut auf dieses Modell verweisen, um diesen speziellen Bereich ebenfalls abdecken zu können. Auch für die Notaufnahme könnte dies sinnvoll sein.

5 Zusammenfassung

In dieser Arbeit wurde eine Vielzahl an Reifegradmodellen für die Unterstützung der Digitalisierung von Krankenhäusern vorgestellt und relevante Anforderungen an ein Reifegradmodell in diesem Kontext erläutert. Die Analyse der Reifegradmodelle HIN, CCMM, EMRAM und O-EMRAM zeigte deren Fokus und Abdeckung verschiedener Bereiche in Krankenhäusern auf. Des Weiteren wurden Überschneidungen zwischen den Reifegradmodellen und größere sowie kleinere Lücken innerhalb der Modelle deutlich.

Insgesamt stellte keines der analysierten Modelle ein umfassendes Modell dar, das generalisiert auf die gesamte Krankenhaus-IT angewandt werden kann und sogleich alle wichtigen Teilbereiche detailliert betrachtet. Dennoch stellte sich HIN als ein recht umfangreiches Reifegradmodell heraus, welches überwiegend alle Bereiche ausreichend abdeckt. CCMM stellt dabei eine gute Ergänzung zu HIN dar. Eine Kombination würde jedoch zu mehreren Überschneidungen führen, kann aber eine ausreichende Abdeckung fast aller Bereiche bieten. Lediglich für den OP und die Notaufnahme konnte kein ausreichendes Reifegradmodell aus der Analyse oder der Literatur identifiziert werden.

Gegebenenfalls wäre es sinnvoll, ein neues Reifegradmodell auf der Grundlage von HIN und ergänzenden Aspekten von CCMM sowie weiteren Modellen zu entwickeln, welches speziell alle Bereiche und Aspekte umfangreich abdeckt, die für die Digitalisierung in Krankenhäusern bedeutend sind. Jede Klinik muss jedoch selbst entscheiden, ob eine Kombination verschiedener Reifegradmodelle trotz Überschneidungen in Frage kommt, nur ein spezielles Modell für einen bestimmten Bereich benötigt wird oder sogar ein neues Modell entwickelt werden sollte, um die Digitalisierung der Klinik zu unterstützen.

6 Literaturverzeichnis

[1] Anna Seidinger. 2016. Zukunft der digitalen Medizin. *Frankfurter Allgemeine Zeitung: Verlagsspezial*, V1-V6.

[2] Balaji Sharma. 2008. Electronic Healthcare Maturity Model (eHMM): A White Paper. Quintegra Solutions Limited.

[3] Blondiau, A., Mettler, T., and Winter, R. 2016. Designing and implementing maturity models in hospitals: An experience report from 5 years of research. *Health informatics journal* 22, 3, 758–767.

[4] Carvalho, J. V., Rocha, A., and Abreu, A. 2016. Maturity Models of Healthcare Information Systems and Technologies: a Literature Review. *Journal of medical systems* 40, 6, 131.

[5] Carvalho, J. V. de, Rocha, A., and Vasconcelos, J. 2015. Towards an Encompassing Maturity Model for the Management of Hospital Information Systems. *Journal of medical systems* 39, 9, 99.

[6] Chassin, M. R. and Loeb, J. M. 2013. High-reliability health care: getting there from here. *The Milbank quarterly* 91, 3, 459–490.

[7] Christoph Schmelter. 2013. Diese rechtlichen Aspekte sind maßgebend für Krankenhaus-Archivierungsleistungen – intern und extern. *Archiv Aktiv,* 19.

[8] Dr. Corinna Falge. 2014. *Informationslogistik als Schlüssel zu medizinischer Performance*. http://www.xulon-consulting.de/fileadmin/files/pdf/Veroeffentlichung_Wuemek_2014.pdf. Zugriff: 21. Februar 2017.

[9] Dr. Dr. Martin Siebert, Jens-Peter Neumann, Martin Menger, and Prof. Dr. Bernd Griewing. 2016. *Technische Innovation und Digitalisierung*. https://www.rhoen-klinikum-ag.com/fileadmin/files/konzern/Dokumente/Broschuere_2016_Medizintechnik.pdf. Zugriff: 21. Februar 2017.

[10] Dymond, K. M. 2002. *CMM® Handbuch. Das Capability Maturity Model® für Software*. Xpert.press. Springer, Berlin, Heidelberg.

[11] Fraunhofer-Institut für Software- und Systemtechnik ISST. 2013. Das Krankenhaus der Zukunft: Innovationen rund um die OP.

[12] Fraunhofer-Institut für Software- und Systemtechnik ISST. 2013. Hospital Engineering: Innovationspfade für das Krankenhaus der Zukunft.

[13] Fraunhofer-Institut für Software- und Systemtechnik ISST. 2015. Digitalisierungs-Check für Krankenhäuser.

[14] Geffen, M. 2015. Health Information Network (HIN) Maturity Model. Discussion Paper for Canada Health Infoway.

[15] Hecht, S. 2014. *Ein Reifegradmodell für die Bewertung und Verbesserung von Fähigkeiten im ERP-Anwendungsmanagement*. Springer Fachmedien Wiesbaden, Wiesbaden.

[16] HIMSS Analytics. 2017. *Adoption Model for Analytics Maturity. Information Sheet and Requirements*. http://www.himssanalytics.org/amam. Zugriff: 21. Februar 2017.

[17] HIMSS Analytics. 2017. *Continuity of Care Maturity Model. Information Sheet and Requirements*. http://www.himssanalytics.org/ccmm. Zugriff: 21. Februar 2017.

[18] HIMSS Analytics. 2017. *Electronic Medical Record Adoption Model. Information Sheet and Requirements*. http://www.himssanalytics.org/emram . Zugriff: 21. Februar 2017.

[19] HIMSS Analytics. 2017. *Outpatient Electronic Medical Record Adoption Model. Information Sheet and Requirements*. http://www.himssanalytics.org/oemram. Zugriff: 21 Februar 2017.

[20] Kamila Smolij and Kim Dun. 2006. Patient Health Information Management: Searching for the Right Model. Perspectives in Health Information Management / AHIMA, American Health Information Management Association. 3:10.

[21] Langen, H.-L., Bielmeier, J., Wittenberg, G., Selbach, R., and Feustel, H. 2003. Workflowverbesserung und Effizienzsteigerungsaspekte durch nahezu vollständige Digitalisierung einer Röntgenabteilung. *RoFo : Fortschritte auf dem Gebiete der Röntgenstrahlen und der Nuklearmedizin* 175, 10, 1309–1316.

[22] Mettler, T. and Blondiau, A. 2012. HCMM - a maturity model for measuring and assessing the quality of cooperation between and within hospitals. In *25th IEEE International Symposium*, 1–6. DOI=10.1109/CBMS.2012.6266397.

[23] NHS Digital. 2017. *NHS Infrastructure Maturity model NIMM*. https://digital.nhs.uk/NHS-infrastructure-maturity-model/overview. Zugriff: 6. März 2017.

[24] Pfannstiel, M. A., Rasche, C., and Mehlich, H. 2016. *Dienstleistungsmanagement im Krankenhaus*. Springer Fachmedien Wiesbaden, Wiesbaden.

[25] Rimmer, C., Hagens, S., Baldwin, A., and Anderson, C. J. 2014. Measuring Maturity of Use for Electronic Medical Records (EMRs) in British Columbia: The Physician Information Technology Office (PITO). *Healthcare quarterly (Toronto, Ont.)* 17, 4, 75–80.

[26] Schmied, J. 2008. *Mit CMMI Prozesse verbessern! Umsetzungsstrategien am Beispiel requirements engineering*. Safari Books Online. Dpunkt-Verl., Heidelberg.

[27] Schmola, G. and Rapp, B. 2016. *Compliance, Governance und Risikomanagement im Krankenhaus*. Springer Fachmedien Wiesbaden, Wiesbaden.

[28] van de Wetering, R. and Batenburg, R. 2009. A PACS maturity model: a systematic meta-analytic review on maturation and evolvability of PACS in the hospital enterprise. *International journal of medical informatics* 78, 2, 127–140.

[29] Wittpahl, V. 2017. *Digitalisierung*. Springer Berlin Heidelberg, Berlin, Heidelberg.

Wearable für Pferde – Standortbestimmung und Konzeption einer Umfrage

Anastasia Schmieder
Reutlingen University
anastasia.schmieder@Student.Reutlingen-University.DE

Abstract

Der folgende Artikel befasst sich mit Wearables für Pferde. Ziel ist es die Sicherheit der Tiere bei einem Ausbruch von einer Weide zu erhöhen und damit Personen- und Sachschäden zu minimieren. Hierzu wird der Stand der Technik zur Standortbestimmung im Freien zusammengetragen und durch eine Klassifizierung der unterschiedlichen Ansätze ermittelt, welche Standortbestimmung pferdegerecht erscheint. Zudem soll ein Fragebogen konzipiert werden, um Charakteristiken und Funktionalitäten für einen Prototypen festzustellen.

Schlüsselwörter

Standortbestimmung, Geofencing, Tracking, Pferd, Zielgruppenbefragung

CR-Kategorien

A.1 INTRODUCTORY AND SURVEY, B.4.1 Data Communications Devices, Tracking

---

Betreuer Hochschule: Prof. Dr. rer nat Gabriela Tullius
Hochschule Reutlingen
gabriela.tullius@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1 Einleitung

Heutzutage sind intelligente tragbare Computersysteme (wie Smartwach) zunehmend populär [1]. Die Nachfrage nach verschiedenen Systemen, des Internet of Things (IoT) und deren technologische Fortschritte, machen Platz für neue Wege und ermöglichen es verschiedene Lebensbereiche *smarter* zu machen. Dies lässt die Überlegung zu, Wearables für den Bereich der Tierhaltung zu entwickeln.

1.1 Motivation

Pferde sind Fluchttiere, daraus können bei einer Flucht auf einer abgelegenen Weide Verletzungsgefahren für die Tiere entstehen. Aber auch Personen- oder Sachschäden sind nicht auszuschließen. Zudem gibt es (Stand 2016) 1,03 Millionen Pferdebesitzer in Deutschland [2]. Dies ist eine große Zielgruppe, die von einem Überwachungssystem durch eine Standortermittlung profitieren könnte. Hinzu kommt, dass eine passive Überwachung der Tiere, sobald sie sich aus dem überwachten Bereich entfernen, nicht mehr ausreicht.

1.2 Zielsetzung

Diese Arbeit erfolgt im Rahmen der wissenschaftlichen Vertiefung des Studiengangs Human-Centered Computing (M.Sc.).

Es werden verschiedene Konzepte zur Bestimmung der eigenen Position zusammen-

getragen und ein Fragebogen erarbeitet. Der Fragebogen soll später dazu dienen, die Auswahl der Hardware, für einen Prototypen, auswählen zu können. Außerdem soll dieser helfen, die Akzeptanz solcher Geräte zu steigern, indem die Nutzer mögliche Anbringungsweisen am Pferd, sowie Handhabung des Gerätes durch ihre Antworten beeinflussen können.

1.3 Pferdehaltung

Damit die Tiere nicht erkranken und ihre Bedürfnisse ausleben können, werden Pferde, die in Einzelboxen gehalten werden in der Regel zeitweise auf Weiden gebracht um sich mehr und artgerechte Bewegung zu verschaffen und um das Futter in Bewegung aufnehmen zu können [3]. Hierbei besteht die Gefahr, dass die Tiere sich aus dem eingezäunten Bereich entfernen und Personen- oder Sachschäden verursachen können.

1.4 Zielgruppen

Bei den anfänglichen Überlegungen zu diesem Thema sind zwei Zielgruppen hervorgegangen, die Interesse an einer Nutzung von Wearables für Pferde haben können. Die Informationen zum folgenden Absatz sind den Quellen [3] und [4] entnommen.

Die erste Zielgruppe sind Zuchtbetriebe. Hier werden Pferde in großer Anzahl gehalten. Zur Weidehaltung, kommt die Lauf- oder Offenstallhaltung in Gruppen. Die zweite Zielgruppe bilden die Freizeit- und Turnierreiter. Hierbei handelt es sich um Privatpersonen, die in ihrem Beruf eher seltener mit Pferden arbeiten. Das Pferd ist ein Hobby und wird in der Freizeit zum Beispiel geritten oder gefahren (im Sinne von Pferd mit Kutsche und Kutschenführer). Hier werden die Tiere in der Regel in Einzelboxen mit Weidegang gehalten.

2 Stand der Technik

Da sich die Entwicklung eines Wearables im Bereich des IoT befindet, sollte darauf geachtet werden, dass die Umsetzung der verschiedenen Standortbestimmungen sich mit dem Grundgedanken des IoT verbinden lassen. Konkret, wird ein Pferd mit einem Gerät ausgestattet, dass über Sensoren, eine Software und andere Komponenten (z.B. GPS-Empfänger) verfügt, um einen permanenten Standort über das Internet an den Besitzer weitergeben zu können [5].

In der Theorie aber auch in der Praxis, gibt es bereits einige Verfahren, um einen Standort für Tiere festzustellen. Nachstehend werden einige Verfahren beschrieben.

2.1 Standortbestimmung durch das GPS

Dodel und Häupler [6] beschreiben die Standortbestimmung mittels GPS (engl. Global Positioning System), indem zwischen einem Empfänger und mindestens drei Satelliten die Entfernung und Uhrzeit übertragen werden. Daraus errechnen sich drei Entfernungen (Laufzeit der Funksignale oder Pseudostrecke genannt), die den Radius von Kugeloberfläche definieren. Der gemeinsame Schnittpunkt der drei Kugeln bildet die Position (den eigenen Standort) des Empfängers zu einer bestimmten Zeit. Die Genauigkeit wird verbessert, wenn mindestens drei Schnittstellen so orthogonal wie möglich zueinander stehen. Der gesamte Vorgang wird als Lateration bezeichnet.

Für die Nutzung von GPS benötigt man lediglich einen Empfänger, ein System (Software) mit Hilfe dessen man seinen Standort einsieht und eine Energiequelle für den Empfänger, wobei diese eine Batterie sein kann.

Herausforderungen bilden Signalabschattungen durch Berge und hohe Häuserzeilen (Urban Canyon), der Mehrwegeffekt (Multipath Effects), der bei Messvorgängen zwischen oder innerhalb von Gebäuden auftritt und die Signaldämpfung durch Wetter, Bäume oder dadurch, dass sich ein GPS-Empfänger innerhalb eines Fahrzeugs oder Gebäudes befindet. Außerdem gibt es noch Ionosphärenfehler, Mehrwegefehler,

Empfängerfehler, Geometriebedingte Fehler, Fehler der Satellitenuhr, Fehler der Bahnparameter und Troposphärenfehler, auf die nicht im Detail eingegangen wird, die aber in der Quelle [6] nachgeschlagen werden können.

GPS ist weltweit verfügbar und gebührenfrei. Es ermöglicht die Bestimmung von Ort und Zeit, Geschwindigkeit und Himmelsrichtung. Es bietet eine weltweite, tages- und jahreszeitunabhängige Standortbestimmung, bei jedem Wetter. Außerdem ist die Anzahl der Nutzer unbegrenzt (es wird nicht langsamer oder ungenauer bei einer hohen Nutzerzahl) und durch die hohe Beliebtheit des Systems, werden viele kostengünstige Empfänger angeboten [6].

Radoi et al. [7] beschreiben in ihrer Arbeit ein Verfahren, um Wildpferde in Andalusien zu tracken. Die Architektur besteht aus einem drahtlosen Netzwerk von mobilen körpernahen Schnittstellen (Prospeckz-5-Mobilplattform [8]) an den Tieren und stationären Schnittstellen als Basisstation, die mit dem IP-Netzwerk verbunden ist. Die Sensoren auf jeder Plattform beinhalten ein GPS-Modul, einen Beschleunigungsmesser zur Erfassung der Kopfausrichtung und Messung der Aktivität, ein Magnetometer zur Messung der Orientierung der Pferde und eine Photovoltaikzelle für Lichtintensitätsmessungen. Das Gerät ist in einem robusten, handgefertigten Gehäuse untergebracht, das mit einem Riemen am Hals der Pferde befestigt ist (Siehe Abbildung 1).

Abbildung 1: Mit Sensoren markierte Wildpferde [7]

Da das Prinzip der Ortung von Pferden dasselbe ist, wie für andere Tiere, werden verschiedene Ansätze vorgestellt.

Eine laut Autoren günstige und Platzsparende Methode zur Ortung von Ottern, wird in der Arbeit von Quaglietta et al. [9] beschrieben. Als GPS-Empfänger wird das kleinste GPS Modul, kombinierte mit einem GSM / GPRS Modul, welches zur Zeit der Studie erhältlich war verwendet. Um das Gerät zu versorgen, wird ein Akku mit 2500 mAh Kapazität und einer geschätzten durchschnittlichen Lebensdauer von 42 Tagen an 4 Standortaufzeichnungen pro Tag gewählt. Zudem wird eine GPS-Antenne für Marine- und U-Boot-Anwendungen (da Otter größtenteils im Wasser leben) und eine PCB GSM-Antenne angeschlossen. Die Gesamtabmessungen erreichten ca. 65 mm Länge, 645 mm Breite und 628 mm Dicke. Das Gesamtgewicht beträgt 84 Gramm.

In der Arbeit *Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet* von Juang et al. [10] warden in der Wildnis lebende Zebras über GPS verfolgt, hier wird besonders Wert darauf gelegt, dass die Geräte ein Jahr lang funktionsfähig sind, ohne das ein Mensch eingreifen muss (z.B. um die Batterien zu wechseln). Die Daten werden über Satelliten übertragen, da der Speicher auf den Geräten nicht sehr groß ist. Hierbei wird jedoch eine größere Akkukapazität benötigt.

In weiteren gefunden Arbeiten zu diesem Thema, die hier keine Nennung finden, wurden in der Regel GPS-Tracker verwendet, um Tiere im Freien Gelände zu lokalisieren oder sie digital zu verfolgen.

2.2 Weitere Möglichkeiten der Standortbestimmung

Zunächst wird die Standortbestimmung über ein Wireless Local Area Network (WLAN) laut Schelewsky et al. [11] als Alternative zu GPS beschrieben.

Ein WLAN-Hotspot sendet Signale zur Identifizierung (Name, Mac-Adresse) und

gibt Auskunft über seine Empfangsfeldstärke (Receive Signal Strength Indicator, RSSI), daraus lässt sich eine Art Fingerabdruck generieren, der charakteristisch für bestimmte Orte ist. Dieser Fingerabdruck bekommt eine Geokoordinate zugeordnet. Anhand dieser Koordinate erfolgt die Lokalisierung. Ein Empfänger analysiert die eingehenden Daten der Hotspots, vergleicht sie mit einer Datenbank, in der die digitalen Fingerabdrücke hinterlegt sind und kann so die zugehörige Geokoordinate ermitteln.

Man benötigt für die Umsetzung also mehrere Hotspots in Form von Routern und ein Empfänger, der an dem Objekt befestigt ist, welches lokalisiert werden soll.

Die zweite Möglichkeit über WLAN eine Lokalisierung vorzunehmen ist ähnlich dem GPS-Ansatz. Hierbei werden die Entfernungen zu verschiedenen Hotspots gemessen und anhand einer Multilateration berechnet.

Die Lokalisierung über WLAN setzt eine vorhandene Infrastruktur und gegebenenfalls entsprechende Datenbanken, in denen die Positionen der Infrastruktur-Elemente georeferenziert wurden, voraus. Somit benötigt man einiges an Hardware (Empfänger und mehrere Hotspots/Router) sowie eine Stromquelle für die Hardware. Außerdem muss man einen Vertrag für die Bereitstellung eines Internetanschlusses bezahlen.

Zudem kann man den Standort über mobile Netze bestimmen.

Laut Schelewsky et al. [11] sprechen die hohe Flächenabdeckung von Mobilfunkstandards (z. B. GSM, UMTS, Long Term Evolution (LTE)) und eine hohe Anzahl an Endgeräten, die diese Standards unterstützen, für eine Funkzellenortung. Grundlage hierfür ist die Identifizierung der Cell-ID eines GSM-, UMTS- oder LTE-Funknetzes.

Eine Herausforderung besteht in der großen Varianz der Lokalisierungsgenauigkeit, da sie von der Größe der Funkzellen abhängt. In ländlichen Gegenden ist diese zum Teil auf einen Radius von über 35 km ausgedehnt. Somit kann eine Lokalisierung mitunter nur auf 100 m genau erfolgen. Werden die Cell-IDs weiterer Funkzellen berücksichtigt, lässt sich die Genauigkeit erhöhen. Durch das TA-Parameter (Timing Advance) in Kombination mit dem EOTD-Verfahren (Enhanced Observed Time Difference) lassen sich durchschnittliche Genauigkeiten von 30 m oder weniger erreichen [11].

Für die Funkzellenortung benötigt man außer dem Empfänger eine SIM-Karte. Auch die Netzabdeckung ist je nach Anbieter besser oder schlechter.

Eine vierte Möglichkeit, ist die Lokalisierung über Kamerasysteme. Da die Objektlokalisation ein sehr ausführliches Thema ist, wird im nächsten Abschnitt eine Zusammenfassung laut Süße et al. [12] dargestellt.

Bei diesem Ansatz der Objektlokalisierung findet eine Klassifikation von einzelnen Bildausschnitten statt. An jeder Position des Fensters wird ein Klassifikator angesetzt, welcher zur Merkmalsberechnung nur die Bildinformation innerhalb des Fensters verwendet. Der Klassifikator trifft für die aktuelle Position eine Entscheidung, ob das Fenster gerade eine Instanz der Objektkategorie zeigt. Hierfür verwendet man eine Merkmalsberechnung für ein gegebenes Fenster. Anschließend erfolgt die Auswertung des Klassifikators. Zudem können die Klassifikatoren mit vielen Lernbeispielen bestückt werden um ihre Genauigkeit zu verbessern. Bei diesem Ansatz können jedoch folgende Probleme auftreten:

- Verdeckung: Objekte verdecken sich gegenseitig
- Hintergrund: Darstellung von Objekten und Bildelementen erschwert die Erkennung zusätzlich
- Intraklassenabstand: Die Erscheinungen der Objekte variieren sehr stark durch unterschiedliche Rotationen, Skalierungen, andere Perspektiven, nichtstarre Defor-

mationen, farbliche Gestaltung, Unterkategorien anderer Ausprägungen

- Interklassendistanz: Bestimmte Objekte sind ähnlich zueinander und lassen sich schwierig voneinander trennen

Hinzu kommt, dass diese Art der Lokalisierung einen gewissen Rechenaufwand mit sich bringt, was bei den Anforderungen für die Hardware und Software berücksichtigt werden muss. Von allen vorgestellten Systemen, braucht dieses das meiste Equipment.

2.3 Beispiele aus der Praxis

Es gibt in Deutschland bereits verschiedene GPS-Tracking Systeme. Diese sind in der Regel Groß und haben eine geringe Akkulaufzeit.

Abbildung 2: TIER FINDER von PAJ [13]

Das Unternehmen *PAJ UG* bietet zum Beispiel einen GPS-Tracker an, der mit einer SIM-Karte genutzt werden kann. Das Gerät bietet eine Standortabfrage und die Möglichkeit einen *Geofence* einzurichten außerdem ist das Gerät laut Angaben des Herstellers Spritzwasserdicht, klein und leicht und bietet einen ausgezeichneten GPS Empfang [13].

Ein Nachteil wäre hier die Größe (81 mm X 39 mm X 29 mm) des Gerätes bei der Weidennutzung. Da das Pferd sich auch hinlegt, könnte das Gerät, wenn das Gehäuse nicht stabil genug ist brechen. Angaben zur Stoßfestigkeit des Materials werden leider nicht gemacht. Das Gerät kostet 99 Euro und hat eine Laufzeit von ca. 7 Tagen (Angaben laut Hersteller), danach muss es mit einem Netzteil geladen werden.

Eine weitere Firma, die GPS-Tracker für Pferde anbietet, ist *GPS-WATCH GmbH*. Leider bekommt man zu dem Produkt für die Tierortung nur auf Anfrage Detailangaben. Aus der Internetseite lässt sich also nicht entnehmen, wie das Gerät am Tier befestigt wird. Es gibt jedoch angaben, dass *Geofencing (*Zusammengesetztes Kunstwort aus Geographie und fence: Geoinformationen und Aufenthaltsorte eines Objektes werden ermittelt, wenn das Objekt einen vorab definierten Bereich verlässt, wird ein Alarm ausgelöst) unterstütz wird und dass das Gerät aus wasserdichtem Kunststoff besteht und somit draußen genutzt werden kann. Kosten und Laufzeit erfährt man aber nur auf Anfrage [14].

GEOHORSE fence ist ein Produkt der *Firma Libify Technologies GmbH*. Es kostet 249 Euro und ist am Halfter des Pferdes anzubringen. Die Größe des Gerätes beträgt 68 mm x 40 mm x 27 mm und hat ein Gewicht von 72 Gramm, es ist also etwas schwerer, als das Gerät von PAJ UG. Es hat eine Akkulaufzeit von 48 Stunden und muss öfter geladen werden. Laut Hersteller ist es spritzwassergeschützt, stoßfest und hat eine GPS, GSM, GPRS und RF-Funkeinheit [15].

Abbildung 3: GEOHORSE fence [15]

Außerdem gibt es zu dem Thema eine ähnliche Arbeit. Hier wurden jedoch Schafe getrackt. Das System nennt sich *Electronic Shepherd*. Hierbei handelt es sich laut den Autoren um ein drahtloses Kommunikationsnetzwerk. Ein Herdenführer fragt den

Standort der Restlichen Herdenmitglieder über Funkkommunikationsgeräte ab und sendet die Standorte anschließend weiter. Das System nutzt dabei GPS-Empfänger, UHF-Frequenz Kommunikationstransceiver und GPRS-Modems [16].

Es gibt weitere Unternehmungen und Arbeiten, welche die Tierortung aufgreifen, jedoch ist das Prinzip Peilsender am Halsband immer das Selbe. Die angegebenen Beispiele sollten ausreichen um das Defizit an kostengünstigen Lösungen aufzuzeigen, die meist nie speziell an das Bedürfnis der Pferde und ihrer Halter angepasst sind. Meist sind die Peilsender für alle Tierarten gedacht und haben eine zu geringe Laufzeit, als dass man sie für einen langzeitigen Einsatz nutzen könnte.

Bei einer wirtschaftlichen Nutzung, in einem Zuchtbetrieb zum Beispiel wäre das wöchentliche Laden bei mehreren 100 Pferden ein erheblicher Zeitaufwand. Wenn das Laden der Geräte mehrmals die Woche durchgeführt werden müsste, wäre der Zeitaufwand noch viel erheblicher.

Auch ist die Nutzung von SIM-Karten bei einem großen Betrieb eher unwahrscheinlich, da eine große Menge von SIM-Karten beschafft und verwaltet werden müsste.

Abbildung 4: Trackacow Pedometer [17]

Bei anderen Großtieren gab es auch die Möglichkeit einer Art Fußfessel (siehe Abbildung 4). Dies ist für Pferde jedoch schwierig in der Umsetzung, da sie sich viel mehr und schneller, als zum Beispiel Kühe bewegen und das Band um das Gelenk eventuell reiben und Verletzungen nach sich ziehen könnte. Außerdem sind die Fesseln von Pferden anders Gebaut, sodass das Gerät beim Wälzen auf und ab rutschen könnte und auch hier eine mögliche Verletzungsquelle darstellen könnte.

Die meisten Kamerasysteme funktionieren über eine Datenübertragung per SIM-Karte. Hierbei wird ein Kamerasystem an einem Weidezaun installiert und das Bildmaterial anschließend über mobile Datenübertragung an einen PC oder ein Smartphone übertragen. Es gibt je nach Hersteller verschiedene Kameraausführungen, zum Beispiel auch für Nachtsicht, und die Geräte werden über eine Stromquelle versorgt, die vorher zum Beispiel in Form eines 12 Volt Batterieblocks

an der Weide angebracht wird.

Abbildung 3: XRay Kamerasystem der Firma Weidewächter [18]

Ein praktisches Beispiel ist die Weidekamera *Xray* der Firma *WEIDEWAECHTER Elektronik UG*. Ihre Überwachungskamera kann autark arbeiten, also an abgelegenen Standorten ohne Infrastruktur (DSL-Anschluss, Strom) zur Überwachung eingesetzt werden. Die Kosten für dieses System belaufen sich auf 499 Euro [18].

3 Klassifikation und Vergleich

Die vier vorgestellten Systeme eignen sich alle zur Standortbestimmung, jedoch eignen sich nicht alle zur Standortbestimmung von Pferden, der Nutzung von Geofencing oder lassen sich zu einem Tracking-System erweitern.

Tabelle 1: Vergleich der Systeme aus Kapitel 2

Anforderungen	GPS	WLAN	mobile Netze	Kamera
Equipment	Empfänger Sender zur Datenübertragung	Empfänger Router oder andere Hotspots Internetleitung	Empfänger Sender zur Datenübertragung	Kameras Router oder andere Hotspots mit Internetleitung oder SIM-Karte(n)
Erreichbarkeit/ Reichweite/ Empfang	Weltweit	Deutschlandweit (Anbieter abhängig)	Deutschlandweit (Anbieter abhängig)	Deutschlandweit (Anbieter abhängig)
Störfaktoren	Signalabschattungen durch Berge, Wälder, etc.	ländliche Gegend ergibt evtl. schwache Netzabdeckung	ländliche Gegend ergibt evtl. schwache Netzabdeckung	ländliche Gegend ergibt evtl. schwache Netzabdeckung
Anschaffung	Empfänger	Empfänger Router	Empfänger SIM-Karte	Kameras Router oder SIM-Karte
Stromversorgung	Batteriebetrieb	Dauerstromquelle erforderlich	Batteriebetrieb	Dauerstromquelle erforderlich
laufende Kosten	keine	Vertrag für Internetanbindung	Vertrag für SIM-Karte	Vertrag für Internetanbindung
Sonstiges				Ein Rechner, der die Bilddaten analysiert und auswertet
Geeignet für Nutzung auf Weide	ja	nein	ja	Nein
Geeignet für Nutzung am Pferd	ja	ja	ja	nein

Anhand der Tabelle (siehe Tabelle 1), sollen die verschiedenen Systeme miteinander verglichen werden, um entscheiden zu können, welches sich am besten bei der Nutzung mit Pferden eignet.

Aus den ermittelten Eigenschaften für die verschiedenen Systeme eignen sich zwei für die Nutzung an abgelegenen Standorten. Da die Netzabdeckung von SIM-Karten sehr hoch ist und die Satellitenübertragung von GPS sogar weltweit genutzt werden kann, heben sich diese beiden Verfahren besonders gut für die ländliche Gegend hervor. Außerdem benötigen Sie am wenigsten Zubehör und können durch die Größe des Empfängers auch am Pferd platziert werden. Die Stromzufuhr kann bei beiden Geräten über Batterien erfolgen, womit sie besonders mobil sind.

4 Befragung der Zielgruppen

Zur genauen Eingrenzung und Analyse der Anforderungen, wird eine Befragung konzipiert und durchgeführt. Diese findet über das Internet statt, in Form eines Onlinefragebogens. Die Ergebnisse der Auswertung fließen in die Umsetzung eines Prototypen ein, indem beispielsweise die Nutzer mögliche Anbringungsweisen am Pferd oder Handhabung des Gerätes durch ihre Antworten beeinflussen.

5 Konzeption der Befragung

Für die Erstellung des Fragebogens wurde ein mehrstufiger Ansatz gewählt. Zunächst wurden Fragen, die sich aus der Recherche ergaben notiert und anschließend mit verschiedenen Experten besprochen. Aus den Gesprächen heraus wurden die Fragen für eine Onlinebefragung ausgearbeitet, erweitert oder weggelassen.

5.1 Experteninterviews

Um den Fragebogen zu erarbeiten wurden Gespräche mit Experten geführt. Diese konnten bereits von vornherein verschiedene Ansätze als gut oder schlecht abschätzen. Außerdem wurden die Interviewpartner zur Handhabung solcher Geräte befragt und welche Risiken sie im Zusammenhang mit verschiedenen Pferdegruppen sehen könnten.

5.1.1 Zuchtbetriebe

Als Experte gelten in diesem Kapitel Angestellte eines Zucht- oder Reitbetriebes. Da die Mitarbeiter eine Ausbildung zum Thema Pferd absolviert haben und sich täglich im Betrieb mit der Haltung der Tiere auseinander setzen, können sie als Experten bezeichnet werden.

Für die Zuchtbetriebe wurde das Haupt- und Landesgestüt Marbach am 15.03.2017 besucht. Hierbei wurden mehrere Personen an verschiedenen Standorten besucht und befragt. Es wurde ein Gespräch mit dem Leiter der Junghengststation, eines mit dem Leiter des Stalles für Stuten und Fohlen, eines mit dem Reitlehrer der Landesreitschule und eines mit dem Verantwortlichen für die Seniorenpferde geführt.

5.1.2 Privatpersonen

Als Experten wurden Personen befragt, die mindestens 15 Jahre ununterbrochen mit Pferden zu tun haben, in Form von reiten, fahren oder ähnlichem, dies aber nicht als ihren Beruf ausüben und ein eigenes Pferd besitzen. Gefragt wurde also nach der Dauer der Erfahrung und dem Alter der Personen. Diese können Freizeit- oder Turniersportler sein. Außerdem wurde abgefragt, wie sie ihre Pferde halten, damit besser nachvollzogen werden kann, ob die Pferde Halfter, Halsriemen oder ähnliches bei der Weidehaltung tragen. Zuletzt wurde abgefragt wie ein Gerät sein sollte, dass sie nutzen würden.

5.2 Ausarbeitung der Fragen

Der Fragebogen besteht aus 26 Fragen, die im Folgenden verkürzt dargestellt werden.

Als erstes werden Fragen zur Person gestellt, das bedeutet, Geschlecht, Alter und Zielgruppe (Pferdehalter, Züchter, Stallbesitzer oder Reitbeteiligung, Pferdepfleger) werden abgefragt, sowie die Anzahl der eigenen Pferde und die Anzahl der zu betreuenden Pferde. Anschließend werden die Haltungsformen der Pferde abgefragt, um ermitteln zu können, wie der Prototyp später am Pferd befestigt werden kann. Es folgt die Abfrage, ob das Pferd sich bereits in einer Gefahrensituation nach einer Flucht befunden hat und was der Grund dafür war. Anschließend wurde abgefragt ob bereits ein Kontrollgerät am Pferd genutzt wird, wenn ja welches und wenn nein, was die Gründe dagegen sind. Dadurch soll geklärt werden, wieso solche Geräte nicht genutzt werden. Die Frage, aus welchen Gründen man ein Pferd überwachen sollte, soll dabei helfen festzustellen, was sich die Nutzer von dem Gerät wünschen würden, um die Akzeptanz zu steigern. Dann werden zwei Fälle mit denselben Fragen abgefragt. Im ersten Fall wird ermittelt, wie man einen Peilsender am Pferd befestigen würde, wie viel Geld man für ein solches Gerät ausgeben möchte und wie oft man es warten würde. Für den zweiten Fall sind die Fragen identisch, aber auf ein Kamerasystem bezogen. Um eine Art best practice zu erhalten, wird von den Zielgruppen erfragt, wo sich das jeweilige Gerät ihrer Meinung nach am besten am Pferd platzieren lassen würde und in welchem Bereich die Akzeptanz eines Preises

liegt. Dies soll später mit in die Evaluation der Hardware einfließen. Bei der Frage zur Wartung wird ermittelt, wie oft die Nutzer bereit wären zum Beispiel einen Akkuladestand zu prüfen oder Batterien zu wechseln. Es wird abgefragt, wann der Nutzer benachrichtigt werden möchte und wie. Dies könnte bei der Umsetzung des Geräts die User Experience positiv beeinflussen, da man vorher geklärt hat, wie die Zielgruppen das Gerät am liebsten nutzen würden. Und als letzte Frage wurden Verwendungsmöglichkeiten für ein Gerät am Pferd ermittelt. Dies könnte später in der Thesis ein Ausblick sein.

5.3 Verteilung des Fragebogens

Der Fragebogen soll über verschiedene Vereine und Verbände, sowie Fachzeitschriften über deren Social Media Kanal verteilt werden. Außerdem werden mehrere Emails an Privatpersonen verschickt. Es wird um die Teilung der Umfrage gebeten, sodass möglichst viele Personen erreicht werden können. Da die Anzahl der angeschriebenen Personen nicht bekannt ist, kann keine Rücklaufquote errechnet werden.

6 Fazit

Bereits während der Recherche ist klar geworden, dass ein Kamerasystem nicht in Frage kommt, da es sich dabei eher um eine passive Überwachung handelt. Im Falle der Kameras, können die Tiere zwar beobachtet aber nicht verfolgt werden. Auch der Aufbau eines WLAN ist in abgelegenen, ländlichen Gebieten eher schwierig, vor allem, da die ganze Apparatur im freien stehen würde. Wenn die Weide in der Nähe eines Stalles ist, kann dieser Aspekt gegebenenfalls überdacht werden, jedoch bietet es sich eher an, vom Ressourcenärmsten fall auszugehen, der keine Internet- oder Stromquelle bietet.

Da die Pferde mobil sind und es im Vordergrund darum geht sie bei einem Ausbruch schnell wiederzufinden, eignen sich die Varianten eines GPS-Trackers oder einer Standortbestimmung über mobile Netze, wie GSM, GPRS, UMTS oder LTE.

Zur Entscheidung, welches dieser beiden Systeme genutzt werden soll, steuert auch das Ergebnis des Fragebogens mit, da unter anderem gefragt wurde, wie viel für ein solches System gezahlt werden würde. Außerdem soll die Umfrage Aufschlüsse darüber geben, wie der Prototyp später am Pferd angebracht werden soll.

7 Literaturverzeichnis

[1] Anzahl der momentanen und potenziellen Nutzer einer Smartwatch in Deutschland in den Jahren 2015 und 2016 (in Millionen), 2016. Online verfügbar unter https://de.statista.com/statistik/daten/studie/482158/umfrage/umfrage-in-deutschland-zu-kaufabsicht-und-besitz-einer-smartwatch/, besucht am 21. März 2017.

[2] Anzahl der Personen in Deutschland, die persönlich ein Pferd besitzen, von 2013 bis 2016 (Personen in Millionen), 2016. Online verfügbar unter https://de.statista.com/statistik/daten/studie/265024/umfrage/umfrage-in-deutschland-zum-persoenlichen-besitz-eines-pferdes/, besucht am 21. März 2017.

[3] Deutsche Reiterliche Vereinigung e. V. (Hrsg.) - Richtlinien für Reiten und Fahren, Band 4: Haltung, Fütterung, Gesundheit und Zucht; FN-Verlag, Warendorf, 2003.

[4] A. Schmelzer - Sachkundenachweis Pferdehaltung, Prüfungswissen kompakt, Cadmos Verlag, Schwarzenbek, 2014. ISBN 978-384041516-6.

[5] A. Rayes, S. Salam - Internet of Things — From Hype to Reality, The Road to Digitization, Springer International Publishing AG 2017, 2017. ISBN 978-3-319-44858-9.

[6] H. Dodel, D. Häupler - Satellitennavigation, 2., korrigierte und erweiterte Auflage, Springer-Verlag Berlin Heidelberg 2010, 2010. ISBN 978-3-540-79443-1.

[7] I. E. Radoi, J. Mann, D.K. Arvind, Tracking and Monitoring Horses in the Wild using Wireless Sensor Networks, 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2015. Online verfügbar unter http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7348035, besucht am 18.05.2017.

[8] J. Mann, I. E. Radoi, D.K. Arvind, Prospeckz-5 – A Wireless Sensor Platform for Tracking and Monitoring of Wild Horses, 2014 17th Euromicro Conference on Digital System Design, 2014. . Online verfügbar unter http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6927317, besucht am 18.05.2017.

[9] L. Quaglietta, B. H. Martins, A. de Jongh, A. Mira, L. Boitani, A Low-Cost GPS GSM/GPRS Telemetry System: Performance in Stationary Field Tests and Preliminary Data on Wild Otters (Lutra lutra), 2012 Quaglietta et al., 2012. Online verfügbar unter http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0029235,besucht am 18.04.2017.

[10] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, D. Rubenstein, Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet, ASPLOS X Proceedings of the 10th international conference on Architectural support for programming languages and operating systems Pages 96-107, 2002. Online verfügbar unter http://delivery.acm.org/10.1145/610000/605408/p96-juang.pdf?ip=134.103.241.46&id=605408&acc=ACTIVE%20SERVICE&key=2BA2C432AB83DA15%2E48AAA2B1417E043E%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=925396514&CFTOKEN=55657313&__acm__=1492519317_a5a1df6e45e21a0a19c2ed141a720213, besucht am 18.04.2017.

[11] M. Schelewsky, H. Jonuschat, B. Bock, K. Stephan (Hrsg.), Smartphones unterstützen die Mobilitätsforschung, Neue Einblicke in das Mobilitätsverhalten durch Wege-Tracking, Springer Fachmedien Wiesbaden 2014; 2014. ISBN 978-3-658-01847-4.

[12] H. Süße, E. Rodner - Bildverarbeitung und Objekterkennung, Computer Vision in Industrie und Medizi,; Springer Fachmedien Wiesbaden 2014, 2014. ISBN 978-3-8348-2605-3.

[13] Online verfügbar unter www.pajgps.de/pferde.html, besucht am 12.03.2017.

[14] Online verfügbar unter www.gpswatch.de, besucht am 12.03.2017.

[15] Online verfügbar unter www.geohorse.de, besucht am 12.03.2017.

[16] B. Thorstensen, T. Syversen, T. Bjørnvold, T. Walseth - Electronic She-pherd – A Low-Cost, Low-Bandwidth, Wireless Network System in MobiSys '04 Proceedings of the 2nd international conference on Mobile systems, applications, and services, Pages 245-255, Boston, MA, USA — June 06 - 09, 2004; ACM New York, NY, USA ©2004, 2004. ISBN 1-58113-793-1.

[17] Online verfügbar unter www.trackacow.co.uk, besucht am 12.03.2017.

[18] Online verfügbar unter www.weidewaechter.de, besucht am 12.03.2017.

Evaluierung von Frameworks zur Detektion von Facial Feature Points *

Tobias Fleischer
Reutlingen University
Tobias.Fleischer@Student.Reutlingen-University.DE

Abstract

Ein stark erforschtes Gebiet der Computer Vision ist die Detektion von markanten Punkten des Gesichtszuges (englisch: facial feature detection), wie der Mundwinkel oder des Kinns. Daher lassen sich eine Vielzahl von veröffentlichten Verfahren finden, die sich jedoch teils deutlich hinsichtlich der Detektionsgenauigkeit, Robustheit und Geschwindigkeit unterscheiden. So sind viele Verfahren nur bedingt echtzeitfähig oder liefern nur mit hochaufgelösten Bildquellen ein zufriedenstellendes Ergebnis. In den letzten Jahren wurden daher Verfahren entwickelt, die versuchen diese Problematiken zu lösen. In dieser Arbeit erfolgt eine Betrachtung dreier dieser State-of-the-Art Verfahren: Constrained Local Neural Fields (CLNF), Discriminative Response Map Fitting (DRMF) und Structured Output SVM (SO-SVM), sowie deren Implementierungen. Dazu erfolgt ein empirischer Vergleich hinsichtlich der Detektionsgenauigkeit.

Schlüsselwörter

Facial Feature Points, Detection, Evaluation

CR-Kategorien

I.4.8 [**Scene Analysis**]: Object recognition; I.5 [**PATTERN RECOGNITION**]

1 Einleitung

Als facial feature points werden Punkte im menschlichen Gesichtszug, wie die Mundwinkel oder die Nasenspitze, bezeichnet. Ein Beispiel für 68-Positionen solcher Landmarken ist in Abbildung 1 zu sehen. Für die menschliche Kommunikation sind diese von eminenter Wichtigkeit, lassen sich anhand dieser doch etwa Gefühle wie Verwunderung oder Ärger des Gesprächspartners ablesen. Daher sind diese Punkte auch für die Mensch-Maschinen-Interaktion von Interesse, da sich mit diesen beispielsweise Systeme für das automatische Gesichts-Tracking oder die Emotionserkennung realisieren lassen. Damit dies jedoch möglich wird, muss ein System in der Lage sein diese Punkte zu bestimmen. Hierbei handelt es sich jedoch um kein triviales Problem. Aus diesem Grund gibt es eine Vielzahl veröffentlichter wissenschaftlicher Arbeiten, die sich mit dieser Problematik befassen.

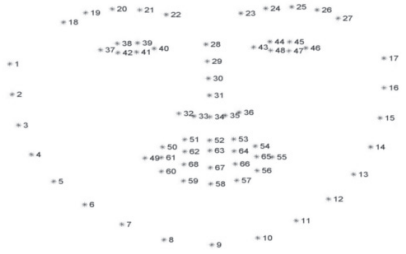

Abbildung 1: 68-Landmarken umfassendes Modell der "300 Faces In-The-Wild Challenge"[8]

*

Betreuer Hochschule: Prof. Dr.-Ing. Cristóbal Curio
Hochschule Reutlingen
Cristobal.Curio@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1.1 Stand der Technik

Frühere Arbeiten im Bereich der Detektion von Facial Feature Points lassen sich in der Regel anhand der Verwendung von Features einteilen. So wird bei holistischen Ansätzen, wie dem Active Appearance Model (AAM) [4], die gesamte Gesichtstextur betrachtet und versucht ein lineares generatives Modell daran anzupassen.
Dagegen wird bei den Teil-basierten Modellen, wie dem Active Shape Model (ASM) [3], jedes Feature separat betrachtet. Anhand dem Vorhandensein und der Position der einzelnen Landmarken wird versucht ein Modell anzupassen.
Da bei den Teil-basierten Modellen nur einzelne Ausschnitte betrachtet werden, sind diese in der Regel robuster gegen Einflüsse wie Verdeckung oder unterschiedliche Beleuchtung. Aus diesem Grund befassen sich viele aktuelle Arbeiten [1],[2],[5] mit den Teil-basierten Modellen und der Erweiterung dieser. Eines der bekanntesten Beispiele hierfür ist das Constrained Local Model (CLM) [5], das von Cristinacce und Cootes im Jahr 2006 vorgestellt wurde. Dieses stellt bis heute eines der State-of-the-Art Verfahren dar. Deshalb handelt es sich bei vielen aktuell veröffentlichten Verfahren um Erweiterungen von CLM, wie etwa [1] und [2], um nur zwei zu nennen.

1.2 Problemstellung

Viele der veröffentlichten Verfahren unterscheiden sich jedoch häufig stark hinsichtlich ihrer Detektionsgenauigkeit. Zusätzlich stehen viele dieser Verfahren unter Patenten und können daher nicht ohne weiteres verwendet werden.
Aus diesem Grund werden in dieser Arbeit drei für die Verwendung im wissenschaftlichen Kontext freigegebenen Verfahren anhand ihrer Detektionsgenauigkeit evaluiert.
Bei den Frameworks handelt es sich um OpenFace[1], CLandmark[2] sowie die Implementierung des Discriminative Response Map Fitting (DRMF) Ansatzes[3].
Nach Betrachtung verschiedener Frameworks wurden diese 3 aus folgenden Gründen ausgewählt: Alle drei Frameworks implementieren ein aktuelles Verfahren und wurden von den jeweiligen Autoren selbst geschrieben. Alle drei Verfahren sollen mit niedrig aufgelösten Bildern auskommen, zusätzlich echtzeitfähig sein und erfüllen damit aktuelle Anforderungen. Zusätzlich handelt es sich bei den in OpenFace und DRMF verwendeten Verfahren um Erweiterungen des CLM Ansatz, wobei es sich wie bereits erläutert um eine der aktuellsten State-of-the-Art Methoden handelt.

2 Frameworks

Als Nächstes erfolgt eine allgemeine Beschreibung der drei untersuchten Frameworks, sowie eine detaillierte Betrachtung der in den Framworks eingesetzten Ansätze zur Landmarkendetektion. Alle drei Ansätze orientieren sich hinsichtlich der Landmarkenpositionen am in Abbildung 1 dargestellten Modell. Für weiterführende Informationen zu den unterschiedlichen Ansätzen sei hiermit auf die jeweiligen Veröffentlichungen verwiesen.

2.1 OpenFace

Bei OpenFace handelt es sich um ein am Computer Laboratory der University of Cambridge entwickeltes Framework. Dieses kann unter Linux, Mac OSX und Windows verwendet werden, jedoch stehen nur für Windows ausführbare Projektdateien zur Verfügung. Auf den anderen Plattformen muss das Projekt kompiliert werden, hierfür steht der C++-Sourcecode bereit. Neben einer C++-API bietet OpenFace eine Schnittstelle für die Einbindung in Matlab. Für die Landmarkendetektion wird ein trainiertes Modell zur Verfügung gestellt, das Projekt bietet jedoch auch einen Code der das eigene Trainieren eines Modells ermöglicht.

[1] OpenFace: https://www.cl.cam.ac.uk/~tb346/res/openface.html
[2] CLandmark: http://cmp.felk.cvut.cz/~uricamic/clandmark/
[3] DRMF: http://ibug.doc.ic.ac.uk/resources/drmf-matlab-code-cvpr-2013/

In OpenFace erfolgt die Bestimmung der Landmarken mit dem Constraint Local Neural Field (CLNF) [2] Ansatz. Hierbei handelt es sich um eine Erweiterung des von Cristinacce und Cootes beschriebenen Constraint Local Model (CLM)[5].
Bei CLNF wird sich dafür, wie bei CLM, am menschlichen Prozess der Gesichtserkennung orientiert.
Das menschliche Gehirn hat gelernt wie ein Gesicht aussieht: zirka in der Mitte befindet sich die Nase, links und rechts oberhalb der Nase befindet sich jeweils ein Auge und unterhalb der Nase befindet sich der Mund. Diese Anordnung kann als Gesichtsmodell bezeichnet werden. In diesem Modell ist die grobe Anordnung der in einem Gesicht enthaltenen Elemente gespeichert. Dadurch werden bestimmte Anordnungen bereits ausgeschlossen. Ein Auge sollte in der Regel nicht unterhalb des Mundes auftauchen oder ähnliches.
Aus diesem Grund wird in CLNF als erster Schritt ein Point Distribution Model (PDM) zur Bestimmung der gesuchten Positionen der Landmarken eingesetzt. Eine Gesichtskontur lässt sich mit Hilfe des PDM wie folgt darstellen:

$$X = \overline{X} + \Phi q \tag{1}$$

Wobei es sich bei $\overline{X}$ um die Mittelwertkontur handelt und bei Φ um die Komponenten der linearen Verformung, q stellt die Parameter der elastischen Verformung dar [2]. Die Parameter $\overline{X}$ und Φ des Modells werden anhand von gelabelten Beispielbildern automatisch gelernt, häufig wird hierfür die Principal Component Analysis (PCA) eingesetzt.
Das gelernte PDM kann dann auf ein beliebiges Bild I angepasst werden, um eine erste Positionsbestimmung der gesuchten Landmarken zu erhalten.
Da die so bestimmten Positionen je nach Gesichtspose oder durch auftretende Verdeckungen jedoch nicht exakt sein können, wird bei CLNF um die bestimmten Landmarkenpositionen eine Region of Interest (ROI) definiert. Diese Bereiche werden dann in einem weiteren Schritt durch die sogenannten Patch Experts, welche auch anhand der Trainingsbilder trainiert werden, weiterverarbeitet. Für jede Landmarke gibt es einen eigenen Patch Expert, dieser berechnet für jeden Pixel innerhalb der ROI die Wahrscheinlichkeit, dass die Landmarke exakt ausgerichtet ist, woraus sich eine Response Map ergibt. Bei CLNF wird gegenüber der Umsetzung bei CLM der Einsatz eines Local Neural Field (LNF) als Patch Expert vorgeschlagen, um so die Geschwindigkeit sowie Detektionsgenauigkeit zu steigern [2].
Als dritter und abschließender Schritt erfolgt die schlussendliche Positionierung der Landmarken anhand der Response Maps. Hierfür wird bei CLNF der Regularised landmark mean shift (RLMS) Algorithmus verwendet. Mit Hilfe diesem wird der Mean Shift Vektor berechnet, der zum aktualisieren der PDM genutzt wird, wodurch unwahrscheinliche Konturformen vermieden werden. Dieser Schritt wird solange wiederholt, bis keine Veränderung mehr auftritt und somit die abschließenden Positionen gefunden wurden.

2.2 *Discriminative Response Map Fitting*

Der Discriminative Response Map Fitting (DRMF) [1] Ansatz wurde von Asthana, Zafeiriou, Cheng und Pantic innerhalb der Intelligent Behavior Understanding Group, kurz iBug, entwickelt. Auf der iBug Homepage steht eine Matlabimplementierung des Ansatzes zum Download bereit. In diesem sind außer einem trainierten Modell und dem dazugehörigen Beispielcode keine weiteren Projektdateien enthalten. Das bedeutet, dass eine Verwendung außerhalb von Matlab nicht möglich ist. Zusätzlich kann die eigentliche Funktion, in der das Modell verwendet wird, nicht eingesehen werden, da es sich hierbei um sogenannten Matlab-P Code handelt. Ein Code, der das selbständige Trainieren eines Modells ermöglicht, wird nicht angeboten.

Bei DRMF handelt es sich um eine weitere Anpassung von CLM. Die Erstellung der

Response Maps erfolgt hierbei mit HOG-Features, wie in [9] beschrieben. Jedoch wird anstelle des RLMS Verfahrens, zur Bestimmung der abschließenden Positionen, ein auf der Diskriminanzanalyse basierender Ansatz eingesetzt.
Das Training des Modells teilt sich hierbei in zwei Schritte. Zuerst wird ein "Response Map Dictionary" trainiert, das es ermöglicht jede ungesehene Response Map näherungsweise zu repräsentieren. Mit diesem können die relevanten Features für den zweiten Schritt, dem Lernen des Parameter Update Modells, extrahiert werden.
Im zweiten Schritt erfolgt ein iteratives Lernen des Update Modells mit Hilfe eines angepassten Boosting-Algorithmus [9].

Um das "Response Map Dictionary" zu trainieren, wird nach folgendem Schema vorgegangen:
Für jeden Punkt i (siehe Abbildung 1) liegt ein Response-Trainingsset $\{A_i(\Delta p_j)\}_{j=1}$ vor. Wird das Trainingsset in eine Matrix $X_i = [vec(A_i(\Delta p_1)), ..., vec(A_i(\Delta p_n))]$ (vec: Vektorisierung einer Matrix) überführt, kann mit Hilfe der nichtnegativen Matrix-Faktorisierung (NMF) das "Response Map Dictionary" gelernt werden. Dadurch erfolgt eine Zerlegung der Matrix in $X_i \approx Z_i H_i$, wobei es sich bei Z_i um das Dictionary und bei H_i um ein Gewichtsset handelt [9].
Die Gewichte für eine Response Map können nun durch die Formel

$$h_i = \underset{h_i}{\operatorname{argmax}} ||Z_i h_i - vec(A_i)||^2, \; s.t \; h_i \geq 0 \tag{2}$$

mit der NMF bestimmt werden. Anstatt der Verwendung von NMF bietet sich die Nutzung von PCA für die Bestimmung des Gewichtsvektors h_i an, da hierdurch eine deutliche Performancesteigerung zu verzeichnen ist [9]. Dieses Vorgehen wird als Response Patch Model bezeichnet und lässt sich wie folgt darstellen:

$$\{M,V\} : M = \{m_i\}_{i=1}^{n} \; und \; V = \{V_i\}_{i=1}^{n} \tag{3}$$

Hierbei handelt es sich bei m_i um den Durchschnittsvektor und bei V_i um die PCA Basis [9].

Im anschließenden Schritt erfolgt das Training des Parameter Update Model U. Ziel hierbei ist es, von N Traningsbildern und den dazugehörigen Shapes, iterativ die Beziehung zwischen den niederdimensionalen Projektionen der Response Maps – die vom Response Patch Modell geliefert werden – und den Updateparametern Δp zu bestimmen.
Sei T die Anzahl der Formparameter der Shapes in S, so dass die initialen Parameter durch $P^{(1)}$ repräsentiert werden:

$$P^{(1)} = \{p_j^1\}_{j=1}^{T} \; und \; \psi^{(1)} = \{\Delta p_j^{(1)}\}_{j=1}^{T} \tag{4}$$

Daraufhin wird für jeden Parameter in $P^{(1)}$ der Response Patch extrahiert und mit dem Patch Model $\{M,V\}$ die dazugehörige Projektion berechnet [9]. Die Projektionen werden dann für jeden Shape separat zu einem Projektionsvektor verkettet $c(\Delta p_j^{(1)}) = [h_1(\Delta p_j^{(1)}), ..., h_n(\Delta p_j^{(1)})]^T$, so dass:

$$\chi^{(1)} = \{c(\Delta p_j^{(1)})\}_{j=1}^{T}. \tag{5}$$

Wobei es sich bei $\chi^{(1)}$ um das initiale Set von Projektionen aus dem Trainingsset handelt. Anhand des Trainingsset $T^{(1)} = \{\chi^{(1)}, \psi^{(1)}\}$ kann die Update-Funktion mit Hilfe einer Linear Support Vector Regression (SVR), für den ersten Iterationsschritt gelernt werden:

$$F^{(1)} : \psi^{(1)} \leftarrow \chi^{(1)} \tag{6}$$

Die Formel (6) wird auf alle in $T^{(1)}$ enthaltenen Daten angewendet, hieraus ergibt sich $T_{new}^{(1)}$. Um das Trainingsset $T^{(2)}$ für den zweiten Iterationsschritt zu erhalten, werden die konvergenten Datensätze aus $T_{new}^{(1)}$ entfernt. Unter konvergent wird dabei verstanden, dass der Root Mean Square Error (RSME) zwischen einem Datensatz und der *Ground Truth* kleiner als der Schwellenwert 2 ist [9]. Für die –weil konvergent– eliminierten Beispiele wird ein neues Beispiel-Set mit Hilfe der Formeln (4) und (5) und dem

gleichen Bild generiert [9].
Konvergieren alle Beispiele in einem Trainingsset, wird der Vorgang abgebrochen und die aktuelle Konfiguration als Ergebnis gewählt. Das daraus resultierende Parameter Update Model U besteht aus einem Set von schwachen Klassifikatoren (engl. weak learners):

$$U = \{F^{(1)}, ..., F^{(n)}\}. \quad (7)$$

Mit U können nun für ein unbekanntes Bild iterativ die Parameter Δp berechnet werden.

2.3 CLandmark

Bei CLandmark handelt es sich um eine Open Source Library für die Landmarkendetektion. Die Library lässt sich unter Linux, Mac OSX und Windows verwenden. Da keine ausführbaren Projektdateien zur Verfügung stehen, muss das Projekt für die jeweilige Plattform kompiliert werden. Neben einer C++-API bietet auch CLandmark eine Matlabschnittstelle.
Auf der zu CLandmark gehörenden Projekthomepage steht ein trainiertes Modell zum Download bereit. Jedoch sind auch Klassen für ein eigenes Modelltraining im Sourcecode enthalten.

CLandmark setzt zur Detektion von Landmarken auf den in [11] beschriebenen Structured Output SVM (SO-SVM) Ansatz, hierbei handelt es sich um eine Anpassung des Deformable Part Models (DPM). Bei DPM wird der Ansatz verfolgt, nicht jeweils ein Modell für die Erscheinung, sowie die geometrischen Einschränkungen zu verwenden, sondern diese zu einem einzigen Modell zu fusionieren. Dieses Modell besteht aus einzelnen Parts, die untereinander verbunden sind und dadurch eine deformierbare Struktur annehmen. Dieses Modell kann als Graph $G = (V, E)$ dargestellt werden, wobei es sich bei $V = \{0, ..., M-1\}$ um ein Set von Landmarken handelt und bei $E \subset V^2$ um ein Set von Kanten, die die benachbarten Landmarken definieren [11].
Um die beste Konfiguration für die Landmarkenposition zu finden, wird bei DPM eine einzelne Scoring-Funktion optimiert. Diese setzt sich aus dem Erscheinungsmodell sowie den Verformungskosten zusammen.
Die Komplexität, die beste Konfiguration zu finden, hängt vom zugrundeliegenden Graph ab.
In der Regel wird das Lernen des Erscheinungsmodells und den Verformungskosten in zwei separaten Schritten durchgeführt, dies vereinfacht den Lernprozess. Beim in CLandmark eingesetzten Ansatz dagegen wird dies in einem einzelnen Schritt mit Hilfe der Structured Output SVM [10] durchgeführt.
Dafür wird jeder Landmarke s eine Position $s_i \in S_i \subset \{1, ..., H\} \times \{1, ..., W\}$ zugewiesen. Hierbei handelt es sich bei S_i um ein Set aller möglichen Positionen der Landmarke innerhalb des Bildes. Die Qualität einer Landmarkenkonfiguration $s = (s_0, ..., s_{M-1} \in S = S_0 \times ... \times S_{M-1})$ wird anhand der Scoring-Funktion

$$f(I, s) = \sum_{i \in V} q_i(I, s_i) + \sum_{(i,j) \in E} g_{ij}(s_i, s_j) \quad (8)$$

gemessen, wobei der Abschnitt vor dem Plus das Erscheinungsmodell, das die Übereinstimmung zwischen der Landmarkenposition s und dem Bild I einschätzt, darstellt. Im hinteren Teil handelt es sich um die Verformungskosten [11]. Das bedeutet das Ziel ist die Maximierung von (2):

$$\hat{s} \in \underset{s \in S}{\operatorname{argmax}} f(I, s). \quad (9)$$

Hierbei wird vorausgesetzt, dass es sich bei $q_i : J \times S_i \to \mathbb{R}, i = 0, ..., M-1$ und $g_{ij} : S_i \times S_j \to \mathbb{R}, (i, j) \in E$ um lineare Funktionen

$$q_i(I, s_i) = \langle w_i^q, \Psi_i^q(I, s_i) \rangle \quad (10)$$

$$g_{ij}(s_i, s_j) = \langle w_{ij}^g, \Psi_{ij}^g(s_i, s_j) \rangle \quad (11)$$

handelt. Wobei $\Psi_i^q : J \times S_i \to \mathbb{R}^{n_{iq}}$ den Feature-Descriptor an der Stelle s_i im Bild I darstellt [11]. Als Feature-Descriptor wird die in [11] beschriebene Sparse Local Binary Pyramid eingesetzt.
Bei $\Psi_{ij}^g : S_i \times S_j \to \mathbb{R}^{n_{ig}}$ handelt es sich

um den Verformungsvektor und bei $w_i^q \in \mathbb{R}^{n_{iq}}, w_{ij}^g \in \mathbb{R}^{n_{ig}}, i = 0,...,M-1$ jeweils um einen Parametervektor, die anhand von Beispielen gelernt werden [11]. Nähere Details hierzu sind in [11] zu finden.

3 Evaluation Umsetzung

In diesem Teil der Arbeit werden die drei Frameworks miteinander verglichen, hierfür werden zuerst die über die Landmarkendetektion hinausgehenden Funktionen betrachtet. Im zweiten Teil des Vergleiches erfolgt eine Evaluation der Detektionsgenauigkeit der Frameworks.

3.1 Gebotene Funktionalität

Die Schnittmenge der gebotenen Funktionalitäten, die alle drei Umsetzungen erfüllen, ergibt sich bereits aus der in Kapitel 1.2 beschriebenen Problemstellung. In den darüber hinaus enthaltenen Funktionalitäten unterscheiden sich die drei Frameworks jedoch teils stark. Damit sich die Frameworks für eine spätere Verwendung in weiterführenden Programmen, wie beispielsweise Programme für die automatische Emotionserkennung, anbieten, wären zusätzliche Funktionalitäten wünschenswert:

- Posen und Blickrichtungserkennung: für weiterführende Gesichtsanalyse.
- Landmarken-Tracking: ein Tracking von Landmarken in Bildsequenzen.
- Mehrgesichtsverarbeitung: Verarbeitungsmöglichkeit von mehreren Gesichtern in einem Bild.
- Verarbeitung von Seitenansichten: Verarbeitungsmöglichkeit von Gesichtern die sich nicht in frontaler Pose befinden.

Diese Aufzählung erhebt hierbei keinen Anspruch auf Vollständigkeit, die aufgeführten Punkte haben sich jedoch bei der Recherche für diese Arbeit und beim Betrachten unterschiedlicher Programme in diesem Kontext herauskristallisiert. Daher werden diese zum Vergleich der Frameworks herangezogen. In Tabelle 1 wurde dafür zusammengefasst, welche Funktionalitäten ein Framework bietet.

Wie aus Tabelle 1 hervorgeht, bietet nur OpenFace eine vollständige Posen- und Blickrichtungserkennung.
Zwar bietet die DRMF-Implementierung die Ausgabe der errechneten Orientierungswinkel eines Gesichtes, jedoch erfolgt keine Interpretation um welche Pose es sich hierbei handelt. Eine Blickrichtungserkennung bietet DRMF nicht.
Auch CLandmark ermöglicht keine Blickrichtungserkennung, lediglich die Ausgabe, ob ein Gesicht als frontal oder in der Seitenansicht erkannt wurde, wird unterstützt.

Ein Tracking von Landmarken in Videos bietet sowohl OpenFace als auch CLandmark, in DRMF ist diese Funktionalität nicht enthalten.

Mehrere Gesichter in einem Bild werden ausschließlich von CLandmark unterstützt. Kommen in einem Bild mehrere Gesichter vor, wird bei den beiden anderen Umsetzungen das zuerst detektierte Gesicht für die Landmarkendetektion herangezogen.

Die Detektion von Gesichtslandmarken bei Gesichtern im Seitenprofil ist bei allen drei Frameworks möglich.

Zusammengefasst kann somit festgehalten werden, dass die DRMF-Implementierung gegenüber OpenFace und CLandmark hinsichtlich der gebotenen Funktionalitäten abfällt. OpenFace und CLandmark dagegen bieten ein ähnliches Niveau bei den gebotenen Funktionalitäten.

3.2 Detektionsgenauigkeit

Die Evaluierung hinsichtlich der Detektionsgenauigkeit wurde in Matlab umgesetzt. Hierfür wurden jeweils die zur Verfügung stehenden trainierten Modelle verwendet, um auszuschließen das sich fehlerhafte Ergebnisse aufgrund eines abweichenden Trai-

	Posen- und Blickrichtungs-Erkennung	Landmarken-Tracking	Multigesichter	Seitenansichten
OpenFace	✓	✓		✓
DRMF				✓
Clandmark		✓	✓	✓

Tabelle 1: Darstellung der gebotenen Funktionalitäten der Frameworks

nings ergeben könnten.
Ein Problem, das sich bei allen Verfahren zur Detektion von Landmarken stellt, ist dass diese eine möglichst exakte Position des Gesichtes im Bild benötigen. Um diese Positionen zu ermitteln, werden in der Regel Gesichtsdetektoren eingesetzt. Auch die drei betrachteten Frameworks haben jeweils einen oder mehrere Gesichtsdetektoren eingebunden, damit jedoch eine Vergleichbarkeit der Ergebnisse nicht durch unterschiedliche Genauigkeit dieser verfälscht wird, werden die von den Bilddatenbanken mitgelieferten Positionen verwendet (siehe dazu nachfolgendes Unterkapitel).

3.2.1 Bilddatenbanken

Um die benötigte Anzahl an Bilddaten, die für die Evaluierung der Frameworks benötigt wurden, zu erhalten, wurde auf die Helen [6] und die AFW [13] Bilddatenbanken zurückgegriffen.
Beide Datenbanken enthalten *Faces in the Wild*, das bedeutet die enthaltenen Bilddaten wurden nicht unter kontrollierten Bedingungen aufgenommen (siehe Abbildung 2 a). Daher unterscheiden sich die Bilder hinsichtlich Parametern wie Beleuchtung oder Hintergrund und Kopfposen.
Die Evaluation wurde nur auf den in den Datenbanken enthaltenen Testbildern und nicht auf den Trainingsbildern durchgeführt. Die beiden Datenbanken zusammengenommen ergaben 422 Bilder.
Zu den einzelnen Bildern wird die sogenannte *Ground Truth* mitgeliefert, das heißt die tatsächlichen Landmarkpositionen. Außerdem wird für jedes Bild angegeben, an welcher Position sich ein Gesicht in diesem befindet.
Neben den *Faces in the Wild*, wurden in dieser Arbeit zusätzlich computergenerierte Gesichtsgrafiken für die Evaluierung erstellt, siehe Abbildung 2 b). Durch diese Grafiken ist ein Vergleich der Ansätze auf gleichen Daten und unter kontrollierten Bedingungen möglich. Die Grafiken wurde mit Hilfe des Basel Face Model [7] und der Open Source Matlabtoolbox *Psychtoolbox* generiert.

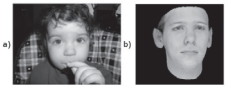

Abbildung 2: a) Beispiel *Face in the Wild* [6], b) Beispiel computergeneriertes Gesicht

3.2.2 Metriken

Um die Genauigkeit der Frameworks zu vergleichen, wird die Abweichung zwischen ermittelter und tatsächlicher Position errechnet. Hierfür wird wie bei der *300 Faces In-The-Wild Challenge* [8] der euklidische Abstand als Error-Maß verwendet. Dieser wird anhand des Abstands der äußeren Augenwinkel normalisiert.

3.2.3 Vorgehen und Ergebnisse

Als erster Schritt im Prozess der Genauigkeitsevaluation wurden die Verfahren nacheinander auf die *Faces in the Wild* angewendet. Das daraus resultierende Ergebnis ist in Abbildung 3 abgebildet.
Hieraus wird direkt ersichtlich, dass die beiden Frameworks OpenFace und CLandmark jeweils eine deutlich genauere Landmarkbestimmung liefern als der DRMF Ansatz. Als zweites fällt ins Auge, dass OpenFace und CLandmark bei einem Fehler < 0.08 relativ dicht beieinander liegen, jedoch mit einer etwas größeren Genauigkeit auf Seiten von OpenFace, was auch aus Tabelle 2 hervorgeht. Interessant hierbei ist, dass ca. ab

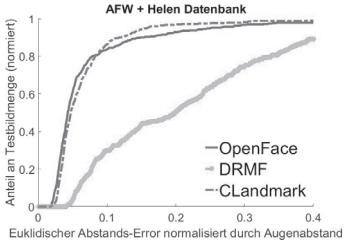

Abbildung 3: Evaluierungsergebnis AFW + Helen Datensatz

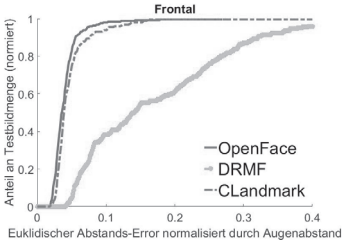

Abbildung 4: Evaluierungsergebnis für Frontal

einem Fehler > 0.8 OpenFace hinsichtlich der Genauigkeit von CLandmark übertroffen wird. Um diesem Verhalten näher auf den Grund zu gehen, wurde der Datensatz in drei Unterkategorien aufgeteilt. Diese unterscheiden sich hinsichtlich der darin enthaltenen Kopfposen:

- Frontal: In dieser sind 247 Frontalansichten mit einem Yaw-Winkelbereich von -15 bis +15 enthalten.
- Seitenansicht Links: Enthält 85 Bilder mit Gesichtern die einen Yaw-Winkel < -15 enthalten.
- Seitenansicht Rechts: Enthält 91 Bilder mit Gesichtern die einen Yaw-Winkel > 15 enthalten.

Bei der Aufteilung der Bilder wurde dabei wie folgt vorgegangen: Zuerst erfolgte eine händische Einteilung der Bilder in die drei Kategorien. Um diese Einteilung zu überprüfen wurde mit dem in [12] beschriebenen und als Matlabcode veröffentlichten Verfahren, die Einteilung anhand der Yaw-Winkel überprüft.
Für den Datensatz Frontal ergibt sich das in Abbildung 4 dargestellte Bild. Wie zu sehen ist, ergibt sich ein ähnlicher Verlauf wie in Abbildung 3. Das bedeutet DRMF liefert die ungenausten Positionen und OpenFace sowie CLandmark sind wieder dicht beieinander. Jedoch wird dieses Mal OpenFace nicht von CLandmark "überholt", sondern liefert sogar die genausten Positionen

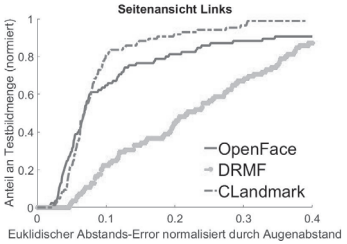

Abbildung 5: Evaluierungsergebnis für Seitenansicht Links

(siehe Tabelle 2). Daraus lässt sich schließen, dass OpenFace bei Gesichtern, die frontal abgebildet sind durchweg genauere Ergebnisse als CLandmark liefert.
Anders gestaltet sich dies jedoch bei Gesichtern in der Seitenansicht. Zwar liefert, wie aus Abbildung 5 und Abbildung 6 sowie Tabelle 2 hervorgeht, DRMF immer noch die ungenausten Positionen, jedoch ergibt sich ein anderes Bild für OpenFace und CLandmark. Wie zu sehen ist, übertrifft CLandmark in beiden Fällen bei zunehmender Ungenauigkeit OpenFace. Hieraus lässt sich schließen, dass CLandmark mit Gesichtern in der Seitenansicht besser zurechtkommt als OpenFace, wodurch sich auch das in Abbildung 3 ersichtliche Verhalten erklären lässt.

Nach der Evaluierung auf den *Faces in the Wild* wurde zusätzlich eine Evaluierung auf den selbst generierten Computergrafiken durchgeführt. Hierbei war von Interesse, ob die Frameworks ähnlich gute Ergebnisse liefern wie auf "realen" Bildern. Für

	AFW+Helen	Frontal	Seitenansicht Links	Seitenansicht Rechts	Computergen. Frontal	Computergen. Links	Computergen. Rechts
OpenFace	82.3%	89.75%	70.2%	73.4%	88.4%	60.5%	57.5%
DRMF	48.9%	57.8%	43%	30%	87.4%	77.2%	78.4%
CLandmark	83.5%	88.1%	77.5%	76.7%	89.1%	65%	66.5%

Tabelle 2: Prozentuale Angabe des Flächeninhalts unter den jeweiligen Kurven in Abbildung 3 bis 9.

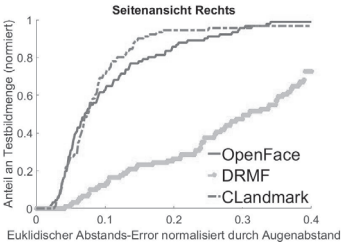

Abbildung 6: Evaluierungsergebnis für Seitenansicht Rechts

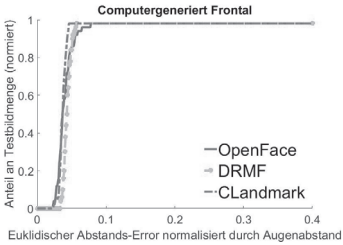

Abbildung 7: Evaluierungsergebnis computergeneriert Frontal

die Evaluierung wurden jeweils 50 Bilder für die drei Kategorien Frontal, Seitenansicht Rechts und Links generiert. Die Winkel wurden hierbei gleich wie bei den *Faces in the Wild* Bildern gewählt.

Wie in den Abbildungen 7, 8 und 9 zu sehen ist, liefern alle drei Frameworks deutlich genauere Positionen, als sie das bei den *Faces in the Wild* tun. Dies kann dadurch erklärt werden, dass bei den computergenerierten Grafiken keine Verdeckungen sowie immer der gleiche Hintergrund auftritt. Was jedoch sehr interessant ist, ist dass die Frameworks bei Computergrafiken sehr dicht beieinander liegen. In diesem Falle liefert DRMF sogar mit die besten Ergebnisse (siehe Tabelle 2). Dies lässt vermuten, dass das DRMF Modell weniger auf *Faces in the Wild* Bilder trainiert wurde, als auf Bilder, die unter kontrollierten Bedingungen aufgenommen wurden.

Bei Gesichtern in der Seitenansicht, bietet sich ein ähnliches Bild wie bei den *Faces in the Wild* Bildern (siehe Abbildung 8 und 9). Zu Beginn liegen OpenFace und CLandmark nah beieinander, bei ansteigender Ungenauigkeit wird OpenFace von CLandmark wieder übertroffen. Auch hier ist wieder zu sehen, dass DRMF bei "kontrolliert" aufgenommenen Bildern sehr genaue Ergebnisse liefert.

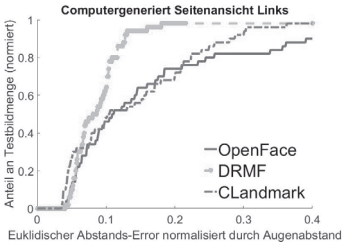

Abbildung 8: Evaluierungsergebnis computergenerierte Seitenansicht Links

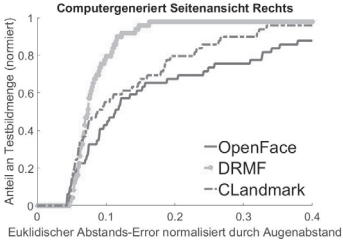

Abbildung 9: Evaluierungsergebnis computergenerierte Seitenansicht Rechts

4 Fazit

Abschließend kann festgehalten werden, dass die beiden Frameworks OpenFace und CLandmark sich besser für die Verwendung in weiterführenden Programmen anbieten. Dies liegt einmal daran, dass diese hinsichtlich der Verwendung nicht nur auf Matlab beschränkt sind und zum anderen das beide eine deutlich bessere Detektionsgenauigkeit von Landmarken bieten. Je nach Verwendungsfall, bietet sich OpenFace mehr bei frontal abgebildeten Gesichtern an und CLandmark bei Gesichtern in der Seitenansicht. Für die Verwendung im Zusammenhang mit computergenerierten Gesichtern bieten sich alle der drei Frameworks an, im besonderen Maße DRMF und CLandmark.

Literatur

[1] A. Asthana, S. Zafeiriou, S. Cheng, and M. Pantic. Robust discriminative response map fitting with constrained local models. In *2013 IEEE Conference on Computer Vision and Pattern Recognition*, pages 3444–3451, June 2013.

[2] T. Baltrusaitis, P. Robinson, and L. P. Morency. Constrained local neural fields for robust facial landmark detection in the wild. In *2013 IEEE International Conference on Computer Vision Workshops*, pages 354–361, Dec 2013.

[3] T. Cootes, C. Taylor, D. Cooper, and J. Graham. Active shape models-their training and application. *Computer Vision and Image Understanding*, 61(1):38 – 59, 1995.

[4] T. F. Cootes, G. J. Edwards, and C. J. Taylor. Active appearance models. In *European conference on computer vision*, pages 484–498. Springer Berlin Heidelberg, 1998.

[5] D. Cristinacce and T. Cootes. Feature detection and tracking with constrained local models. pages 929–938, 2006.

[6] V. Le, J. Brandt, Z. Lin, L. Bourdev, and T. S. Huang. *Interactive Facial Feature Localization*, pages 679–692. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[7] P. Paysan, R. Knothe, B. Amberg, S. Romdhani, and T. Vetter. A 3d face model for pose and illumination invariant face recognition. Genova, Italy, 2009. IEEE.

[8] C. Sagonas, G. Tzimiropoulos, S. Zafeiriou, and M. Pantic. 300 faces in-the-wild challenge: The first facial landmark localization challenge. In *2013 IEEE International Conference on Computer Vision Workshops*, pages 397–403, Dec 2013.

[9] J. M. Saragih, S. Lucey, and J. F. Cohn. Deformable model fitting by regularized landmark mean-shift. *International Journal of Computer Vision*, 91(2):200–215, 2011.

[10] I. Tsochantaridis, T. Joachims, T. Hofmann, and Y. Altun. Large margin methods for structured and interdependent output variables. *J. Mach. Learn. Res.*, 6:1453–1484, Dec. 2005.

[11] M. Uřičář, V. Franc, and V. Hlaváč. Detector of facial landmarks learned by the structured output SVM. In *VISAPP '12: Proceedings of the 7th International Conference on Computer Vision Theory and Applications*, pages 547–556, 2012.

[12] D. R. X. Zhu. Face detection, pose estimation and landmark localization in the wild. In *Computer Vision and Pattern Recognition (CVPR) Providence, Rhode Island, June 2012.*

[13] X. Zhu and D. Ramanan. Face detection, pose estimation, and landmark localization in the wild. In *2012 IEEE Conference on Computer Vision and Pattern Recognition*, pages 2879–2886, June 2012.

IT – Sicherheit beim Autonomen Fahren

Iana Preuß
Reutlingen University
Iana.Preuss@Student.Reutlingen-University.DE

Abstract

In den letzten Jahren beschäftigten sich Forscher und Automobilhersteller mit den Voraussetzungen für die Einführung von autonomem Fahren. Für Innovationen und Geschäftsmodelle im Bereich der intelligenten Mobilität, aber auch innerhalb der digitalen Wertschöpfungskette, spielen generell Zuverlässigkeit und Qualität der digitalen Datenübertragung eine entscheidende Rolle. Bevor das autonome Fahren vollständig eingeführt wird, muss man feststellen, welche Anforderungen an die digitale Infrastruktur beachtet werden müssen, gleichzeitig muss die Bedrohungslandschaft für autonomes Fahren analysiert werden.
Die folgende Arbeit beschäftigt sich damit, die Anforderungen und Gefahren zu analysieren und allgemeine Handlungsempfehlungen vorzuschlagen.

Schlüsselwörter

Autonomes Fahren, Intelligente Mobilität, Fahrerassistenzsysteme, V2X, Big Data, IT-Sicherheit beim autonomen Fahren, vollautomatisiertes Fahren.

Betreuer Hochschule:
Prof. Dr. –Ing. Michael Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

CR-Kategorien

I.2.9 [Robotics]: Autonomous vehicles

1 Einleitung

„Wenn ich die Menschen gefragt hätte, was sie wollen, hätten sie gesagt *schnellere Pferde*.“ Henry Ford, 1863-1947.
Mit der Zeit sind die Anforderungen an das Auto gestiegen. Bald will man mit dem Auto nicht nur schnell von A nach B kommen können, sondern währen der Fahrzeit andere Aufgaben erledigen. In der Zukunft ist zu erwarten, dass die Vernetzung des Verkehrs und seiner Teilnehmer zunehmen wird. [3]
Dabei sollte der Verkehr völlig neu organisiert werden und gleichzeitig müssen die Sicherheit, die Energieeffizienz und die Infrastrukturkapazität erhöht werden. Durch hochautomatisierte Fahrsysteme sowohl im motorisierten Individualverkehr als auch im Transportverkehr, wird die Verkehrssicherheit gesteigert. [3]
Technologien und klare organisatorische und rechtliche Strukturen sind wichtige Aspekte der intelligenten Mobilität. [1]
Im Englischen unterscheiden sich zwei Begriffe „Safety“ und „Security“ voneinander. Unter dem Begriff „Safety“ versteht man die Reduzierung von Gefahren, die aktiv von innen aus dem System heraus nach außen entstehen. Das Ziel ist die Schäden an Personen oder an der Umwelt zu vermeiden, die durch einen Systemausfall bzw. ein fehlerhaftes Verhalten des Systems entstehen. Der Begriff „Security“ bedeutet die Sicherheit des Systems vor einem Angriff von außen. [5]
In dieser Arbeit wird der Aspekt „Security“ dargestellt. Die folgende Arbeit versucht neben ihren positiven Aspekten auch einen

Überblick zu möglichen Problemen des autonomen Fahrens oder sogar negativen Auswirkungen von künstlicher Intelligenz auf die Verkehrssicherheit zu geben.

In Kapitel 2 wird der Begriff „Intelligente Mobilität“ erklärt. In dem darauffolgenden Kapitel werden die technischen Anforderungen an die digitale Infrastruktur und an Dienste und Schnittstellen, sowie die Rahmenbedingungen zur Nutzung von Big Data definiert. In dem Kapitel 4 wird die Kommunikation bei vernetzter Mobilität dargestellt. Kapitel 5 behandelt die Bedrohungslandschaften für das autonome Fahren. Abschließend werden in den Kapiteln 6 allgemeine Handlungsempfehlungen behandelt. In Kapitel 7 folgt die Auflistung der Literatur.

2 Intelligente Mobilität

Ein wichtiges Ziel der intelligenten Mobilität ist die Unterstützung von Fahrzeugen durch Leit- und Sicherungstechnik. Die Fahrzeuge werden durch diese Systeme auf der sichersten Route geführt, dabei mit energieeffizienter Geschwindigkeit und im optimalen Abstand zueinander. Verkehrswege werden automatisch auf Belastung und Unfälle überprüft. Die Fahrspuren werden im Straßenverkehr zu Spitzenzeiten bedarfsgerecht zugeteilt und freigegeben. Das gleiche Prinzip gilt für Lkw-Parkplätze an Bundesfernstraßen. [1]

Die Entwicklung der Automobilindustrie schreitet stets voran und das vollautomatisierte Fahren wird bald möglich sein. Manche Forscher vermuten die Einführung von dem autonomen Fahren in drei bis fünf Jahren. Automatisierte Fahrfunktionen verbessern die Verkehrssicherheit und erleichtern den Verkehrsfluss. [3]

Doch ein Auto, das umfassend vernetzt ist und selbstständig fährt, bietet nicht nur Vorteile, sondern auch Risiken. Bei der Entwicklung von autonomem Fahren verdient die IT-Sicherheit besondere Aufmerksamkeit. Es besteht die Gefahr gestohlene Online-Zugangsdaten oder beispielsweise der Fremdzugriff durch einen Angreifer, der die Bremsen Ihres Autos manipulieren kann. In diesem Fall wird es schwierig einen Unfall zu vermeiden. Solche Eingriffe müssen durch eine durchdachte IT-Sicherheit gänzlich vermieden werden und bieten auch Lösungen für heutige Datenlecks. [8]

3 Anforderungen an die digitale Infrastruktur

Die intelligente Mobilität kann durch zentrale und dezentrale Verbindung zwischen den Elementen der digitalen Infrastruktur erreicht werden.

Die Voraussetzung für intelligente Mobilität ist eine digitale Infrastruktur, die auf der Abbildung 1 dargestellt wird.

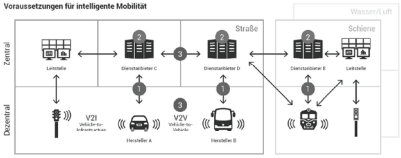

Abbildung 1: Voraussetzungen für intelligente Mobilität [2]

Mit Hilfe der Netzinfrastruktur wird das Mobil- und Festnetz große Datenmengen zeitgerecht bewältigen müssen. Die Kombination von Massendaten (Big Data) bietet die Möglichkeiten für datenbasierte Verbesserung von Produkten und Diensten. Und die Interoperabilität von Diensten und Systemen verschiedener Hersteller und Anbieter muss sichergestellt werden.

Die Elemente einer digitalen Infrastruktur werden detaillierte in den Kapiteln 3.1 und 3.2 erklärt.

3.1 Technische Anforderungen an die Netzinfrastruktur

Der Wandel der Netzinfrastruktur stellt eine hohe Herausforderung an die mobile

Kommunikation zwischen zahlreichen mobilen und stationären Geräten. Jedes im Verkehr befindliche Element sollte verbunden werden, um jegliche Kollisionen zu verhindern. [14]

Die Kommunikation zwischen diesen Elementen ist die eine Anforderung. Da aber nicht jeder auf die Straße rollende Ball ein Signal aussenden kann, sind die Sensoren in aktuellen Fahrassistenzsystemen zu unterstützen. Gemeint ist dabei, dass die aktuellen infrastrukturellen Gegebenheiten optimiert werden können. Fahrbahnmarkierungen, Spurbegrenzungen und Fahrstreifenmarkierungen können kontrastreicher und besser für die Sensoren angepasst, reflektieren. Dazu gehört auch, dass diese Markierungen durchgängig verlaufen und die Fahrbahnoberfläche eben verläuft. Verkehrszeichen müssen gut positioniert und für Sensoren optimierte Lesbarkeit aufweisen. Diese Optimierungen und der Ausbau der bestehenden Standards unterstützen die aktuelle bordeigene Sensorik, die zukünftig in kürzeren Wartungsintervallen geprüft werden müssen, um den Sicherheitsanforderungen gerecht zu werden. [14]

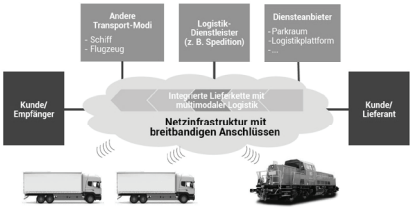

Abbildung 2: Vernetzung der Teilnehmer [3]

Um das autonome Fahren auf allen Straßen mit einer präzisen Positionsangabe möglich zu machen, soll ein flächendeckendes 5G Netz aufgebaut werden. Das aktuelle 4G (LTE) Netz erreicht nicht die erforderliche Latenzzeit für die notwendige Echtzeiterfassung. Die verkehrstechnische Infrastruktur sollte spätestens mit der Einführung von autonomen Fahrzeugen (etwa 2024) über die Erfassungs- und Kommunikationstechnologie ITS-5G (Intelligent Transport System – 5G) verfügen. Moderne Signalanlagen die über diesen Kommunikationsstandard verfügen, wie Ampeln, Verkehrsleitsysteme, Wechselkennzeichen, sowie Bewegungsströmungen im Straßenverkehr müssen in diesem Stadium vorhanden sein. [14]

Neben ITS-5G werden weitere Kommunikationswege und deren Ausbau benötigt. Auf dem Plan steht dabei die bedarfsgerechte Allokation von mehreren Frequenzspektren für die im Verkehr genutzten hybriden Netze aus Festnetz, Rundfunk (DAB4, DVB-T5, LTE Broadcast), Mobilfunk und V2X-Kommunikation. V2X-Kommunikation ist die Kommunikation von Fahrzeugen zu anderen Systemen (X). V2V (Vehicle-to-Vehicle) oder der Kommunikation zwischen Fahrzeug und Ampel V2I (Vehicle-to-Infrastructure). Das X steht also als Variable für die Kommunikation von Fahrzeugen zu anderen stationären oder mobilen Geräten (X). Forscher im Bereich des autonomen Fahrens stellen kritische Fragen zur Nutzung von 5G-Mobilfunk. Was passiert, wenn das Mobilfunknetz nicht flächendeckend verfügbar wird? Es stellt sich die Frage, ob der Umweg über eine zentrale Netzinfrastruktur für die Informationsübertragung zwischen Fahrzeugen sinnvoll ist? [14]

Der dabei genannte Standard, der in der Automotive-Welt auch als „WLAN 11p“ oder- „WLANp“ bekannt, ist eine spezielle Variante der bekannten WLAN-Spezifikationen für die Kommunikation zwischen Fahrzeugen. Er basiert auf der WLAN-Variante 802.11a, wobei auf zeitaufwändige Authentifizierungs-Mechanismen verzichtet wird. Das heißt, dass für das Aushandeln von WLAN-Passwörtern keine Zeit bleibt, wenn sich Fahrzeuge gegenseitig über eine Notbremsung oder einen Spurwechsel informieren möchten. [14]

Dabei muss die Datenübertragung robust sein, damit auch bei höheren Geschwindigkeiten und höherem Verkehrsaufkommen mit vielen sendenden und empfangenden Fahrzeugen und über möglichst große Fahrzeugabstände funktionieren kann. Dieser Anforderung trägt der erwähnte „WLAN 11p“ Standard 802.11p mit verschiedenen Parametern wie längerer Symboldauer und größeren Schutzintervallen zwischen den Datenpaketen Rechnung. Obwohl man geringere Datenraten erreicht, reichen Verbindungsgeschwindigkeiten zwischen 3 und 27 MBit/s für Warnungen und Ziel-, beziehungsweise Richtungsangaben aus. Gleichzeitig müssen die übertragenen Informationen valide sein. [14]

Ein großes Problem sehen die Netzbetreiber in der Netzabdeckung der ländlichen Gebiete. Ohne Investitionen von Ländern und der EU ist dieses Ziel gerade bei den Echtzeit-Technologien nicht zu erreichen.

Laut Angabe des Verkehrsministeriums werden heute von Fahrzeugen eine Datenmenge von 27 MB (Megabyte) je gefahrener Stunde durch das Mobilfunknetz ausgestrahlt. Die zukünftige Datenmenge (BigData) in einem effizienten Datenmanagement bereitzustellen stellt eine weitere Herausforderung dar. [2]

3.2 Rahmenbedingungen zur Nutzung von Big Data

Durch die hohe Vernetzung wird die Sicherheit der Teilnehmer im öffentlichen Verkehr erhöht. Dennoch muss die Privatsphäre vor Missbrauch geschützt werden. Die Massen an erhobenen Daten können gezielt missbraucht werden, wenn kein ausreichender Datenschutz besteht. Hier muss in Zukunft ein einheitliches System entwickelt werden, dass es Hackern unmöglich macht, personenbezogene Daten abzugreifen. [2]

Daten fallen in der Infrastruktur auf verschiedenen Ebenen an. Zum Beispiel Informationen über die derzeitige Verkehrssituation, freie Kapazitäten in Parkhäusern oder auf Rastplätzen und Auslastungsprofile für Straßen- und Schienenstrecken. Diese Grundlagen stellen noch kein hohes Risiko dar. Weiter auf der Fahrzeugebene werden Performancedaten, Transportkapazitäten, sowie Standortdaten gesammelt, um Fernwartung, Assistenzsysteme und Verkehrssteuerung zu ermöglichen. Darüber hinaus werden in der intelligenten Mobilität aber auch Daten zum Fahrgast gesammelt und ausgewertet. Um das volle Potenzial aus der Kombination dieser Daten zu schöpfen und eine Dynamik in der Auslastung zu erreichen, müssen diese Daten auf einer zentralen Plattform zusammenlaufen. [3]

In Deutschland ist es aufgrund des strengeren Datenschutzes schwierig an standort-bezogene Daten über die Mobilfunkanbieter zu gelangen. Dahingegen ist es durch die einmalige Zustimmung des Nutzers über Serviceanbieter Standortdaten über WLAN oder GPS des Smartphones zu gelangen. [3]

Dazu sollen Datensicherheitstechnologien in Europa entwickelt werden und hinsichtlich der nationalen Richtlinien zu Datenspeicherung, -übertragung und -nutzung angepasst werden. Um die gleichen Vorgaben und Systemschnittstellen für alle angebotenen Dienste in Deutschland und in der Europäischen Union zu schaffen, wird eine nach dem Marktortprinzip gerichtete EU-Datenschutz-Grundverordnung verabschiedet. Ziel ist die Harmonisierung der gesamten Branche zu erreichen und mit der neuen EU-Verordnung bereits vorhandene Richtlinien abzuschaffen, um ein Global Level Playing Field zu erreichen. [2]

3.3 Anforderungen an Dienste und Schnittstellen

Die Frage der Schnittstelle ist in vielen Bereichen der Automobilbranche schon

immer eine Herausforderung gewesen. Internationale Standards sind sinnvoll, dennoch unterdrücken manche Hersteller die Kompatibilität durch Eigenentwicklungen. [12]

Bei Datenschnittstellen müssen standardisierte Übertragungsprotokolle geschaffen werden, die einen international anerkannten Sicherheitsstandard abdecken. Aber auch die Entwicklungsplattform in den autonomen Fahrzeugen muss über einheitliche Standards ablaufen. Es ist zu erwähnen, wie wichtig die Sicherheitsanforderungen an die Schnittstellen sind, denn ein autonomes Fahrzeug soll sich ohne jegliches Eingreifen des Fahrers dauerhaft sicher fortbewegen. Die Schnittstellen müssen störungs-, ausfallsicher und sicher gegen äußere Einflüsse sein. Das Sicherheitskonzept muss wie ein roter Faden durch die IT-Architektur des autonomen Fahrzeugs verlaufen. [3]

In den heutigen E/E-Architekturen von Fahrzeugen sind bis zu 100 Steuergeräte verbaut, die zudem über ein nicht zu vernachlässigendes Gewicht verfügen. Zur Gewichtsreduktion ist auch der Entfall von Steuergeräten notwendig, was im Gegensatz zum Wunsch von sicherem autonomem Fahren steht. Einige der Steuergeräte sollen durch Domain-Controller ersetzt werden und die Informationen von einem Zentralrechner in Echtzeit abgerufen werden. Dazu ist eine ständige und echtzeitfähige online Verbindung unabdingbar. Zudem muss die zukünftige E/E-Architektur und deren Schnittstellen schon bei Fahrzeugvorstellung für zukünftige Funktionen vorbereitet werden. Diese Funktionen gibt es zum Zeitpunkt der Fahrzeugvorstellung noch nicht. [4]

4 Kommunikation bei vernetzter Mobilität

Die Industrie hat zur herstellerübergreifenden Kommunikation eine Industriekooperation, das Communication Consortium, einberufen, um die Kommunikation zwischen Fahrzeugen und insbesondere Autos zu vereinheitlichen. [12]

Wie im vorherigen Kapitel erwähnt, sollen in Zukunft hauptsächlich die drahtlose V2X-Koomunikationen etabliert werden. Dazu operiert das Communication Consortium (V2X-CC) auf EU – Basis und besteht aus Automobilherstellern, Zulieferern und wissenschaftlichen Instituten. Daneben existiert bereits ein laufendes EU Projekt mit dem Namen „COMeSafety“, das über europaweite lizenzfreie Frequenzbänder für die Vernetzung von V2X berät. Es sollen sicherheitsrelevante und nicht-sicherheitsrelevante Frequenzbänder bereitgestellt werden. Die Hauptaufgabe besteht in der Standardisierung, Regulierung, Harmonisierung und Erstellung von europaweiten und herstellerübergreifenden Richtlinien für die folgenden Kommunikationsprotokolle. [12]

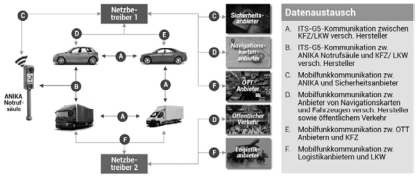

Abbildung 3: Datenverbindung bei der intelligenten Mobilität [3]

Wie schon erwähnt wurde, ist Vehicle-2-Vehicle (V2V) die Verbindung zwischen zwei Fahrzeugen. Die Verbindung zwischen dem Fahrzeug und einem elektronischen Chip (NFC-Technik), auf dem Informationen gespeichert sind, ist die Verbindungsart Vehicle-2-Tag (V2T). [12]

Die Verbindung zwischen dem Fahrzeug und einem mobilen Gerät wie dem Mobiltelefon (Smartphone), Tablets oder Notebooks: Vehicle-2-MobileDevice (V2MD). [12]

Die Verbindung zwischen dem Fahrzeug und einer Verbraucherplattform: Vehicle-2-CustomerPortal (V2CP). [12]

Die Verbindung zwischen dem Fahrzeug und der Sensorik des eigenen Fahrzeugs und fremden Fahrzeugen: Vehicle-2-Enterprise (V2E). [12]

Die Verbindung zwischen dem Fahrzeug und der Haushaltssteuerung (Smart-Home): Vehicle-2-Home (V2H). [12]

Die Verbindung zwischen dem Fahrzeug und dem Verkehrsleitsystem (Ampelsignalen, Bahnschranken, Parkhäusern): Vehicle-2-TrafficInfrastructure (V2TI). [12]

Gerade in den Bereichen Sicherheit und Mobilität besteht hoher Bedarf an herstellerübergreifenden Regelungen, für dessen sicherheitsrelevante Funktionen der Frequenzbereich von 5875 MHz bis 5905 MHz beschlossen wurde. Hierüber kommunizieren vor allem Applikationen der Gefahrenwarnung, des Kreuzungs-Management, Ampeln und Verkehrszeichen (Road-Side-Units: RSU), Umgebungssensoren und weitere Infrastrukturelemente des Bus- und Bahnverkehrs. [4]

Für nicht-sicherheitsrelevante Funktionen soll das ISM-Frequenzband (Industrial, Scientific and Medical Band) von 5855 MHz bis 5875 MHz genutzt werden. [12]

Im Bereich Service, Unterhaltung, Infotainment werden hybride Netze aus Mobilfunk-Datenverbindung, ISM-Frequenzband, Frequenzen des Rundfunks, öffentliche WLAN Signale und WLAN-Signale von Festnetzanschlüssen genutzt werden. Die Festnetzanschlüsse sollen dabei keine Störung oder Leistungsminderung der gebuchten Leistung spüren. Des Weiteren gehört zum Service der besondere Bereich proprietärer Applikationen der Ferndiagnose und Fernwartung. Hierin sollen Daten mit Werkstätten ausgetauscht werden, aber auch notwendige Verschleißteile bei Portalen vom Fahrzeug bestellt werden, damit ein Austausch vor dem Ausfall des Bauteils vorgenommen wird. Die genannten Kommunikationswege im Bereich V2X werden mit den Positionsangaben über GPS (später GALILEO) zusammengeführt, um den Verkehr beziehungsweise eine intelligente Zuflusssteuerung (Ramp Metering) an Auffahrten, Hauptstrecken, Autobahnen und Tunneleinfahrten zu steuern. [12]

Aber nicht nur im Individualverkehr, sondern auch im Schienenverkehr, sollen GPS (später GALILEO) mit dem Rail-GSM-System verbunden und gesteuert werden. Dabei werden alle Sensoren über den Zustand der Ladung, den Ort und den Streckenverlauf über das Mobilfunknetz an eine Kommunikationszentrale gesendet und an Logistikdienstleister und an das System des Individualverkehrs (Straßen) gesendet. [12]

5 Bedrohungslandschaft für Autonomes Fahren

Große Gefahr beim autonomen Fahren entsteht dann, wenn personenspezifische Bewegungsprofile in die falschen Hände geraten. Ebenso gefährlich wird es, beim Fremdzugriff in das Fahrzeug oder in die Verkehrsteuerung. Die Details werden in den nächsten Unterkapiteln behandelt. [3]

Abbildung 4: Bedrohungslandschaft für Autonomes Fahren[3]

5.1 Personenspezifische Bewegungsprofile

Einzelne Positionsdaten zu einem Bewegungsprofil werden über das Smartphone seit etwa einem Jahrzehnt gesammelt. Da das Smartphone ein ständiger Begleiter des Menschen geworden ist, also auch während Fahrten in Fahrzeugen, werden schon lange Bewegungsprofile im Straßen- und

Schienenverkehr aufgenommen. Durch die ständige Positionsangabe eines autonomen Fahrzeugs, ändert sich daher eins: das Fahrzeug stellt einen höheren materiellen Wert gegenüber einem Smartphone dar und stellt damit einen höheres Missbrauchspotential dar. Zudem können in einem Fahrzeug Waren von weiterem materiellem Wert transportiert werden. Es ist also davon auszugehen, dass kriminelle Handlungen in diesem Bereich zunehmen und ein höherer Sicherheitsstandard bei der Datenübertragung und dem Diebstahlschutz notwendig ist. [2]
Zu den kriminellen Handlungen gehören dabei weiterhin die Verfolgung von Personen und Gütern, aber es ist von einem Anstieg an Erpressungen, Überfällen oder Wirtschaftsspionage anzunehmen. [2]

5.2 Eingriff in das Fahrzeug

Neben dem ausspionieren des Bewegungsprofils (s. Kapitel 5.1), können auch Rache an Personen oder gezielte Anschläge auf Personen eine Rolle für kriminelle Handlungen in Bezug auf autonome Fahrzeuge spielen. Der Eingriff in das Fahrzeugsystem stellt dabei mehrere Möglichkeiten zur Manipulation eines ungeschützten autonomen Fahrzeugsystems. Neben der Übernahme der Lenkung, Manipulation der Bremsanlage oder der Schließanlage des Fahrzeugs, können durch das Entertainmentsystem Störgeräusche oder Zugangsdaten und Kontodaten abgegriffen werden. Hierbei wird deutlich, wie wichtig die IT-Sicherheit bei autonomen Fahren ist.
Ein positiver Aspekt des Eingriffs auf das Fahrzeug, stellt die Übernahme der Fahrzeugsteuerung durch die Polizei bei der Verfolgung von Verbrechern dar. Es ist anzunehmen, dass es für Behörden der Strafverfolgung eine Hintertür im Fahrzeugsystem geben wird, um das Fahrzeug gezielt stoppen zu können. Fahrzeugverfolgungen und Geisterfahrten können beendet werden, bevor Unbeteiligte einen sachlichen oder körperlichen Schaden erleiden. [2]

5.3 Eingriff in die Verkehrssteuerung

Die Verkehrssteuerung ist bereits heute eines der am stärksten geschützten Systeme, da es auch ohne die weitere Vernetzung (V2X) bereits eine Leitzentrale für Ampelanlagen gibt, die von Hackern, Geheimdiensten anderer Länder und auch Terroristen angegriffen werden könnten. Möglich wäre durch die einheitliche Vernetzung eine noch größere Bedrohungslage, allerdings ist das Ausmaß durch die Manipulation der Verkehrssteuerung von so großer Bedeutung, dass auch Terroristen, Hacker und Geheimdienste solch einen Eingriff als äußerstes Ziel ansehen. Um in das heutige Verkehrssteuerungssystem eingreifen zu können, ist einschlägiges Fachwissen und ein hohes Maß an kriminellem Tatendrang notwendig, über dieses ein Hobbyhacker und auch Terroristen meist nicht verfügen. Die Folgen solch einer Bedrohung ist dementsprechend gering und nicht akut. [2]

6 Allgemeine Handlungsempfehlungen

Herausforderung ist die sichere Übertragung von Daten, so dass die Hacker keine Möglichkeit haben, sich in die Datenkommunikation einzumischen. Das sollen 802.11p-basierte Kommunikations-protokolle gewährleisten, welche auf bewährten Konzepten wie digitalen Zertifikaten basieren. [13]

Als allgemeine Handlungsempfehlung ist die Beauftragung vieler Hochschulen und Forschungszentren für eine international einheitliche Lösungsfindung zu nennen. Zum Beispiel arbeitet die Universität Paderborn zusammen mit der UCLA (Universität von Los Angeles, Kalifornien) und sie untersuchen die verschiedenen Aspekte der physischen Datenübertragung bis hin zur Gewährleistung bestimmter Servicequalitäts-Level. In der Pierre und Marie Curie Universität in Paris,

der Universität von Rio de Janeiro, der North Carolina State University beschäftigt man sich mit den virtualisierten Netzwerk-Schnittstellen, die mehr Sicherheit und Flexibilität in das System bringen können. Diese Ansätze können einige Lösungen für die IT- Sicherheit bei dem autonomen Fahren anbieten. [13]

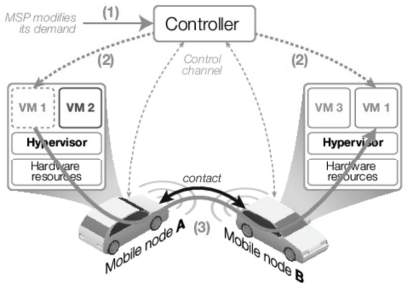

Abbildung 5:Virtualisierung der Netzwerkschnittstellen und Kommunikationsinstanzen bei Car-2-Car [13]

Wichtig für ein sicheres autonomes Fahrzeug, auf das sich der Fahrer bedingungslos verlassen kann, sind im Vorfeld auf staatlicher Ebene festgelegte Regeln, die länder- und herstellerübergreifend als Grundlage dienen. Je größer die Anzahl der Länder, die diese Grundlagen mit ausarbeiten und akzeptieren, ist, desto flexibler und problemloser kann ein sicheres autonomes Fahrzeug realisiert werden. Ein europaweiter Standard sollte zudem auf drei Aspekte hin ausgelegt werden.

1. Das dieser Standard von anderen Ländern außerhalb der EU akzeptiert wird und somit der erarbeitete Standard erweiterungsfreundlich ist.
2. Der Standard sollte verschiedene Kompatibilitätsmöglichkeiten mit anderen Standards bieten. So kann ein sicheres Fahrzeug auch außerhalb seines Ursprungsstandards sicher bleiben.
3. Eine Kompatibilität bzw. Vielfalt an Funktionen, ist wichtig, um ein System für Anwendungen vorzubereiten, die es heute noch nicht gibt.

Eine weitere Handlungsempfehlung ist eine gesetzliche Vorgabe zu Einhaltung der erarbeiteten internationalen Standards, die den Herstellern auferlegt werden. Diese Standards müssen den Herstellern auferlegt werden, um sie von Eigenentwicklungen in diesem Gebiet frühzeitig abzuhalten. Hersteller bestehen sonst auf ihre bereits geleisteten Investitionen und beharren auf ihr individuelles System. Dazu sollten die Hersteller untereinander eine Innovationskooperation vereinbaren, worin alle Hersteller miteinander die staatlich-auferlegten Standards entwickeln. Diese Standards sollten sich nicht nur auf einzelne Gebiete der IT-Sicherheit beschränken, sondern bei der Entwicklungssoftware ansetzen, Hardware und Kommunikationswege mit einbeziehen. So kann auch die Einhaltung der Standards übergreifend auf ihre Einhaltung kontrolliert werden. [13]

Das autonome Fahrzeug wird auf jeden Fall eingeführt und nur mit den Lösungsansätzen für Problemfelder der IT-Sicherheit wird das autonome Fahren vollständig funktionieren.

7 Literaturverzeichnis

[1] Richtlinien zur Förderung von Forschungsinitiativen auf dem Gebiet "IT-Sicherheit und Autonomes Fahren" 31.03.2016, abgerufen am 10.02.2017: https://www.bmbf.de/foerderungen/bekanntmachung-1182.html.

[2] Anforderungen an die digitale Infrastruktur für intelligente Mobilität, Arbeitsgruppe 8, Nationaler IT Gipfel, Hamburg 2014.

[3] AG8 High-Level-Auftrag, Anlage zum High-Level-Strategiepapier, IT-Gipfel, Hamburg 2014.

[4] Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, Markus Maurer, J. Christian Gerdes, Barbara Lenz, Hermann Winner, Daimler und Benz Stiftung, 2015.

[5] Fahrerassistenzsysteme (FAS) und Automatisierung im Fahrzeug – wird daraus eine Erfolgsgeschichte?, Wolfgang Fastenmeier, Psychologische Hochschule, Berlin 2015.

[6] Sicherheit zuerst – Möglichkeiten zur Erhöhung der Straßenverkehrssicherheit in Deutschland, Wissenschaftlicher Beirat beim Bundesminister für Verkehr, Bau und Stadtentwicklung.

[7] Few countries have road safety laws addressing all five key risk factors, 14.03.2013, abgerufen am 01.02.2017: http://www.who.int/mediacentre/news/releases/2013/road_safety_20130314/en

[8] Autonomes Fahren auf der Autobahn – Eine Potentialstudie für zukünftige Fahrerassistenzsysteme, Dipl.-Ing. Sebastian Rauch, M.Sc. Michael Aeberhard, Dipl.-Ing. Michael Ardelt, Dr.-Ing. Nico Kämpchen, BMW Group Forschung und Technik, München.

[9] Automatisiertes Fahren, Verband der Automobilindustrie, Innovation und Technik, 2016, abgerufen am 12.12.2016: https://www.vda.de/de/themen/innovation-und-technik/automatisiertes-fahren/automatisiertes-fahren.html.

[10] Zukunftsszenarien autonomer Fahrzeuge: Chancen und Risiken für Verkehrsunternehmen, Die Verkehrsunternehmen, Positionspapier, November 2015.

[11] Die Fahrzeugarchitektur des autonomen Fahren, Heise Developer, 13.12.2016, abgerufen am 04.01.2017: https://www.heise.de/developer/artikel/Die-Fahrzeugarchitektur-des-autonomen-Fahrens-3568991.html

[12] Kommunikation und Mobilität: Innovation durch vernetzte System, Alcatel-Lucent Stiftung für Kommunikationsforschung, 2008.

[13] Forschung fürs Autonome Fahren: so vernetzen sich Autos, Intelligente Welt, 15.11.2016, abgerufen am 15.01.2017: http://intelligente-welt.de/forschung-autonomes-fahren-vernetzte-autos/

[14] Gesetzentwurf für selbstfahrende Autos, Spiegel Online, 10.03.2017, abgerufen am 15.03.2017: http://www.spiegel.de/auto/aktuell/alexander-dobrindt-kritik-an-gesetzentwurf-fuer-selbstfahrende-autos-a-1138153.html

Der Einsatz von Perception Neuron bei schneller Bewegungsausführung

Tobias Fluck
Reutlingen University
Tobias.Fluck@Student.
Reutlingen-University.DE

Abstract

Mittlerweile ist der Einsatz von technischen Hilfsmitteln zu Analysezwecken im Sport fester Bestandteil im Trainingsalltag von Trainern und Athleten. In nahezu jeder Sportart werden Videoaufzeichnungen genutzt, um die Bewegungsausführung zu dokumentieren und zu analysieren. Allerdings reichen Aufnahmen von einem statischen Standort oftmals nicht mehr aus.

An dieser Stelle kann Virtual Reality (VR) eine Lösung dieses Problems bieten. Durch VR kann der aufgezeichneten Szene eine weitere Ebene hinzugefügt und die Bewegungsabläufe neu und detaillierter bewertet werden. Um Bewegungen in einer virtuellen Umgebung abzubilden, müssen diese mittels Motion Capturing (MoCap) aufgezeichnet werden.

Ziel dieser Arbeit ist es, herauszufinden, ob das MoCap System Perception Neuron in der Lage ist, Bewegungen in hoher Geschwindigkeit zu erfassen.

Betreuer Hochschule: Prof. Dr. Uwe Kloos
Hochschule Reutlingen
Uwe.Kloos@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

Schlüsselwörter

Motion Capturing, Motion Capturing System, Motion Capturing Suit, Perception Neuron, Sport, Track and Field, Sprint.

CR-Kategorien

I.4.8 [**Scene Analysis**]: Motion;
I.6.8 [**Types of Simulation**]: Animation;
I.2.10 [**Vision and Scene Understanding**]: Motion;

1 Einleitung

Für Trainer und Athleten ist der Einsatz von technischen Hilfsmitteln im Sport mittlerweile fester Bestandteil der Analyse-, Bewertungs- und Optimierungstechniken von Bewegungsabläufen.

Dabei spielt die Sportart, welche zum Gegenstand der Betrachtung gemacht wird, eine untergeordnete Rolle. Bei Mannschaftssportarten, wie beispielsweise Fußball oder Basketball, werden in erster Linie taktische Bestandteile des Spiels analysiert. Bei Individualsportarten, wie der Leichtathletik, steht hingegen die Analyse der individuellen technischen Ausführung der Bewegungsabläufe im Vordergrund. Allerdings reicht eine zweidimensionale Aufzeichnung aus einem statischen Betrachtungswinkel, wie es bei der Videoanalyse der Fall ist, oftmals nicht mehr aus, um eine tiefergehende Analyse der ausgeführten Bewegungen durchzuführen.

An dieser Stelle kann Virtual Reality (VR) eine Lösung für diese Problemstellung

darstellen. Mittels VR kann der Szene eine weitere Ebene hinzugefügt werden. Dadurch ist es möglich, die aufgezeichneten Bewegungsabläufe aus mehreren Perspektiven zu betrachten. Infolgedessen bieten sich Trainern und Athleten neue detailliertere Möglichkeiten der Bewegungsanalyse.

Um die Bewegungen in einer virtuellen Umgebung abbilden zu können, müssen diese vorab aufgezeichnet werden. Mittels Motion Capturing (MoCap) ist es möglich, reale Bewegungsabläufe eines Sportlers in ein dreidimensionales für Computer lesbares Format zu übertragen. Ziel dieser Arbeit ist es, den Nutzen des MoCap System Perception Neuron im Trainingsalltag von Leichtathleten zu evaluieren. Zudem soll diese Arbeit als Grundlage für weitere tiefergehende Arbeiten dienen.

In den folgenden Kapiteln wird zunächst die Problemstellung, sowie der Stand der Wissenschaft und die sich daraus ergebenen Lösungsansätze beschrieben. Des Weiteren wird die Methode, mit welcher das MoCap System evaluiert wird, dargestellt und abschließend die Ergebnisse der Untersuchungen diskutiert.

2 Problemstellung

Der Fortschritt in der Technik, sowie der Wissenschaft und die verbesserte Infrastruktur, ermöglichen sowohl bessere Trainingsbedingungen als auch bessere Trainingsmethoden, die zum Einsatz kommen, um die Leistungsentwicklung eines Sportlers weiter zu steigern.

Neue Erkenntnisse auf dem Gebiet der Medizin führen dazu, dass sich die Methoden der Trainings- und Regenerationssteuerung drastisch weiterentwickeln. Zudem führt der Ausbau der Infrastruktur zu verbesserten Trainingsbedingungen für Trainer und Sportler. Die Weiterentwicklung der Werkstoffe, welche in der Bekleidungsindustrie zum Einsatz kommen, können ebenfalls Einfluss auf die Leistung des Athleten haben. Leichtere und elastischere Materialien führen zu reduziertem Gewicht und steigender Bewegungsfreiheit beim Ausführen der Bewegungen.

Im Kontrast zu diesen Fortschritten stehen die Analysemethoden der sportlichen Leistung. Seit mehreren Jahrzehnten werden Videoanalysen verwendet, um Bewegungsabläufe eines Sportlers zu evaluieren. Im Trainings- und Wettkampfalltag von Trainern und Athleten werden klassische Videoanalysen eingesetzt. Die Videoaufnahmen werden zum einen genutzt, um die Korrekturen des Trainers zu überprüfen und ggf. eine tiefergehende Analyse zu ermöglichen. Zum anderen wird dem Athleten eine visuelle Darstellung der fehlerhaften Ausführung ermöglicht. Dabei ergeben sich bei dieser Vorgehensweise einige Nachteile. Beispielsweise gehen bei zweidimensionalen Aufnahmen Tiefeninformationen verloren. Dadurch ist es möglich, dass Arme, Beine oder andere Körperteile in der Szene verdeckt werden und dadurch wichtige technische Bestandteile der Bewegungsabläufe verloren gehen. Darüber hinaus werden die Beobachtungen von einem statischen Betrachtungswinkel aus aufgezeichnet, was zur Folge hat, dass die Aufnahmen Bewegungsabläufe falsch oder anders darstellen als sie ursprünglich ausgeführt werden.

Neben der herkömmlichen Videoanalyse werden auch biomechanische Analysen mit Hilfe von markerbasierten optischen Trackingverfahren durchgeführt. Dazu werden reflektierende Marker an allen wichtigen Gelenkpunkten des Körpers angebracht. Um die Bewegungen aufzuzeichnen, werden Infrarotkameras genutzt, die während der Ausführung der Bewegungen Infrarotblitze abgeben und das von den Markern reflektierende Licht aufzeichnen. Diese Systeme sind jedoch zum einen sehr kosten- und zum anderen sehr zeitintensiv zu nutzen. Die Kosten belaufen sich auf hohe fünf- bis sechsstellige Summen. Zudem müssen viele Marker für ein optimales Ergebnis angebracht werden, was wiederrum zu einem hohen Zeitaufwand führt. Deshalb werden diese Systeme hauptsächlich in wissenschaftlichen Arbeiten für tiefergehende

Analysen, welche über die Anwendung im Trainings- und Wettkampfalltag hinausgehen, verwendet.

3 Stand der Wissenschaft

Erst in den letzten Jahren können auf dem Gebiet der Analysemethoden signifikante Fortschritte verzeichnet werden. In der Wissenschaft finden sich daher vor allem Arbeiten aus den letzten Jahren, die sich mit dieser Thematik beschäftigen. Dort wird bereits erkannt, dass die Videoanalyse, wie sie heute eingesetzt wird, einige Nachteile aufweist und ein großes Verbesserungspotential in diesem Bereich besteht.

Bideau et. al. beschreiben in [1] die Limitierungen, welche sich durch den Einsatz von Videoaufzeichnungen bei der Analyse ergeben. Der Verlust von Tiefeninformationen wird als ein großer Nachteil angesehen. Als weiteren Vorteil von VR nennen sie die Möglichkeit, in der virtuellen Umgebung zu interagieren. Zudem heben sie die Option hervor, den Betrachtungswinkel in VR zu verändern. Diese Thesen belegen sie am Beispiel von zwei Studien. Vignais et. al. untersuchen in [2] die unterschiedlichen Leistungen von Handballtorhütern mit unterschiedlichen Trainingsmethoden. Hierbei wird ein direkter Vergleich zwischen der Videoanalyse und VR durchgeführt, in dem eine Testgruppe mit Videoaufzeichnungen und eine Gruppe mit virtuellen Umgebungen trainiert. Durch die Untersuchungen kommen die Autoren zum Ergebnis, dass die Probanden, welche mit dem VR System trainieren, signifikant bessere Leistungen aufweisen, als die Probanden, welche mit Videoanalysen trainieren. In [4] beschreiben Brault et. al. eine Versuchsreihe, in der überprüft wird, ob Experten, Täuschungsversuche in den Laufwegen von Rugbyspielern besser und schneller erkennen als Anfänger. Dabei kommen sie zum Ergebnis, dass die Experten signifikant schneller und präziser die endgültige Richtung vorhersagen als Anfänger.

In [5] untersucht Wang die Einsatzgebiete von VR im Sport. Zu den Einsatzgebieten zählt Wang unter anderem verschiedene Trainingszustände, die simuliert werden können. Dabei hebt er explizit die Einstellbarkeit der Intensität der Trainingseinheit hervor. Durch das Hinzufügen von virtuellen Gegnern in der Szene, sieht Wang entscheidende Vorteile der kontrollierten Trainingssteuerung.

Pan beschreibt in [6] die Auswirkungen des Einsatzes von VR im Universitätssport. Dabei geht er auf grundlegende Aspekte, wie das selbstständige Lernen von Bewegungsabläufen bei Studenten ohne Lehrkraft ein und ordnet dieser Methode einen weiteren Vorteil von VR zu.

Kulpa et. al. gehen in [7] auf die generellen Vorteile von VR im Sport ein. Dabei beschreiben sie die virtuelle Szene als kontrollierte Umgebung, welche in der Lage ist, Risiken des Trainings, wie beispielsweise das Verletzungsrisiko zu minimieren. Zudem beschreiben sie Kriterien zur Auswahl für ein Tracking System, mit dem die Bewegungen aufgezeichnet werden. Hierzu zählen sie das Maß an Genauigkeit und an Interaktion, welche durch das Trackingsystem die virtuelle Umgebung interaktiv machen.

Liwei beschreibt in [8] die Vorteile von VR. Besonders hebt er dabei hervor, dass durch VR der Szene eine weitere Ebene hinzugefügt werden kann und dadurch eine tiefergehende Analyse der Bewegungsabläufe möglich ist. Des Weiteren beschreibt er, dass mit Hilfe von VR Schwächen von Athleten besser aufgedeckt werden können.

In [9] untersucht Liao den Stand der Wissenschaft von VR im Sport sowie deren Einsatzgebiete. Dazu unterteilt Liao die Einsatzgebiete in vier unterschiedliche Kategorien. Hierzu zählt der Einsatz von VR im Wettkampfsport, in der Rehabilitation nach Verletzungen, in bekannte Sportarten, sowie in die physische Erziehung, den Schul- und Universitätssport. Zusätzlich ordnet er VR einzigartige Charakteristika zu, welche Videoaufzeichnungen nicht aufweisen. Dabei nennt er die Interaktion,

die Immersion und die Multisensorik als wichtigste Eigenschaften von VR.

4 Lösungsansätze

Aus der vorherig beschriebenen Problemstellung ergeben sich generelle Anforderungen (im Folgenden nummeriert) an Tracking Systeme für VR Anwendungen. Dabei lassen sich zwei grundlegende Aspekte ableiten. Das System sollte nach Möglichkeit mit *(i) wenig Kosten* verbunden sein, um mit der herkömmlichen Videoanalyse konkurrieren zu können. Des Weiteren sollte der Aufbau des Systems einen *(ii) geringen zeitlichen Aufwand* beanspruchen. Weitere Anforderungen können aus dem Stand der Wissenschaft abgeleitet werden. Aus der Arbeit [7] von Kulpa et. al. geht hervor, dass bei der Auswahl des Trackingsystems zwischen der *(iii) Genauigkeit* des Trackingsystems und dem *(iv) Maß der Interaktion*, welches während der Laufzeit genutzt wird, um das System interaktiv zu gestalten, unterschieden wird.

Für das Ziel der Arbeit lässt sich festhalten, dass für die Analyse von Bewegungsabläufen keine Interaktion notwendig ist. Daher kann die Anforderung (iv) für den Zweck dieser Arbeit vernachlässigt werden. Allerdings sollte das System eine hohe Präzision bei der Aufnahme der Bewegungen aufweisen. Dadurch kann gewährleistet werden, dass die Vorteile von VR gegenüber der Videoanalyse wirklich genutzt werden können.

4.1 Perception Neuron

Mit dem MoCap Anzug Perception Neuron liegt der Arbeit ein passendes System zu Grunde, welches Anforderung (i) erfüllt. Mit einem Gesamtpreis im niedrigen vierstelligen Bereich, ist das System in Betrachtung des Marktes in einem erschwinglichen Bereich. Zudem besteht Perception Neuron aus 15 Einzelteilen, die mit Kabelverbindungen miteinander verbunden werden. Dadurch lässt sich ableiten, dass die Anbringung des Systems am Körper in einem überschaubaren zeitlichen Rahmen (ii) bleibt. Dies wird während der Versuche bestätigt werden, um dessen Alltagstauglichkeit nachzuweisen. Jedoch gibt es bisher keine Angaben, mit welcher (iii) Genauigkeit und Zuverlässigkeit der Anzug bei frequenter Bewegungsausführung die Bewegungen aufzeichnet. Dies soll ebenfalls während der Versuche evaluiert werden.

4.1.1 Funktionsweise

Der Anzug besteht aus insgesamt 15 Einzelteilen. Dazu gehört ein Hub, welcher für die Verbindung mit dem Computer bzw. im kabellosen Modus mit dem WLAN Router zuständig ist. Des Weiteren wird ein Akku für den kabellosen Modus benötigt. Zusätzlich wird ein Verbindungskabel zwischen Akku und Hub benötigt, um die Stromversorgung des Anzugs bzw. der einzelnen Module sicherzustellen. Die Module bestehen aus einer Verbindungseinheit auf der die so genannten Neurons befestigt werden. Am Körper selbst werden diese mit Hilfe von elastischen Klettverschlüssen festgemacht.

Die Neurons messen in der Länge und Breite je 12mm und in der Höhe 6mm. Im Inneren des Sensors gibt es drei Hauptkomponenten, den 9-Achsen Sensor, bestehend aus einem 3-Achsen Gyroskop von +/- 2000dps, 3-Achsen Beschleunigungsmesser von +/- 16g, einem 3 Achsen Magnetometer sowie Onboard Kalibrierung und Kalkulation. Des Weiteren wird die Koordinatentransformation mit Eulerschen Winkeln durchgeführt.[10]

Der Anzug kann in unterschiedlichen Modi betrieben werden. Bei dem kleinsten Betriebsmodus werden Neurons lediglich an Ober-, Unterarm und an der Hand benötigt. Der Ganzkörpermodus ist der größte Aufbau des Systems. Dabei werden Sensoren an allen wichtigen Körperstellen angebracht, inklusive der Fingergelenke. Für die der Arbeit zu Grunde liegenden Untersuchungen, wird der Ganzkörpermodus verwendet. Allerdings werden hierbei die Finger vernachlässigt und lediglich die gesamte Hand, repräsentativ für alle Finger genutzt.

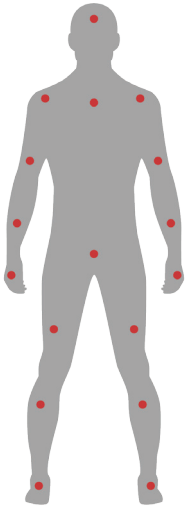

Abbildung 1:
Verteilung der Sensoren am Körper
(eigene Darstellung nach [10])

In Abbildung 1 ist die Verteilung der Sensoren am menschlichen Körper zu sehen. In der Abbildung wird allerdings nicht unterschieden, ob die Sensoren sich vorn oder hinten am Körper befinden, dies ist folgender Beschreibung zu entnehmen. Am Hinterkopf wird der erste Sensor befestigt. Zusätzlich folgen Sensoren am Rücken, den Schultern, den Ober- und Unterarmen, dem Handgelenk, dem Handrücken sowie den Ober- und Unterschenkeln und den Füßen.

5 Methode

Um die Nutzbarkeit von Perception Neuron im Trainingsalltag von Leichtathleten, im speziellen Fall von Sprintern nachzuweisen, wird eine Studie mit insgesamt zehn Probanden durchgeführt. Dabei soll herausgefunden werden, ob die Bewegungsabläufe des Probanden durch das Tragen des Anzugs eingeschränkt werden. Die Studie wird am Olympia Stützpunkt in Stuttgart der Molly Schaufele Halle durchgeführt. Dort besteht die Möglichkeit Strecken in 10m Abschnitte zu unterteilen und Zwischenzeiten zu stoppen.

Die Studie wird mit insgesamt zehn Athleten durchgeführt je fünf weiblichen und fünf männlichen Probanden. Die Teilnehmer lassen sich dabei in vier Altersklassen unterteilen, U16, U18, U20 und die Aktiven. Bei den Probanden handelt es sich um Athleten, welche mindestens schon auf Landesebene Wettkämpfe bestritten haben und mehr als die Hälfte schon an nationalen und internationalen Wettkämpfen teilgenommen hat.

Im Rahmen der Studie werden zwei Strecken mit unterschiedlichen Ausführungen gelaufen. Zum einen werden 10m aus dem Hochstart absolviert, das bedeutet, dass der Proband eine ruhende Position zu Beginn der Strecke einnimmt und komplett ohne jegliche Vorbeschleunigung die Strecke absolviert. Der Hochstart ist vergleichbar mit einem Tiefstart, allerdings mit dem Unterschied, dass der Tiefstart mit den Armen bzw. Händen am Boden gestartet wird. Beim Hochstart hingegen, werden die Hände komplett in der Luft gehalten. Zum anderen 10m fliegend mit 10m Anlauf bzw. 20m in der Gesamtlänge, das bedeutet, dass der Proband eine Beschleunigungsphase von 10m hat und im Anschluss 10m fliegend mit maximaler Geschwindigkeit durchläuft. Durch die Beschleunigungsphase können größere Geschwindigkeiten erreicht werden. Dadurch wird gewährleistet, dass überprüft wird, ob der Anzug auch größeren Geschwindigkeiten, welche im Trainingsalltag von Sprintern üblich sind, aushält.

Für den Umfang der Studie werden zwei Testtage benötigt. Dadurch kann garantiert werden, dass die Probanden beide Strecken mit größtmöglicher Intensität bestreiten können und die Ergebnisse nicht verfälscht werden. Zudem dient der erste Tag der Versuche der Gewöhnung der Probanden an den Anzug.

5.1 Bewertungskriterien

Bevor die Studie durchgeführt wird, müssen einheitliche Bewertungskriterien geschaffen werden, um eine Grundlage für eine abschließende Betrachtung zu ermöglichen.

Hierbei werden zwei verschiedene Kategorien von Bewertungen unterschieden.

5.1.1 Technische Bewertungskriterien

Bei den technischen Bewertungskriterien handelt es sich um alle Eckpunkte, die sich auf die Qualität der erzeugten Daten beziehen. Des Weiteren werden trainingsrelevante Aspekte wie beispielsweise die korrekte Darstellung der Bewegungsausführung im Vergleich zum Original genutzt.

In der nachfolgenden Aufzählung werden die technischen Bewertungskriterien definiert. Der (a) Aufbau des Systems wird hierbei betrachtet. Damit ist gemeint, wie Lange es dauert, das System aufzubauen und zu konfigurieren. Des Weiteren soll die (b) Robustheit des Anzuges dokumentiert werden. Dabei werden Aspekte betrachtet, wie schnell sich beispielsweise die Verbindungen zwischen den Sensoren lösen oder ob Sensoren bei höherer Bewegungsgeschwindigkeit ausfallen. Die (c) Laufzeit des Akkus ist ein Bewertungskriterium, welches sich nur indirekt auf den Anzug bezieht, aber dennoch überprüft werden sollte. Darüber hinaus wird die (d) Reichweite des Anzuges bewertet. Diese beschreibt, wie realitätsnah die Bewegungen wiedergegeben werden können, ohne dass die Verbindung zwischen Hub und WLAN Router unterbrochen wird, wobei diese Anforderungen ähnlich wie beim Akku vom WLAN Router beeinflusst werden kann. Die (e) Qualität der Daten kann erst nach Beendigung der Testreihe überprüft werden und bezieht sich daher eher auf die Funktionsweise des Anzugs. Die (f) realitätsnahe Bewegungsdarstellung stellt ebenfalls ein Kriterium dar, welches bei der Nachbereitung überprüft werden kann. Das Verhalten des Anzugs (g) bei unterschiedlichen Geschwindigkeiten, bezieht sich auf die Hardware, welche der Proband am Körper trägt und zum anderen auf die aufgezeichneten Daten, die am Ende der Aufzeichnung zur Bewertung herangezogen werden.

Diese Kriterien werden durch die Dokumentation der Versuche, die in Protokollen festgehalten werden und durch die Nachbereitung überprüft.

5.1.2 Menschliche Bewertungskriterien

Neben den technischen sind auch die menschlichen Bewertungskriterien von entscheidender Bedeutung. Die individuelle subjektive Einschätzung des Probanden hat unmittelbaren Einfluss auf die Leistungsfähigkeit. Deshalb umfassen diese Kriterien alle Punkte, die sich in Verbindung zwischen dem Probanden und dem Anzug ergeben.

Die (h) Passform und Passgenauigkeit beziehen sich auf den Tragekomfort des Anzugs am Körper des Probanden. Dabei werden nahezu alle Körperstaturen durch die Probanden abgedeckt. Als weiteres Kriterium zählt die (j) Bewegungsfreiheit. Dadurch ist es möglich, zu erfahren, ob die Ausführung der Bewegungen des Probanden durch das Tragen eingeschränkt wird. Zusätzlich zählt die (k) subjektive Einschätzung des Gewichts sowie (l) das Gewicht des Akkus zu den grundlegenden Bewertungskriterien. Darüber Hinaus zählt auch die (m) Größe des Akkus zu den Aspekten, die von den Probanden eingeschätzt werden soll.

5.2 Der Fragebogen

Bei dem Fragebogen handelt es sich um einen insgesamt schlanken Fragebogen, welcher sich aus den in 5.1.2 gesammelten Kriterien zur individuellen subjektiven Einschätzung des Probanden zusammensetzt. Mit Hilfe dieser Einschätzung kann herausgefunden werden, ob diese Beurteilung Einfluss auf die Leistung des Probanden hat.

Die Fragen im Fragebogen beinhalten Folgendes:

1. Passform: Anzug war zu eng oder zu weit? (Abstufung in zu eng,

eng, weder noch, weit und zu weit)

2. Haftung der Marker: Sind die Marker gerutscht? (Abstufung in nein, wenig, stark und sehr stark)
3. Gewicht des Anzugs: War der Anzug leicht genug? (Abstufung in stimme voll zu, stimme eher zu, weder noch, stimme weniger zu, stimme gar nicht zu)
4. Gewicht des Akkus: War der Akku leicht genug? (Abstufung in stimme voll zu, stimme eher zu, weder noch, stimme weniger zu, stimme gar nicht zu)
5. Größe des Akkus: War der Akku klein genug? (Abstufung in stimme voll zu, stimme eher zu, weder noch, stimme weniger zu, stimme gar nicht zu)
6. Bewegungsfreiheit: War die Ausführung der Bewegung problemlos möglich? (Abstufung in stimme voll zu, stimme eher zu, weder noch, stimme weniger zu, stimme gar nicht zu)

5.3 Der Versuchsaufbau

Die einzelnen Versuche werden mit insgesamt zwei Computern durchgeführt. Ein Computer dient zur allgemeinen Dokumentation. Dort werden die gelaufenen Zeiten notiert und Protokoll geführt. Das Protokoll beinhaltet Probleme oder sonstige Anmerkungen, welche bei der abschließenden Bewertung herangezogen werden können. Auf dem zweiten Computer werden die Bewegungsdaten von Perception Neuron mit Hilfe der AXIS Software von NOITOM aufgezeichnet. Dazu kommt eine Kamera, damit die digitalen Bewegungsdaten mit den Videoaufzeichnungen verglichen und bewertet werden können. Zusätzlich wird der Computer auf dem die Bewegungen aufgezeichnet werden, mit einem WLAN Router verbunden, damit die Bewegungsfreiheit des Probanden nicht eingeschränkt wird. Die Verbindung zwischen Computer und Anzug wird mittels des Hubs, der selbst mit dem Akku verbunden ist, hergestellt.

6 Ergebnisse

Die Ergebnisse der Untersuchungen können grob in zwei Kategorien unterteilt werden. In einem ersten Schritt wird überprüft, ob das Tragen des Anzuges unmittelbare Auswirkung auf die allgemeine Leistungsfähigkeit des Probanden hat. Damit ist gemeint, ob der Proband mit dem Anzug an Leistungsfähigkeit verliert und die Strecken dann in einer langsameren Zeit zurücklegt als zuvor, ohne den Anzug am Körper.

6.1 Hochstart

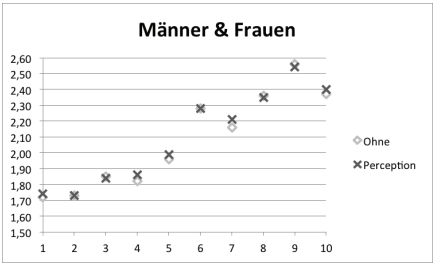

Abbildung 2: Sprintzeiten (Hochstart)

Anhand der gestoppten Zeiten, welche mit und ohne den Anzug gelaufen werden, ist zu erkennen, dass die vermeintliche Einschränkung, welche sich durch das Tragen des Anzuges ergibt, individuell abhängig ist. Bei den Männern lagen die durchschnittlichen Zeiten bei 1,816 ohne den Anzug bzw. 1,832 Sekunden mit dem Anzug. Was wiederrum eine durchschnittliche Differenz von 0,016 Sekunden bedeutet. Des Weiteren war bei der Auswertung der Daten zu beobachten, dass ein Proband sogar mit Anzug schneller war als ohne den Anzug. Bei den Frauen beträgt die durchschnittliche Laufdauer 2,346 Sekunden ohne den Anzug und bei 2,356 Sekunden mit dem Anzug dabei liegt die durchschnittliche Differenz bei 0,010 Sekunden, wobei zwei Probanden mit Anzug schneller waren als ohne. Die Daten sind aus Abbildung 2 zu entnehmen.

6.2 Fliegende Sprints

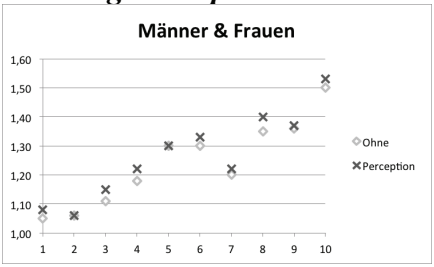

Abbildung 3: Sprintzeiten (Fliegend)

Am zweiten Testtag wurde eine Strecke von 10 Metern fliegend mit 10 Metern Anlauf gelaufen. Bei den Männern lagen die durchschnittlichen Zeiten bei 1,140 Sekunden ohne bzw. 1,162 Sekunden mit Anzug. Was eine durchschnittliche Differenz von 0,022 Sekunden bedeutet. Bei den Frauen liegen die durchschnittlichen Zeiten bei 1,342 bzw. bei 1,370 Sekunden was wiederrum eine durchschnittliche Abweichung von 0,028 Sekunden bedeutet. Auffällig war hier, dass kein Proband mit Anzug schneller läuft als ohne Anzug.

Die Zeit, welche benötigt wird, bis der erste Athlet läuft, beschränkt sich auf 20 Minuten. Die durchschnittliche Zeit für das Anlegen des Anzugs beträgt am ersten Tag 3:53 Minuten und am zweiten Tag 3:45 Minuten.

Die Akkulaufzeit (c) war während beiden Tagen ohne Probleme nutzbar ohne zwischenzeitliches Aufladen. Die Reichweite (d) des Anzuges hat für den Umfang der Versuchsstrecken vollkommen ausgereicht.

Bei insgesamt vier der 20 Sprints wurde die Verbindung entweder zwischen den Neuronen oder zwischen dem Anzug und des Akkus unterbrochen (b), so dass an dieser Stelle unvollständige Daten vorhanden waren. Bei sechs der 20 Sprints wurden die Bewegungen aufgrund des Ausfalls eines Neuronen nicht vollständig aufgezeichnet.

6.3 Fragebogen

Die Ergebnisse des Fragebogens lassen sich wie folgt aufteilen:

Bei der Passform (h) antwortete ein Proband mit der Antwort zu eng, zwei Probanden mit der Antwortmöglichkeit weder noch sowie drei mit der Möglichkeit eng und vier mit der Antwort weit. Bei insgesamt sechs Probanden sind die Marker gerutscht, bei drei Probanden wenig und bei einem Proband stark. Bei der Frage, ob der Anzug leicht genug war (k), antworteten acht Probanden mit der Antwort stimme voll zu, und zwei Probanden mit der Antwortmöglichkeit stimme eher zu. Die Frage, ob der Akku leicht genug war (l), beantworteten die Probanden mit sieben Mal stimme weniger zu und drei Mal mit stimme gar nicht zu. Bei der Frage, ob der Akku klein (m) genug war, stimmten jeweils fünf der Probanden mit stimme gar nicht zu oder stimme weniger zu. Die Frage, ob die Bewegungsausführung (j) problemlos möglich war wird mit neun Mal stimme voll zu und mit einmal stimme eher zu beantwortet und Einschränkungen gab es keine.

6.4 Qualität der Daten

Die Qualität der Daten (e) wird mittels den während der Aufzeichnung aufgenommenen Video und der MoCap Daten durchgeführt.

Abbildung 4: Gegenüberstellung Video und MoCap Daten (Seitenansicht)

Von der seitlichen Betrachtung der Aufnahmen in Abbildung 4 ist kein erheblicher Unterschied zu erkennen. Lediglich an Gelenkpunkten, wie den Fußgelenken oder Handgelenken, an denen sich nicht so viele Sensoren befinden, kann ein minimaler Unterschied beobachtet werden. Dennoch erscheinen die Bewegungen realitätsnah (f). Ähnlich verhält sich das bei der Ansicht von hinten siehe Abbildung 5.

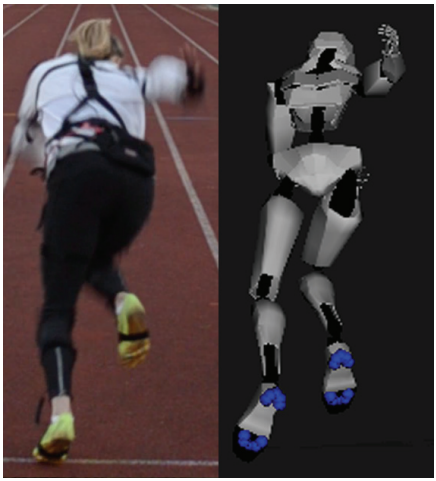

Abbildung 5: Gegenüberstellung Video und MoCap Daten (Hinteransicht)

7 Diskussion

Nachdem die Methode und die Ergebnisse in den beiden vorangegangen Kapiteln dargestellt werden, beschäftigt sich dieses Kapitel mit der Einordnung der während der Studie dokumentierten Ergebnisse.

Die (a) Vorbereitungszeit für den Versuch liegt mit 20 Minuten in einer akzeptablen Zeit. Das bedeutet, dass der Trainer während sich die Athleten erwärmen, problemlos das System aufbauen könnte und es schnell zur Verfügung steht.

Bei der durchschnittlichen Zeit, um den Anzug anzulegen, ist derweil ein Fortschritt von gut acht Sekunden zu erkennen, was bedeutet, dass der Anzug bei jeder Verwendung weniger fremd wirkt und damit schneller angelegt werden kann. Generell ist festzuhalten, dass beide Geschlechter bei der Ausführung nur wenig bis gar nicht beeinträchtigt werden. Lediglich die Größe des Akkus wird bemängelt.

Die Abweichung zwischen den gemessenen Zeiten mit und ohne Perception Neuron belaufen sich bei der 10 Meter Distanz aus dem Hochstart auf ein durchschnittliches Maximum aller Probanden von 0,016 Sekunden und ist daher nahezu vernachlässigbar. Bei den fliegenden Sprints, wird eine Differenz von 0,025 Sekunden gemessen. Die Differenz der beiden Mittelwerte ist relativ einfach zu erklären, bei höheren Geschwindigkeiten (g) besteht ein größeres Fehlerpotential und dadurch ist es möglich, dass selbst eine unbemerkt anders ausgeführte Bewegung zu langsameren Zeiten führt. Allerdings sind die Differenzen zwischen den Zeiten mit und ohne den MoCap Anzug fast zu vernachlässigen. Da eine Streuung von +/- 5/100 Sekunden bei einem Sprint vollkommen der Normalität entspricht.

Dass sich die Verbindungen zwischen den Neuronen lösen (b), konnte erwartet werden, dass sich die Verbindungen allerdings in nur vier der 20 Fälle lösen stellt ein zufriedenstellendes Ergebnis dar.

Die Qualität der Daten (e) lässt sich durch den Vergleich von Video und MoCap feststellen. Dabei ist zu beobachten, dass trotz der Anbringung der Sensoren an wenigen Gelenken die Aufnahmen eine hohe Qualität aufweisen und die Bewegungen realitätsnah aufgezeichnet werden (f), wie aus den Abbildungen 4 und 5 zu entnehmen ist. Die Aufnahmen müssen lediglich nachbearbeitet werden, wenn die Kalibrierung fehlschlägt. Dies kann aber mit mehrfacher Wiederholung der Kalibrierung reduziert werden.

8 Abschlussbetrachtung

Abschließend bleibt festzuhalten, dass der Anzug zur Leistungsanalyse und -bewertung von Sprintern eingesetzt werden kann. Die Differenzen von lediglich wenigen hundertstel Sekunden zwischen den Zeiten, welche mit und welche ohne den Anzug gelaufen werden, sind anhand von Erfahrungswerten zu vernachlässigen.

Allerdings müssen die Bewegungen an manchen Stellen, vor allem dann, wenn die Kalibrierung nicht erfolgreich war, nachgebessert werden. Dies stellt aber nur einen kleinen Nachteil dar, welcher sich bei der Aufzeichnung und Nachbereitung der Daten ergibt.

9 Literatur

[1] Bideau B., Kulpa R., Vignais N., Brault S., Multon F., Craig C. 2010. Using Virtual Reality to Analyze Sports Performance. University of Rennes 2, France. IEEE Computing Graphics Applications. 14-21 (Mar, 2010). DOI=http://ieeexplore.ieee.org/document/5339124/?reload=true.

[2] Vignais, N., Kulpa, R., Brault S., Presse D. 2014. Which technology to investigate visual perception in sport: Video vs. virtual reality. *M2S Laboratory, UFR APS, Rennes 2-ENS Cachan University.* Human Movement Science, 12-26 (Nov, 2014). DOI=http://www.sciencedirect.com/science/article/pii/S0167945714001833.

[3] Bideau B., Multon F., Kulpa R., Fradet, L., Arnaldi, B., Delamarche, P. 2004. Using virtual reality to analyze links between handball thrower kinematics and goalkeeper's reactions. Universit´e de Rennes 2. Neuroscience Letters (Nov, 2004). DOI= http://dx.doi.org/10.1016/j.neulet.2004.09.023

[4] Brault, S., Bideau, B., Kulpa, R., Craig, C. 2012. Detecting Deception in Movement: The Case of the Side-Step in Rugby. University of Rennes 2, Rennes, France, Queens University of Belfast, Belfast, United Kingdom. PLoS one. DOI= http://dx.doi.org/10.1371/journal.pone.0037494

[5] Wang, J. 2012. Research on Application of Virtual Reality Technology in Competitive Sports. Physical Education College of Zhengzhou University. I-WIEE, Procedia Engineering 29, 3659-3662 (Dez, 2012). DOI=http://www.sciencedirect.com/science/article/pii/S1877705812005589.

[6] Pan, H. 2015. Research on Application of Computer Virtual Reality Technology in College Sports Training. Jingdezhen Univ., China. 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation. (Jun, 2015). DOI= http://ieeexplore.ieee.org/document/7263701/.

[7] Kulpa, R., Multon, F., Argelaguet, F. Virtual Reality & Sport. University of Rennes 2, France. 33rd International Conference on Biomechanics in Sports, Poitiers, France. (Jun, 2015). DOI= https://ojs.ub.uni-konstanz.de/cpa/article/view/6694.

[8] Liwei, L. 2012. Applications of Computer Virtual Reality Technology in Modern Sports. Dept. of Phys. Educ., Harbin Univ. of Sci. & Technol., Harbin, China. 2012 Fourth International Symposium on Information Science and Engineering, (Dec, 2012). DOI= http://ieeexplore.ieee.org/document/6495364/.

[9] Liao, T. 2015. Application of Virtual Reality Technology to Sports. Sports training Dept., Wuhan Sports University, Wuhan 430079, China. DOI=http://www.atlantis-press.com/php/download_paper.php?id=23007.

[10] NOITOM. Kickstarter Campain 2014. DOI=https://www.kickstarter.com/projects/1663270989/project-perception-neuron?lang=de

Inwiefern werden IT-Risiken durch ein Risikomanagement reduziert?

Gamze Gök
Reutlingen University
Gamze.goek@Student.
Reutlingen-University.DE

Abstract
Im Rahmen der wissenschaftlichen Vertiefung soll auf Basis der vorhandenen Ansätze das IT-Risikomanagement evaluiert werden. Hierbei soll die Frage, inwiefern das IT-Risikomanagement dem Unternehmen eine Hilfestellung bieten kann, geklärt und anschließend anhand von zwei Fallbeispielen dargestellt werden.

Schlüsselwörter
Risikomanagement, IT-Risiken

CR-Kategorien
H. [Information Systems], H.1 [Models and Principles]: Human information processing, H.1.1 [Systems and Informatics Theory]: Information theory, H.4.1 [Office Automation]: Workflow management, K.6 [Management of Computing and Information Systems], K.6.m [Miscellaneous]: Security.

1 Einleitung
IT-Systeme bilden immer mehr die Grundlage für neue Geschäftsmodelle, was bedeutet, dass ohne IT vieles nicht mehr funktionieren würde. Die Abhängigkeit von der IT steigt. Je komplexer die IT-Systeme, desto größer werden die Risiken, die aus dem Einsatz von Computersystemen und Netzwerken, Software und Datenspeichern erwachsen. Aus diesem Grund ist es umso wichtiger, sich mit dem IT-Risikomanagement auseinanderzusetzen, da es die Unternehmensleitung dabei unterstützt, einen Überblick über bestehende Risikosituationen zu gewinnen, die Steuerung der kritischen Risiken transparent zu machen und belastbare Aussagen zu Risiken und Risikomanagement zu treffen [1].

Die Abbildung 1 zeigt eine Auswertung des deutschen Online Portals für Statistik, wie viel Prozent im Schnitt aller Unternehmen je nach Betriebsgröße Computer nutzen. Es lässt sich darüber hinaus ableiten: je größer ein Unternehmen ist, desto unerlässlicher scheint die Nutzung von Computern.

Anteil der Unternehmen mit Computernutzung nach Betriebsgröße in Deutschland 2016	
250 Beschäftigte und mehr	100%
50-249 Beschäftigte	99%
10-49 Beschäftigte	98%
1-9 Beschäftigte	90%
Gesamt	91%

Abbildung 1: Anteil der Unternehmen mit Computernutzung nach Betriebsgröße in Deutschland im Jahr 2016 [2]

Betreuer Hochschule: Prof. Dr. – Ing. Michael Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1.1 Motivation

Prozesse im Unternehmen werden durch viele Techniken unterstützt. Damit die Informationstechnik erfolgreich funktioniert, ist die Sicherheit der eingesetzten Systeme wichtig. Durch die Einführung des IT-Risikomanagements werden sowohl wirtschaftliche Aspekte als auch Sicherheitsaspekte beachtet. Unternehmen sind abhängig von Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit der eingesetzten Systeme.

1.2 Zielsetzung

Anhand von vorhandenen Ansätzen soll untersucht werden, inwiefern das IT-Risikomanagement eine Hilfestellung für Risikosituationen bieten kann. Wesentliche Punkte des Risikomanagementprozesses sollen beschrieben und analysiert werden. Hierbei wird geklärt, welchen Stellenwert die IT-Risiken im unternehmensweiten Risikomanagementprozess einnehmen.

2 Grundlagen

In diesem Kapitel wird der Begriff Risiko definiert und ein Überblick über die Schutzziele innerhalb des Risikomanagements gegeben.

2.1 Der Risikobegriff

Primär versteht man unter dem Begriff "Risiko" eine negative Abweichung vom erwarteten Zielzustand. Bei IT-Risiken geht es um Verlustereignisse. Hier wird das Risiko als negative Abweichung vom Erwartungswert aufgefasst. Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance) [7]. Das Risikomanagement ist der geplante Umgang mit Risiken in einem Projekt. Es ist eine Funktion der Unternehmensführung und beschäftigt sich damit, noch nicht eingetretene Probleme möglichst zu eliminieren. Das Risikomanagement beinhaltet die aufbau- sowie ablauforganisatorischen und technischen Richtlinien in Bezug auf den Umgang mit Risiken und darüber hinaus klare Kompetenzstrukturen [3].

2.2 Schutzziele

Schutzziele spiegeln den erwünschten Zustand von zu schützenden Objekten (z.B. IT-Anwendung) wieder. IT-Risiken entstehen dann, wenn die Schutzziele verletzt und somit nicht durchgesetzt werden können. Diese sind:

Vertraulichkeit:
Informationen werden vor unberechtigter Kenntnisnahme geschützt. Das System muss so aufgebaut sein, dass ein Zugriff nur für befugte Personen oder Dienste möglich ist [6].

Integrität:
Informationen, Systeme und Netzte können nicht unbemerkt verändert werden. Fälschungen von Nachrichteninhalten sowie des Absenders sollen erkannt werden [6].

Verfügbarkeit:
Informationen, Systeme und Netze müssen verfügbar sein. Das Kommunikationsnetz soll die Kommunikation zwischen allen Partnern ermöglichen, die das wünschen und denen es nicht verboten ist [6].

3 Risikoidentifikation

Der Risikomanagementprozess der ISO/IEC 27005 beginnt mit der Festlegung der Rahmenbedingungen, die sich z.B. auf den Geltungsbereich, die Vorgehensweise beim Risikomanagement und die grundlegenden Kriterien bei der Risikoevaluation beziehen [4]. Hier erfolgt eine Bestandsaufnahme, in der alle möglichen Risiken für ein Projekt aufgedeckt werden. Es entsteht eine Risikoliste, welche eine Kurzbeschreibung, Daten zur Risikoart und Angaben zu Ursachen des Risikos enthält. Frühwarnsysteme sollen anzeigen, woran ein Risikoeintritt erkannt werden kann [3]. Diese Prozessphase nimmt eine Schlüsselrolle im gesamten Prozess ein, da die Identifikation der Risiken den Ausgangspunkt für die nachfolgenden Prozessphasen bildet. Es gibt Methoden, die den Kategorien Kollektionsmethode, Kreativitätsmethode und analytische Suchmethoden zugeordnet werden können [8].

3.1 Kollektionsmethoden

Kollektionsmethoden basieren auf der Sammlung risikospezifischer Daten und sind zur Identifikation von bereits bekannten IT-Risiken geeignet. Dabei entsteht eine Liste mit Punkten, die eine Identifikation zukünftiger IT-Risiken vereinfacht.

Checkliste:
Erfahrungen, die über den Zeitablauf gewonnen werden, werden anhand von Checklisten genutzt, um eine Liste von bekannten Schwachstellen und Angriffen zu erstellen. Die Liste wird Punkt für Punkt abgearbeitet und hinsichtlich aktueller Bedrohungen untersucht. Das Bundesamt für Sicherheit in der Informationstechnologie bietet beispielsweise derartige Checklisten auf seiner Homepage [8]. Aufgrund der einfachen Durchführung innerhalb der IT-Abteilung wird die Checkliste in der Praxis sehr häufig eingesetzt [6].

Befragungstechniken:
Bei der Befragungstechnik wird das Wissen von internen und externen Experten herangezogen. Bei der Befragung von internen Experten (Mitarbeiter im Unternehmen) stehen nicht schriftlich festgehaltene Verlustereignisse sowie die Gewinnung zusätzlicher Informationen zur Verfügung. Bei externen Experten können Schwachstellen und Angriffe anderer Unternehmen in Erfahrung gebracht werden, die auch für das eigene Unternehmen relevant sein können [6].

Bewertung:
Die vorgestellten Methoden ermöglichen verschiedene Risiken zu erfassen. Dabei ist aber zu beachten, dass nicht jede Methode für jedes Unternehmen anzuwenden ist. Einige verursachen durch den Einsatz externer Personen hohe Kosten. Andere entfalten ihr Potential erst bei einem genügend großen Unternehmen.

3.2 Kreativitätsmethoden

Diese Methode ist in der Lage, zukünftige und bisher unbekannte IT-Risiken aufzudecken.

Brainstorming:
Beim Brainstorming versucht man hinsichtlich der Identifikation von Schwachstellen die Kreativität der am Prozess beteiligten Personen zu fördern. In der Praxis wird diese Ideenfindung häufig eingesetzt. Die Probanden sollen in einer ungezwungenen Atmosphäre zu einer Problemstellung viele spontane Äußerungen tätigen. Am Ende sollten die gesammelten Ideen strukturiert werden, um ein konsolidiertes Ergebnis zu erhalten [6].

Synektik:
Bei der Synektik werden zusammenhanglose Elemente in den Prozess eingebracht. Aus den gegebenen Elementen versucht man durch Kombination und Reorganisation neue Muster zu entwickeln. Wie das Brainstorming beruht diese Methode auch auf den spontanen Lösungsvorschlägen der Probanden [6].

Delphi-Methode:
Bei dieser Methode geht es um eine Expertenbefragung, wobei die Teilnehmer festgelegte Fragebögen beantworten müssen. Die Auswertung erfolgt mittels statistischen Verfahren. Durch mehrmaliges Ausfüllen, Überdenken und Modifizieren möchte man eine einheitliche Tendenz ableiten [6].

Bewertung:
Das Brainstorming ermöglicht eine kostengünstige und schnelle Identifikation von bestehenden Risiken. Der Aufwand bei der Synektik ist aufgrund ihrer Komplexität hoch. Bei der Delphi Methode können unternehmensrelevante Bedrohungen entdeckt werden, jedoch besteht der Nachteil, dass bei vielen Iterationen ein hoher Aufwand entstehen kann.

3.3 Analytische Methoden

Diese analytische Methode ist ebenso in der Lage, zukünftige und bisher unbekannte IT-Risiken aufzudecken.

Fehlermöglichkeits- und Einflussanalyse (FMEA):
Das Ziel der FMEA ist, mögliche Fehler in Produkten oder Prozessen schon vor ihrem

Auftreten zu erkennen. Das IT-System wird in einzelne Komponenten zerlegt, welche auf mögliche Störungszustände analysiert werden. Daraufhin wird ein Rückschluss über die Auswirkungen auf das Gesamtsystem vollzogen. Es handelt sich um einen Ansatz, der durch Formblätter unterstützt wird. Die Formblätter beinhalten folgende drei Schritte: Untersuchung, Bewertung und Optimierung, die den ersten drei Phasen des Risikomanagementprozesses entsprechen. Die konkrete Formalisierung der Untersuchung und Erfassung der Ergebnisse bietet eine breite Grundlage für Detailanalysen.

Diese Methode eignet sich aufgrund ihrer hohen Komplexität und des hohen Aufwandes nicht zur breiten Identifikation aller Risiken im Unternehmen [6].

Fragenkatalog:
Anhand der Fragekataloge werden IT-Risiken aufgedeckt. Mit Hilfe von detaillierten Fragen und deren Antworten sollen Hinweise auf mögliche Schwachstellen bzw. Bedrohungen gegeben werden.

Das Bundesministerium für Sicherheit in der Informationstechnik hat bspw. standardisierte Fragebögen zur Identifikation von IT-Risiken ausgearbeitet. Das Problem hier ist, dass bei standardisierten Fragebögen unternehmensspezifische Faktoren unberücksichtigt bleiben. Wenn Angriffe bekannt sind, können Fragebögen selbst entwickelt oder angepasst werden [6].

Bewertung:
Fragebögen und FMEA sind geeignete Methoden zur Identifikation. Da in vielen Unternehmen eine standardisierte IT-Systemlandschaft existiert, eignen sich besonders Fragebögen, um einen Überblick über die meist verbreiteten IT-Risiken zu erhalten. Sie stellen eine sehr kostengünstige Form der Identifizierung von Standardrisiken dar. Um hochkritische Systeme zu unterstützen, würde sich die FMEA eignen. Aufgrund der exakten Detaillierung werden bei einem solchen System möglichst viele Risiken aufgedeckt.

4 Risikoanalyse

Die Risikoanalyse ist die zweite Phase des Risikomanagementsystems. Hierbei ist das Ziel, zu den Ursachen des Risikos vorzudringen und eine möglichst genaue Beschreibung der Risikosituation zu liefern. Die Risikoanalyse dient als Grundlage für die Risikosteuerung (siehe Kapitel 5) und ermöglicht die Entwicklung von geeigneten Maßnahmen gegen das Risiko [3]. Ihre Aufgabe ist, die in der vorausgegangenen Phase der Risikoidentifikation entdeckten Risiken zu beurteilen und zu bewerten.

4.1 Quantitative Bewertungsansätze

Die quantitative Analyse liefert numerische Werte einer Kardinal-Skala. Das heißt, zur Messung der potentiellen Schäden und Eintrittswahrscheinlichkeiten werden quantitative Skalen verwendet. Die Eintrittswahrscheinlichkeit eines Schadens und der potentielle Schaden kommen in metrischen Zahlenwerten zum Ausdruck [5].

Ein typisches Beispiel ist der so genannte Annual Loss Expectancy (ALE) [7]. ALE ist ein Schadenserwartungswert, der sich aus dem Produkt der erwarteten Schadenshöhe und der geschätzten jährlichen Eintrittswahrscheinlichkeit zusammensetzt. Dieser Wert ergibt für das betreffende Risiko eine Kennziffer, die den Vergleich zwischen mehreren, auch verschiedenen Risiken ermöglicht. Der ermittelte Wert kann z.B. als Anhaltspunkt für die Höhe eines Budgets für Sicherungsmaßnahmen verwendet werden [9]. Diese Form der Risikobewertung bietet den Vorteil, dass das Risiko in einer mit Geldwerten zu beziffernden Größe ausgedrückt werden kann.

4.2 Qualitative Bewertungsansätze

Qualitative Bewertungsansätze beschäftigen sich mit Risiken, die sich nicht mit Erwartungswerten und Eintrittswahrscheinlichkeiten beschreiben lassen. Die qualitative Ana-

lyse unterscheidet sich von der Quantitativen, dass der Schaden und die Häufigkeit nicht mit absoluten numerischen Größen, sondern mit verbalen Aussagen (Schadenskategorie: von klein bis hin zu katastrophal; Eintrittshäufigkeit: von unwahrscheinlich bis hin zu sehr oft) beschrieben werden [5].

Zur Bewertung des Risikos müssen die Verantwortlichen die Eintrittshäufigkeit und das Schadenspotential des gefährdenden Ereignisses schätzen und anschließend den unternehmensindividuell zu erstellenden Häufigkeits- und Schadenskategorien zuordnen. Bei qualitativen Ansätzen wird versucht, die Einstufungen argumentativ zu begründen.

4.3 Zusammenfassung

Auf den ersten Blick scheint die Risikoanalyse nach der einfachen Formel „Eintrittswahrscheinlichkeit * erwartete Schadenshöhe“ eine simple Aufgabe zu sein. Jedoch ist es schwer, ohne entsprechende Datenbasis Aussagen über Risiken zu treffen. Bei unzureichender Basis müssen vielmehr Annahmen über Auswirkung, Eintrittswahrscheinlichkeit und Schadenshöhe getroffen werden. Die vorgestellten Möglichkeiten zur Risikoanalyse stellen nur einen Ausschnitt aus der Methodenvielfalt dar.

5 Risikosteuerung

Auf Basis der Risikoanalyse werden hier Strategien festgelegt, die auf die Risiken anzuwenden sind. Die Risikosteuerung hat das Ziel, Risiken aktiv und gezielt zu beeinflussen. Die Risikolage eines Unternehmens soll positiv verändert und ein ausgewogenes Verhältnis zwischen Gewinnen (Chancen) und Verlusten (Risiken) erreicht werden. Die ISO 27001 weist hierzu geeignete Techniken aus. Den Unternehmen ist es freigestellt, diese mit weiteren Möglichkeiten beispielsweise aus anderen Standards oder Frameworks zu ergänzen [7].

5.1 Risikovermeidung

Risiken, die eine hohe Eintrittswahrscheinlichkeit und einen hohen Schaden haben könnten, sollten vermieden werden. Risikovermeidung erfordert Maßnahmen, die die Eintrittswahrscheinlichkeit auf null senken, womit das Risiko keine Möglichkeit mehr haben soll, Realität zu werden. Beispielsweise könnte durch den Verzicht auf Lesegeräte am Rechner vermieden werden, dass durch Mitarbeiter Viren oder unlizenzierte Software in das Unternehmensnetz eingebracht werden.

5.2 Risikominderung

Bei der Risikoverminderung wird versucht, die Eintrittswahrscheinlichkeit und/oder das Schadenausmaß zu reduzieren. Das kann für IT-Risiken durch den Einsatz von technischen Sicherheitsmechanismen und organisatorischen Maßnahmen erreicht werden. Die dabei eingesetzten Maßnahmen sind beispielsweise Virenscanner und Datensicherungssoftware, aber auch Hochverfügbarkeitslösungen für IT-Systeme oder Verschlüsselungstechniken [6].

5.3 Risikotransfer

Der Risikotransfer sieht vor, Risiken auf andere Parteien zu übertragen. Diese Strategie wird für Risiken angewandt, die zu hohen Schäden führen könnten. Eine typische Maßnahme ist hier der Abschluss einer Versicherung. Die Grundbedingung für einen Risikotransfer ist also die Existenz einer Vertragspartei, die die Auswirkungen bei einem Risikoeintritt trägt, so dass die negativen Folgen nicht vom Unternehmen selbst getragen werden [6].

5.4 Risikoübernahme

Risikoübernahme bedeutet die Akzeptanz des Eintretens eines Risikos. Für Risiken, welche eine niedrige Eintrittswahrscheinlichkeit und/oder Risikohöhe haben, wird bewusst auf Steuerungsmaßnahmen verzichtet. Ebenso eignet sich diese Strategie bei Risiken, deren Steuerungsaufwand den erwarteten Schaden überschreiten würde. Auf eine systematische Überwachung des Diebstahls von Büroartikeln durch Mitarbeiter sollte zum Beispiel verzichtet werden [3].

6 Risikokontrolle

Die letzte Phase des Prozesses ist die Risikokontrolle. Hier wird untersucht, inwieweit die getroffenen Annahmen aus der Risikoidentifikation und Risikoanalyse eingetreten sind und ob die Methoden aus der Risikosteuerung im Verhältnis zum erzielten Nutzen aus diesen Methoden standen. Eine weitere Aufgabe ist die Übermittlung der Ergebnisse, wobei den Anspruchsgruppen und dem Management im Unternehmen ein Bericht erstattet wird.

Die Kontrolle findet sowohl auf der operativen als auch auf der strategischen Prozessebene statt. Die operative Kontrolle beinhaltet die Überwachung der Einzelrisiken in Form von Soll-Ist-Vergleichen. Diese Abweichungsanalyse dient der Kontrolle, ob die ausgewählten Kriterien und Kennzahlen innerhalb der definierten Grenzen liegen. Parallel zur operativen Risikokontrolle findet auf strategischer Ebene die Überwachung und Anpassung des Risikomanagementprozesses statt. Hierzu werden die Wirksamkeit, die Angemessenheit und die Effizienz der eingeleiteten Maßnahmen überprüft, ob sie die Zielvorgaben der Risikostrategie erfüllen.

Die Risikokontrolle ermittelt, kommuniziert und dokumentiert inwieweit die durchgeführten Maßnahmen in Bezug auf die Risikosteuerungen den prognostizierten Erwartungen entsprechen [6].

7 Fallbeispiel

In diesem Kapitel wird das IT-Risikomanagement anhand von zwei Beispielen dargestellt. Zuerst wird ein Fallbeispiel gezeigt, wie das IT-Risikomanagement an unserer Hochschule Reutlingen gehandhabt wird und im Vergleich, wie das IT-Risikomanagement in einem großen Unternehmen funktioniert.

7.1 Hochschule Reutlingen

Die IT Systeme dürfen an unserer Hochschule nicht ausfallen. Der Emailverkehr, das Netzwerk und die Infrastruktur müssen funktionieren. Auch darf von unbefugten Personen auf die Hochschuldaten nicht zugegriffen werden. Es gibt Technologien, durch die Risiken vermindert und vermieden werden können. Ein Beispiel für den Einsatz dieser an der Hochschule Reutlingen sind Antivirenprogramme. Das Risikomanagement ist an unserer Hochschule nicht explizit, sondern implizit implementiert. Die IT-Infrastruktur an der Hochschule Reutlingen betreibt die Software VMWare vSphere 6.0. Es ist eine Software, die virtuelle Maschinen (VM) für Hardware und deren Betriebssysteme bereitstellt. 250 virtuelle Maschinen, auf denen unterschiedliche Projekte laufen, stehen momentan bei uns zur Verfügung. Anstelle von vielen physikalischen Rechnern werden dedizierte Server eingesetzt, d.h. Server, die die entsprechenden Ressourcen (RAM-Speicher, Anbindung an das Internet, Prozessorleistung) bereitstellen können. Für die Ressourceneinsparung gibt es 7 physikalische Rechner mit insgesamt 250 virtuellen Maschinen.

Ein Vorteil hier ist, wenn es zu einem Absturz kommt, kann der physikalische Rechner nicht sofort wieder gestartet werden. Bei einer virtuellen Maschine hat man einen ortsunabhängigen Zugriff drauf. Jedoch ist ein **Berechtigungskonzept** definiert, so dass nicht jeder freiwillige Zugriff hat. Ein weiterer Vorteil ist die ***Snapshot***-Funktion. Dadurch können Fehlkonfigurationen sichergestellt und im Falle eines Ausfalls auf den Ursprungszustand gebracht werden. Ein Snapshot enthält eine Kopie des Datenbestandes. Unabhängig von einem Hardwareausfall gibt es auch die Remotion – Möglichkeit. Das bedeutet, dass man eine virtuelle Maschine auf einen bestimmten Host verschieben/migrieren kann, ohne dass es zu einer Downtime kommt. Im Normalfall müsste man einen physikalischen Rechner wieder hochfahren.

RAID (*=Redundant Array of Independent Disks)* ist ein System, welches an unserer Hochschule eingesetzt wird und zur Organisation mehrerer physischer Massenspeicher zu einem logischen Laufwerk dient. Man möchte eine höhere Ausfallsicherheit und einen größeren Datendurchsatz ermöglichen.

Hier werden gezielt redundante Informationen erzeugt, das heißt, dass dieselben Daten mehrfach vorkommen, damit bei einem Ausfall einer Festplatte das RAID nach Ersetzen der ausgefallenen Komponente durch einen Rebuild den ursprünglichen Zustand wiederherstellen kann. Wenn an der Hochschule eine Netzwerkkarte eines Storages ausfallen sollte - die mehrere Netzwerkkarten besitzt - dann geht automatisch die zweite Netzwerkkarte an. Die Hochschule Reutlingen besitzt 6 Storagsysteme mit jeweils 4-6 Terabyte. Damit es überhaupt zu einem kompletten Ausfall eines Storages kommt, müssen also all seine Netzwerkkarten ausfallen. Folglich würden die virtuellen Maschinen, die auf dem Storage sind, nicht mehr laufen.

Seit sieben Jahren ist zum ersten Mal ein Storage, die 7 Festplatten und 25 VM's enthalten hat, ausgefallen. Die betroffenen VM's wurden auf einen anderen Storage übertragen. Es wird drauf geachtet, dass die Storages für einen Ausfall Puffer haben müssen, so dass die virtuellen Maschinen jederzeit auf einen anderen Storage verschoben werden können. Ebenso bestehen für solche Fälle zeitgesteuerte Backups. Der Nutzer einer VM kann definieren, in welchem Zeitraum ein Backup seiner VM durchgeführt werden soll. Hierzu muss ein entsprechender Antrag ausgefüllt werden.

Auf die Bezeichnung/Nomenklaturen der Maschinen wird sehr viel Wert gelegt, weil in einem Krisenfall abgelesen werden muss, wer der Nutzer ist und wann das letzte Backup war. Die Identität ist wichtig, damit die VM im System wiedergefunden und auf einen anderen Storage übertragen werden kann.

Die Konsequenzen hier sind, dass die Übertragung der VM's manuell durchgeführt werden muss. Der Datenverlust stellt für die Hochschulmitarbeiter eine Blackbox dar, da sie über den Inhalt nicht Bescheid wissen und nicht einschätzen können, welche Daten verloren gegangen sind. Wenn keine qualifizierten Mitarbeiter für die Installation zur Verfügung stehen, kann es bis zu 4 Wochen dauern, dass eine VM wiederhergestellt wird.

Da die Ursache des Ausfalls nicht bekannt ist, wurde als Maßnahme an erster Stelle festgelegt, dass alte Hardware nicht zu lange betrieben werden soll. Geräte müssen hinsichtlich ihrer Performance klassifiziert bzw. aussortiert werden [10].

Wenn also ein Schutzziel verletzt und nicht durchgesetzt wird, können IT-Risiken auftauchen. In dem Beispiel der Hochschule Reutlingen wurde das Schutzziel „Verfügbarkeit" verletzt, da aufgrund des Storageausfalls die darin enthaltenen Festplatten und virtuellen Maschinen nicht zur Verfügung standen. Das Kommunikationsnetz ist ein sehr wichtiger Punkt, damit die Kommunikation zwischen allen Partnern ermöglicht wird.

7.2 Risikomanagement in einem großen Konzern

Im nachfolgenden Beispiel wird ein börsennotiertes Unternehmen (Aktiengesellschaft) mit rund 300.000 Mitarbeitern vorgestellt. Da es sich um interne Informationen handelt, wir das Unternehmen nicht genannt und anonymisiert behandelt. Die Informationen wurden aus einem Gespräch mit dem internen Verantwortlichen für das IT-Risikomanagement am 06.03.2017 entnommen.

Das Risikomanagement wird sowohl im Konzern als auch in all seinen Gesellschaften (Tochterunternehmen) ausgeführt. Das Risikomanagement ist ein kontinuierlicher Prozess. Wenn außerhalb der Planung ein Risiko identifiziert wird, wird es dem Verantwortlichen gemeldet.

Dauerhafte Risiken sind z.B. Hackerangriffe, Wirtschaftskriminalität oder Erdbeben. Hier kann sich die Schadenshöhe und Eintrittswahrscheinlichkeit über die Jahre geringfügig oder gar nicht ändern. Gegenmaßnahmen können dazu dienen, dass das Risiko nicht weiterhin steigt, sondern stabil gehalten wird. Wobei die Gegenmaßnahmen sich über die

Jahre ändern können (z.B. neue Technologien).

Der Vorstand ist durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zur Einrichtung eines Risikofrüherkennungssystems verpflichtet. Die Anforderungen an das Risikomanagement wurden durch das in Kraft treten des Bilanzrechtsmodernisierungsgesetzes (BilMoG) verschärft. Das BilMoG umfasst zahlreiche neue Regelungen für die Rechnungslegung und führt auch zu vielfältigen Änderungen beim Risikomanagement. So erweitert das Gesetz die Verantwortung des Aufsichtsrats und des Wirtschaftsprüfers und fordert für alle Bereiche das Risikomanagement.

7.2.1 Vorgehen

- Eine Risikomanagement Organisation ist eingerichtet, Aufgaben und Verantwortliche sind definiert.
- Alle Risiken werden identifiziert und bewertet.
- Alle wesentlichen Risiken werden innerhalb des Konzerns berichtet.
- Zur Steuerung der Risiken werden geeignete Maßnahmen ergriffen. Um Transparenz über die Risikolage der Geschäftseinheit herzustellen und frühzeitig übergreifende Gegenmaßnahmen einleiten zu können, sind wesentliche Risiken an die nächste organisatorische Ebene zu berichten.
- Die Umsetzung und der Erfolg der Maßnahmen werden verfolgt.
- Die Risikomanagementaktivitäten werden regelmäßig geprüft.

7.2.2 Implementierung

Es gibt eine Checkliste, die dabei unterstützen soll, dass an alle wichtigen Kriterien oder Punkte hinsichtlich Risikomanagements gedacht wird.

Vor dem Start:
Der Ablauf der Planungsperiode wird geprüft. Die Kontaktpersonen und Ansprechpartner müssen den Prozessbeteiligten bekannt sein. Auch die Rollen und damit verbundene Aufgaben, Kompetenzen und Verantwortlichkeiten sind bekannt. Anschließend kann die Risikoplanung beginnen.
Risikoidentifikation:
Es werden Risiken, welche die Zielerreichung der betroffenen organisatorischen Einheit (Verfügbarkeit einer Applikation oder Bereitstellung einer gesicherten Infrastruktur) gefährden oder verhindern, identifiziert. Des Weiteren müssen Dokumente (Handbuch, Leitfaden, Templates etc.) zur methodischen Unterstützung bekannt sein. Aktivitäten (z.B. Brainstorming) zur Risikoidentifikation werden durchgeführt. Um nachzuweisen, dass Risikoidentifikation durchgeführt wurde, müssen Dokumente zentral archiviert werden.
Risikobewertung:
Für die Risikobewertung werden Parameter ermittelt, um Kosten für die Wiederbeschaffung zu ermitteln. Entweder quantitativ oder qualitativ wird sie durchgeführt. Die Bewertung wird kritisch auf Plausibilität, Verständlichkeit und Klarheit geprüft, damit sie für alle verständlich ist.
Risikosteuerung:
Die Handlungsstrategie (Risikovermeidung, -minderung, -transfer, -übernahme) wird festgelegt. Entsprechende Gegenmaßnahmen werden definiert und eine textliche Zusammenfassung dieser wird erstellt.
Risikodokumentation:
Risiken sind von allen eingebundenen Einheiten zu dokumentieren und an den Verantwortlichen zu melden. Eine Berichterstattung wird an die nächst höhere Ebene weitergeleitet.
Risikoüberwachung:
Die Inhalte der Risiken und Gegenmaßnahmen werden überprüft. Es wird kontrolliert, ob neue Risiken hinzugekommen bzw. entstanden sind. Der komplette Risikomanagementprozess wird für die kommenden zwei Jahre auf jeder Ebene durchlaufen. Risiken werden auch hinsichtlich veränderten Rahmenbedingungen überprüft und angepasst (z.B., wenn neues Gesetz eingeführt wird.).

Nach der Risikoplanung:
Ein Treffen namens „Lessons learned“ wird geplant, um offene Themen, Punkte und Fragen zu klären bzw. Verbesserungsvorschläge zu erarbeiten. Bei einem Lessons learned werden also gewonnene Erkenntnisse, neues Wissen oder Erfahrungen, die während der Arbeit an einem Projekt entstehen in Form einer Dokumentation aufgezeichnet.

7.2.3 Beispiele

Beispiel 1 - Auswirkungen des demografischen Wandels: Das Durchschnittsalter der Mitarbeiter steigt und es können nicht genügend junge Mitarbeiter eingestellt werden, um das Ausscheiden älterer Mitarbeiter zu kompensieren. Aufgrund dessen geht das Know-how durch den Weggang der älteren Mitarbeiter verloren, sofern es nicht auf jüngere übertragen werden kann. Das ist z.B. bei Kernthemen kritisch, wenn Mitarbeiter ausscheiden, für die es keinen Stellvertreter gibt. **Maßnahmen**: Einstellung und Nachwuchsförderung intensivieren, aktive Nutzung des bestehenden Erfahrungsschatzes (z.B. Schulung).

Beispiel 2 - Integration von Fremdleistungen: Fremdvergabe kann ein wirksames Mittel zur Kostenoptimierung und Effizienzsteigerung sein. Damit einher geht die Gefahr des Kontrollverlusts über einige Bereiche der Leistungserbringung. Wenn Kernkompetenzen verloren gehen, insbesondere solche, die für die Beratung und Auftragserfüllung zur Auswahl, Integration, Qualitätssicherung und Abnahme von zugelieferten Services erforderlich sind, sollte eine Fremdvergabe kritisch überdacht werden. Durch räumliche, zeitliche und sprachliche Barrieren können sich Aufwand und Kosten zusätzlich erhöhen. **Beispiele**: Kunden können nicht kompetent beraten werden; Know-how fehlt; Preiswertigkeit erbrachter Leistungen kann nicht verlässlich beurteilt werden; bei Applikationen besteht die Gefahr, dass die erforderlichen Kontrollen nicht im erforderlichen Umfang erbracht und regulatorische Anforderungen erfüllt werden. **Maßnahmen**: Mitarbeiter schulen.

Beispiel 3 - Datenabfluss infolge von unzureichender Schnittstellenabsicherung: USB-Anschlüsse und CD-Brenner sind nicht gesperrt. Der Einsatz mobiler Datenträger wird nicht kontrolliert. Daten und Informationen können über diese Wege in die Hände Unbefugter gelangen. **Maßnahmen**: Sicherheitsunterweisung für Mitarbeiter, Umsetzung von Berechtigungskonzepten, abgestimmte und angemessene Überwachungsmaßnahmen für sensible Bereiche.

7.3 Fazit

Risikomanagement hört sich kompliziert an, aber es geht lediglich um die Identifikation, der Bewertung und dem Umgang mit den erkannten Risiken. Es ist egal, ob das Risikomanagement explizit oder implizit implementiert wird – Risiken sind immer da. Das Risikomanagement wird, ohne sich dessen bewusst zu sein, täglich genutzt. Wenn man sich vor dem Verlassen des Hauses über die Wetteraussichten informiert und wegen der hohen Wahrscheinlichkeit von Niederschlägen den Regenschirm mitnimmt, so ist das ein Risikomanagementprozess. Risikomanagement ist meiner Meinung nach unbestritten ein nützliches Werkzeug, welches bewusst oder unbewusst eingesetzt wird. Ein Risikomanagementprozess trägt dazu bei, die Gefahren in- und außerhalb optimal zu kontrollieren und zu steuern. Beispielsweise muss ein Unternehmen schnell auf bestimmte Ereignisse und Umweltveränderungen reagieren können. Die Systeme sollten zu jeder Zeit zur Verfügung stehen. Das Risikomanagement kann nicht die Zukunft beeinflussen, aber dabei helfen, mögliche erfolgskritische Szenarien zu antizipieren.

8 Zusammenfassung

Das Risikomanagement darf nicht als einmalige zeitpunktbezogene Durchführung von Maßnahmen verstanden werden, sondern

muss als kontinuierlicher Prozess im Unternehmen etabliert und integriert werden. Der Risikomanagementprozess lässt sich in eine strategische Phase, in der die Ziele und die organisatorische Ausgestaltung des Risikomanagements festgelegt werden, und die operativen Phasen der Risikoidentifikation, Risikoanalyse und Risikosteuerung einteilen. Um bestehende IT-Risiken effizient zu identifizieren, bieten sich die Checklisten in Kombination mit einer Expertenbefragung an. Mit der intuitiven Kreativitätsmethode des Brainstormings können zahlreiche Risikoaspekte zusammengetragen und neue, unbekannte IT-Risiken identifiziert werden. Die Kreativitätsmethoden tragen dazu bei, ein besseres Verständnis von IT-Risiken und ihren vielfältigen Ursachen herbeizuführen. Im Anschluss an die Identifikation der Risiken erfolgt deren Bewertung, die quantitativ oder qualitativ erfolgen kann. Bei beiden Bewertungsansätzen ergibt sich die Schwierigkeit, die Eintrittshäufigkeit und Schadenshöhe zu ermitteln. Zur Steuerung der identifizierten und bewerteten Risiken bieten sich die Alternativen der Risikovermeidung, Risikominderung, des Risikotransfers und der Risikoübernahme an. Um die mit den Risiken verbundenen Chancen zu nutzen, ist es für ein Unternehmen erforderlich, aktives Risikomanagement zu betreiben.

9 Literaturverzeichnis

[1] http://www.pwc.de/de/strategie-organisation-prozesse-systeme/unternehmensweites-risikomanagement.html abgerufen am 10.02.2017.

[2] https://de.statista.com/statistik/daten/studie/497298/umfrage/computernutzung-in-unternehmen-nach-betriebsgroesse-in-deutschland/

abgerufen am 10.02.2017.

[3] Fabian Ahrendts, Anita Marton: IT-Risikomanagement leben! Wirkungsvolle Umsetzung für Projekte in der Softwareentwicklung; Springer Verlag Berlin Heidelberg; 2008.

[4] Klaus-Rainer Müller: IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanageent – Sichere Anwendungen – Standards und Practices; 5. Auflage, Springer Verlag, Wiesbaden 2014.

[5] Hans-Peter Königs: IT Risikomanagement mit System. Praxisorientiertes Management von Informationssicherheits- und IT-Risiken. 4. Auflage, Springer Verlag, Wiesbaden 2013.

[6] Oliver Prokein: IT Risikomanagement. Identifikation, Quantifizierung und wirtschaftliche Steuerung. Hrsg.: Arnold Picot, Ralf Reichwald, Egon Franck, Kathrin Möslein: Martk- und Unternehmensentwicklung. Gabler Verlag, Wiesbaden 2008.

[7] Fred Wagner: Risk Management im Erstversicherungsunternehmen: Modelle – Strategien – Ziele – Mittel. VVW, Kalrsruhe 2000.

[8] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, abgerufen am 17.02.2017.

[9] Stefanie Fiege: Risikomanagement- und Überwachungssystem nach KonTraG. Deutscher Universitätsverlag: Wiesbaden 2006.

[10] Andé Backe, M.Sc. Mitarbeiter der Hochschule Reutlingen. Gespräch geführt am 01.03.2017.

Zukunft des neuen elektronischen Personalausweises

David Schneider
Reutlingen University
David.Schneider@Student.
Reutlingen-University.DE

Abstract

Diese Arbeit beschäftigt sich mit dem neuen elektronischen Personalausweis. Zum einen werden in diesem Paper die Sicherheitsziele des Personalausweises und die technische Umsetzung der Architektur und Protokolle erklärt. Es wird der Ablauf einer Online-Identifizierung für einen Nutzer mithilfe des Ausweises aufgezeigt. Risiken und Schwachstellen der Technologie im Software- oder Hardwarebereich werden diskutiert und die bereits erfolgten Hack-Angriffe aufgezeigt. Die Arbeit legt Möglichkeiten dar, wie sich der Nutzer vor Angriffen schützen kann. Es werden die Gründe genannt warum der neue Personalausweis online nur schwer Anklang findet und warum die Aufklärung, über die zur Verfügung stehenden Anwendungen, eine Preisreduzierung der Lesegeräte sowie die vom Europa Parlament und Europarat erlassene eIDAS-Verordnung nicht helfen werden um die Nutzung voranzutreiben. Ergebnisse hierfür liefert eine Nutzerstudie. Zum anderen werden Ideen genannt wie die Nutzung der elektronischen Funktionen des Ausweises stattdessen zu fördern ist.

Schlüsselwörter

RFID, Authentification Security, Hacking, Risks, German Identity Card.

CR-Kategorien

Algorithms, Design, Human Factors, Security, Standardization.

1 Einführung

Der neue elektronische Personalausweis (nPA) wurde am 1. November 2010 eingeführt und unterscheidet sich von seinem Vorgänger dadurch, dass er über einen integrierten Chip verfügt, welcher sich unsichtbar in der Plastikkarte verbirgt. Durch diesen Chip ist es möglich kontaktlos auf die Daten des nPA zuzugreifen. Die Funktechnik, die hierbei zum Einsatz kommt nennt sich RFID. Das Kürzel stammt aus dem Englischen und steht für *Radio Frequency Identification* zu Deutsch Identifizierung über Funkwellen. Die Technologie bietet die Möglichkeit, Daten auszulesen und auf einem Datenträger (hier: der integrierte Chip) zu speichern, ohne dass eine physische Verbindung oder direkter Sichtkontakt der Kommunikationspartner bestehen muss. Für die Verbindung wird ein Lesegerät benötigt.

1.1 Ziele dieser Arbeit

In dieser Arbeit wird sich ausschließlich mit dem neuen elektronischen Personalausweis

Betreuer Hochschule: Prof. Dr.-Ing. Marcus Schöller
Hochschule Reutlingen
Marcus.Schoeller@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

befasst, welcher seit dem 1. November 2010 an deutsche Staatsangehörige ausgegeben wird. Personalausweise die vor diesem Datum ausgestellt wurden, verfügen über keine Funktechnologie und werden daher in dieser Arbeit nicht betrachtet.

Die wesentlichen Neuerungen im Vergleich zum Vorgänger sind nachfolgend beschrieben. Der Ausweis wird nun im ID-1 Format ausgegeben. Es gibt einen Chip im Ausweis mit einer Online-Ausweisfunktion, Lichtbilder können auf dem Chip gespeichert werden, sowie die Fingerabdrücke, dies jedoch auf freiwilliger Basis. Es gibt eine Unterschriftsfunktion die es ermöglicht, rechtsverbindliche Verträge, Anträge, Urkunden etc. elektronisch zu unterschreiben.

Auf die physischen Sicherheitsmerkmale [1], wie Guillochen, Mikroschriften, UV-Aufdruck, optisch variable Farben, holografische Porträts, 3D-Bundesadler, kinematische Bewegungstrukturen etc., wird in dieser Arbeit nicht näher eingegangen, da sich diese Arbeit ausschließlich mit den elektronischen Funktionen des nPAs beschäftigt. Der Grund, warum dem nPA eine Chipkarte eingebettet wurde, liegt neben der Speicherung der Daten darin die Fälschungssicherheit zu erhöhen und neue Funktionalitäten zu unterstützen. Dies wird noch näher in den folgenden Kapiteln erläutert. Am Ende der Arbeit wird sich mit der Fragestellung auseinandergesetzt, inwiefern der nPA bei den Verbrauchern Anklang findet und ob durch die neue eIDAS-Verordnung der EU-Kommission die Nutzung des nPA vorangetrieben werden kann. Dazu wird eine Nutzerstudie durchgeführt.

2 Technologie und Sicherheit des Personalausweises

Der neue Personalausweis enthält zahlreiche Sicherheitsmerkmale, die bestmöglichen Schutz vor Fälschung und Missbrauch bieten; diese Merkmale machen den Ausweis zu einem der sichersten der Welt [1]. Durch den integrierten Chip im nPA kann der Ausweisinhaber sich via Online-Authentisierungsfunktion (engl. electronic identity, kurz eID) bei Anwendungen und Webseiten anmelden. Eine Auflistung der aktuellen Anwendungsmöglichkeiten findet sich auf dem Personalausweisportal [2]. Diese erhalten nach Zustimmung des Inhabers Zugriff auf personen- und dokumentenbezogene Daten. Nicht auf dem Chip abgelegt sind eigenhändige Unterschrift, Körpergröße und Augenfarbe [3]. Mithilfe der Qualifizierten elektronischen Signatur (QES) kann der Nutzer Verträge rechtskräftig unterschreiben. Durch die eIDAS-Verordnung [4] wird das ab 2018 europaweit der Fall sein.

Die Vorteile der eID Funktion liegen auf der Hand, es gibt einen vollkommen digitalen, öffnungszeitenunabhängigen und medienbruchfreien (nur bei QES) Vorgang, bei dem zusätzlich Wartezeiten entfallen und Papier und Porto gespart werden.

2.1 Lesegeräte für den nPA

Für das Auslesen des nPA ist neben Treibern und Software ein spezielles Lesegerät notwendig. Es gibt verschiedene Modelle, die dafür zu verwenden sind. Der Kunde hat die Möglichkeit sich auf dem freien Markt ein Gerät zu besorgen. Das einzige Kriterium, das an das Lesegerät gestellt wird, ist, dass es von Bundesamt für Sicherheit in der Informationstechnik (BSI) anhand der Technischen Richtlinie TR-03119 zertifiziert ist [5]. Solche Geräte sind auch am nPA Logo zu erkennen [6]. Die Lesegeräte gibt es in drei Ausführungen: Basisleser, Standardleser und Komfortleser. Der Basisleser unterstützt die Onlineausweisfunktion und stellt damit einen Sicherheitsgewinn dar. Der Standardleser besitzt zusätzlich eine eigene Tastatur und optional ein eigenes Display. Der Komfortleser hat grundsätzlich ein eigenes Display und alle Funktionen der beiden anderen Geräte. Er beinhaltet damit die Vollausstattung und unterstützt darüber hinaus noch die elektronische Unterschriftsfunktion (QES).

2.2 Sicherheitsziele

Neben einem schnellen Sperrvorgang durch ein persönliches Sperrkennwort nach einem Diebstahl des Ausweises ist es in erster Linie für den Ausweisinhaber wichtig, dass die Daten während des Auslesevorgangs nicht abgefangen oder verfälscht werden. Dies dient dem Sicherheitsziel der Authentizität und Integrität. Daher ist es erforderlich, die Kommunikation durch einen Mechanismus zu verschlüsseln. Des Weiteren muss auch die Kommunikation des Lesegerätes zum Server im Internet verschlüsselt ablaufen. Außerdem soll es dem Ausweisinhaber möglich sein auszuwählen, welche Daten an welches Unternehmen gesendet werden. Dies geschieht im Dialog mit dem Lesegerät (falls Display und Tastatur vorhanden) oder mit der Anwendersoftware.

Daneben gibt es verschiedene Ziele für den Datenschutz wie Aufenthaltsort des Inhabers, Wiedererkennen eines Nutzers (Tracking) auf die in dieser Arbeit nicht näher eingegangen wird.

2.3 Auslesevorgang

Das Protokoll [11] für den Auslesevorgang ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und in der Technischen Richtlinie TR-03127 festgehalten.

Für den Zugriff auf die Chip-Daten kommen folgende Anwendungsfälle infrage [11]:

1. eine auf dem Kartenkörper aufgedruckte sechsstellige Nummer (CAN – Card Access Number);
2. Hash über Dokumentennummer, Geburtsdatum und Ablaufdatum aus der maschinenlesbaren Zone (MRZ);
3. die eID-PIN: dies ist entweder eine dem Karteninhaber im PIN-Brief mitgeteilte fünfstellige eID-Transport-PIN oder eine nur dem Karteninhaber bekannte operationelle sechsstellige eID-PIN;
4. ein dem Karteninhaber im PIN-Brief mitgeteilter zehnstelliger PUK

In dieser Arbeit wird sich ausschließlich mit dem dritten Anwendungsfall beschäftigt, da dieser der Hauptanwendungsfall, insbesondere für die Ausweisinhaber selbst, ist.

Voraussetzung für den Lesevorgang am Computer ist die Installation der „AusweisApp“ des BSIs sowie der Treiber des Lesegerätes.

Die AusweisApp ist für Windows, Macintosh und Linux erhältlich. Das Lesegerät empfängt vom Diensteanbieter das Berechtigungszertifikat. Der Ausweisinhaber gibt nun seine persönliche Benutzer-PIN ein und erteilt hierdurch die Einwilligung zum Zugriff auf seine Ausweisdaten.

Der Vorgang wird im nachfolgenden Kapitel auf Protokollebene erläutert.

2.3.1 PACE

Nachdem der Chip im Personalausweis das die PIN überprüft hat startet das *Password Authenticated Connection Establishment* (PACE) Protokoll und erstellt einen verschlüsselten und integritätssicheren Kanal zwischen Terminal und Chip [11] (siehe Abbildung 1). Das PACE-Verfahren besteht im Kern aus einem Diffie-Hellman-Schlüsselaustausch-protokoll, wobei die ausgetauschten Schlüssel mittels (einfachen) Passwörtern (PINs) abgesichert werden; bei der PACE-Authentisierung generieren sowohl der Chip als auch das Lesegerät dynamisch flüchtige (ephemeral) DH-Schlüsselpaare, basierend auf den auf dem Chip abgelegten DH-Parametern, den sogenannten Domänen-Parametern [15].

Die Authentizität der öffentlichen DH-Schlüssel wird über den Nachweis der Kenntnis des gemeinsamen Geheimnisses, der 6-stelligen PIN, sichergestellt [15]. Beim nPA kommen zur Abwicklung des PACE-Protokolls die elliptischen Verfahren *Elliptic curve Diffie–Hellman* (ECDH) und *Elliptic Curve Digital Signature Algorithm*

(ECDSA) mit 224 Bit-Schlüsseln zum Einsatz [15].

Nachfolgend eine Vergröberung des Protokolls nach Eckert [15]:

1. Der Chip wählt eine Zufallszahl *s* und verschlüsselt diese mit einem aus der PIN π abgeleiteten Schlüssel $K\pi$: $C = E(s, K\pi)$.
2. Der Chip überträgt den Kryptotext *C* und seine DH-Parameter zum Lesegerät.
3. Das Lesegerät erhält die PIN π durch die Eingabe über den Benutzer.
4. Das Lesegerät leitet seinerseits den Schlüssel $K\pi$ aus der PIN ab und entschlüsselt den erhaltenen Kryptotext: $s = D(C, K\pi)$.
5. Chip und Lesegerät erzeugen jeweils flüchtige DH-Schlüsselpaare basierend auf den neu berechneten DH-Parametern. Dazu wenden sie jeweils eine Abbildungsfunktion an, die als Eingabe die ursprünglichen Domänen-Parameter des Chips sowie die verschlüsselt ausgetauschte Zufallszahl *s* verwendet.
6. Beide Partner tauschen ihre jeweiligen öffentlichen DH-Schlüssel aus.
7. Beide Partner berechnen den gemeinsamen, geheimen DH-Schlüssel *K* und leiten davon einen gemeinsamen Integritäts- K_{MAC} und Sitzungsschlüssel K_{Enc} ab.
8. Beide Partner erzeugen jeweils ein Authentisierungstoken. Dies ist ein MAC über den Integritätsschlüssel K_{MAC} und den öffentlichen DH Schlüssel des Partners.
9. Beide prüfen den MAC und verwenden danach die neuen Schlüssel für das nachfolgende Secure Messaging zwischen dem Chip und dem Lesegerät.

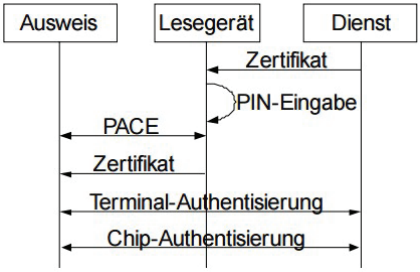

Abbildung 1 – Schema PACE-Protokoll [17]

Das PACE zählt, wie die nachfolgendene Terminal- und Chip-Authentisierung, zum *Extended-Access-Control* (EAC) Protokoll, welches speziell für den nPA entwickelt wurde. Nachdem über PACE gemeinsame Sitzungsschlüssel ausgehandelt wurden, überträgt das Lesegerät das Berechtigungszertifikat des Diensteanbieters zum Ausweis [15]. Nun folgt die Terminal-Authentisierung.

2.3.2 Terminal-Authentisierung

Die Terminal-Authentisierung (TA) dient der Autorisierung der Leserechte, sowohl für das Terminal selbst, als auch für den Dienstanbieter, welcher bei einer Online-Authentisierung die Daten benötigt [11]. Der Ausweisinhaber muss dieser Abfrage zustimmen. Somit behält er neben der Zugriffskontrolle auf seinen Ausweis, geschützt durch seine PIN, auch die Kontrolle über die Daten, die abgefragt werden. Durch das Challenge-Response-Protokoll weist der Diensteanbieter durch die Erstellung einer Signatur die Kenntnis seines privaten Schlüssels nach, der zu dem öffentlichen Schlüssel passen muss, der im Berechtigungszertifikat enthalten ist [15]. Der Chip prüft die Signatur, jedoch ist er nicht in der Lage Sperrlisten abzufragen, um zu prüfen, ob das Berechtigungszertifikat noch gültig ist; deshalb haben derartige Zertifikate nur eine sehr kurze Gültigkeit von max. 3 Tagen [15].

Bei der TA kommt für das EAC-Protokoll eine Public-Key-Infrastruktur (PKI) zum Einsatz. Die PKI besteht aus der Wurzelinstanz Country-Verifying-Certification-Authority (CVCA) und Document-Verifiers (DV) (siehe Abbildung 2). Diese DVs haben die Aufgabe die Schlüsselpaare der einzelnen Lesegeräte oder Dienstanbieter zu signieren.

Die Terminal-Authentisierung unterbindet das unbefugte Auslesen der Daten. Die Leserechte können detailliert via Zertifikat festgelegt werden. Zudem ist es möglich die Rechte vor dem Auslesevorgang weiter einzuschränken. Die Leserechte sind hierbei an die Sitzungsschlüssel gebunden, die im nachfolgenden Schritt ausgehandelt werden; dadurch ist sichergestellt, dass die Daten nur in einem stark gesicherten Ende-zu-Ende-Kanal zwischen Chip und Dienstanbieter übertragen werden, der nur durch den authentisierten Dienstanbieter aufgebaut werden kann [17].

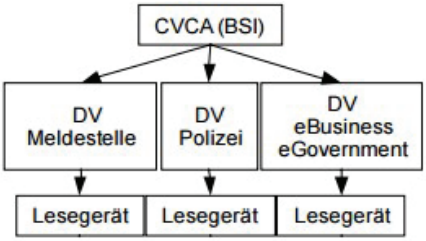

Abbildung 2 - EAC-PKI [17]

Um ein Erraten der eID-PIN durch Ausprobieren zu verhindern, enthält die Karte einen Fehlbedienungszähler (FBZ), der nach drei falschen PIN-Eingaben die eID-PIN sperrt; dadurch bestünde die Gefahr eines Denial of Service Angriffs (DoS) über die kontaktlose Schnittstelle auf die eID-PIN durch mehrmaliges Falscheingeben der eID-PIN ohne Kenntnis des Inhabers; um dies zu verhindern, wird der dritte Eingabeversuch erst nach erfolgreicher Eingabe der auf der Karte aufgedruckten CAN ermöglicht [11].

Nun folgt die Chip-Authentisierung.

2.3.3 Chip-Authentisierung

Die Chip-Authentisierung (CA) hat den Zweck einen sicheren Kanal zwischen Terminal bzw. Dienstanbieter und Chip aufzubauen. Sie prüft, ob der Chip in Besitz des privaten Schlüssels ist, der zum gespeicherten öffentlichen Schlüssel gehört und sorgt hierbei für Integrität und Authentizität [11].

Basierend auf den ausgetauschten DH-Werten berechnen Chip und Diensteanbieter ein gemeinsames MAC-Geheimnis sowie einen gemeinsamen, geheimen Sitzungsschlüssel *K* [15]. Der Dienste-anbieter kann anhand des vom Personalausweisaussteller (Bundesdrucker-ei) signierten, im Chip abgelegten, öffentlichen Schlüssels des Chips dessen Authentizität prüfen [15]. Der Chip verschlüsselt die zu übertragenen Daten mit dem Sitzungsschlüssel *K* und überträgt sie zum Diensteanbieter [15].

2.4 Angriffe auf den nPA

Bisher wurde gezeigt, dass der nPA bekannte und häufige Schwachstellen durch die Implementierung des PACE-Protokolls und der Zwei-Faktor-Authentifizierung vermeidet. Das BSI hat PACE entwickelt und patentieren lassen; es gilt bis heute (Februar 2017) als sicher. Es gibt jedoch weitere Angriffsmöglich-keiten auf die in diesem Abschnitt näher eingegangen wird.

2.4.1 PIN Phishing

Wie bei gängigen Passwort-Phishings ist es auch beim nPA möglich die PIN zu stehlen, z.B. durch ein gefälschtes Online-Plugin der AusweisApp oder der AusweisApp selbst. Durch eine optisch ähnliche Eingabemaske könnte der Nutzer seine PIN dem Angreifer unbeabsichtigterweise übermitteln.

Wird dieser Angriff mit einem Trojaner auf dem Rechner des Opfers kombiniert, könnte der Angreifer den Ausweis direkt online für seine Zwecke benutzen.

2.4.2 PIN Diebstahl

Die PIN kann auch durch Ablauschen eines Basislesegeräts gestohlen werden [19]. Hierbei wird über E-Mail ein Tool installiert, dass den Bildschirm zum Angreifer spiegelt und dadurch persönliche Daten, welche von Nutzer eingegeben werden, im Klartext einsehbar sind. Dieser Angriff ist nur möglich beim Basis-Lesegerät, da dieses nicht über eine integrierte Tastatur verfügt. Auch die optionale Bildschirmtastatur der AusweisApp ist keine Verbesserung, da das Tastenfeld nicht randomisiert ist. Von diesem Angriff sind Standard- und Komfortleser ausgeschlossen, da sie über eine eigene Tastatur verfügen.

Der Ausweis kann nur dann vom Angreifer verwendet werden, solange er auf dem Lesegerät liegt. Da die Adressdaten des Opfers nach dem Angriff bekannt sind sollte der Diebstahl des physischen Ausweises ebenfalls möglich sein.

2.4.3 Manipulierte AusweisApp

In der Vergangenheit ist es einem Angreifer gelungen, die Update-Funktion der AusweisApp (erhältlich für Windows, Linux, Mac) zu manipulieren [12]. Dies war möglich, da das Programm nicht prüfte ob das SSL-Zertifikat zum Servernamen passt. Daher bedurfte es keinem gültigen Zertifikat für den Updateserver, sondern es genügte ein gefälschtes SSL-Zertifikat. Der Updatefunktion kann auf diesem Weg eine manipulierte Antwort untergeschoben werden, um etwa einen Trojaner von einer beliebigen URL herunterzuladen und zu installieren.

2.4.4 Skimming

Beim Skimming besteht das Risiko der Nutzung eines infizierten oder gar falschen Lesegerätes. Die AusweisApp auf dem Nutzer-Computer prüft die Zertifizierung der Lesegeräte. Da die Bezeichnung des Lesers vom Betriebssystem stammt, sollte es nicht zu schwierig sein sie zu fälschen [20]. Wie auch bei Bankautomaten können die öffentlichen Lesegeräte z.B. in Behörden etwa durch zusätzliche Hardware gefälscht werden.

2.5 Zusammenfassung und Bewertung der Ergebnisse

Mit der Anwendung des PACE-Protokolls ist eine sichere Möglichkeit gegeben die Daten des nPAs vor unbefugtem Auslesen zu schützen. Der Beweis ist von Bender et al. bestätigt [14]. Viele bekannte Schwachstellen sind bei der Entwicklung von PACE bereits eliminiert vermieden worden z.B. in dem es einen verschlüsselten, integritätssicheren Kanal zwischen Karte und Lesegerät aufbaut. Es ist praktisch sehr unwahrscheinlich, dass durch Brute-Force die Benutzer-Pin gebrochen wird, da nur drei Versuche zur Verfügung stehen. Die Benutzer-PIN besteht im Vergleich zu Bankkarten aus sechs Ziffern anstatt nur vier.

Gängige Social-Engineering-Angriffe, wie Erraten des Passworts, Phishing aber auch Skimming Angriffe, sind möglich. Im Vergleich zu RFID Kreditkarten, welche über Funk nachweislich über größere Distanzen als angegeben im Klartext ihre Daten senden, findet die Kommunikation zwischen nPA und Terminal verschlüsselt statt. Zusätzlich ist eine beidseitige Authentifizierung integriert und der Diensteanbieter muss eine Berechtigung zum Auslesen der Daten vorweisen. Die auszulesenden Daten gibt der Ausweisinhaber im nächsten Schritt manuell frei.

Die Kritik an dem nPA ist somit verglichen mit anderen Funkkarten auf hohem Niveau. Vielfach wird auch der Datenschutz respektiert und für Anfragen, in denen kein Name erforderlich ist, nur ein Pseudonym gesendet. Ähnlich verhält es sich bei Altersabfragen, wobei nur ein Ü18 Signal gesendet wird und nicht das Alter selbst.

Einige der aufgezeigten Hackangriffe wies das BSI zurück, da es für unwahrscheinlich empfunden wird, dass ein Trojaner auf dem PC des Opfers ist [7]. Sie beziehen sich darauf, dass die Endanwender verpflichtet

sind ihre PCs zu schützen. Hier geben sie Vorgaben, wie den Einsatz einer Firewall, Virenscanners und die Einspielung regelmäßiger Software-Updates. Der Ausweis soll nach der Verwendung sofort vom Lesegerät entfernt werden. Da ein Trojaner permanent auf dem infizierten Rechner aktiv ist, spielt es keine Rolle wann der Ausweis auf das Lesegerät gelegt wird. Die Argumentation des BSI ist somit sehr schwach und es schiebt die Verantwortung auf den Bürger ab.

Für den nPA gibt es ein Sperrkennwort, mit welchem die Benutzer den Ausweis sofort selbst sperren können.

2.5.1 Handlungsempfehlungen

Neben den vom BSI empfohlenen Handlungen, wie Einsatz von Firewall, Virenscanner und Einspielung regelmäßiger Software-Updates sowie das sofortige Entfernen des Ausweises von Lesegerät nach Gebrauch, sollte auf jedenfall nur der Komfortleser verwendet werden, da dieser viele Angriffe durch die integrierte Tastatur vermeiden kann. Beim Kauf eines Lesers sollte darauf geachtet werden, das Lesegerät nur vom Hersteller direkt zu kaufen um Fälschungen zu vermeiden. Auch sollte die AusweisApp nur von Herausgeber selbst heruntergeladen werden. Öffentliche Terminals sollten aufgrund von Skimming-Attacken vermieden werden.

3 Nutzerstudie

Weil diese Arbeit eine Vorarbeit für die Master-Thesis ist, wird anhand einer Nutzerstudie evaluiert, wie es um die Nutzung des Personalausweises zukünftig steht. In der darauffolgenden Thesis werden verschiedene Möglichkeiten zur Identifizierung und zum Vertragsabschluss im Internet geprüft, wobei auch der nPA im Mittelpunkt stehen wird. Daher kam die Frage auf, inwiefern die eIDAS-Verordnung dabei helfen kann.

Wie in Kapitel 2 erwähnt, bietet eIDAS die Möglichkeit rechtssichere Verträge mithilfe der QES europaweit abzuschließen, da sie einen einheitlichen rechtlichen und organisatorischen Rahmen bietet [13].

Im Jahr 2010 begrüßten 52% der teilnehmenden Internet-Nutzer die Einführung des neuen Personalausweises [16].

Bei einer Umfrage zur geplanten Nutzung der Funktionen des nPA antworteten 52,2%, dass sie den Ausweis als Internetausweis und 45% für die elektronische Signatur möchten benutzen [10].

Fünf Jahre später (2015) hat das Marktforschungsunternehmens GFK festgestellt, dass nur ca. 30% die Onlinefunktion des nPA aktivieren ließen und nur ca. 5% die Onlinefunktion tatsächlich nutzen [9].

Vermutlich ist auch der Preis für ein teures Endgerät, wie den Komfortleser mit ca. 160€ (Stand Februar 2017), ein starkes Problem, wurden anfangs sogar Basis-Lesegeräte von den Bundesländern verschenkt, um die Nutzung voranzutreiben.

In einer Bitkom-Studie wurde 14+-jährigen Internet-Nutzern folgende Frage gestellt: „Wie viel Geld wären Sie bereit, für ein Personalausweis-Kartenlesegerät auszugeben, damit Sie Internet-Dienste nutzen können?“. Darauf antworteten 30%, mit „gratis“, 57%, „weniger als 50 Euro“ und gerade mal 5% mit „mehr als 50 Euro“ [18]. Allgemein gesehen betrachtet beginnt die Zahlungsbereitschaft für ein Lesegerät, bei Personen die älter als 30 Jahre sind.

3.1 Hypothesen

Die Nutzerzahlen zeigen ein ernüchterndes Ergebnis und es stellt sich die Frage, weshalb die Nutzer den Personalausweis so selten nutzen und wie die Nutzerzahlen verbessert werden können. Interessant ist auch, ob die neue eIDAS-Verordnung hilft, die Online-Funktion des Personalausweises bei den Bürgern beliebter zu machen. Dies führt zu folgenden Hypothesen.

3.1.1 Hypothese 1

„Wären die aktuellen Funktionen des elektronischen Personalausweises den Nutzern bekannt, würden Sie den Ausweis häufiger online verwenden."

3.1.2 Hypothese 2

„Durch die eIDAS-Gesetzesänderung wird der neue elektronische Personalausweis zukünftig häufiger online verwendet"

3.1.3 Hypothese 3

„Der sichere Komfortleser ist zu teuer, da die Nutzer wenig oder gar kein Geld für ein Lesegerät ausgeben möchten."

3.1.4 Hypothese 4

„Durch vielfach erweiterbare Anwendungsmöglichkeiten würden mehr Nutzer den Komfortleser verwenden."

3.2 Durchführung

Als Zielgruppe wird, wie bei vergleichbaren Studien, eine Stichprobe aus der Bevölkerung Deutschlands genommen. Größere Studien benutzen den Mikrozensus (Stichprobe mit ca. 1% der Bevölkerung), welchem die Daten des Statistischen Bundesamts zugrunde liegen. Die Stichprobe dieser Arbeit umfasst 60 Personen, aus unterschiedlichen Altersklassen und mit verschiedenem technischem Hintergrundwissen. Für 60 Teilnehmer entspricht die Verteilung der Bevölkerung, gemessen im Jahr 2015 [8], zwischen 14-29 Jahren 12,6 Personen (21,31%), 30-49 Jahren 20,4 Personen (34,06%), 50-64 Jahren 12,6 Personen (21,31%) und 65+ Jahren 13,8 Personen (23,31%). Natürlich kann diese Nutzerstudie nicht repräsentativ für alle Bundesbürger gelten aufgrund der begrenzten Teilnehmerzahl. Die Fragen der Nutzerstudie waren in vier Bereiche eingeteilt: allgemein, nPA, eIDAS + Kosten, Sicherheit und Mehrwert. Die Einteilung ist wichtig für den Umfrageverlauf da zum Einstieg einfache Fragen und zum Schluss sicherheitskritische Fragen gestellt wurden. Die Nutzerstudie hat sowohl in persönlichen Interviews als auch in einer Online-Befragung stattgefunden.

3.3 Ergebnis und Diskussion

70% der Befragten besitzen den neuen Personalausweis wovon 20% die Online-Funktion aktivieren ließen. Die Hauptgründe hierfür waren Neugierde, Kostenvermeidung durch nachträgliches Aktivieren und die Annahme, dass die Funktionen oft zu verwenden seien. Dies deckt sich nicht mit dem generellen Interesse der Bevölkerung gemessen im Einführungsjahr 2010 in der Befragung von Statista. 80% haben sich dagegen entschieden, da sie entweder kein Interesse hatten (30%), Sicherheitsbedenken äußerten (55%) oder die Funktionen nicht kannten (77%). Daher muss über die Funktionen deutlich besser aufgeklärt werden sofern die Nutzung der eID Funktionen vorangetrieben werden möchten. Jedoch konnten eine Aufklärung und ein konkretes Nachfragen in dieser Nutzerstudie kein gesteigertes Interesse aufzeigen. Daher konnte die erste Hypothese nicht eindeutig belegt werden.

Die Möglichkeit der Nutzung innerhalb der gesamten EU hat nur einen geringen Einfluss auf das zukünftige Verhalten. 29% würden dadurch die Online-Funktion häufiger nutzen und 77% entschieden sich dagegen. Daher konnte die zweite Hypothese ebenfalls nicht eindeutig belegt werden.

97% würden den Kauf des Komfortlesers ablehnen auch wenn sie durch eIDAS europaweit Verträge abschließen könnten. Hypothese drei wurde dadurch bestätigt und bekräftigt damit die Ergebnisse der Bitkom-Umfrage von 2010 zur Zahlungsbereitschaft der Kartenlesegeräte. Insbesondere junge Menschen, welche sich vorwiegend mit den neuen Technologien auseinandersetzen, möchten keinen oder nur einen geringen zusätzlichen Geldbetrag für ein Lesegerät aufbringen. Auch der Sicherheitsvorteil gegenüber günstigen Lesegeräten spielt hier keine Rolle.

Die vielfach erweiterbaren Nutzungsmöglichkeiten wie Datenabfrage der elektronischen Gesundheitskarte (Krankenkasse), Nutzung beim Online-Banking, Aufladung der Geldkarte und Personalausweis als Personennahverkehr-Ticket würden 67% der Teilnehmer nicht dazu überzeugen einen Komfortleser zu kaufen. Damit konnte Hypothese vier nicht bestätigt werden.

Allgemein ist festzuhalten, dass die Teilnehmer den Kosten-Nutzen-Faktor des teureren Komfortlesers schlecht einschätzen, insbesondere wenn im privaten Bereich die Online-Funktion sehr selten genutzt werden. Einige Teilnehmer schrieben, dass sie die zusätzliche Hardware wie das Lesegerät als unkomfortabel empfinden. Sie favorisieren eher eine Möglichkeit ohne zusätzliche Hardware.

Wenn die Nutzung des nPA vorangetrieben werden soll, müssen jedenfalls die Lesegeräte billiger werden, aber besser noch durch eine andere Technologie ersetzt werden, welche keine Lesegeräte voraussetzt, da die Nutzer die Verwendung zu unkomfortabel finden. Die eIDAS-Verordnung schafft hierbei die Voraussetzung in dem es die gesetzliche Grundlage dafür bietet. Zusätzlich könnten die Bürger mit Bonussen oder Rabatten gelockt werden falls die Verträge digital abgeschlossen würden.

Mitunter haben Hackangriffe auch eine gewisse Furcht oder Ablehnung bei den Bürgern verursacht. So wurde in einigen Ämtern der BRD den Nutzern empfohlen die Ausweisfunktion nicht freizuschalten nach Bekanntwerden diverser Gefahren für den Nutzer durch die einfachen Lesegeräte und einer Sicherheitslücke in der AusweisApp. Dies veranlasste die BSI dazu die AusweisApp für einige Zeit zur Verbesserung vom Download-Portal zu entfernen.

Dazu kommt das Problem, dass das Interesse der Wirtschaft gering bleibt, solange sich die Nutzerzahlen gering halten. Daher kommt die Entwicklung von Anwendungen für den nPA erst allmählich in die Gänge.

Den Mehrwert, den sich die Nutzer vom nPA wünschen sind: Integration anderer Ausweise wie Führerschein, Schwerbeschädigtenausweis, Zug- oder Busticket, Reisepass, Kreditkartenfunktion, Punkte in Flensburg abfragen, vereinfachte Altersverifizierung E-Mail Signaturen abseits von der DE-Mail, Gesundheitskarte, Bankkarte, Kreditkarte, Büchereiausweis, Jahreskarten für Freizeitaktivitäten.

Der Konsens lautet, dass solange nicht deutlich mehr elektronische Medien in einem Identifikationsmedium zusammengeführt werden, sind Teillösungen relativ unbedeutend. Hierbei ist Estland ein Vorreiter, welche als erste die eID-Funktion mit vielen weiteren Funktionen wie Online-Banking kombinierte und bereits seit 2005 Wahlen über das Internet ermöglicht.

Andere Nutzer möchten den nPA nur als Sichtausweis nutzen und wünschen daher eine Kostenreduzierung.

4 Literaturverzeichnis

[1] Sicherheitsmerkmale elektronsicher Personalausweis. Bundesdruckerei GmbH in Kooperation mit Bundesministerium des Innern, Berlin, 2014.

[2] Hier können Sie die Online-Ausweisfunktion nutzen. Webseite, 2017. https://www.personalausweisportal.de/DE/Buergerinnen- und-Buerger/Anwendungen/Anwendungen_node.html; abgerufen am 13.3.2017.

[3] Daten im Chip. Webseite, 2017. https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html; Besucht am 8.3.2017.

[4] eIDAS-Verordnung Nr. 910/2014 des europäischen Parlaments und des EU-Rates. EU-Kommission. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910; abgerufen am 13.3.2017.

[5] Bundesministerium des Innern - Chipkarten-Lesegeräte. Website, 2017. Online verfügbar unter https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/das-brauchen-Sie/Kartenlesegeraete/Kartenlesegeraete_node.html; Besucht am 28.2.2017.

[6] Bundesministerium des Innern – Daten auf dem Ausweis. Webseite, 2017. https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Details/DatenAusweis/datenAusweis_node.html; Besucht am 28.2.2017.

[7] Bundesministerium des Innern – Sicherheitsbedenken Personalausweis. Webseite, 2010. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2010/Sicherheitsbedenken_ Personalausweis_240810.html; abgerufen am 13.3.2017.

[8] Statista. Bevölkerung - Verteilung der Einwohner in Deutschland. Studie, 2015.

[9] K. Hilbinger, Frage des Monats Mai – Elektronischer Personalausweis - GFK Studie im Auftrag der WeltN24 GmbH, Nürnberg, 2015.

[10] Geplante Nutzung von Funktionen des neuen Personalausweises in Deutschland 2010; Webseite, 2010 https://de.statista.com/statistik/daten/studie/167117/umfrage/geplante-nutzung-von-funktionen-des-neuen-personalausweises/; Besucht am 28.2.2017.

[11] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-03127 - eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control - Elektronischer Personalausweis und elektronischer Aufenthaltstitel. Bonn, Version 1.16, 2015.

[12] J. Schejbal. AusweisApp gehackt (Malware über Autoupdate). Webseite, 2010. https://janschejbal.wordpress.com/2010/11/09/ausweisapp-gehackt-malware-uber-autoupdate/; abgerufen am 13.3.2017.

[13] eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste ,Bundesamt für Sicherheit in der Informationstechnik, Webseite, 2017. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html, abgerufen am 12.3.2017.

[14] J. Bender, M. Fischlin, D. Kügler. Security analysis of the pace key - agreement protocol. Bundesamt für Sicherheit in der Informationstechnik, Darmstadt, 2009.

[15] C. Eckert. IT-Sicherheit - Konzepte – Verfahren – Protokolle, Oldenbourg Wissenschaftsverlag GmbH, München, 2014.

[16] Statista. Begrüßen Sie die Einführung des neuen elektronischen Personalausweises?, Studie, 2010.

[17] J. Bender, D. Kügler, M. Margraf, I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. Datenschutz und Datensicherheit, Gabler Verlag, Wiesbaden, Ausgabe 03.2008.

[18] Bitkom. Zahlungsbereitschaft für Kartenlesegeräte. Studie, 2010.

[19] N. Kohnert und R. Stumpf. CCC Plusminus. WDR, Fernsehmagazin, Sendezeit: 24. August 2010 21:50–22:15. 2010.

[20] D. Oepen, F. Morgner. Die gesamte Technik ist sicher - Besitz und Wissen: Relay-Angriffe auf den neuen Personalausweis, Humboldt-Universität, Berlin, 2010.

Sicherheitsinfrastruktur in einem VANET – Architektur und Schwachstellen

Marc Roswag
Reutlingen University
Marc.roswag@Student.
Reutlingen-University.DE

Abstract
Das Ziel dieser Arbeit ist die Infrastruktur einer modernen Fahrzeug-zu-Fahrzeug Kommunikation auf ihre Sicherheit zu prüfen. Dazu werden die Sicherheitsstandards für die Funkkommunikation genauer beschrieben und anschließend mit möglichen Angriffsmodellen geprüft. Mit dem erläuterten Wissen der VANET Architektur werden verschiedene Angriffe verständlicher. Dadurch werden die Schwachstellen offengelegt und Gegenmaßnahmen an passenden Punkten in der Architektur verdeutlicht.

Schlüsselwörter
IT-Security, VANET, 802.11p, C2C, V2X

CR-Kategorien
B.4.1 Data Communications Devices, B.4.2 Input/Output Devices, D.4.6 Security and Protection, C.2.0 Security and protection

1 Einleitung

Betreuer Hochschule: Prof. Dr.-Ing. Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
13.03.2017 Hochschule Reutlingen

Das Fahrzeuge immer mehr über eine kabellose Verbindung in ein gemeinsames Netzwerk integriert werden sollen, ist in der Automobil Branche deutlich ersichtlich. Sobald ein Gerät kabellos in ein Netzwerk integriert wird, besteht eine deutlich höhere Gefährdung durch Cyber Angriffe auf ein solches Gerät. Die Motivation ein Fahrzeug über ein solches Netzwerk anzugreifen sind trivial. Es besteht durch das hohe Risiko, welches sich daraus ergibt, ein hoher Bedarf an Gegenmaßnahmen. Das dies bereits im Gange ist und auch durchaus nie mit Sicherheit vermieden werden kann zeigt der Angriff von den Sicherheitsforschern Charlie Miller und Chris Valasek, den es offenbar gelungen ist über ein Uconnect-Infotainmentsystem von Fiat Chrysler Kontrolle über das Internet von der Ferne aus über ein Fahrzeug gelangen konnten. [17] Es konnten sogar über den CAN-Bus das Bremsen und Beschleunigen des Fahrzeuges betätigt werden, ohne dass der Fahrer Einfluss darauf hatte. [17]

Für die Sicherheit eines solchen Netzwerkes haben sich sechs bedeutende europäische Automobilhersteller zusammengeschlossen, um einen Sicherheitsstandard für die Fahrzeug-zu-Fahrzeug Kommunikation zu bestimmen. Dieser Zusammenschluss nennt sich Car-to-Car Communication Consortium C2C CC. [13]

Im folgenden Abschnitt wird der Begriff V2X Kommunikation eingeführt und anhand dessen das Themengebiet VANET

verdeutlicht. Dabei wird auch auf die übertragenden Informationen eingegangen, um ein Verständnis darüber zu erlangen, wie wichtig die Sicherheit eines solchen Netzwerkes ist.

Anschließend wird der Standard 802.11p beschrieben, welcher speziell für VANETs konzipiert wurde. Dabei werden auch Sicherheitsstandards beschrieben.

In Kapitel 4 wird die Architektur mit allen wichtigen Komponenten in einem VANET beschrieben. Anhand dieser Komponenten wird der Ablauf des Systems offengelegt, um daran Schwachstellen der Architektur zu verdeutlichen.

Abschließend werden verschiedene bekannte Angriffe vorgestellt, welche ein VANET gefährden. Für diese Angriffe werden auch Schutzmaßnahmen angesprochen.

Abgeschlossen wird diese Arbeit mit einer kurzen Zusammenfassung der Fakten und einen Ausblick, welcher die Gegenmaßnahmen gegen einige Angriffe nochmals aufgreift.

2 V2X Kommunikation

V2X Kommunikation ist ein allgemeiner Begriff für den Austausch von Informationen zwischen Fahrzeugen selbst oder mit dessen Umgebung (Die Umgebung bildet sich aus der Architektur, welche in Kapitel 4 genauer beschrieben wird). V2X Kommunikation unterteilt sich in zwei Bereiche, welche in den folgenden Abschnitten genauer beschrieben werden. Zum einen geht es um den Austausch zwischen einem Fahrzeug und einer Infrastruktur (V2I), welche Straßenbaken [1] oder umliegenden Tankstellen und ähnliches bestehen kann. Diese senden einem Fahrzeug in der Nähe Informationen über den aktuellen Verkehrsstand und den Straßenzustand. Zum anderen gibt es den Bereich Fahrzeug-zu-Fahrzeug Kommunikation (V2V), bei welchem sich Fahrzeuge in der Nähe untereinander Informationen senden können. Bei dieser Technik verhält sich jedes Fahrzeug ähnlich wie ein Router, welcher Informationen entgegennehmen kann und diese auch weiterleiten kann. So können also auch Informationen über eine größere Distanz versendet werden, als es die Reichweite eines einzelnen Routers auf einer bestimmten Frequenz zulässt. [2]

2.1 V2I

Bei V2I Kommunikation, handelt es sich ausschließlich um den Nachrichtenaustausch zwischen einem Fahrzeug und einer statischen Instanz. Diese statischen Instanzen können am Straßenrand oder Tankstellen installierte Geräte sein, welche das Fahrzeug mit Informationen für den umliegenden Streckenbereich versorgen. [1] In dieser Arbeit wird jedoch der Schwerpunkt auf die im folgenden beschriebene V2V Kommunikation gelegt.

2.2 V2V

Es gibt für die Fahrzeug-zu-Fahrzeug Kommunikation viele ähnliche Abkürzungen, welche ähnliches oder sogar das gleiche bedeuten. Beispielsweise C2C (Car-to-Car) oder auch VANET, welches sich spezifischer auf die Technologie dahinter bezieht.[3]

2.2.1 Technische Probleme

V2V nutzt eine WLAN Technik, welche im Ad-Hoc Modus fungiert. Das bedeutet, dass dabei Daten direkt zwischen den Clients übertragen werden. Alle Clients sind dabei gleichberechtigt und können ohne Umwege mit einander kommunizieren. Direkt bedeutet in diesem Sinne ohne über einen Router bzw. Access-Point als Nachrichtenübermittler Daten auszutauschen. [4] Vergleicht man jedoch ein V2V Ad-Hoc Netzwerk mit einem alltäglichen WLAN, welches im Ad-Hoc Modus ohne zusätzliche Infrastruktur agiert, gibt es entscheidende Unterschiede.

Die herausstechenden Anforderungen an das Ad-Hoc Netzwerk bei V2V sind kurz gesagt die folgenden:

- Schnell wechselnde Kommunikationspartner
- Stark schwankende Kommunikationsdichte
- Schneller Informationsaustausch ohne Verzögerung
- Sicherheit

Bei der Fahrzeug-zu-Fahrzeug Kommunikation wechseln beispielsweise die Kommunikationspartner ständig. Nachdem ein Fahrzeug an einer Kreuzung abbiegt, wechseln Kommunikationspartner sehr schnell. Hinzu kommt, dass die stark wechselnde Anzahl an Kommunikationspartnern und die dabei entstehenden Nachrichten. Auf einer Autobahn mit viel Verkehr und sehr vielen weiteren Fahrzeugen, wird es viel Kommunikation geben, welche redundante Informationen beinhalten und die zur Verfügung stehenden Kanäle belegen. Dagegen kann es auch sein, dass bei Nacht auf einer großen Straße keine Kommunikationspartner vorhanden sein können. Zusammenfassend lässt sich feststellen, dass eine stark schwankende Kommunikationsdichte eine Herausforderung an das Ad-Hoc Netzwerk bei der V2V Kommunikation darstellt. [3] Außerdem wird eine Anforderung sein, dass Informationen ohne Verzögerungen übertragen werden. Bei großen Geschwindigkeiten beim aneinander Vorbeifahren auf einer Autobahn in entgegengesetzter Richtung müssen Informationen schnell ausgetauscht werden können. [1,3]

2.2.2 Sicherheitsaspekte

Ein weiterer sehr relevanter Aspekt und Großteil in dieser Ausarbeitung ist die IT-Sicherheit bei einer V2X Kommunikation. Die Sicherheit zielt in diesem Feld weniger auf die Verschlüsselung von Daten hin, welches im Normalfall bei IT-Sicherheit eine große Rolle spielt und als *Confidentiality* bekannt ist, sondern viel mehr auf die Zuverlässigkeit, Echtheit von Daten und die Anonymität der Fahrer. Dafür werden in der IT-Sicherheit allgemein die Begriffe *Integrity*, für eine unveränderliche Nachricht und *Authority*, für das Authentifizieren eines Netzwerkteilnehmers verwendet. Es werden Sicherheitsmechanismen eingesetzt, welche verhindern sollen, dass gefälschte Warnnachrichten versendet werden können. Durch eine solche Manipulation des Systems wird die Sicherheit, worauf V2X hinzielt, viel mehr gefährdet als geschaffen. [1]

3 Der 802.11p Standard für V2X Kommunikation

Für die Architektur eines VANET, hat das Institute of Electrical and Electronics Engineers IEEE einen neuen Standard für 802.11 Wireless Verbindungen definiert. Dieser Standard nennt sich 802.11p. Für diesen Standard wird die Dedicated Short Range Communication DSRC verwendet, welche für eine Kommunikation auf kurze Reichweiten und sehr geringe Latenzzeiten verantwortlich ist. [8]

Dafür wurde ein Frequenzband im 5,9 GHz Spektrum reserviert. USA hat ein 75 MHz Band (von 5,850 GHz – 5,925 GHz) dafür vorgesehen und Europa ein 30 MHz Band. [16] In folgender Abbildung ist zu erkennen, dass Europa das Frequenzband in dem höheren Frequenzbereich erweitern kann bei Bedarf. Der Frequenzraum ist in 7 Kanäle unterteilt. [2]

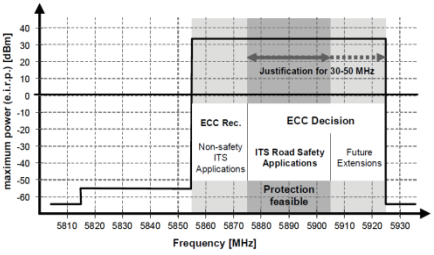

Abbildung 1: Genutzer Frequenzbereich für 802.11p in Europa [2]

Die Arbeitsgruppe 802.11p ist aus den Aktivitäten von 802.11a und 802.11g entstanden und nutzt die hohe Datenrate von 54 Mbit/s für die Fahrzeugkommunikation. Mit der 802.11p-Technik wird eine zuverlässige Schnittstelle für intelligente Transportsysteme (ITS) etabliert.

Die Randbedingungen für diesen Standard sehen eine Fahrgeschwindigkeit von bis zu 200 km/h, einen Entfernungsbereich von 1 km und eine Datentransferrate zwischen 4 ms und 50 ms und eine äußerst geringe Latenzzeit von 4 ms vor. [2]

Für den 802.11p Standard ist das Widerrufen von Zertifikaten eine Kernfunktion, um die Sicherheit zu gewährleisten. [13] In folgender Abbildung ist die Sicherheitsinfrastruktur beschrieben. Dabei ist A der Sender und B der Empfänger.

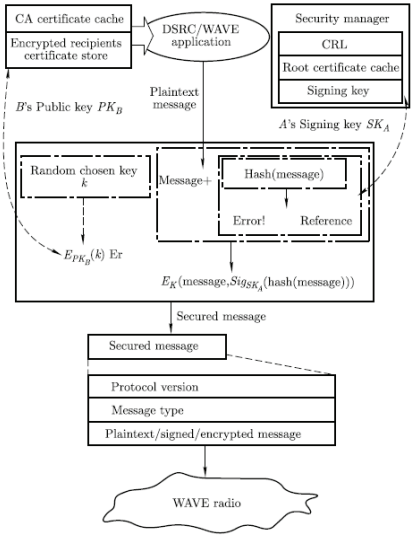

Abbildung 2: Sicherheitsinfrastruktur nach dem 802.11p Standard [13]

Es ist zu erkennen, dass es einen Zertifikatspeicher gibt, welches mit dem PK_b verschlüsselt wird. Dieses wird zusammen mit der eigentlichen Nachricht mit Hilfe einer Hashfunktion zusammen in ein Paket verpackt und dann als sichere Nachricht versendet. Daraus entsteht eine WAVE-Nachricht. So ist die Nachricht am Ende durch das Zertifikat und den öffentlichen Schlüssel signiert und verschlüsselt.

4 VANET

VANET (engl. Vehicular ad-hoc network) ist ein wichtiges Thema im Bereich der V2V Kommunikation. Es handelt sich dabei um ein eine besondere Form von MANET (engl. Mobile ad-hoc network), welches jedoch eigene technische Ansprüche stellt, wegen der bereits erwähnten technischen Anforderungen bei V2V Kommunikation aus Kapitel 2.2. [6] Da es sich bei VANET um ein Ad-Hoc Netz handelt, lässt sich sagen, dass ohne eine feste Infrastruktur zwischen den Fahrzeugen kommuniziert wird. Es bilden sich dynamische vermaschte Netze, zwischen denen Nachrichten entweder Broadcast oder Multicast gesendet werden können. [4] Bei Broadcast Nachrichten, ist allgemein zu beachten, dass es für einen Angreifer erstmal möglich ist diese Nachrichten abzufangen. Dies wird bei einigen Angriffen aus Kapitel 5 ausgenutzt.

4.1 Architektur

Die allgemeine Architektur für die V2V Kommunikation wurde vom „Car 2 Car Communication Consortium“ vorgeschlagen. Bei der Architektur wird zwischen 3 Kommunikationsbereichen Unterschieden. [4]

- Inter-vehicle communication
- Vehicle-to-roadside communication
- Inter-roadside comunication

Der erste Bereich „Inter-vehicle communication“ bezeichnet die Kommunikation zwischen den Fahrzeugen. De zweite Bereich „Vehicle-to-Roadside“ bezeichnet die Kommunikation zwischen Fahrzeug und den Straßenbaken. Der Dritte Bereich „Inter-roadside communication“

bezeichnet die Kommunikation zwischen den Straßenbaken selbst. [6]

Die Infrastruktur am Straßenrand, wie es hauptsächlich in den USA und Japan genutzt wird [3], werden als sogenannte RSUs (engl. road-side unit) bereitgestellt. [6] Das C2C CC gibt auch die vorausgesetzte Hardware in einem Fahrzeug vor. Es wird erwartet, dass jedes Fahrzeug über eine OBU (engl. On-board unit) und eine AU (engl. application unit) besitzt. [6] Die folgende Abbildung 4 zeigt die daraus entstehende Architektur für VANETs.

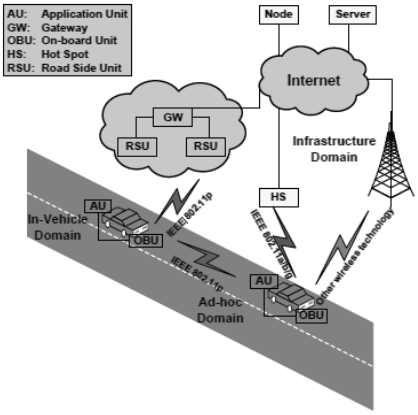

Abbildung 3: VANET Architektur nach den Vorgaben von C2C CC [6]

4.1.1 Die Road-Side Unit

RSUs sind Geräte, welche an festen Positionen am Fahrbahnrand befestigt sind. Im Laufe dieser Arbeit wurde diese bereits als Straßenbaken bezeichnet. Sie enthalten mindestens eine Kommunikationseinheit, um die Kommunikation mit Fahrzeugen (der OBU) oder anderen RSU ermöglicht. RSUs bilden die Infrastruktur für ein VANET Netzwerk. [6] Zusätzlich zu der Kommunikationseinheit, welche für den Datenaustausch mit Fahrzeugen und umliegenden RSUs zuständig ist, haben RSUs weitere Kommunikationseinheiten installiert, welche, wie in Abbildung 3 zuerkennen, über das Internet die Infrastruktur für den Informationsaustausch erweitern.

4.1.2 Die On-Board Unit

Jedes Fahrzeug empfängt und sendet Nachrichten über die On-Board Unit (OBU). [7] Diese Sendeleistung dieser OBU ist so dimensioniert, dass sie über kurze Reichweiten schnell eine hohe Datenrate übertragen kann. Diese basiert auf dem 802.11p Standard, welche in einem hohen Frequenzbereich Daten überträgt. Durch diese Eigenschaft, wird die V2V Kommunikation zu einem hochdynamischen mobilen Ad Hoc Netzwerk (VANET), welches kleine Cluster von Fahrzeugen erzeugt, die wiederum miteinander kommunizieren können. [10]

Die Forschung beabsichtigt OBUs auf einen Authentifizierungsplan basierend zu konstruieren, bei welchem die Fahrzeuge selbst zertifizierende Schlüsselpaare erzeugen.[7] Ein Schlüsselpaar besteht wie bei asymmetrischen Kryptoverfahren üblich aus einem öffentlichen und einem privaten Schlüssel. Die selbst Zertifizierung soll mit Hilfe eines Prüfwertes bei der *Trusted Authority* TA initialisiert und geprüft werden bei der Registrierung in ein VANET. [7] TAs gehören wie RSUs zu den statischen Komponenten in einem VANET. Das heißt sie sind festinstallierte Geräte am Straßenrand. Der Prüfwert wird durch eine Einweg-Hashfunktion berechnet. Dieser Wert wird darauf hin an mehrere Fahrzeuge in der Umgebung gesendet, damit diese Nachrichten ebenfalls überprüfen können. [7]

4.1.3. Die Application Unit

Application Units (AUs) können sich als einfach Anwendungen definieren lassen, welche mit der OBU kommunizieren und darüber die eigentliche Kommunikation bei VANET einleiten. [9] AUs lassen sich in zwei Kategorien unterteilen. Zum einen die Unterhaltungsanwendungen, welche beispielsweise das Chatten mit umliegenden Fahrzeugen erlauben.[6] Wichtiger für diese Arbeit ist jedoch die andere Kategorie,

welche sich auf die sicherheitsrelevanten Anwendungen bezieht. [6]Diese überwachen den Datenverkehr. Beispielsweise welche Daten vertraulich sind und auch welche Datenrelevant sind, um das VANET nicht zu überlasten.

Außerdem kann man auch unterscheiden zwischen festinstallierten AUs und portable AUs. Sicherheitsrelevante AUs sind oft auch festinstalliert. Die Architektur gibt jedoch auch die Möglichkeit, Geräte über eine drahtlose Verbindung mit der OBU zu verbinden. Das können zum Beispiel Smartphones sein. [6] AUs haben zum einen die Möglichkeit die Kommunikation über das VANET zu nutzen, können jedoch auch auf viele Sensoren wie GPS, welche ein Fahrzeug zur Verfügung stellt, zugreifen. [6] An dieser Stelle ist bereits zu erkennen, dass die Sicherheit nicht unterschätzt werden sollte, da über diesen Eingang schnell in das System eingedrungen werden kann. Die Anzahl an AUs, welche einem Fahrzeug hinzugefügt werden können ist derzeit noch nicht beschränkt. [6]

Bei der V2X Kommunikation sind schon verschiedene Anwendungen in Überlegung. Besonders für den sicherheitsrelevanten Bereich, welcher durch V2X erreicht werden soll. Dazu gehören Anwendungen, welche V2V Kommunikation nutzen, um Fahrzeuge zu warnen vor Unfallstellen oder auch die Verbindung mit einem Rettungswagen, welcher seine Route an umliegende Fahrzeuge weitergibt, damit eine Rettungsschleuse schnell entstehen kann. [6] Außerdem soll auch die V2I Kommunikation für Rettungseinsätze genutzt werden, damit ein Rettungswagen eine Ampelschaltung beeinflussen kann, so dass dieser schneller und sicherer zu einem Unfallort gelangen kann. [6] Auch an dieser Stelle, ist die bösartige Absicht eines Angreifers keineswegs auszuschließen und es muss in einem VANET durch entsprechende Sicherheitsmaßnahmen entgegengewirkt werden.

4.1.4 Sicherheitskomponenten

Event Data Recorder EDR:

Die EDR ist vergleichbar mit einer Black-Box in einem Flugzeug, welche für das mitschreiben von Daten während der Fahrt verantwortlich ist. Es werden hier Daten gespeichert wie beispielsweise GPS Daten, Geschwindigkeit, Zeit und empfangene Nachrichten. Dies hilft besonders bei der Nachprüfung bei einem Unfall. [11]

Trusted Component TC oder auch Tramper Proof Device TPD:

Die TC ist für den Schutz der kryptografischen Materialien verantwortlich. Es handelt sich hierbei um eine Hardware, welche Schlüssel speichert und Verschlüsselungsoperationen ausführt. [11] Diese Hardware nutzt eine eigene Stromversorgung, welche sich gelegentlich mit Hilfe der Fahrzeugelektronik wieder auflädt. [7] In dieser wird auch ein sogenanntes *Wurzelzertifikat* des Landes gespeichert, bei der Herstellung eines Fahrzeuges. [18]

Electronic Licence Plate ELP:

Bei ELP handelt es sich um eine elektronische Lizenz, welche ähnlich wie das Nummernschild eines Fahrzeuges für die einzigartige Identität eines Fahrzeug steht. So kann bei einem Diebstahl geprüft werden, ob es sich um das korrekte Auto handelt. [12]

Vehicular Public Key Infrastructure VPKI:

Es gibt eine sehr große Anzahl an Fahrzeugen, welche aus verschiedenen Ländern und Regionen kommen und weite Strecken zurücklegen. Dabei ist ein robustes, internationales und skalierbares Schlüssel-Management sehr wichtig. VPKI steht für eine solche Infrastruktur, welche sich aus den verschiedenen Trustet Authoritys TAs und den Fahrzeugen bildet. TAs können hierbei auch durch zertifizierte Fahrzeuge bereitgestellt werden. [7]

Authentification:

Um das Einmischen von Dritten in den Datenverkehr oder gefälschten Daten im Netzwerk vorzubeugen, ist eine Authentifizierung der Pakete erforderlich, bei der sich der Sender in gewisser Hinsicht ausweißt. Bei V2X Kommunikation wird hier für derzeit das *elliptic curve cryptography EEC* Verfahren verwendet. [11] Dies ist ein sehr komplexes asymmetrisches Kryptoverfahren, welches der Nachfolger des *Rivest, Shamir and Adleman RSA* Verfahrens darstellt. Bei asymmetrischen Verschlüsselungsverfahren entsteht durch die Komplexität der Berechnungsfunktionen ein hoher Grad an Overhead. Dies könnte weiterhin reduziert werden, in dem nur kritische Nachrichten signiert werden. [7]

Privatsphäre:

Privatsphäre ist ein wichtiger Faktor für die Akzeptanz von VANETS bei der Bevölkerung und ist demnach auch für den Erfolg und die Durchsetzung sehr relevant. Die Gefährdung der Geheimhaltung wird besonders durch den großen Overhead und dem Datenverkehr zwischen den Fahrzeugen beeinflusst. Dabei werden Informationen über die Zeit, der Position und der Identität übermittelt, welche präzise den Sender ermitteln lassen. [13] Es ist jedoch für die Authentifizierung Voraussetzung, dass sich ein Teilnehmer in einem Netzwerk identifizieren kann um autorisiert zu werden. Ein Nummernschild an einem Fahrzeug ist gewissermaßen nichts anderes als die Identität eines Fahrzeuges. Man kann bei der Identität zwischen Personen gebundener Identität und Fahrzeug gebundener Identität unterscheiden. [14,15] Es ist in einem VANET sinnvoll, ein Fahrzeug von dem falsche Nachrichten ausgehen zu identifizieren, da der Fahrer nicht in jedem Fall dafür verantwortlich ist. Es können Fehler in der Software vorliegen, durch Implementierungsfehler oder durch absichtliche bösartige Manipulation von Dritte. Für die Identifizierung eines Fahrzeugs kann in der Nachricht einfach gehalten die ELP mitgesendet werden.

Die Gesetzeslage steht jedoch derzeit dem gegenüber und macht grundsätzlich den Fahrzeughalter für derartige bösartige Gefährdung des Straßenverkehres verantwortlich. (§7 StVG) [14]

Sichere Positionierung:

Ein Fahrzeug könnte eine gefälschte GPS Position senden, um beispielsweise in einem Haftungsfall zu flüchten oder benachbarte Fahrzeuge zu täuschen. Dafür ist eine Prüfung der Positionsdaten durch mehrere Instanzen notwendig. [7] Es wird die Position von mehreren Fahrzeugen geprüft, welche sich in der Nähe des betroffenen Fahrzeuges befinden. Dies wird außerdem von einer Basis-Station vorgenommen. [7]

4.1.5 CA – Zertifizierungsinstanz

Als zentrale und vertrauenswürdige Instanz für die Erstellung von Zertifikaten, ist die CA verantwortlich. Von dieser Instanz werden VANET-Identitäten als gültige Netzwerkteilnehmer zertifiziert. Dafür sendet ein Teilnehmer Informationen zur seiner Identität an die CA, welche diese mit ihrem privaten Schlüssel verschlüsselt und so eine Identität zertifiziert. Die CA sollte daher einen sehr hohen Grad an Sicherheit genießen, da der private Schlüssel einer solchen Instanz ein primäres Ziel eines Angreifers ist. Wenn ein Angreifer diesen Schlüssel bekommen würde, könnte dieser selbst Zertifikate erstellen, welche nicht von echten Zertifikaten zu unterscheiden wären. [15] Zudem wird eine CA-Hierarchie gebildet, in welcher sich CAs gegenseitig Zertifizieren können.

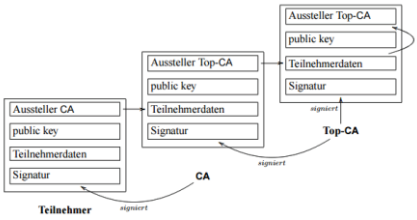

Abbildung 4 Zertifizierung- Hierarchie [15]

5 Angriffe auf ein VANET

Sobald ein Risikomanagement im Bereich Verkehrskommunikation über VANET zum Einsatz kommt, wird schnell deutlich, dass es einen sehr hohen Bedarf an Gegenmaßnahmen vor Angriffen verlangt. Dies ergibt sich aus einmal dem Grad der Wahrscheinlichkeit, dass es potenzielle Angreifer gibt und die Auswirkungen, welche dadurch entstehen können. Dass die Motivation von Angreifern in diesem Bereich gegeben ist, wurde bereits zu Beginn dieser Arbeit gezeigt. Auch die Auswirkungen sind teilweise vorgestellt worden. Verkehrsteilnehmer können statt unterstützt, verwirrt werden durch falsche Nachrichten. Dadurch würde sich das Risiko für einen Unfall stark erhöhen. Die genaue Auswirkung, müsste im Einzelfall betrachtet werden. Es muss dabei die Art eines Angriffes klar sein. Im Folgenden werden einige verschiedene Angriffsmöglichkeiten vorgestellt und die Auswirkungen und mögliche Gegenmaßnahmen untersucht.

- Eavesdropping / Sniffing

Bei Eavesdropping oder auch Sniffing handelt es sich um das Abhören von Datenpaketen. Dies ist nur Hilfreich für den Angreifer, wenn die Pakete unverschlüsselt sind. Diese Art von Angiffen ist auch für Angreifer mit wenig Knowhow und Ressourcen einfach durchzuführen. In Erinnerung an Kapitel 4.1.4 im Abschnitt Authentifikation, wird klar, dass dieser Angriff durch die Verschlüsselung mit einem modernen asymmetrischen Verfahren verhindert wird.

- Spoofing / Masquerading

Bei diesem Angriff versucht ein Angreifer die Identität eines anderen Netzteilnehmers anzunehmen oder zumindest seine eigene Identität zu fälschen. Der Angreifer muss dafür seine Hardware Adresse ändern können. Die Quelladeresse einer Nachricht sollte in einem VANET ebenfalls auf ihre Korrektheit und Gültigkeit geprüft werden.

- Replay Attack

Hierbei wird eine Nachricht kopiert und wiederholt gesendet, um eine gültige Signatur nachzuahmen. Mit Hilfe von Zufallszahlen in einem Paket (Nonces) kann ein solcher Angriff unterbunden werden.

- Cheating with positioning information

Der Angreifer versucht seine GPS-Informationen zu fälschen. Auch hier sollten Nachrichten verglichen werden und so auf ihre Korrektheit überprüft werden. [15]

- Movement patterns

Bei dieser Art von Angriff, versucht der Angreifer nach mehrmaligem Abhören von Nachrichten und dessen Position ein Bewegungsmodell eines oder mehrerer Teilnehmer zu erstellen. Hierbei sollte das Abhören der Nachrichten unterbunden werden. Auch die Quelladresse sollte verschlüsselt sein. [15]

- Denial of service

Einer der bekanntesten und oft auch effektivsten Angriffe. Hier bei versucht ein oder mehrere Angreifer sehr viele Nachrichten in das Netz einzuschleusen, um das System außerbetrieb zu nehmen. Nachrichten von anderen Teilnehmern werden durch Nachrichtenstau blockiert oder Router (Fahrzeuge) durch den Nachrichtenstau überlastet. Es ist schwierig sich von dieser Art von Angriffen effektiv zu schützen, jedoch gibt es verschiedene Ansätze. Einer wäre, frühzeitig ungewöhnliches Verhalten von Netzteilnehmern zu entdecken und Nachrichten von diesen Teilnehmern sofort zu verwerfen bzw. zu blockieren. [6]

- Sinkhole Attackes /selective forwarding

Hierbei werden vereinzelnd Pakete verworfen, um ein gezieltes Verhalten eines Verkehrsteilnehmers zu erzeugen oder zu unterbinden. Möglich ist dies beispielsweise durch einen Man-in-the-Middle Angriff. Dies ist in einem Ad-Hoc Netzwerk wie ein VANET, jedoch nur schwer möglich, da Nachrichten auf direktem Wege gesendet werden. Es müssten dafür die Routing-Tabelle eines Netzwerkteilnehmers manipuliert werden, was durch

entsprechende Gegenmaßnahmen zu unterbinden ist.[15]

- Sybil attackes

Bei diesem Angriff versucht ein Angreifer mehrere Netzwerkteilnehmer zu erstellen, um dadurch die Kooperation zwischen den Netzwerkteilnehmern zu untergraben. Dies ist durch Identitätsüberprüfung bei der Registrierung in ein VANET zu unterbinden. Es sollten hier nur gültige Teilnehmer zugelassen werden. [15]

- Worm hole

Dieser Angriff ist nach dem Prinzip eines Wurmloches zwischen zwei Galaxien aufgebaut. Zwei Angreifer arbeiten dabei zusammen und versuchen Nachrichten von Netzteilnehmern zu kopieren und an einem anderen Ort im Netz einzuspeisen. Beispielsweise steht Angreifer 1 in einem Stau und sendet alle Nachrichten weiter an Angreifer 2, welcher sich weit weg auf einer wenig befahrenden Straße befindet. Angreifer 2 speist die Nachriten in seinem Gebiet ein, um so falsch Informationen zu verbreiten - *Bogus Information*. [vgl. 18]

Anhand dieser Angriffe erkennt man, dass ein Großteil durch die Verschlüsselung der beschriebenen PKI unterbunden wird. Die gesamte Infrastruktur eines VANET sollte für die IT-Sicherheit jedoch noch einige weitere Sicherheitsmechanismen aktivieren, um einen hohen Grad an Sicherheit zu gewährleisten. Durch die Verhaltensanalyse von Netzwerkteilnehmern können Angriffe frühzeitig erkannt werden und entsprechende Gegenmaßnahmen *(siehe Kapitel 4 – sichere Positionierung)* eingeleitet werden.

6 Literaturverzeichnis

[1] Robert K. Schmidt, Tim Leinmüller, Bert Böddeker, V2X Communication https://www.tu-ilmenau.de/fileadmin/media/telematik/schmidt/080718_V2X-Kommunikation.pdf, 2008, letzter Zugriff: 27.02.2017

[2] Andreas Lübke, The current status of Car-to-X communication, Volkswagen AG, Wolfsburg, Deutschland, https://www.hs-osnabrueck.de/fileadmin/HSOS/Homepages/Personalhomepages/Personalhomepages-IuI/luebke/VDE_2008_Luebke_Paper.pdf, 2008, letzter Zugriff: 27.02.2017

[3] Benjamin Schinzel, V2V Vehicle-to-Vehicle Communication, https://www.cs.hs-rm.de/~linn/fachsem0809/V2V_Komm/V2V_Fachseminar_Schinzel.pdf, Fachhochschule Wiesbaden, 2009, letzter Zugriff: 15.02.2017

[4] Jogendra Majhi, Optimized Collision Warning Protocol in VANET, http://ethesis.nitrkl.ac.in/6800/1/Optimized_Majhi_2015.pdf, 2015, letzter Zugriff: 06.03.2017

[5] Michael Meincke, Peter Tondl, María Dolores Pérez Guirao, Klaus Jobmann, Wireless Adhoc Networks for Inter-Vehicle Communication https://www.ikt.uni-hannover.de/uploads/tx_tkpublikationen/MTP2002.pdf, 2002, letzter Zugriff: 08.03.2017

[6] Lars Klein, Herausforderungen in Fahrzeug-Ad-hoc Netzwerken, Communciation and Networked Systems (ComSys), https://www.uni-muenster.de/imperia/md/content/comsys/lehre/ws1516/seminar/klein-kfzfunkkommunikation.pdf, Institute of Computer Science, 2016, letzter Zugriff: 23.02.2017

[7] Saroj Kumar Biswal, On Board Unit Based Authentication for V2V Communication in VANET, http://ethesis.nitrkl.ac.in/6244/1/E-8.pdf, Department of Computer Science and Engineering National

Institute of Technology, 2014, letzter Zugriff: 27.02.2017

[8] D. Jiang and L. Delgrossi, Towards an International Standard for Wireless Access in Vehicular Environments," in Vehicular Technology Conference, "IEEE 802.11p, 2008. VTC Spring 2008. IEEE, ISBN: 978-1-4244-1644-8

[9] Mrunmayi S Sahasrabudhe, Meenu Chawla, Survey of Applications based on Vehicular Ad-Hoc Network (VANET) Framework, ISSN: 0975-9646 https://pdfs.semanticscholar.org/ff5b/25e0ab35547460118fd53bd3af1ab9ecce23.pdf, 2014, letzter Zugriff: 08.04.2017

[10] Bernhard Wiegel, Quality of Service in Fahrzeug-Fahrzeug-Netzen – dezentrale und schichtübergreifende Steuerung des Nachrichtenaufkommens, https://oparu.uni-ulm.de/xmlui/bitstream/handle/123456789/2553/vts_8887_13294.pdf?sequence=1&isAllowed=y, 2013, letzter Zugriff: 03.03.2017

[11] Raya Maxim, Panos Papadimitratos, and Jean-Pierre Hubaux. "Securing vehicular communications." IEEE Wireless Communications 13, no. 5, 2006

[12] Raya Maxim, Daniel Jungels, Panos Papadimitratos, Imad Aad, and Jean-Pierre Hubaux. "Certificate revocation in vehicular networks." Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland, 2006

[13] Weidong, Security in Vehicular Ad Hoc Networks (VANETs), https://www.researchgate.net/file.PostFileLoader.html%3Fid%3D55b40f1c5e9d9748938b457d%26assetKey%3DAS%253A273819204292614%254014422,94993693+&cd=1&hl=de&ct=clnk&gl=de, 2013

[14] Klaus Plößl, Hannes Federath, Vorschlag für eine Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks, http://svs.informatik.uni-hamburg.de/publications/2006/PlFe2006AutomotiveVanetSecInfra.pdf, Universität Regensburg, 2006

[15] Manuel Reil, Entwurf einer Sicherheitsinfrastruktur für Vehicular Ad-hoc Networks (VANETs), http://manuel.reil.co/Sicherheitsinfrastruktur_vanet.pdf, 2006, letzter Zugriff: 27.03.2017

[16] Ram Shringar Raw , Manish Kumar , Nanhay Singh, Security challenges, issues and their solutions for VANET, http://airccse.org/journal/nsa/5513nsa08.pdf, 2013, letzter Zugriff: 25.02.2017

[17] Ronals Eikenberg, Hacker steuern Jeep Cherokee fern, Heise Security, https://heise.de/-2756331, 2015, letzter Zugriff: 05.04.2017

[18] Ram Shringar Raw , Manish Kumar, Nanhay Singh, Security challanges, issues and their solutions for VANET, http://airccse.org/journal/nsa/5513nsa08.pdf , 2013, letzter Zugriff: 26.02.2017

IT-Sicherheit in der Industrie 4.0

Mücahit Karabulut
Reutlingen University
Muecahit.Karabulut@Student.
Reutlingen-University.DE

Abstract
Durch Industrie 4.0 kann die individuelle Fertigung von kleineren Stückzahlen zu geringen Kosten ermöglicht werden. Dafür müssen alle Anlagen miteinander vernetzt werden, um Daten austauschen und kommunizieren zu können. Durch die Vernetzung können neue Risiken und Gefahren entstehen. In dieser Arbeit wird die IT-Sicherheit in der Industrie 4.0 anhand möglichen Bedrohungsszenarien,
Herausforderungen und Gegenmaßnahmen evaluiert. Dabei wird untersucht, welche Möglichkeiten Industrieunternehmen haben, um Hackerangriffen vorzubeugen und ob bereits etablierte Sicherheitskonzepte für industrielle Anlagen einfach übernommen werden können.

Schlüsselwörter
Industrie 4.0, IT-Sicherheit, Industrial Control System (ICS)

CR-Kategorien
J. [COMPUTER APPLICATIONS], J.7 [COMPUTERS IN OTHER SYSTEMS]: Industrial control. K. [Computing Milieux], K.6 [MANAGEMENT OF COMPUTING AND INFORMATIONS SYSTEMS], K.6.5 [Security and Protection]: Authentication, Unauthorized access.

1 Einleitung
Die vierte industrielle Revolution wird auch Industrie 4.0 genannt und wird durch den Einzug des Internets in die Produktion gekennzeichnet. Bei Industrie 4.0 steht nicht der Computer, sondern das Internet als zentrale Technologie im Vordergrund. Dies ermöglicht durch Sensoren, Werkstücke und Produktionsmittel digital miteinander zu verknüpfen, sodass jedes Element miteinander kommunizieren und permanent Informationen über den Produktionsstand austauschen kann. Diese Vernetzung durch das Internet bringt jedoch viele Gefahren mit, aufgrund der durch die Vernetzung entstehenden Angriffsmöglichkeiten. In den folgenden Kapiteln werden Maßnahmen für Industrieunternehmen beschrieben, wodurch sich Unternehmen gegen einen Hacker-Angriff absichern können.

1.1 Ziel der Arbeit
Ziel der Arbeit ist es herauszufinden, ob für industrielle Anlagen bereits etablierte Sicherheitskonzepte übernommen werden können und welche Möglichkeiten Industrieunternehmen haben, um sich gegen Risiken und Bedrohungen abzusichern.

1.2 Aufbau der Arbeit
In **Kapitel 2** werden die vier industriellen Revolutionen vorgestellt. Danach werden

Betreuer Hochschule: Prof. Dr.-Ing. Michael Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

die Schutzziele der IT-Sicherheit, die Top 5 Bedrohungen der ICS (Industrial Control System) und bereits bekannte Vorfälle vorgestellt. In **Kapitel 3** erfolgt ein Praxisbeispiel der Industrie 4.0. **Kapitel 4** stellt die Ergebnisse dar. Die Arbeit wird mit **Kapitel 5** der Schlussbetrachtung abgeschlossen.

2 Von Industrie 1.0 bis Industrie 4.0

Mit der ersten Massenproduktion durch Maschinen, startete circa 1800 die Industrie 1.0. Wie in der Abbildung 1 zu sehen ist, wurden hier Webstühle noch durch menschliche Kraft betrieben [2].

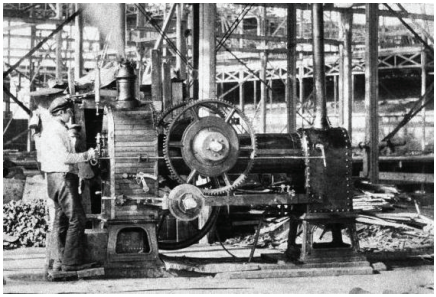

Abbildung 1: Industrie 1.0 [1]

Ende des 19. Jahrhunderts begann durch die Einführung der Elektrizität als Antriebskraft die 2. industrielle Revolution. Durch Motoren konnte die Arbeit weitgehend automatisiert werden. Außerdem konnten bestimmte Prozesse beschleunigt werden durch Telekomunikation mit Telefon und Telegramm [2]. Die 3. industrielle Revolution begann etwa ab 1970, welches den Fokus auf die Automatisierung durch Elektronik und IT legte [2]. Die ersten programmierbaren Steuerungen kamen auf den Markt, was dazu führte, dass Informatiker als Programmierer in den Fabriken gefragt waren.

Die 4. industrielle Revolution startete Ende des 20.Jahrhunderts. Industrie 4.0 wird durch die Individualisierung und Hybridisierung der Produkte ausgezeichnet [3]. Ein weiterer Kernpunkt ist die Integration von Kunden in Geschäftsprozesse [3]. Durch Industrie 4.0 sollen alle Maschinen vernetzt werden, um permanent Informationen austauschen zu können und den Fertigungsprozess zu observieren. In der Abbildung 4 ist das Modell „Yumi“ [4] zu sehen, welcher nicht mehr hinter Sicherheitszäunen, sondern gemeinsam mit den Mitarbeitern produziert und Hilfestellung in Prozessen leistet, die für den Menschen recht mühsam sind [4].

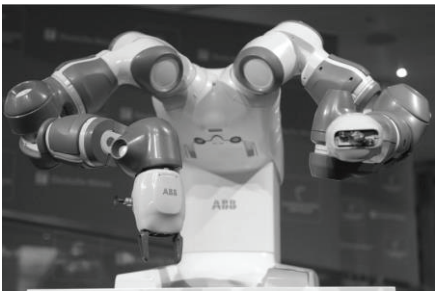

Abbildung 2: Industrie 4.0 - Interaktiver Roboter "Yumi" [2]

2.1 Industrial Control System

Als Industrial Control System (Industrielle Steuerungsanlagen, ICS) werden Systeme bezeichnet, die zur Fertigungs- und Prozessautomatisierung eingesetzt werden. Ein ICS kann Prozesse wie zum Beispiel die Energieerzeugung/-verteilung, Gas- und Wasserversorgung etc., automatisch steuern [5]. Dadurch können verschiedene Angriffsmöglichkeiten für Angreifer entstehen. Betreiber der ICS müssen sich im Klaren sein, dass Angreifer neue Schwachstellen entdecken und dadurch einen großen Schaden anrichten können [5].

2.2 Schutzziele der IT-Sicherheit

Durch die Vernetzung und Interaktion innerhalb des eigenen Unternehmens oder auch mit anderen Unternehmen, hat die IT-Sicherheit immer mehr an Bedeutung gewonnen und zählt somit auch zu den wichtigsten Elementen der Industrie 4.0.

Hauptsächlich sind folgende Bereiche der Industrie 4.0 betroffen:

- Produktion/ Fertigung
- Daten, Big Data
- Cloud
- Mobile Lösungen

Schutzziele sind zentrale Bestandteile der IT-Sicherheit [8] und werden in den folgenden Unterkapiteln genauer erläutert.

2.2.1 Authentizität

Anhand der Authentizität kann die Echtheit eines Objekts bzw. Subjekts durch eine eindeutige Identität und durch charakteristische Eigenschaften wie zum Beispiel Fingerabdrücke oder Passwörter überprüft werden [6]. „*Authentizität einer Nachricht bedeutet, dass seit der Erstellung der Nachricht keine Veränderungen an der Nachricht vorgenommen wurden und dass keine falschen Informationen über den Absender der Nachricht beim Empfänger vorliegen*“ [6].

2.2.2 Datenintegrität

Die Datenintegrität wird gewährleistet, indem ein unautorisierter Zugriff vom System verweigert wird [6]. Bei der Datenintegrität spielt die korrekte Vergabe von Benutzerrechten wie Lese- oder Schreibrechte auf Daten eine wichtige Rolle [6]. Bei der Datenintegrität wird vorausgesetzt, dass unautorisierte Manipulationen nicht unbemerkt bleiben dürfen [6]. Um die Datenveränderungen nachvollziehen zu können werden kryptografisch sichere Hashfunktionen verwendet [6].

2.2.3 Informationsvertraulichkeit

Die Informationsvertraulichkeit eines Systems wird gewährleistet, indem das System eine unautorisierte Informationsgewinnung nicht ermöglicht [6]. Es muss also sichergestellt werden, dass keine Informationen an unbefugte durchdringen [6]. Häufig können auch aus Einzelinformationen weitere Informationen abgeleitet werden, die der Person jedoch nicht zugänglich sein sollten. Dies wird in der Langversion dieses Papers [9] anhand eines Beispielszenarios genauer erläutert.

2.2.4 Verfügbarkeit

Das System muss authentifizierten und autorisierten Subjekten die Verfügbarkeit von Informationen und Ressourcen gewährleisten, damit die Subjekte die gewünschten Informationen des Systems nutzen können [6]. Die Gefährdung der Verfügbarkeit, kann zu einem Produktionsstillstand führen [14].

2.2.5 Verbindlichkeit

Die Verbindlichkeit wird vom System gewährleistet, wenn nach der Durchführung einer Aktion im Nachhinein das Subjekt die Durchführung der Aktion nicht abstreiten kann [6]. Besonders im Bereich E-Commerce und E-Business hat dies eine große Bedeutung, da die Verbindlichkeit durchgeführter Transaktionen garantiert werden muss. Die Verbindlichkeit kann durch den Einsatz von digitalen Signaturen gewährleistet werden [6].

2.3 Top 5 Bedrohungen, Gegenmaßnahmen und Anforderungen

Durch existierende Schwachstellen können Angreifer dem ICS und dem Unternehmen großen Schaden zufügen. In der Abbildung 5 sind die Top 5 Bedrohungen für 2016 dargestellt.

Nr. (Nr. alt)	Top 10 2016
1 (3)	Social Engineering und Phishing+
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet
4 (5)	Einbruch über Fernwartungszugänge
5 (4)	Menschliches Fehlverhalten und Sabotage

Abbildung 3: ICS - Top 5 Bedrohungen 2016 [3]

Diese Bedrohungen stellen nur Primärangriffe dar, die über Folgeangriffe vom Angreifer weiter ausgebaut werden können und somit auch mehr Schaden angerichtet werden kann als bei einem Primärangriff (Abbildung 4) [5].

Zu den Folgeangriffen zählen folgende [5]:

- Das Auslesen von Zugangsdaten zur Rechteerweiterung
- Zugriff auf weitere interne Systeme durch mangelhafte Methoden zur Authentifizierung und Autorisierung der Dienste und Komponenten im Unternehmensnetz
- Das Mitlesen, Manipulieren oder Einspielen von Steuerungsbefehlen
- Das Manipulieren von Netzwerkkomponenten wie Router oder Firewall, um gezielt Sicherheitsmechanismen außer Kraft zu setzen

Durch einen Primär- bzw. Folgeangriff können unterschiedliche Schäden verursacht werden wie zum Beispiel folgende [5]:

- Beeinträchtigung der Verfügbarkeit des ICS
- Datenverlust
- Physische Schäden an Anlagen
- Minderung der Qualität

Abbildung 4: Ablauf von Primär- und Folgeangriffen sowie Schadensfolgen [3]

2.3.1 Social Engineering und Phishing

Social Engineering ist eine Methode, bei dem der Angreifer menschliche Eigenschaften wie zum Beispiel Vertrauen, Neugier, Hilfsbereitschaft und Respekt ausnutzt, um bestimmte Informationen zu gewinnen [5]. Ein Angreifer kann mithilfe der Methode Social Engineering einen Zugang zu einem Computernetzwerk eines Unternehmens verschaffen, indem er versucht das Vertrauen eines Angestellten zu gewinnen. Gelingt es dem Angreifer das Vertrauen zu gewinnen, so kann er den Angestellten dazu auffordern, ihm vertrauliche Daten über die Netzwerk-Sicherheit des Unternehmens zu geben [5]. Auch die Hilfsbereitschaft der Mitarbeiter zählt zu den Schwachstellen, auf die Social Engineering setzt. Mitarbeiter könnten auch telefonisch vom Angreifer kontaktiert werden unter dem Vorwand, dass ein dringendes Problem bestehe und sofort behoben werden muss [11]. Um das dringende Problem zu lösen wird angeblich ein Zugriff auf das Netzwerk benötigt [11]. Betrügerische E-Mails (Phishing-Mails) sind ebenso ein beliebtes Verfahren für Angreifer, bei der sie die Mitarbeiter dazu verleiten Links zu öffnen, die zu manipulierten Webseiten führen oder eine Schadsoftware herunterlädt [5].

Wie in der Abbildung 5 zu erkennen ist, können E-Mails mit einer Schadsoftware manipuliert sein, oder per Drive-by-Download wird die Schadsoftware direkt auf die Rechner der Mitarbeiter geladen. Von der Unternehmensebene aus kann der Angreifer über Folgeangriffe (Abbildung 4) den Angriff weiter ausbreiten und weitere Bereiche angreifen, um an sensible Daten des Unternehmens zu gelangen. Gelangt es dem Angreifer den Angriff auszubreiten und in die Leitebene einzudringen, so ermöglicht sich der Angreifer einen Zugriff auf Informationen der Steuerungs- und Feldebene (Abbildung 5). Von diesen Ebenen aus, kann der Angreifer Daten manipulieren und sogar für einen gesamten Ausfall des ICS sorgen. Wie in der Abbildung 3 zu erkennen ist, stellen Social Engineering und Phishing 2016 die größten Gefahren für jedes Sicherheitssystem dar. Als Gegenmaßnahmen können Unternehmen Security-Awarenesstraining durchführen [5], Sicherheitsrichtlinien erstellen und durchführen [5], technische Sicherheitsmechanismen zur automatischen Erkennung bei Fehlverhalten oder Angriffen einführen und eine regelmäßige Datensicherung ausführen [5], um Daten und Anwendungen wieder herstellen zu können.

Wichtige Kriterien zur Erstellung und Durchführung der Sicherheitsrichtlinien sind in der Langversion dieses Papers enthalten [9].

2.3.2 Einschleusen von Wechseldatenträger und externer Hardware

Vielen Mitarbeitern ist die Auswirkung von Schadsoftware nicht bewusst [5]. Speichermedien können im privaten Umfeld mit einer Schadsoftware infiziert worden sein, welches direkt den Weg in die ICS-Netze finden kann [5]. Externe Mitarbeiter führen meist eigene Speichermedien und Notebooks mit sich, welches aufgrund der externen Daten und Wartungssoftware ebenfalls Gefahren mit sich bringen kann [5]. Als Gegenmaßnahmen können Unternehmen alle zulässige Datenträger inventarisieren und ausschließlich diese verwenden. Alle inventarisierten Datenträger sollen verschlüsselt werden und durch physische Sperren wie USB-Schlösser soll das unbefugte Anschließen von Speichermedien verhindert werden. Für externe Dienstleister oder Mitarbeiter Quarantänenetze[1] einrichten, um vor dem Zugriff die notwendigen Aktualisierungen für die Sicherheit zu installieren [5].

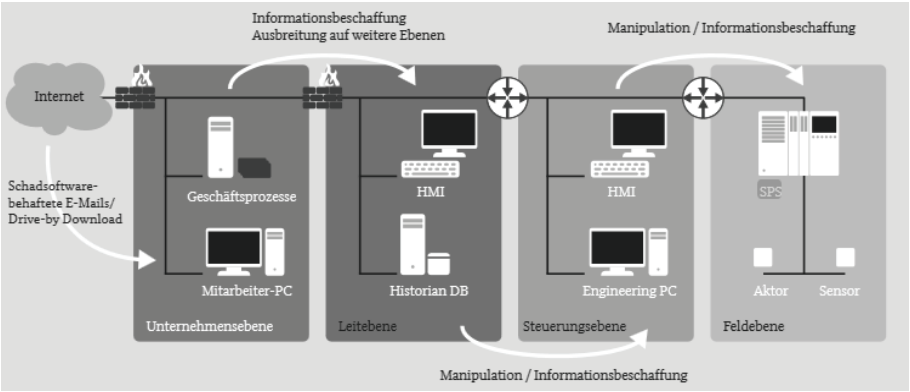

Abbildung 5: Ablauf mehrstufiger Angriffe auf eine typische ICS-Infrastruktur [4]

[1] Ein besonders geschütztes Netz mit sehr eingeschränkten Kommunikationsmöglichkeiten.

2.3.3 Infektion mit Schadsoftware über Internet und Intranet

In den meisten Unternehmen sind die Browser und E-Mail Clients an das Internet angebunden, wodurch Angreifer immer wieder neue Schwachstellen finden [5], um in das Intranet eindringen zu können und eine Infektion durch Schadsoftware ausrichten. Die Schadsoftware kann auch über Wechseldatenträger direkt im Intranet platziert werden [5], um direkt oder mit Folgeangriffen in das ICS-Netz einzudringen. Angreifer nutzen diese Schwachstellen indem sie externe Webseiten manipulieren durch einen Drive-By-Download [5, 10, 12] wie in der Abbildung 7 zu sehen ist, sodass das Infizieren ohne Benutzerinteraktionen ausgeführt werden kann [12]. Um sich gegen diese Risiken abzusichern, sollten Unternehmen durch Firewalls und VPN-Lösungen die unterschiedlichen Netze vollständig abschotten [5]. Das Patchen der Betriebssysteme, Office- und ICS-Netze sollte regelmäßig durchgeführt werden [5], um durch die Aktualisierung teilweise bekannte und dringende Fehlerbehebungen durchzuführen. Alle IT-Komponenten die für das Office-Netz und ICS-Netz eingesetzt werden, sollten abgehärtet werden [5].

2.3.4 Einbruch über Fernwartungszugänge

ICS Systeme haben einen externen Zugang für Wartungszwecke, welches mit einem Standartpasswort oder fest kodierten Passwort gesichert ist [5]. Die Wartung der ICS Komponenten werden von den jeweiligen Herstellern oder externen Dienstleistern über externe Wartungszugzugänge durchgeführt [5]. Eine zusätzliche Herausforderung für das Sicherheitsmanagement ist die Sicherheitskonzepte aller Parteien in Übereinstimmung zu bringen [5]. Über VPN (Virtual Private Network) kann sich sonst der Angreifer einen Zugang über den Wartungsserver verschaffen und anschließend weitere Bereiche steuern [5]. Dabei werden die Schutzziele Authentizität und Datenintegrität welche in 4.1.1 und 4.1.2 genauer beschrieben werden verletzt. Mangelnde Authentifizierung und Autorisierung, aber auch flache Netzwerkhierarchien führen hauptsächlich zu dieser Bedrohung [5]. Standartpasswörter der Hersteller sollten daher immer gelöscht oder geändert werden [5]. Eine weitere Maßnahme wäre das Einrichten eines Zugriffspunktes für Fernwartung in einer demilitarisierten Zone (DMZ)[2] [5]. Um auf das Zielsystem zugreifen zu können müssen sich externe Dienstleister zuerst in eine DMZ verbinden, statt direkt ins ICS-Netz. Vom DMZ aus erhält der externe Dienstleister dann den Zugriff auf das Zielsystem. Außerdem sollten die Fernzugänge über die Firewall laufen, damit diese die Zugänge zu den jeweiligen Zielsystemen überwacht [5].

2.3.5 Menschliches Fehlverhalten und Sabotage

Jeder, der im Umfeld eines ICS-Systems arbeitet trägt Verantwortung bezüglich der Sicherheit, unabhängig davon, ob durch einen Zugriff auf ein System oder durch Zutritt zu den Anlagen [5]. Technische Maßnahmen sind zwar ein wichtiger Baustein für die Sicherheit, jedoch reicht dies alleine nicht aus. Es müssen immer organisatorische Regelungen erstellt und eingehalten werden [5]. Zum Beispiel könnte die Konfiguration von Netzwerkkomponenten oder ICS-Komponenten fehlerhaft sein [5]. Außerdem könnte das System manipuliert werden durch nicht genehmigte Soft- und Hardware wie zum Beispiel Smartphones oder USB-Sticks [5]. Deswegen ist bei der Sicherheit zu beachten, dass durch Spionage, Sabotage, Fahrlässigkeit oder sonstiges menschliches Fehlverhalten große Gefahren entstehen können [5]. Darum sollte der Zugriff auf sensible Daten nur, wenn nötig erfolgen [5].

---

[2] Definition DMZ: https://www.iternas.com/dmz [Letzter Zugriff am 13.01.2017]

2.4 Bekannte Vorfälle im Sicherheitsbereich

Die Hackergruppe „Dragonfly“ (auch „Energetic Bear“ genannt) griff 2014 mit der Schadsoftware „Havex“ mehrere deutsche Unternehmen an [13]. Der Angriff wurde in mehreren Schritten aufgeteilt. Wie im Kapitel 2.3.1 beschrieben, griffen die Hacker im ersten Schritt die Softwarehersteller der Industrieanlagen an [13]. Hierbei handelte es sich um einen Primärangriff (Abbildung 4), bei der die Angreifer die Schadsoftware „Havex“ in den Installationsdateien auf den Downloadservern der Anbieter unbemerkt platzierten [13]. Kunden die die Installationsdateien geladen haben, haben somit auch unbemerkt die Schadsoftware mit heruntergeladen. Die Schadsoftware lädt für den Folgeangriff (Abbildung 4, 5) ein Modul herunter, um das Auslesen von Informationen über die gesamten Geräte und Systeme im Produktionsnetz dem Täter zu ermöglichen [13]. Diese Informationen wurden anschließend für weitere Folgeangriffe verwendet. In der Langversion dieses Papers wird auch der Angriff mit der Schadsoftware „Stuxnet“ beschrieben [9].

3 Industrie 4.0 in der Praxis

In diesem Kapitel wird als Praxisbeispiel die Daimler AG verwendet. Die Langversion dieses Papers [9] beinhaltet zusätzlich noch die Siemens AG als Praxisbeispiel.

Die Daimler AG ist ein deutscher Hersteller von Personenkraftwagen und Nutzfahrzeugen mit Hauptsitz in Stuttgart.
Ende 2016 waren 282.488 Mitarbeiter im Konzern beschäftigt und das Unternehmen erzielte einen Umsatz von 153,261 Mrd. Euro [8]. Das Unternehmen wird mit folgenden Herausforderungen konfrontiert [8]:

- Globalisierung
- Individualisierung
- Digitalisierung/vernetzte Fabrik

3.1 Ziele

Durch Industrie 4.0 möchte die Daimler AG folgende Ziele erreichen [8]:

- Verkürzung der Anlaufzeiten durch digitale Absicherung
- Reduzierte Beschaffungszeiten für Produktionsanlagen
- Optimierung der Fertigung und Montage
- Erhöhung der Interaktionen durch Mensch-Roboter-Interaktionen
- Flexibilisierung der Produktion durch eine wandlungsfähige Produktion

3.2 Lead-Werk Bremen

Das Daimler Werk in Bremen soll künftig alle Prozesse vernetzen, um die Idee der Industrie 4.0 umsetzen zu können [14]. Zukünftig sollen Produktionsplanung und Fertigungsprozesse vollständig digital gesteuert werden. In der Produktion kann somit der Materialbedarf beobachtet und bei Bedarf automatisch gedeckt werden [14]. Hierfür werden automatisierte, fahrerlose Transportsysteme (FTS) eingesetzt. Auch in der Fahrzeugmontage sollen Schraubvorgänge zukünftig von Robotern automatisch durchgeführt werden. Komplexe Vorgänge in der Montage, die der Mensch nur mühsam erledigt, werden vom Roboter übernommen und problemlos erledigt [14]. Dieses Konzept wird als „Robot Farming“ bezeichnet, welches die Präzision und Ausdauer des Roboters mit den kognitiven Fähigkeiten des Menschen kombiniert [14]. Ein weiterer vollautomatisierter Bereich des Werkes ist das Presswerk. Durch vorinstallierte Presslinien können bis zu 40 Bauteile pro Minute hergestellt werden [14]. Durch FTS gelangen die Rohteile automatisiert in die Presse, werden nach der Verformung von Robotern auf einen Ladungsträger gestellt und werden anschließend von FTS in die Montage transportiert [14].

3.3 Smart Factory

Daimler verfolgt folgende fünf Hauptziele mit der Smart Factory [15]:

- **Größere Flexibilität:** schnellere Reaktion der Fertigung auf individuelle Nachfrage der Kunden. Die Fertigung immer komplexerer Produkte wird durch die Digitalisierung der Produktion erleichtert.
- **Erhöhte Effizienz:** Ein entscheidender Wettbewerbsfaktor ist das effiziente Nutzen von Ressourcen wie Vorräte. Für eine durchgängig digitale Prozesskette sollten Bauteile jederzeit vorhanden und überall identifizierbar sein.
- **Höhere Geschwindigkeit**: Einfachere und effizientere Fertigungsabläufe werden durch flexible Produktionsprozesse, Installation neuer Anlagen und durch das Anpassen der bestehenden Anlagen ermöglicht.
- **Attraktives Arbeitsumfeld:** Durch Interkationen zwischen Mensch und Maschine können Bereiche wie Qualifizierung und Ergonomie verbessert werden.
- **Smarte Logik:** Von der Konfiguration und Bestellung bis zur Produktion und Auslieferung

3.4 IT-Sicherheit

Um die Sicherheitsvorkehrungen hoch zu halten, hat die Daimler AG ein Lagezentrum gegründet, um alle weltweiten Sicherheitsvorfälle zu analysieren. Um möglichst frühzeitig Schwachstellen zu entdecken und zu beheben, hat Daimler fest eingestellte Hacker, die das Firmeneigene Netz permanent angreifen. Dadurch werden bei der Daimler AG Hacker Angriffe frühzeitig erkannt und bevor Schäden entstehen werden die Gegenmaßnahmen eingeleitet [14].

4 Ergebnisse

Die meisten Hackerangriffe auf industrielle Anlagen starten mit einem Primärangriff, um einen Zugriff auf das Computernetzwerk eines Unternehmens zu verschaffen. Dies kann bereits durch einfache Methoden wie Social Engineering und Phishing (Kapitel 2.3.1) erreicht werden. In den meisten Fällen versucht der Hacker anschließend über Folgeangriffe an weitere Informationen heranzukommen, um in weiteren Ebenen wie zum Beispiel die Steuerungsebene einer industriellen Anlage (Abbildung 5) einzudringen. Unternehmen sollten daher durch Firewalls und VPN-Lösungen die unterschiedlichen Netze vollständig abschotten [5]. Für Fernwartungszugänge wäre es sinnvoll einen Zugriffspunkt in einer demilitarisierten Zone (DMZ) einzurichten [5], um das direkte Verbinden der externen Mitarbeiter oder Dienstleister in das ICS-Netz zu vermeiden. In der DMZ können dann die benötigten Sicherheitsvorkehrungen wie zum Beispiel das Aktualisieren bestimmter Software durchgeführt werden, bevor der eigentliche Zugriff auf das ICS-Netz freigegeben wird [5]. Zulässige Datenträger sollten inventarisiert und verschlüsselt werden [5]. Zusätzlich kann das unbefugte Anschließen von Speichermedien durch USB-Schlösser verhindert werden [5]. Außerdem müssen auch alle Mitarbeiter auf die Industrie 4.0 vorbereitet werden, indem Unternehmen durch Weiterbildungen in die IT-Kompetenz der Mitarbeiter investieren.

5 Schlussbetrachtung

Technische Maßnahmen können zwar viele Risiken und Bedrohungen abschirmen, jedoch genügt dies allein in den meisten Fällen nicht aus um gegen einen Angriff vorbereitet zu sein. Wie in Kapitel 2.3 festgestellt wurde, können viele Risiken und Bedrohungen minimiert werden indem organisatorische Regelungen und technische Maßnahmen kombiniert werden. Bereits etablierte Sicherheitskonzepte können nicht ohne weiteres übernommen werden, denn

diese wurden speziell entworfen für die klassische IT, bei der die höchste Priorität die Vertraulichkeit hat [14]. Bei industriellen Anlagen dagegen steht die Verfügbarkeit im Fokus [14]. Die etablierten Sicherheitskonzepte sind so entworfen, dass wenn die Vertraulichkeit gefährdet wird, auch automatisch die Verfügbarkeit der Systeme eingeschränkt wird. Dies würde bei industriellen Anlagen zu einem kompletten Stillstand der Produktion führen. Daher sollten speziell für industrielle Anlagen Sicherheitskonzepte entworfen werden, bestehend aus der Kombination von technischer Maßnahmen und organisatorischer Regelungen.

Literaturverzeichnis

[1] Com!proffesional. Vor Industrie 4.0 kommt Industrie 3.0. Website 15.10.2015. Online verfügbar unter: http://www.com-magazin.de/praxis/business-it/industrie-4.0-kommt-industrie-3.0-1013483.html ‘Abgerufen am 10.12.2016.‘

[2] Herbert Beesten. Von Industrie 1.0 zu 4.0 – Der Weg zur intelligenten Fabrik führt zurück zum Individuum. Website 09.12.2013. Online verfügbar unter: http://crosswater-job-guide.com/archives/39557 ‘Abgerufen am 13.12.2016.‘

[3] Prof. Dr. Oliver Bendel. Industrie 4.0

Website Online unter: http://wirtschaftslexikon.gabler.de/Archiv/-2080945382/industrie-4-0-v2.html ‘Abgerufen am 31.03.2017.‘

[4] Spiegel Online. Industrielle Revolutionen: Von der Dampfmaschine zum intelligenten Roboter. Website 11.04.2015. Online verfügbar unter: http://www.spiegel.de/fotostrecke/von-der-industrie-1-0-bis-4-0-fotostrecke-125537-4.html ‘Abgerufen am 13.12.2016.‘

[5] Bundesamt für Sicherheit in der Informationstechnik. PDF Online 01.08.2016. Online verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile ‘Abgerufen am 20.12.2016.‘

[6] Prof. Dr. Claudia Eckert. IT-Sicherheit, Konzepte-Verfahren-Protokolle, 9.Auflage. Oldenbourg Wissenschaftsverlag GmbH, München 2014, S.7. ISBN 978-3-486-77848-9.

[7] Bundesamt für Sicherheit in der Informationstechnik – Kryptografische Verfahren: Empfehlung und Schlüssellängen. PDF Online 08.02.2017, S.viii. Online Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile ‘Abgerufen am 04.04.2017.‘

[8] Walter Huber. Industrie 4.0 in der Automobilproduktion. Springer Fachmedien Wiesbaden 2016. ISBN 978-3-658-12731-2.

[9] Mücahit Karabulut. IT-Sicherheit in der Industrie 4.0 (Langversion). PDF 2017.

[10] Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland. PDF Online November 2015. Online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=84E512FF997AD42F6497FF1DBABDE754.1_cid360?__blob=publicationFile&v=5 ‘Abgerufen am 22.03.2017.‘

[11] Margaret Rouse. Social Engineering. Website, Oktober 2016. Online verfügbar unter: http://www.searchsecurity.de/definition

/Social-Engineering ‘Abgerufen am 10.01.2017.‘

[12] Margaret Rouse. Drive-by-Download. Website, Januar 2017. Online verfügbar unter: http://www.searchsecurity.de/definition/Drive-by-Download ‘Abgerufen am 04.04.2017.‘

[13] Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2014. PDF Online 01.11.2014. Online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile ,Letzter Zugriff am 22.03.2017‘ BSI-LB15503.

[14] Werner Grosch. Mercedes-Werk in Bremen wird zur Fabrik 4.0. Website Online 22.05.2015. Online verfügbar unter: http://www.ingenieur.de/Themen/Industrie-40/Mercedes-Werk-in-Bremen-Fabrik-40 ‘Abgerufen am 26.02.2017.‘

[15] Daimler AG. Fünf Hauptziele verfolgt Mercedes-Benz mit der Smart Factory. Website Online 2017. Online verfügbar unter: https://www.daimler.com/innovation/digitalisierung/industrie4.0/smart-factory.html ‘Abgerufen am 12.02.2017.‘

[16] J. van Ackeren, T. Schröder. Fraunhofer-Gesellschaft. Trends für Industrie 4.0. Online 2016. Online verfügbar unter: https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/Produktion-Dienstleistung/Trends-fuer-Industrie-40.pdf ‘Abgerufen am 13.03.2017.‘

Abbildungsquellen

[1] Industrie 1.0 zitiert von: Spiegel Online. Industrielle Revolutionen: Von der Dampfmaschine zum intelligenten Roboter. Website 11.04.2015. Online verfügbar unter: http://www.spiegel.de/fotostrecke/von-der-industrie-1-0-bis-4-0-fotostrecke-125537.html ‘Abgerufen am 31.03.2017.‘

[2] Industrie 4.0 – Interaktiver Roboter „Yumi“ zitiert von: Spiegel Online. Industrielle Revolutionen: Von der Dampfmaschine zum intelligenten Roboter. Website 11.04.2015. Online verfügbar unter: http://www.spiegel.de/fotostrecke/von-der-industrie-1-0-bis-4-0-fotostrecke-125537-4.html ‘Abgerufen am 31.03.2017.‘

[3] Bundesamt für Sicherheit in der Informationstechnik. PDF Online 01.08.2016. Online verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile ‘Abgerufen am 20.12.2016.‘

[4] Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland. PDF Online November 2015. Online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=84E512FF997AD42F6497FF1DBABDE754.1_cid360?__blob=publicationFile&v=5 ‘Abgerufen am 22.03.2017.‘

Sicherheitsbetrachtung des Internet of Things am Beispiel Smart Home

Oliver Streicher
Reutlingen University
Oliver.Streicher@Student.Reutlingen-University.DE

Abstract
Die Arbeit stellt die Vision des Internet of Things (IoT) vor und betrachtet sowohl Möglichkeiten der Nutzung als auch Gefahrenpotentiale für die Sicherheit der Nutzer. Insbesondere wird hierbei der Anwendungsfall Smart Home näher betrachtet und am Beispiel ZigBee gravierende Schwächen dieser Geräte aufgezeigt.

Schlüsselwörter
Smart Home. Internet of Things. Security

Kategorien und Themenbeschreibungen
K.6.5 [**Management of computing and information systems**]: Security and Protection - *Authentication, Invasive software (e.g., viruses, worms, Trojan horses), Physical security, Unauthorized access (e.g., hacking, phreaking)*

1 Einleitung
Mehr und mehr entwickelt sich die Menschheit zu einer vernetzten Gesellschaft. Angefangen mit statischen Verbindungsnetzen wie das Telefonnetz mit Festnetzleitungen über die Entwicklung von dynamischen Verbindungsnetzen wie Mobilfunknetze bis hin zur Konzeption eines Semantischen Netzwerkes, welches über eine eigene KI verfügt, wird die Vernetzung der Menschen immer dichter. Mit Hilfe von sozialen Netzwerken wie Facebook und Twitter oder Chatprogrammen wie WhatsApp wird diese Vernetzung heutzutage erreicht und gefestigt. Das Internet und die daraus resultierende Integration in das Netzwerk sind aus dem heutigen Alltag der Menschen kaum noch wegzudenken.

Das Internet der Dinge (IoT; engl. Internet of Things) beschreibt einen aufkommenden Trend, der nicht nur die persönlichen Computer der Menschen wie Rechner und Mobilfunkgeräte, sondern jedes moderne technische Gerät in das Internet integrieren will. Diese Vision einer vernetzten Welt in einer digitalen Zukunft wird in Kapitel 2 genauer thematisiert und beschrieben. Da mit dem Internet verbundene Geräte generell öffentlicher ansprechbar sind als bisherige private Computer, ist auch die Sicherheit, die den Schutz vor unbefugten Zugriffen gewährleisten muss, ein wichtiger Punkt und wird in der nachfolgenden Arbeit genauer thematisiert. Zum Schluss soll noch ein Ausblick darauf gegeben werden, wie real diese Vision aus heutiger Sicht ist und ob bisherige Sicherheitskonzepte den neuen Anforderungen gerecht werden.

Betreuer Hochschule: Prof. Dr.-Ing. Michael Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

2 Internet of Things

Der Begriff Internet of Things wurde erstmals von Kevin Ashton geprägt bei einer seiner Präsentationen im Jahre 1999. [1] Gemeint ist eine moderne vernetzte Welt, in der ganz alltägliche Geräte über das Internet miteinander oder mit den Benutzern kommunizieren. Technologien wie Radio Frequency IDentification (RFID) und Sensornetzwerk-Technologien gehen einen ersten Schritt in Richtung eines unsichtbar eingebetteten Informations- und Kommunikationssystems in unsere Umgebung. Als Konsequenz entsteht hieraus natürlich eine Fülle von Daten, die entsprechend gespeichert, verarbeitet und einfach interpretierbar dargestellt werden müssen. Das hierfür verwendete Modell wird über Services laufen, die ähnlich wie gewöhnliche Waren gehandhabt werden. Die nötige Infrastruktur kann über Cloud Computing realisiert werden und beinhaltet Geräte zur Überwachung und zur Speicherung, Analyse-Tools sowie Visualisierungsplattformen zur entsprechenden Darstellung der Daten für den Nutzer. Desweiteren bringt Cloud Computing den Vorteil mit sich, dass die Dienste auf Nachfrage von überall zugänglich sind und somit dem Nutzer die ständige Kontrolle und Übersicht über alle vernetzten Geräte gegeben wird. [2]

Mit der sich rasch verbreitenden Präsenz von WiFi und 4G-LTE in der Gesellschaft ist der drahtlose und mobile Zugang zum Internet bereits auf dem besten Weg, sich zu einem allgegenwärtigen Informations- und Kommunikationsnetzwerk aufzuschwingen. Neben einem gleichen Verständnis der Situation seiner Nutzer und deren Anwendungen sind Softwarearchitekturen und tiefgreifende Kommunikationsnetze, um kontextuelle Informationen zu verarbeiten und zu vermitteln, sowie Analyse-Tools, die auf autonomes und intelligentes Verhalten abzielen, vonnöten, um die eigentliche Technologie des Internet of Things aus dem Bewusstsein des Nutzers verschwinden zu lassen. Dann ist der Nutzer imstande, mit seiner Umgebung zu interagieren, ohne sich direkt um jedes einzelne Gerät kümmern zu müssen. [2]

Das erklärte Hauptziel des IoT ist, Computer dazu zu bringen, Informationen mithilfe von Sensoren und ohne menschliches Eingreifen zu erfassen und zu verarbeiten. Gesundheitswesen, Versorgungswirtschaft und Transport sind nur einige Anwendungsgebiete für IoT aus einem weiten Spektrum von Möglichkeiten. Es soll für eine radikale Evolution des momentanen Internets sorgen, bei der aus den bestehenden Internet-Standards für die Bereitstellung von Diens-

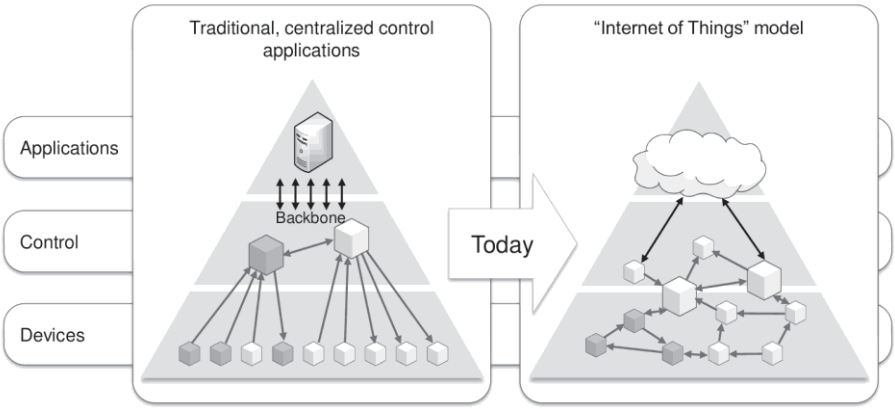

Abbildung 1: Wandel zum Modell des Internet of Things [3]

ten für Informationsvermittlung, Analysen, Anwendungen und Kommunikation ein zukünftiges vollständig integriertes Internet entsteht, in welchem die Geräte selbstständig Informationen ihrer Umgebung sammeln und aufgrund dessen mit der physischen Welt interagieren. Dieses integrierte Netzwerk von Objekten wird ein intelligentes Netzwerk erschaffen, wie beispielsweise das Smart Home. [2]

In Abbildung 1 ist schematisch der Wandel vom traditionellen Modell mit zentralisierten Kontrollanwendungen und Client-Server-Szenarien hin zu einem Modell des Internet of Things dargestellt. Sie veranschaulicht die Kernkomponente Cloud-Computing als zentralen Ansprechpunkt der Kontrollschicht und die interaktive Maschine-zu-Maschine-Kommunikation der einzelnen Geräte untereinander.

2.1 Smart Home

Das wahrscheinlich bekannteste Anwendungsgebiet von IoT ist das sogenannte Smart Home. Hier dreht sich demnach alles darum, Haushaltsgeräte in einem Netzwerk miteinander zu verbinden und über Befehle steuern zu können. Dabei spielt es keine Rolle, ob die Befehle per Fernbedienung oder per Sprachsteuerung gegeben werden, damit das Haus reagiert. Die am häufigsten angebrachten Anwendungen für Smart Home sind Beleuchtung, Unterhaltungsmedien, Thermostate und natürlich Sicherheitssysteme. [4]
In Abbildung 2 sind Geräte dargestellt, die alle in einem Smart Home Netzwerk integriert sein könnten.

Zunächst sollen die Möglichkeiten und Technologien von Smart Homes vorgestellt werden, während in Kapitel 3 auf die Sicherheit dieser Systeme eingegangen wird.

Als Smart Home wird für gewöhnlich ein modernes Haus bezeichnet, welches mit einer speziell strukturierten Verkabelung ausgestattet ist, die es den Benutzern ermöglicht, mehrere Geräte gleichzeitig mit einem einzigen Befehl zu steuern. [4]

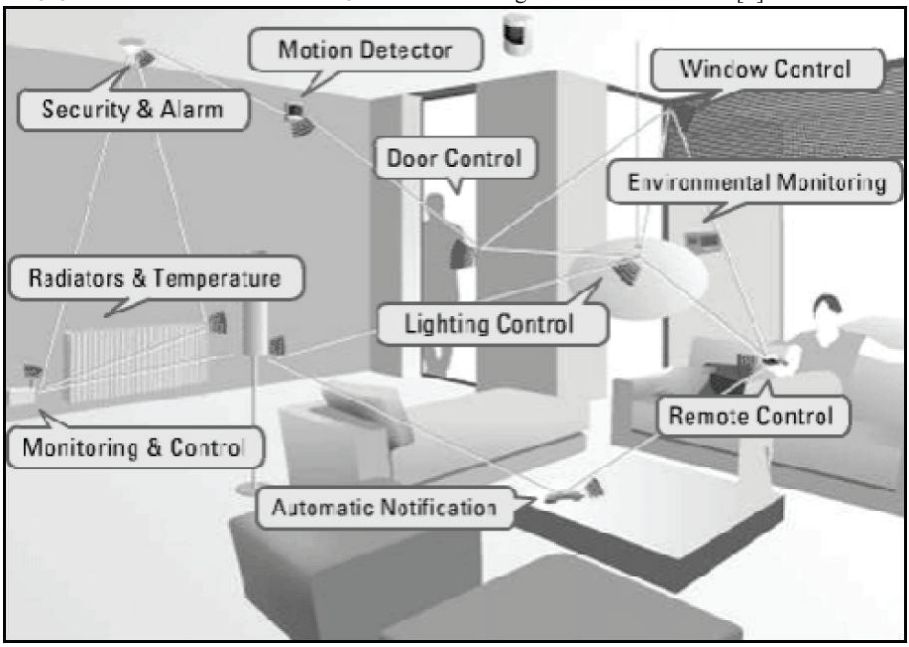

Abbildung 2: Geräte in einem Smart Home Netzwerk [4]

Ein Beispiel hierfür ist, wenn der Benutzer die Nachrichten im Fernsehen auf einem speziellen Programm anschauen möchte. Hierzu nimmt er die Fernbedienung und drückt einen Knopf, der für dieses Szenario vorgesehen wird. Die Aktion sendet Signale an alle dafür benötigten Geräte: Es werden Fernseher, Satellitenreceiver und Soundanlage eingeschaltet, danach pausiert die Aktion bis der Receiver hochgefahren ist und schaltet dann auf das gewünschte Programm um.

Realisiert wird solch ein Szenario beispielsweise mit einer Technologie namens Powerline Carrier Systems (PCS), welche kodierte Signale durch die bestehenden Stromleitungen eines Hauses zu den an das Stromnetz angeschlossenen Geräten schickt. Damit die Signale nicht von der eigentlichen Stromversorgung gestört werden, unterscheiden sich die Frequenzen dieser beiden Funktionen stark voneinander. Während das normale Stromnetz mit einer Frequenz von ca. 50 Hz durch die Leitungen geschickt wird, befindet sich die Frequenz der PCS in einem Bereich von mindestens 3 kHz. [5]
Ein verbreitetes Protokoll für PCS ist das im Jahre 1975 entwickelte X10, welches eine Fernsteuerung von Geräten über Stromleitungen ermöglicht. Die X10-Signale werden als kurze Radiofrequenz-Bursts, welche digitale Informationen repräsentieren, übermittelt und ermöglichen so eine Kommunikation zwischen Sender und Receiver. Jedes im Haus platzierte und vernetzte Gerät ist ein Receiver und jede Fernbedienung oder ähnliches ist ein Sender. Soll ein Befehl an einen entsprechenden Receiver geschickt werden, so verschickt der Sender einen aus den folgenden Teilen aufgebauten numerischen Code:

- ein Alarm zum System, dass nun ein Befehl folgt
- eine ID des Gerätes, für das der Befehl gedacht ist
- ein Code, der für den eigentlichen Befehl steht (z.B. ‚ausschalten')

Der Nachteil dieses Systems über elektrische Leitungen ist, dass die Verbindung nicht immer verlässlich ist. Wegen der Stromzufuhr auch für andere Geräte entsteht ein Rauschen innerhalb der Leitungen, welches die mitgesendeten Befehle überdeckt oder verändert, sodass Geräte entweder gar nicht oder sogar andere Geräte reagieren, obwohl sie gar nicht gemeint waren. [4]

Andere Systeme vermeiden den Weg über die Stromleitungen und gehen wie WiFi und Mobilfunkgeräte über Funkwellen. Auch hierfür wurden bereits Systeme entwickelt, wovon Z-Wave und ZigBee die beliebtesten sind.
Z-Wave verwendet einen Source Routing Algorithmus, um den kürzesten Weg für die Nachricht zum Ziel zu bestimmen. Jedes Gerät verfügt über einen eigenen Kennungscode, der beim Integrieren in das Netzwerk vom System erkannt und zu einer Liste von Geräten hinzugefügt wird. Mit Hilfe des Algorithmus kann der Controller entscheiden, auf welchem Weg die Nachricht am besten zum Zielgerät gesendet werden kann. [4]
ZigBee verdankt seinen Namen den Bienen, die im Zick-Zack fliegen, um zum Beispiel die Quelle einer Duftspur zu finden. Der Unterschied zu Z-Wave besteht darin, dass bei ZigBee keine proprietäre Technologie verwendet wird und somit lizenzfreie Geräte produziert werden können, die das Protokoll unterstützen. [4]
Bei beiden Technologien handelt es sich um sogenannte Mesh-Netzwerke, was so viel bedeutet wie es gibt mehr als nur einen Weg für die Übermittlung von Befehlen. [4]

In Abbildung 3 ist ein Vergleich der beiden Netzwerk-Topologien Sterntopologie und Meshtopologie dargestellt. Die sternförmige Variante ist üblicherweise in privaten Heimnetzwerken zu finden, in denen der Router als zentrale Kernkomponente agiert. Über ihn läuft sämtliche Kommunikation zwischen im Netzwerk befindlichen Gerä-

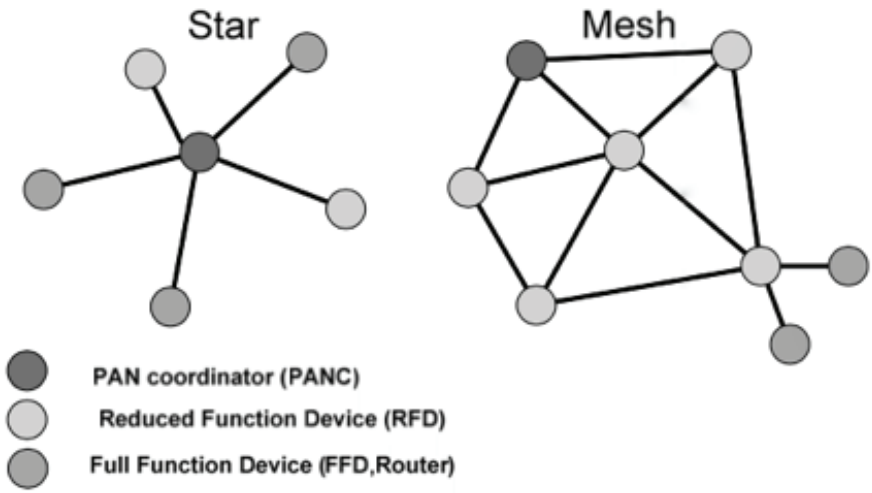

Abbildung 3: Vergleich Mesh- und Sterntopologie in einem Netzwerk [6]

ten. Die Mesh-Topologie dagegen verbindet alle Netzwerkgeräte untereinander, sodass mehrere Kommunikationswege zwischen zwei Komponenten entstehen. Auf diese Weise ist das Netzwerk weniger anfällig gegenüber Ausfällen einzelner Knoten und auch gegenüber einem Ausfall der Koordinator-Komponente (PANC).

Die Vorteile des Smart Homes beziehen sich meist darauf, das Leben der Benutzer einfacher zu machen. Neben vereinfachter Bedienung von Geräten ist auch der psychologische Aspekt zu nennen, den ein ständig überwachendes System hat. So können Benutzer sorgloser in den Urlaub gehen während das Haus allein steht und können trotzdem vom Heimsystem benachrichtigt werden, falls etwas vorfallen sollte. Ein weiterer Vorteil ist die Einsparung von Energie. Über ein intelligentes Management von Licht und Heizung kann viel Strom in einem Haus gespart werden. Nicht zuletzt bringt ein Smart Home einen immensen Vorteil für ältere Bewohner mit sich, bei denen das System im Haushalt unter die Arme greifen kann oder Benachrichtigungen an Angehörige etc. verteilt, falls etwas Unvorhergesehenes wie ein Sturz geschieht. [4]

3 Sicherheit von IoT

Das Internet der Dinge setzt zwar mit neuen Funktionen auf das bestehende Internet auf, erbt damit aber auch einige grundlegende Eigenschaften des Internets. Dazu zählt auch das Sicherheitskonzept mit seinen Problemen und Herausforderungen. In [7] wird eine vollständige Liste von möglichen Schwachstellen des IoT erstellt:

Integrierter Cyber-Physischer Raum bezieht sich auf die gegenseitige Beeinflussung der realen und virtuellen Welt. Viele dieser Beziehungen können bei Versagen großen Schaden an physischen Systemen oder sogar beim Menschen anrichten. Hauptziele von böswilligen Angreifern könnten zum Beispiel kritische Infrastrukturen wie Energie- und Wasserversorgung oder Transportsysteme sein, welche bei einer Störung große Auswirkungen auf das Gesundheitswesen oder den wirtschaftlichen Stellenwert der Bevölkerung haben.

Der *Netzwerk-Effekt* tritt vor allem in sehr großen und komplexen Netzwerken, wie das IoT mit all seinen modernen Kommunikationsgeräten eines ist, in Erscheinung. Nach dem Verstärkungsprinzip [7] können in großen Netzwerken selbst kleine Ereignisse große Auswirkungen auf das Gesamt-

system haben. Ebenso gilt das Kopplungsprinzip, welches besagt, dass die Wahrscheinlichkeit eines Folgefehlers in größeren Netzwerken höher ist als in kleinen, da die Abhängigkeit verschiedener Komponenten untereinander mit ihrer steigenden Anzahl zunimmt.

Als nächste Gefahrenstelle ist der *Bestand* von mobilen Geräten zu nennen. Schätzungen zufolge wird die Zahl der mobilen Geräte bis zum Jahr 2020 dramatisch ansteigen [8]. Aus diesem Zuwachs an Geräten folgt die Generierung von enormen Datenmengen. Diese Explosion von verfügbaren Daten bringen wiederum Bedenken im Hinblick auf Datenspeicherung, -sicherheit und Informationsverarbeitung auf. Jedes der intelligenten Geräte benötigt selbst Informationen, um seine Funktionen korrekt ausführen zu können, was immer eine potenzielle Möglichkeit für Missbrauch durch Hacker bedeutet.

Auch die *Mobilität* stellt das IoT vor eine schwierige Aufgabe. Aufgrund der sich schnell verändernden Umgebungen der Nutzergeräte werden Sicherheitsfunktionen wie Zugriffskontrolle, Identitätsmanagement und Geräteüberwachung erschwert. Zusätzlich muss eine sichere Kommunikation und Datenübertragung mit entsprechender Authentifikation der Geräte im aktuellen Netzwerk sichergestellt sein.

Weitere Bedenken vor allem im Hinblick auf Identitätsmanagement, Überwachung und Privatsphäre werden durch die *Allgegenwärtigkeit und weite Verbreitung* von intelligenten Geräten laut. Dazu kommt, dass die dafür nötigen Basistechnologien immer billiger werden und sich somit leicht über die ganze Welt verteilen lassen. Dadurch jedoch gelangen Systeme auch in abgelegenere Orte, wo eine Wartung der physischen Geräte erschwert wird.

Mit mehr zur Verfügung stehenden Ressourcen steigt die *Komplexität* der IoT-Geräte. Ein Netzwerk besteht aus sehr vielen Geräten unterschiedlicher Komplexität, welche unterschiedliche Angriffsvektoren bieten. Je höher die Komplexität, desto mehr Angriffsfläche bietet ein Gerät. Allerdings ist die Zahl der einfacheren Systeme sehr viel größer als die der komplexen, weshalb eine Angriffsmöglichkeit auf einfache Systeme aufgrund deren weiten Verbreitung trotzdem ein hohes Gefahrenpotential birgt.

Eine große Bedrohung für das IoT sind im Netzwerk eingebundene Geräte, die nur *eingeschränkte Ressourcen* zur Verfügung haben. Hier besteht das Problem, ein gutes Sicherheitsprotokoll zu kreieren, welches auf verlustreichen und kleinen Bandbreiten mit leistungsschwächeren Geräten kommu-

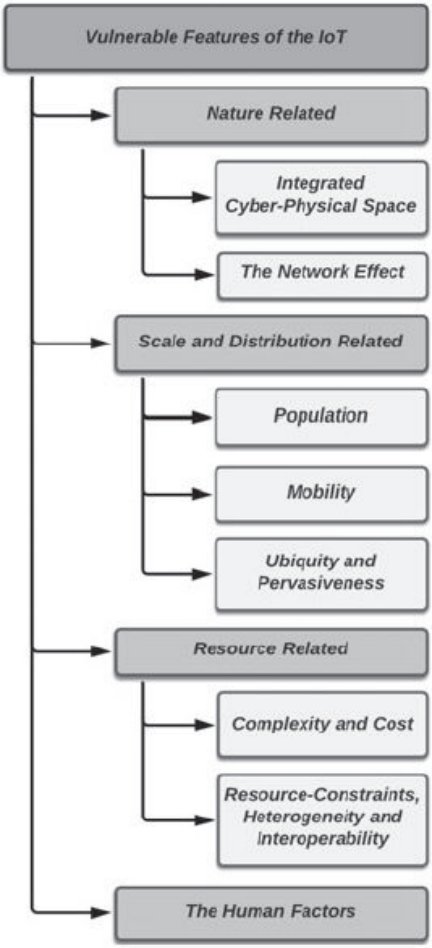

Abbildung 4: Schwachstellen im IoT [7]

nizieren können muss. Oft sind diese schwächeren Geräte nicht in der Lage, aktuelle kryptografische Standards zu bedienen und stellen somit eine Gefahr für das gesamte Netzwerk dar.
Als letzter sehr wichtiger Punkt ist der *menschliche Faktor* zu nennen. Generell wird hier zwischen zwei unterschiedlichen Typen unterschieden. Nutzer könnten Opfer von böswilligen Herstellern oder Dienstleistern werden, die beispielsweise versteckte Funktionen in ihren Systemen verwenden, um so an vertrauliche Daten der Nutzer zu gelangen. Oft sind es aber die Nutzer selbst, die durch ihr unverantwortliches und ignorantes Handeln eine Gefahr für das Gesamtsystem darstellen. Der zweite Typ Nutzer ist diejenige, der selbst zum Täter wird und mit böswilligen Absichten versucht, Systeme zu kompromittieren.

Eine kategorisierte Übersicht aller genannten Schwachstellen ist in Abbildung 4 dargestellt.

3.1 Sicherheit im Smart Home

Als ein Anwendungsgebiet des IoT setzt auch Smart Home auf die bestehende Internettechnologie auf. Aus den Sicherheitsanforderungen an das Internet lassen sich die Schutzziele für Smart Home ableiten.
Mit dem Schutzziel *Vertraulichkeit* sollen vertrauliche Daten geschützt werden. Im Umfeld eines Smart Home sind dies zum Beispiel Sensordaten des Thermostats oder Werte des Energieverbrauchs im Haus. Gelangt ein Angreifer an diese Informationen, so könnte er anhand der Daten feststellen, zu welchen Zeiten das Haus unbewohnt ist, und so einen optimalen Zeitpunkt für einen Einbruch bestimmen. [9]
Mit *Authentifizierung* soll verhindert werden, dass Sensor- oder Kontrollinformationen gefälscht werden. Ohne diese wäre es möglich, einen nicht authentifizierten Alarm an das System zu senden, woraufhin dieses alle Türen und Fenster öffnet, um eine Flucht zu ermöglichen. Ein Einbrecher kann solche gefälschten Nachrichten gezielt nutzen, um in ein Haus einzudringen. [9]
Zu den größten Bedrohungen zählen Angriffe, die die *Zugriffskontrolle* aushebeln. Erhält ein Hacker Zugriff auf die Systemsteuerung mit Administratorrechten, ist das gesamte System unsicher. Dies könnte durch unangemessenes Passwort- oder Schlüsselmanagement geschehen, oder indem ein nicht authentifiziertes Gerät am Netzwerk angemeldet wird. Selbst wenn nicht die Kontrolle über das System übernommen werden kann, so kann dennoch Schaden durch Denial of Service-Angriffe angerichtet werden. [9]

Im Weiteren soll die Sicherheit von aktuellen Smart Home Geräten an einem Fallbeispiel weiter analysiert werden. Für diesen Zweck wird das in Kapitel 2.1 beschriebene ZigBee genauer betrachtet.
Die Sicherheit von ZigBee basiert hauptsächlich auf vier Konzepten [10]:
Es werden zwei verschiedene *Sicherheitsstufen* unterstützt. Hohe Sicherheit oder auch Kommerzielle Sicherheit genannt, sowie Standardsicherheit oder auch Häusliche Sicherheit genannt. Der Unterschied der beiden Stufen besteht im Schlüsselmanagement und in der Schlüsselverteilung. In der Hohen Sicherheit wird also der Netzwerkschlüssel nur verschlüsselt über die Luft übertragen und in der Standardsicherheit wird er im Klartext übertragen. Dies stellt eine ungemein große Sicherheitslücke dar und wird Kernstück eines später beschriebenen Angriffs.
Beim *Trust Center (TC)* handelt es sich um ein Gerät in einem ZigBee-Netzwerk, welches für das Sicherheitsmanagement verantwortlich ist. Das TC verwaltet drei unterschiedliche Sicherheitsschlüssel, den Netzwerkschlüssel, den Masterschlüssel und den Linkschlüssel. Über diese drei Schlüssel authentifizieren sich ZigBee-Geräte und kommunizieren miteinander.
Als *Authentifizierung und Datenverschlüsselung* wird der Verschlüsselungsstandard AES mit 128 Bit Schlüssellänge gemeinsam mit dem Counter with Cipher Block

Chaining Message Authentication Code (CCM) verwendet.
Zum Schutz der *Integrität* kommt ein Message Integrity Code (MIC) zum Einsatz.

In [10] wird die sogenannte *ZigBee Network Key Sniffing Attack* beschrieben, die die vorher erwähnte Schwachstelle in der Standardsicherheitsstufe ausnützt. Um den Angriff auszuführen, wird ein Packet-Sniffing-Tool benötigt, mit dem die Kommunikation der ZigBee Endgeräte überwacht werden kann. Im nächsten Schritt wird eine frei erhältliche Software namens *KillerBee* verwendet, die wie ein Parser für die mitgeschnittene Kommunikation funktioniert. Sie sucht im Application Support Sublayer (APS) nach den entsprechenden Frames, die den Schlüssel beinhalten, und identifiziert den Netzwerkschlüssel anhand des Typs 0x01. Sobald der Schlüssel dem Angreifer bekannt ist, kann dieser sich mit einem eigenen Gerät in das Netzwerk einklinken und sämtliche andere Geräte angreifen.

Die Empfehlung der ZigBee Spezifikation besagt zwar, die Standardsicherheitsstufe nicht zu verwenden, jedoch ist dies kein Zwang und wird standardmäßig verwendet. Aus diesem Grund sind unzählige ZigBee-Geräte über diese Schwachstelle angreifbar. Die klare Empfehlung lautet hier, komplett auf diesen Standard zu verzichten und nur die hohe Sicherheitsstufe zu verwenden.

Auch andere Angriffe auf ZigBee-Geräte sind bekannt. Viele davon zielen auf Denial-of-Service ab, wodurch entweder die Funktionalität der Geräte selbst gestört wird oder deren Energieverbrauch in die Höhe getrieben wird, sodass die eingebauten Batterien schnell versagen und so das Gesamtsystem beeinträchtigen. [10]

Ein weiteres Beispiel für die Anfälligkeit von Smart Home-Geräten zeigt ein Experiment der Sicherheitsexperten Andrew Tierney und Ken Munro. Diese haben ein Thermostat mit einer Ransomware versehen und somit dem eigentlichen Benutzer die Kontrolle über dessen eigene Heizung entzogen. In einem echten Hackerszenario würde der Hacker in so einem Fall nur gegen Bezahlung die Kontrolle wieder auf den rechtmäßigen Besitzer übertragen. Wie einfach der Angriff auszuführen war, beschreiben sie in einem Blog. [11]
Selbst wenn es sich bei diesem Experiment nur um ein Thermostat gehandelt hat, zeigt dies doch, wie anfällig auf dem Markt verfügbare Geräte sind. Eine solche Schwachstelle reicht einem Hacker schon aus, um einen Einstiegspunkt in das Netzwerk des Opfers zu finden. Noch schlimmer wäre ein solches Szenario, bei dem beispielsweise ein automatisches Türschloss gehackt wird und somit Tür und Tor für Einbrecher offen stehen.

4 Ausblick

Die Möglichkeiten, die IoT bietet, sind vielfältig und vielversprechend. Aus diesem Grund ist auch die Entwicklung hin zum Vernetzen aller Dinge ein unaufhaltsamer Fortschritt, der schon längst in Gang gesetzt wurde. Mit zukünftigen Technologien können sogar einzelne Autos oder Flugzeuge miteinander vernetzt werden sowie innerhalb sicherheitskritischer Anlagen wie Atomkraftwerken einzelne Komponenten, die für die Überwachung und Steuerung des Betriebs zuständig sind. Das IoT lockt mit einem bemerkenswerten Nutzen, der bisher allerdings immer auf Kosten der Sicherheit und Privatsphäre geht. Es besteht kein Zweifel daran, dass in nicht so ferner Zukunft IoT-Geräte in das alltägliche Leben zuhause und auf der Arbeit integriert werden, allerdings reicht das heutige Sicherheitskonzept bei Weitem nicht für diesen großflächigen und weitreichenden Einsatz aus. Je mehr die Technologie aus dem sichtbaren Blickfeld der Nutzer verschwindet und im Hintergrund agiert, umso mehr muss der Nutzer wissen, mit was er interagiert, und umso stärker müssen die Sicherheitsanforderungen an die Hersteller ebendieser Technologien sein.

5 Fazit

IoT und seine Anwendungen wie Smart Home sind sicherlich eine Bereicherung für die Nutzer im Hinblick auf Nutzen und Komfort. In Zukunft wird noch viel an diesen Anwendungsfällen und den dafür nötigen Geräten geforscht und weiterentwickelt werden, denn diese Verbesserung wird auch nötig sein, um eine sichere Verwendung für die Allgemeinheit zu gewährleisten. Aktuelle Geräte, die bereits auf dem Markt für den privaten Gebrauch verfügbar sind, weisen weitgehend enorme Schwächen auf, die von Hackern ausgenutzt werden könnten. So wird sehr schnell aus dem Traum eines vollautomatischen und überwachten Zuhauses ein Paradies für Hacker und Einbrecher und gleichzeitig ein Albtraum für die Bewohner. Bis die benötigte Sicherheitsarchitektur für Anwendungsfälle wie das Smart Home entworfen und umgesetzt wird, sollte der Umgang mit den verfügbaren Geräten mit großer Vorsicht genossen werden.

6 Literaturverzeichnis

[1] Ashton, K.: That 'Internet of Things' Thing, RFID Journal, 2009, http://www.rfidjournal.com/articles/pdf?4986, Abgerufen am 12.03.2017.

[2] Gubbi, J. et al.: Internet of Things (IoT): A vision, architectural elements, and future directions, Elsevier B.V., 2013.

[3] Kemper, A. et al.: Blockseminar: The "Internet of Things" for industrial applications, Technische Universität München, 2014, http://db.in.tum.de/teaching/ws1314/industrialIoT/, Abgerufen am 12.03.2017.

[4] Robles, R. J., Kim, T.: A Review on Security in Smart Home Development, International Journal of Advanced Science and Technology, Vol. 15, 2010.

[5] Telecom ABC: Powerline Communications (PLC), 2005, http://www.telecomabc.com/p/plc.html, Abgerufen am 13.03.2017.

[6] Fan, C. et al.: A middleware of Internet of Things (IoT) based on Zigbee and RFID, in Communication Technology and Application (ICCTA), IET International Conference, 2011.

[7] Misra, S. et al.: Security Challenges and Approaches in Internet of Things, SpringerBriefs in Electrical and Computer Engineering, 2017.

[8] Evans, D.: The Internet of Things – How the Next Evolution of the Internet is Changing Everything, Cisco IBSG, 2011.

[9] Lin, H., Bergmann, N. W.: IoT Privacy and Security Challenges for Smart Home Environments, School of Information Technology and Electrical Engineering, 2016.

[10] Vidgren, N. et al.: Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned, 46th Hawaii International Conference on System Sciences, 2013.

[11] Tierney, A.: Thermostat Ransomware: a lesson in IoT security, PenTestPartners, 2016, https://www.pentestpartners.com/blog/thermostat-ransomware-a-lesson-in-iot-security/, Abgerufen am 10.04.2017.

Messung der Qualität einer automatischen Warendisposition

Nils Lindholm
DHBW Stuttgart
n.lindholm@live.de

Abstract
Eine optimale Warenversorgung ist für Filialen im Lebensmitteleinzelhandel von höchster Wichtigkeit. Insbesondere die neuen Möglichkeiten einer softwaregestützten automatischen Warendisposition sind dabei von Interesse. Die vorliegende Arbeit untersucht diese Fragestellung am Beispiel des Unternehmens Lidl durch einen Vergleich des aktuellen Dispositionsprozesses mit einem automatischen Dispositionsprozess. Hierzu wird ein Messinstrument definiert, werden Messdaten erhoben und diese statistisch ausgewertet. Erste Ergebnisse bestätigten die Qualität der automatischen Warendisposition.

Schlüsselwörter
Lebensmitteleinzelhandel, Automatische Warendisposition, Optimal Shelf Availability, Out-of-Stock

CR-Kategorien
H.4.2 [**Types of Systems**]: Logistics

Betreuer Hochschule: Prof. Dr. Kai Holzweißig
DHBW Stuttgart
kai.holzweissig@dhbw-stuttgart.de
Betreuer Firma: Andreas Wolf
Lidl Stiftung & Co. KG
andreas.wolf@lidl.com
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1 Einleitung
Der Lebensmitteleinzelhandel zeichnet sich durch eine hohe Wettbewerbskonzentration aus [4]. Die zunehmende Komplexität des Einzelhandels durch die Digitalisierung und das sich ändernde Kundenverhalten machen Prozessveränderungen notwendig [3]. Auch die Lidl Stiftung stellt sich auf diesen Trend ein und hat sich entschieden, die Möglichkeiten einer automatischen Warendisposition mittels des Produktes „SAP Forecasting and Replenishment (F&R)“ zu untersuchen. Die elementare Forschungsfrage dabei, die Gegenstand dieser Arbeit ist, lautet: Sorgt dieser neue Prozess für eine Qualitätsverbesserung der Warenverfügbarkeit?

2 Automatische Warendisposition
Vor einigen Jahren noch ist eine Bestellung bei den meisten Einzelhändlern durch ein manuelles Bestellsystem durchgeführt worden. Die Filialmitarbeiter haben die verfügbare Artikelmenge im Regal geprüft und anhand dieser Information und der eigenen Erfahrungswerte die Bestellung getätigt [1]. Durch technische Weiterentwicklungen wie standardisierten Artikelnummern (bspw. EAN) und Electronic Data Interchange (EDI) ist eine Automatisierung dieses Prozesses für Einzelhändler zunehmend einfacher [1]. Die automatische Warendisposition lässt sich dabei als eine systemgestützte Nutzung von Verbrauchs- und Bestandsdaten bezeichnen, welche das Ziel hat, automatisierte Bestellungen zu generieren, die für eine optimale Warenverfügbarkeit sorgen [5].

3 Messinstrumentsauswahl

Für den Vergleich der beiden Prozesse sind Kennzahlen auf Basis der von CRONE definierten Messgrößen [2] zur Qualitätsmessung einer Warendisposition in Kombination mit den Lidl-spezifischen Anforderungen an die Warenoptik ausgewählt worden. Dabei ist die elementare Messgröße das Auftreten von Out-of-Stock-Situationen. Diese sind unbedingt zu vermeiden, da nach [1] alle Optimierungen entlang der Wertschöpfungskette vergeblich sind, wenn der Kunde nicht die Möglichkeit erhält, seinen Bedarf zu decken. Die zentrale Messgröße ist demnach die Anzahl der auftretenden Nullbestände je Periode. Die Vergleichsgröße für die Bestimmung dieses Ereignisses ist die Regalfüllmenge der Artikel je Filiale. Wenn demnach innerhalb eines betrachteten Zeitraums der Bestand eines Artikels auf null sinkt, wird das Auftreten dieses Ereignisses gezählt. Die Summe dieser Ereignisse wird nach Durchführung der Datenerhebung durch die Anzahl aller erhobenen Bestandsdaten der Periode dividiert, um eine Out-of-Stock-Quote (OoS-Quote) zu ermitteln.

4 Untersuchungsergebnisse

Zur Überprüfung der Hypothese, dass eine automatische Warendisposition die OoS-Quote senken kann, sind über einen Zeitraum von elf Wochen die beschriebenen Kennzahlenwerte für drei Sortimentsgruppen und 300 Artikel im Bereich des Trockensortimentes in drei Filialen erhoben worden. Für eine statistische Auswertung werden die OoS-Quoten der drei Filialen über die verschiedenen Wochen aggregiert und zwei Stichproben gebildet. Stichprobe A mit den OoS-Quoten für die Wochen 1-6, in denen keine automatische Warendisposition genutzt worden ist ($\bar{x} = 0{,}0136$; $s = 0{,}0041$) und Stichprobe B für die Wochen 7-11, in denen eine automatische Warendisposition zum Einsatz gekommen ist ($\bar{x} = 0{,}0037$; $s = 0{,}0136$). Die Anwendung des Welch-Tests zeigt, dass zwischen den beiden Stichproben ein signifikanter Unterschied besteht ($t = 5{,}52$; $df = 6{,}57$; $p < 0{,}001$; *einseitig*). Die Hypothese kann somit – vorbehaltlich der Effekte anderer Einflussfaktoren auf die OoS-Quoten – bestätigt werden.

5 Kritische Reflexion

Die vorliegende Arbeit zeigt, dass der Einsatz einer automatischen Warendisposition unter bestimmten Voraussetzungen zu einer Verbesserung der Warenverfügbarkeit führen kann. Da die Studie nur auf Basis einer Stichprobe im Trockensortiment durchgeführt worden ist, besteht weiterer Forschungsbedarf für andere Sortimentsbereiche. Das Ergebnis beruht weiterhin auf einer Stichprobe aus nur einem Land und muss daher durch Daten anderer Länder verifiziert werden, um eine allgemeingültige Aussage für das Unternehmen Lidl treffen zu können. Das Ergebnis ist auf die Gesamtheit des Lebensmitteleinzelhandels nur bedingt übertragbar, da unterschiedliche Geschäftsprozesse sowie äußere Faktoren einen Einfluss ausüben können. Daher sollten diese Faktoren ebenfalls Gegenstand weiterer Untersuchungen sein.

6 Literaturverzeichnis

[1] A. Angerer. The Impact of Automatic Store Replenishment Systems on Retail. Dissertation, Universität St. Gallen, 2005.

[2] S. F. Crone. Neuronale Netze zur Prognose und Disposition im Handel, 1. Aufl., Wiesbaden, Gabler, 2010.

[3] S. Gabriel. Jetzt die mittelständischen Einzelhändler unterstützen. In: Handelsfakten 2016, Wie wir shoppen werden, Handelsverband Deutschland, corps. Verlag, 2015.

[4] J. Haucap (Hg.). Wettbewerbsprobleme im Lebensmitteleinzelhandel, DICE Ordnungspolitische Perspektiven, Band Nr. 48, Düsseldorf Institute for Competition Economics (DICE), 2013.

[5] M. B. Myres. P. J. Daugherty C. W. Autry. The effectiveness of automatic inventory replenishment in supply chain operations: antecedents and outcomes, in: Journal of Retailing, 76. Jg., Nr. 4, S. 455–481, 2000.

Methodik zur Analyse der Auswirkung von Fahrerassistenzsystemen bei PKW

Sandra Kaufmann
DHBW Stuttgart
kaufmann-sandra@gmx.de

Abstract

In dieser Arbeit wird eine Methodik zur Überprüfung der Fragestellung, ob ein Zusammenhang zwischen den an der Front wirkenden Fahrerassistenzsystemen (FAS) und den an der Front auftretenden Schäden bei PKW besteht, dargelegt. Diese Fragestellung resultiert aus einer vorangegangenen Analyse, bei der eine annähernd gleiche Verteilung der Front- und Heckschäden nachgewiesen wurde. Weiter zurückliegende Analysen hingegen zeigen eine deutliche Häufung der Frontschäden. Die Datenbasis dieser Arbeit geht auf Schadengutachten der DEKRA Automobil GmbH zurück. Diese ist mit Hilfe von SQL-Abfragen und statistischer Methoden analysiert worden.

Schlüsselwörter

PKW, Fahrerassistenzsysteme, Frontschäden, deskriptive Statistik, induktive Statistik, Datenbankabfrage, Sekundäranalyse

CR-Kategorien

G.3 [Probability and Statistics], H.2.4 [Systems]

Betreuer Hochschule: Prof. Dr. Kai Holzweißig
DHBW Stuttgart
kai.holzweissig@dhbw-stuttgart.de

Betreuer Firma: Herr Walter Niewöhner
DEKRA Automobil GmbH
walter.niewöhner@dekra.com

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1 Zielsetzung

Die Motivation zu der vorliegenden Arbeit stellt eine interne Untersuchung zur Lage von Unfallschäden dar. Dabei ist beobachtet worden, dass Schäden an Fahrzeugfront und Fahrzeugheck mit annähernd gleicher Häufigkeit auftreten. Dies war bei früheren Analysen nicht der Fall, da hier ein deutlich höheres Schadensaufkommen an der Front gefunden wurde. Aus dieser Tatsache resultiert die Hypothese, dass bei PKW, die mindestens ein an der Front wirkendes FAS verbaut haben, die Anzahl der Schäden an der Fahrzeugfront geringer ist als bei PKW, die keines dieser FAS verbaut haben.

Das Ziel dieser Arbeit ist es, eine geeignete Methodik zur Analyse des Zusammenhangs zwischen dem Auftreten von Frontschäden bei PKW und den an der Front wirkenden FAS zu entwickeln.

2 Eingrenzung der zu untersuchenden PKW

Es werden ausschließlich diejenigen FAS näher betrachtet, die das Potential aufweisen, aktiv Schäden an der Front verhindern zu können. Es erfolgt keine Betrachtung derjenigen FAS, die Schäden am gesamten Fahrzeug verhindern können oder am Fahrzeugheck beziehungsweise an den Fahrzeugseiten wirken.

Zur besseren Vergleichbarkeit werden ähnliche Modelle verschiedener Premiumhersteller untersucht, wie auch schon bei der vorangegangenen Untersuchung, die die Ausgangssituation dieser Arbeit darstellt. Zum

Abgleich erfolgt im zweiten Schritt eine Untersuchung zusätzlicher PKW. Alle untersuchten PKW der Premiumhersteller werden in die Kategorien *mit FAS* und *ohne FAS* unterteilt, wobei zur Kategorie *mit FAS* nur bestimmte, vorher eingehend diskutierte FAS, gezählt werden. Daher zählen zu der Kategorie *ohne FAS* alle Fahrzeuge, die keines dieser ausgewählten FAS enthalten, wobei alle anderen FAS enthalten sein können. Ergänzend werden die am Markt aktuellen PKW der untersuchten Modelle mit ihren jeweiligen Vorgängermodellen verglichen, um zu überprüfen, ob eine generell höhere Anzahl an FAS eine Reduktion der Frontschäden bewirkt.

3 Methodisches Vorgehen

Die Datenerhebung erfolgt mittels Sekundäranalyse mit Hilfe der DEKRA Fachdatenbank. Entsprechend werden nur diejenigen Merkmalsträger untersucht, deren Daten in der DEKRA Fachdatenbank vorhanden sind. Es wird davon ausgegangen, dass die vorhandene Stichprobe repräsentativ für die Grundgesamtheit ist, da mit großer Wahrscheinlichkeit nicht vorwiegend Fahrzeuge mit einem bestimmten Schadensaufkommen zu DEKRA gebracht werden. Die Auswahl der Stichprobe beschränkt sich auf ausgewählte Fahrzeugmodelle. Hierzu gehören die Premiummodelle Mercedes C-Klasse, Audi A4, BMW 3er und zusätzlich die Modelle Skoda Octavia und VW Golf.

Die Daten werden mit Hilfe deskriptiver Statistik und Datenbankabfragen ermittelt und auf Basis der resultierenden Relativzahlen erstmals betrachtet. Dadurch ist es möglich, Verhältnisse zwischen Front- und Heckschäden der einzelnen Modelle zu analysieren. Anschließend werden die Daten mit Methoden der induktiven Statistik überprüft. Dies geschieht anhand eines Chi-Quadrat-Tests und, sollte hierdurch Signifikanz nachgewiesen werden können, zusätzlich mit einer Überprüfung des Zusammenhangsmaßes Phi [1]. Erste Untersuchungsergebnisse unter Anwendung der zuvor beschriebenen Methodik zeigen, dass mit Hilfe deskriptiver Mittel ein Unterschied sichtbar wird. Durch die anschließende Überprüfung mittels induktiver Statistik hingegen kann kein Zusammenhang nachgewiesen werden.

4 Kritische Reflektion

Statistische Verfahren sind sicherlich ein guter Ansatz, um einer solchen Fragestellung nachzugehen. Allerdings konnten im Rahmen der Studie nur ausgewählte statistische Verfahren berücksichtigt werden. Statistiken weisen zudem Toleranzen auf [2]. Eine genaue Abgrenzung der Modelle *mit FAS* und *ohne FAS* kann bei den bisher untersuchten Modellen nicht erfolgen, da bei aktuellen Modellen viele FAS serienmäßig verbaut sind und somit nicht mehr berücksichtigt werden. Zudem kann es zu einer Verfälschung der Ergebnisse kommen, da auch bei Fahrzeugen, die mindestens eines der vorher ausgewählten an der Front wirkenden FAS verbaut haben, andere FAS zur Ausstattung gehören können, die am Fahrzeugheck oder an den Fahrzeugseiten wirken. Dies kann dazu führen, dass sich die Effekte der FAS gegenseitig aufheben und so in der Statistik nicht sichtbar werden.

Diese Arbeit ist als erster Ansatz zu betrachten, um die genauen Effekte der FAS hinsichtlich der Vermeidung von Frontschäden näher zu untersuchen. Es kann hieran angeknüpft werden und weitere Forschungsarbeit erfolgen.

Literatur

[1] U. Kuckartz, S. Rädiker, T. Ebert, J. Schehl. Statistik, Eine verständliche Einführung, Wiesbaden, Springer VS, 2., überarb. Aufl., 2013.

[2] I. Stelzl. Fehler und Fallen der Statistik, für Psychologen, Pädagogen und Sozialwissenschaftler, Münster, New York, München, Berlin, Waxmann, 2005.

Eine domänenspezifische Sprache für die prozedurale Dimensionierung im analogen IC Entwurf *

Florian Leber, Jürgen Scheible
Robert Bosch Zentrum für Leistungselektronik, Reutlingen University
{florian.leber, juergen.scheible}@Reutlingen-University.DE

Abstract

Der Entwurf von analogen Schaltungen basiert bis heute weitgehend auf Erfahrungswissen und bedarf einer weitergehenden Automatisierung. Eine Möglichkeit dafür sind prozedurale Verfahren, welche das Expertenwissen in einem Ablaufskript speichern. Die Erfassung des Expertenwissens ist dabei essenziell, aber jedoch bis heute nur unzureichend gelöst. Mit EDPL (Expert Design Plan Language) stellen wir einen neuen Lösungsansatz für dieses Problem vor. EDPL ist eine domänenspezifische Sprache, welche die intuitive und schnelle Eingabe von Expertenwissen ermöglicht.

Schlüsselwörter

Mikroelektronik, Chipentwurf, CAD Software, EDA, Prozedurale Generatoren

CR-Kategorien

J.2 [**PHYSICAL SCIENCES AND ENGINEERING**]: Electronics; D.3.2 [**Language Classifications**]: Specialized application languages

1 Einleitung

Die Dimensionierung von analogen Schaltungen ist ein wesentlicher Bestandteil des Entwurfs integrierter Schaltkreise. Da die Komplexität der analogen Schaltungen steigt, muss dieser Entwurfsschritt weiter automatisiert werden. Dadurch wird der Aufwand reduziert und die Entwurfseffizienz verbessert. Die Verfahren dieser Automatisierung können grundlegend in zwei Arten unterschieden werden [3]: (a) Optimierende Verfahren suchen anhand von Algorithmen eine Lösung. (b) Prozedurale Verfahren generieren auf Basis von gespeicherten Expertenwissen ein Ergebnis. Dabei wird das prozedurale Ablaufskript durch einen Experten selbst erstellt. Der Lösungsweg ist somit vorgedacht.

2 Problemstellung

Bisher konnten sich die prozeduralen Verfahren für die Dimensionierung von analogen Schaltungen nicht durchsetzen. Das Problem dieser Verfahren ist der hohe Aufwand, um das Ablaufskript zu erstellen [2]. So wird z.B. in OASYS [1] bis zu einem Monat für die Erstellung des Ablaufskripts gebraucht, während eine typisch händische Dimensionierung einige Stunden benötigt.

3 Unser Ansatz: Eine domänenspezifische Sprache

Bisherige prozedurale Verfahren bauen auf generischen Programmiersprachen (z.B. Franz LISP in OASYS [1]) auf. Im Unterschied hierzu, schlagen wir eine domänenspezifische Sprache vor. Die Idee ist, dass diese (a) die Eingabe des Expertenwissens vereinfacht und (b) Metabefehle enthält, welche typische Arbeitsschritte automatisieren.

*
Danksagung: Wir danken Philipp Lamprecht für seine Arbeit an der prototypischen Umsetzung der EDPL.
-
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

3.1 Anforderungen

Anhand der EDPL sollen die Experten genau ihre Vorgehensweise eingeben können. Dies erfordert für jeden Schritt einen entsprechenden Befehl. Da die Eingabe durch den Experten selbst erfolgt, ist zudem eine hohe Akzeptanz wichtig. Deshalb muss die Eingabe sehr intuitiv sein und keinen (bemerkbaren) Mehraufwand darstellen.

3.2 Expert Design Plan Language (EDPL)

Die EDPL besteht aus Expertenbefehlen, die sich auf reale Schritte der Dimensionierung beziehen. Diese Befehle stellen das Interface für den Experten dar. Daher werden auch keine primitiven Datentypen, sondern für Experten bekannte Performance Parameter verwendet. Insgesamt ist die Verwendung der EDPL für Experten intuitiv und schnell. Im Hintergrund rufen die Expertenbefehle verschiedene Libraries auf. Diese enthalten die dahinter liegenden Automatismen.
Die Expertenbefehle können in vier Kategorien unterteilt werden:

1. Formelbefehle - diese werden benutzt um die initiale Dimensionierung zu berechnen und um die Abhängigkeiten zwischen den Parametern zu bestimmen.

2. Simulationsbefehle - dies sind Befehle um den Simulator und die Testbench zu initialisieren, um einen Autorun der Simulation durchzuführen, für die qualitative Bewertung von Ergebnissen sowie für das Auslesen der Performance Parameter.

3. Bauteilbefehle - diese ermöglichen das Lesen und Schreiben von Bauteilwerten.

4. Strukturbefehle - diese werden für Bedingungen, Iterationen, Ausgaben und Abbruchbedingungen benötigt.

4 Prototypische Umsetzung

Wir haben unseren Ansatz für eine Source-Schaltung prototypisch umgesetzt. Unser Ziel war hierbei die prinzipielle Eignung unserer Idee zu prüfen. Dazu modellierten wir den manuellen Ablauf und leiteten von diesem insgesamt 10 EDPL-Befehle ab. Diese implementierten wir mit Skill++ in Cadence Virtuoso in einer internen DSL. Für das Erstellen des Ablaufskripts eines typischen Szenarios benötigten wir mit Hilfe dieser EDPL 2,5h (ohne das Erlernen der Sprache). Das Ablaufskript selbst hatte eine Laufzeit von 5 Minuten. Im Vergleich dazu benötigt der manuelle Entwurf von Hand 3h.

5 Zusammenfassung und Ausblick

In diesem Paper stellten wir den Ansatz einer domänenspezifische Sprache für die Dimensionierung analoger Schaltungen vor. Anhand einer prototypischen Umsetzung konnten wir die prinzipielle Eignung unseres Ansatzes nachweisen. Im nächsten Schritt wollen wir die EDPL generalisieren, sodass der ganze analoge Schaltungsentwurfsprozess unterstützt wird. Außerdem planen wir eine visuelle Implementierung, um eine noch intuitivere Eingabe zu ermöglichen.

Literatur

[1] R. Harjani, R. A. Rutenbar, and L. R. Carley. „OASYS: a framework for analog circuit synthesis“. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 8(12):1247–1266, Dec 1989.

[2] N. Lourenço and N. Horta. „GENOM-POF: Multi-objective Evolutionary Synthesis of Analog ICs with Corners Validation“. In *Proceedings of the 14th Annual Conference on Genetic and Evolutionary Computation*, GECCO ’12, pages 1119–1126, New York, NY, USA, 2012. ACM.

[3] J. Scheible and J. Lienig. „Automation of Analog IC Layout: Challenges and Solutions“. In *Proceedings of the 2015 Symposium on International Symposium on Physical Design*, ISPD ’15, pages 33–40, New York, NY, USA, 2015. ACM.

Datenbankgestützte Generierung von Rulefiles für MEMS-Fertigungsprozesse

Raphael Eißler
Hochschule Reutlingen
Raphael.Eissler@Student.Reutlingen-University.de

Prof. Dr.-Ing. Jürgen Scheible
Hochschule Reutlingen
Robert Bosch Zentrum für Leistungselektronik
Juergen.Scheible@Reutlingen-University.de

Abstract
Vorgestellt wird ein Softwareprojekt aus dem Bereich der *Electronic Design Automation (EDA*), in dem eine Datenbank zur standardisierten Erfassung und Pflege von Entwurfsregeln für Halbleitertechnologien entwickelt wurde, sowie eine Software, die auf dieser Basis die automatische Generierung der zugehörigen Rulefiles ermöglicht.

Schlüsselwörter
Electronic Design Automation, EDA, Rulefiles, Design Rule Check, DRC, Datenbank

CR-Kategorien
J.6 [**Computer Aided Engineering**]: Computer Aided Design; H.2.4 [**System**]: Relational Databases, Oracle; H.5.2 [**User Interfaces**]: Standardization.

1 Einleitung
Mikroelektromechanische Systeme (*MEMS*) werden wie integrierte Schaltkreise auf Halbleiterscheiben (*Wafern*) gefertigt, aus denen sie dann als sog. *Chips* ausgeschnitten werden. Die Strukturen werden zunächst als zweidimensionale geometrische Figuren (*Polygone*) auf durchsichtige Masken aufgebracht, die anschließend photolithografisch auf die Waferoberfläche abgebildet werden (z.B. [1] Kap. 4). Die nur wenige Mikrometer dünnen räumlichen Strukturen entstehen durch Implantation von Fremdstoffen und Ätzverfahren, die insbesondere bei MEMS sehr kompliziert sind, da hier komplexe frei bewegliche Gebilde freizustellen sind

Die Menge aller Polygone, die einen Entwurf beschreiben, heißt *Layout*. Jedes Polygon ist dabei einem *Layer* zugeordnet, der die zugehörige Maske definiert (s. [2] Kap. 21). Um die Fertigbarkeit der mikroskopisch feinen Strukturen sicherzustellen, müssen die Polygone Entwurfsregeln (*Rules*) einhalten (s. [2] Kap. 22). Es gibt Regeltypen für Polygone nur eines Layers (typisch: Mindestweite und -abstand) und für Polygone zweier Layer (typisch: Mindestabstand oder -überlappung).

In einem *Design Rule Check (DRC)* wird ein Layout auf Einhaltung der Rules automatisch geprüft. Dazu liest ein Prüfprogramm (*DRC-Tool*) die in einer toolspezifischen Syntax formulierten Regeln als *Rulefile* ein und wendet diese auf die Layoutdaten an. Ein fehlerfreier DRC ist für jeden Fertigungsdurchlauf obligatorisch.

Das hier vorgestellte Projekt wird im Auftrag eines Herstellers von MEMS-Sensoren durchgeführt, der seine Halbleiterprozesse selbst entwickelt. Durch die stetige Weiterentwicklung der Prozesse sind die Rulefiles einer dynamischen Änderung unterworfen. Projektziel ist die Entwicklung einer Datenbank für die Erfassung und Pflege von Entwurfsregeln für verschiedene Prozesse und deren Varianten, sowie ein Programm, das für jeden Fertigungsdurchlauf ein korrektes Rulefile automatisch generiert.

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

2 Anforderungen

Da die Prozessexperten in der Regel keine EDA-Expertise haben, soll die Eingabe der Regeln in die Datenbank ohne Kenntnisse der Rulefile-Syntax möglich sein. Weitere Anforderungen an die Datenbank sind:

- Versionierung der einzelnen Regeln
- Unterstützung von Regelvarianten
- Rollenbasierte Zugriffsrechte
- Unterstützung unterschiedl. DRC-Tools
- Unterstützung von „Sonderchecks“ und „Init-Files“ (s. Kap. 4)

Anforderungen für die Software zur automatischen Generierung von Rulefiles sind:

- Umsetzung in Python 2.7
- Umfassende Dokumentation
- Eine benutzerfreundliche Eingabemaske
- Reportfunktionen (Ausdruck kompletter Regelsätze mit/ohne erläuternde Bilder)
- Ein- und ausschaltbare Hilfefunktionen
- Rollenbasierte Zugriffsrechte

3 Rulefile-Datenbank

Die relationale Datenbank ist mit Oracle umgesetzt und besitzt 18 Tabellen. Die wichtigsten werden nachfolgend erläutert (Tabellennamen in eckigen Klammern).

Der Kern der Datenbank ist [Process]. An diese sind [Regeln], [Layer] und [Projekte] angebunden. [Projekte] speichert die in einem Prozess gefertigten MEMS-Projekte. Angebunden an [Regeln] sind [Versions] und [Options] zur Versionierung der Regeln und zur Handhabung unterschiedlicher Prüfmaße in Abhängigkeit von Prozessoptionen.

In [Tool] bzw. [Template] befinden sich die für die Rulefile-Generierung benötigten syntaktischen Beschreibungen, wie ein Rulefile bzw. wie die DRC-Checkbefehle für die einzelnen Regeltypen aufgebaut sind. Diese beiden Tabellen ermöglichen die Toolunabhängigkeit aller restlichen Daten.

Für die Verwaltung unterschiedlicher Zugriffsrechte auf die Daten (z.B. Ändern von Regeln oder Anlegen von Projekten) wird ein einfaches rollenbasiertes Modell genutzt.

4 Rulefile-Generierung

Zur Rulefile-Generierung muss ein Prozess (dieser bestimmt den Regelsatz) und ein (DRC-)Tool ausgewählt werden. Ein Rulefile wird gem. der in [Tool] hinterlegten Struktur erzeugt und besteht gewöhnlich aus den Bereichen (1) „Init-Files“, (2) „Layer“, (3) „Regeln“ und (4) „Virtuelle Layer“.

„Init-Files“ enthält Textdateien zur Ausführung von Initialisierungen. In „Layer“ werden alle Layer des Prozesses deklariert. Im Hauptabschnitt „Regeln“ werden alle Checks für den spezifizierten Regelsatz gem. der in [Template] beschriebenen Syntax generiert. Jeder Check enthält den Regelnamen, die betroffenen Layer, den Regelwert (= Prüfmaß) und einen Kommentar, der dem Auswerter des DRC-Runs bei Regelverletzungen Informationen zu der jeweiligen Regel gibt.

Für den Fall, dass spezielle prozesstechnische Anforderungen nicht mit den verfügbaren Standard-Regeltypen beschreibbar sind, programmieren Experten sog. *Sonderchecks* direkt in der toolspezifischen Syntax. Hierfür sind sog. *virtuelle Layer* zur Speicherung von Zwischenergebnissen nötig. Im Abschnitt „Virtuelle Layer“ werden diese Layer deklariert und die Sonderchecks von außerhalb der Datenbank als Textdatei her kopiert.

5 Status und Ausblick

Erste Softwaretest waren erfolgreich. Zu erwartende Vorteile sind: (1) Prozessänderungen sind nachvollziehbar (2), Prozessvielfalt wird beherrschbar, (3) standardisierte Regelerfassung reduziert Prüflücken. Dadurch werden Entwurfsrisiken und Aufwände zur Rulefile-Erstellung signifikant reduziert.

Literatur

[1] K.-H.. Cordes, A. Waag, N. Heuck. *Integrierte Schaltungen*: *Grundlagen – Prozesse – Design - Layout*, Pearson Studium, München, 2011.

[2] D. Jansen (Hrsg.). *Handbuch der Electronic Design Automation*, Carl Hanser, München, 2001.

TurbFish: An Open Source Smart Sensor for Water Quality Monitoring

Ingo Bloemker
Reutlingen University AC, LFZ PA&T
Ingo_Manfred.Bloemker@Student.Reutlingen-University.DE

Marilena Pagano
Reutlingen University AC, LFZ PA&T
Marilena.Pagano@Student.Reutlingen-University.DE

Abstract
In spring 2016, a massive fish death occurred in the German stream Brigach. With classical analytics, no reason could be investigated yet. This paper describes an open source project, which focusses on the construction of a turbidity measuring sensor. Embedded in a casing shaped like a fish, the sensor will continuously monitor the water quality of rivers without influencing the wildlife. By combining optical components with a networked microprocessor, an autonomous distribution of water quality properties on an internet based platform will be achieved.

Keywords
Water Quality, Turbidity, Embedded Sensor, Autonomous System, Smart Sensor, Sensor 4.0, Internet of Things (IoT), Real-time Measurement, Open Source Project

CR-Categories
C.3 **[Special-Purpose and Application-Based Systems]**: Process control systems, Real-time and embedded systems; I.2.9 **[Robotics]**: Sensors; J.2 **[Physical Sciences and Engineering]**: Chemistry, Engineering; J.3 **[Life and Medical Sciences]**: Health

Supervisor at University: Prof. Dr. Marc Brecht
Reutlingen University
Marc.Brecht@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10th of May 2017, Reutlingen University

Introduction
Environmental pollution in watercourses has become more severe within the last decades [1]. Governments all over the world have set regulations to the quality of drinking water and rivers. As part of these, the monitoring of turbidity is a common method to assess the risk of hazards. Even if there has been much effort on treating water in the past, there still is a lack of sufficient analysis, not only in the developing world, but also in developed countries. The recognizability of turbidity is limited to the fact, that fluids with less than 5 NTU (Nephelometric Turbidity Unit) will occur clear to the human eye [2]. Even though colloidal particles may impede disinfecting efforts, may carry loads of impurities or pathogens and may cause severe human diseases, if used for drinking purposes.

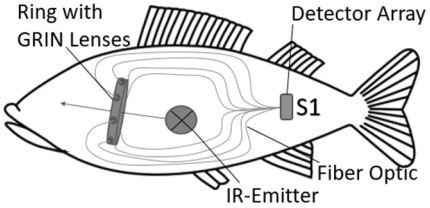

Figure 1: Construction of the TurbFish

The main factor for turbidity is the influence of suspended solids on electromagnetic radiation within a fluid. Depending on the size, the shape and the load of particles, fluids will lose their transparency, and scatter parts of the energy in all directions [3]. Measuring scattered radiation itself is limited by a

saturation of the particle concentration, where the material absorbs all the radiation before it can be detected [4].

Scientific and Technological Goals

The main aspect for the sensor system is a cheap and smart sensor, which works continuously for at least one year without any maintenance. The combination of the sensor signal and the integrated analysis of the data (e.g. chemometric modeling with trend analysis) leads to valuable parameters [5]. In addition, a low energy consuming, power harvesting setup is realized. The casing should be waterproof according to the IEC standard 60529 definition IPX8 [6]. The measuring range shall be between 0.1 and 800 NTU, with the focus on the low turbidity range below 10 NTU. The measuring method shall be equivalent to the standard EN ISO 7027, which provides a turbidity value by detecting the intensity of scattered and transmitted radiation, which is irradiated by an infrared source of 860 nm wavelength [7]. For a higher reliability, we increased the number of detectors from one to seven, which are arranged on a ring around the scattering volume; further noise reduction is achieved by lock-in detection. For an overall reduction of the sensors size, GRIN (GRadient INdex) lenses and optical fibers are used.

Figure 2: Integrated setup of the TurbFish and a wireless shield in a fishing float

The whole set-up is split into two parts to optimize its functionality: The TurbFish and a buoy. The detection and the amplification of the signal is done inside the TurbFish, while the buoy has the task of pre-processing the data in combination with wireless connection to a nearby network. With this feature, the turbidity signal will be directly sent to a server, where it can be obtained on the homepage of the fishermen, who are interested in the water quality of the river e.g. the Brigach.

Conclusion and Outlook

Turbidimetry is a valuable and fast technique to detect the amount of solid particles in watercourses, or to verify the correct function of filter systems, waste water treatment and other process relevant activities [8]. The arrangement of two separate segments, the TurbFish and the buoy, enables us to realize a turbimeter for inline detection in rivers for under 200 €. The possibility of pre-processing and the connection to the internet for exchanging information enhances the system towards a smart sensor. This is provided by adding a microcontroller with a wireless shield. Efforts like this will be necessary in the future: not only controlling fluctuating systems in process plants, discrete factories and the environment, but also predicting trends will be a challenging task within the next decades.

Literature

[1] CWWA, Drinking Water Disinfection and Turbidity Requirements - A Global Perspective, 2002.

[2] C.D. Kelley, A. Krolick, L. Brunner, A. Burklund, D. Kahn, W.P. Ball, M. Weber-Shirk, An affordable open-source turbidimeter, Sensors (Basel, Switzerland) 14 (4) (2014) 7142–7155.

[3] G. Mie, Annalen der Physik. Vierte Folge. Band 25, 1908

[4] M. Sadar, Turbidity standards: Technical Information Series — Booklet No. 12.

[5] D. Schaudel, Sensor 4.0 für Industrie 4.0; DOI 10.5162/12dss2015/4.1

[6] IEC, Degrees of protection provided by enclosures (IP Code), 2013.

[7] DIN EN ISO 7027: Bestimmung der Trübung 13.060.60, 2000.

[8] M.J. Sadar, TURBIDITY SCIENCE: Technical Information Series.

VRLab Hochschule Reutlingen

René Blänsdorf
Reutlingen University
Rene.Blaensdorf@Student.Reutlingen-University.DE

Markus Danilow
Reutlingen University
Markus.Danilow@Student.Reutlingen-University.DE

Lucas Hermann
Reutlingen University
Lucas_Jan.Hermann@Student.Reutlingen-University.DE

Abstract

Dieses Paper gibt einen kurzen Überblick über das Labor für virtuelle Realität (VR) der Hochschule Reutlingen. Dafür wird das HoloLens Tabletop-Spiel und ein Spiel für die HTC Vive mit dem Ziel des „collaborative gaming“ vorgestellt, die dort aktuell entwickelt werden. Bei dem Tabletop-Spiel ist es das Ziel ein rundenbasiertes Rollenspiel auf einen Tisch zu projizieren, damit zwei Nutzer der HoloLens an einem Tisch miteinander spielen können. Bei dem Spiel für „collaborative gaming“ sollen mehrere HTC Vive Spieler gemeinsam mit anderen Spielern ein gemeinsames Ziel verfolgen.

Schlüsselwörter

Virtual Reality, Gaming, HoloLens, HTC Vive, Collaboration, Tabletop

CR-Kategorien

H.5.1 [**Multimedia Information Systems**]: Artificial, augmented, and virtual realities; H.5.2 [**User Interfaces**]; K.4.3 [**Organizational Impacts**] Computer-supported collaborative work

Betreuer Hochschule: Prof. Dr. Cristóbal Curio
Cristobal.Curio@Reutlingen-University.de
Prof. Dr. Uwe Kloos
Uwe.Kloos@Reutlingen-University.de
Prof. Dr. Gabriela Tullius
Gabriela.Tullius@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

1 Einleitung

Das Virtual Reality Laboratory (VRLab) beschäftigt sich mit den unterschiedlichsten Einsatzmethoden und Mitteln der virtuellen Realität. Als virtuelle Realität wird dabei eine computergenerierte Welt bezeichnet, die mit mindestens einem Sinn erlebt wird und mit der interagiert werden kann [Vgl. 1, 2]. Dabei befindet sich der Nutzer jedoch nach wie vor in der physischen Realität. Sie umfasst also sowohl reine VR-Anwendungen, wie auch Augmented Reality (AR) Anwendungen – Anwendungen bei denen die reale Welt lediglich um zusätzliche, computergenerierte Inhalte erweitert wird – und deren Hardware [Vgl. 2]. Dabei kommen neue Technologien zum Einsatz, eigene Variationen werden selbst entwickelt, Visualisierungsmöglichkeiten untersucht und nach neuen oder besseren Methoden der Mensch-Computer-Interaktion auf diesem Gebiet gesucht.

2 HoloLens Tabletop-Spiel

Bei der Microsoft HoloLens handelt es sich um eine AR-Brille, die in der Lage ist computergenerierte Objekte in der realen Welt darzustellen. Dafür ist sie mit Sensoren ausgestattet, die sie den Raum erfassen lassen und verfügt über einen kleinen Bildschirm durch den diese Objekte beispielsweise an Wänden oder auf Tischen dargestellt werden können.

Die Vorteile gegenüber einem klassischen Brettspiel sind unter anderem die höhere Flexibilität und Freiheit. Selbst ohne weiteres Equipment und trotz räumlicher Trennung kann man jederzeit und überall mit

anderen HoloLens-Besitzern spielen. Die Voraussetzungen sind lediglich die HoloLens und ein drahtloser Internetzugang. Dabei wird davon ausgegangen, dass beides in einigen Jahren überall leicht zugänglich sein wird.

Im Rahmen dieses Projekts soll ein rundenbasiertes Rollenspiel entstehen, bei dem virtuelle Figuren in einer virtuellen Landschaft bewegt werden, die mithilfe der HoloLens auf einen Tisch oder ähnliches projiziert werden. Das Spielbrett kann durch die holografische Darstellung leicht gedreht, vergrößert und an die eigenen Bedürfnisse angepasst werden. Bei der Projektumsetzung steht dabei besonders der Umgang und die Interaktion mit der AR im Vordergrund. Dabei wird der Umgang mit der neuen Technologie geübt und die Studenten lernen die Limitationen und Schwierigkeiten aus erster Hand kennen. Dadurch müssen neue Lösungswege erarbeitet und bisherige Vorgehensweisen angepasst werden.

3 Collaborative Gaming

Das Masterprojekt „Collaborative Gaming“ beschäftigt sich mit der Frage, wie Kollaboration in der VR gelingen kann. Im Rahmen aktueller Entwicklungen arbeiten Menschen trotz räumlicher Trennung mehr und mehr zusammen. Während Lösungen wie Video-Konferenzsysteme und kollaborative Arbeit an Text- und Tabellendokumenten schon Teil des Arbeitsalltags sind, bieten sich im Hinblick auf die Zukunft weitere Möglichkeiten. Eine der vielversprechenden davon ist die Zusammenarbeit in einem gemeinsamen virtuellen Arbeitsraum, der virtuellen Realität. Durch diesen Arbeitsraum kann die räumliche Trennung kompensiert und eine direkte Kooperation ermöglicht werden.

Eine Ergänzung zur Zusammenarbeit in der virtuellen Realität, ist die Möglichkeit eines Eingriffs von außen. So ist es denkbar, dass Personen an der gemeinsamen Zielerreichung beteiligt sind, die selbst nur über ein Smartphone, Tablett oder einen einfachen PC verfügen.

Im Rahmen des Masterprojekts wird deshalb eine Beispielanwendung für die HTC Vive geschaffen in der mehrere VR-Benutzer gemeinsam mit Nicht-VR-Benutzern ein Ziel verfolgen. Im Verlauf der Entwicklung soll zusätzlich das technische Grundgerüst für weitere kollaborative Anwendungen entstehen und möglichst umfangreiches Wissen über Kollaboration in der virtuellen Realität gesammelt werden.

Eine besondere Herausforderung für alle kollaborativen Anwendungen ist es, die Zusammenarbeit zu erleichtern und zu forcieren. Durch einen gemeinsamen virtuellen Raum kann die räumliche Trennung teilweise aufgehoben werden. Zagal et al. zeigen in Collaborative Games [2], dass ein Spiel besondere Anforderungen an die Spielmechanik erfüllen muss um Kooperation nicht nur als Möglichkeit, sondern Kollaboration als Kernprinzip bei den Spielern zu verankern. Dazu stellen sie mehrere Prinzipien, wie das Verteilen von Fähigkeiten oder Verantwortungen unter den Spielern, als Kern einer kollaborativen Spielmechanik heraus.

Einschränkungen in der Zusammenarbeit bestehen besonders im Hinblick auf die Haptik. So existiert für ein Objekt das von mehreren VR-Akteuren gehalten wird keine Möglichkeit das Ziehen oder Drücken des anderen Akteurs spürbar zu machen. Eine Koordination beim gemeinsamen Greifen oder Halten von Objekten ist so nur eingeschränkt umsetzbar.

4 Literaturverzeichnis

[1] Steuer J. Defining Virtual Reality: Dimensions Determining Telepresence, Vol. 42, Issue 4, pp. 74-79, 1992.

[2] Mehler-Bicher, A., Steiger, L., Augmented Reality: Theorie und Praxis, edition 2, p. 1, München, 2014.

[3] Zagal, J., Rick, J., Hsi, I., Collaborative games: Lessons learned from board games in Simulation & Gaming, Vol 37, Issue 1, pp. 24 – 40, 2016.

Masterprojekt: Neue Welt 9

Neue Welt 9
Reutlingen University
Neuewelt9@Reutlingen-university.de

Abstract
Architekturen durchleben sehr oft einen Wandel. So können sich beispielsweise das Innenleben und die Kultur eines Gebäudes stark verändern. Für Zeitzeugen bleiben diese früheren Stände meist als Erinnerungen im Gedächtnis, wohingegen diese früheren Stände für andere Menschen häufig verschlossen bleiben. Virtuelle Welten können in diesem Kontext ein Mittel zur Dokumentation darstellen, so dass man damit ohne jeglicher Vorstellungskraft etwas von der früheren Welt erfahren kann. Im Masterprojekt „Neue Welt 9“ wird explizit das älteste Gebäude auf dem Reutlinger Campus auf eine solche Weise wiederbelebt.

Schlüsselwörter
3D-Modellierung, 3ds Max, Spiele-Engine, Unity, virtuelle Welt

CR-Kategorien
Virtual worlds software [Interactive Games]

1 Einleitung
Im Studiengang Human-Centered Computing stehen den Studenten drei verschiedene Projekte zur Auswahl an denen im Zuge des Masterprojektes gearbeitet werden kann. Die Neue Welt 9 ist eines dieser Projekte. Der Name wurde aus der Idee abgeleitet, die Informatik-Fakultät (Gebäude 9 auf dem Campus) virtuell nachzubauen, sodass das Gebäude selbst, aber auch die Geschichte dieses ältesten Gebäudes auf dem Campus spielerisch erkundet werden kann. Die Studenten bauen mit Hilfe von Tools, mit denen auch bekannte Spieletitel entwickelt werden, die reale Welt nach und erstellen Interaktionskonzepte mit der virtuellen Umgebung.

2 Stand der Technik
Zum heutigen Stand der Technik werden virtuelle Welten mithilfe verschiedener Werkzeuge am Computer erschaffen. Vor allem zwei Werkzeuge sind bei diesem Erschaffungsprozess meist unentbehrlich: Eine Software für die 3D-Modellierung, um Objekte möglichst detailgetreu für virtuelle Welten nachzubauen - und eine sogenannte Spiele-Engine, die verschiedene Funktionalitäten ermöglicht, wie beispielsweise Spieler-Eingaben, optimierte und effiziente grafische Darstellungen, sowie auch das Einbringen von interaktiven Aufgaben innerhalb der virtuellen Welt. Diese zwei Werkzeuge werden innerhalb des Masterprojektes „Neue Welt 9“ durch die 3D-Modellierungssoftware „3ds Max“ von Autodesk und durch die Spiele-Engine „Unity“ von Unity Technologies repräsentiert. Dabei wird stets von dem Projektteam angestrebt, die Werkzeuge möglichst auf dem aktuellsten Stand zu halten, um durch die Kontinuität des

Betreuer Hochschule: Prof. Dr. Rer. Nat. Gabriela Tullius
Hochschule Reutlingen
Gabriela.Tullius@Reutlingen-University.de
Prof. Dipl-Journalist Boris Terpinc
Hochschule Reutlingen
Boris.Terpinc@Reutlingen-University.de

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

technischen Fortschrittes eine möglichst realitätsnahe virtuelle Welt zu erzielen.

3 Ursprung des Projekts

Das Projekt besteht schon seit mehr als 10 Jahren. Angefangen hat alles mit dem Grundgerüst des Gebäude 9 auf dem Reutlinger Campus. Dieses Gebäude wurde über die Jahre hinweg immer mehr durch die Bachelor- und Master-Studenten belebt. Die Ursprungsidee des Projektes bildet die Kombination aus 3D-Modellierung, Visualisierung und Interaktionen mit Gegenständen. Es wird die Bearbeitung von Audio und Video Dateien gefordert. Es soll das älteste Gebäude des Campus – Gebäude 9 – in unterschiedlichen Generationen spielerisch entdeckt werden können. Dabei können vergängliche Ausstattungen angesehen werden oder Visionen aus der Zukunft entdeckt werden. Durch verschiedene Interaktionen, welche durch kreative Studenten ins Leben gerufen wurden, können Räume verändert werden und der Spieler wird in eine andere Generation des Gebäude 9 versetzt. So wird die Geschichte des Gebäudes spielerisch entdeckbar und Studenten lernen den professionellen Umgang mit Game Design Werkzeugen.

4 Aktueller Stand

Derzeit wird bei Neue Welt 9 eine Portierung von Cry Engine zu Unity vorgenommen. Dabei wird die Architektur des Gebäudes vervollständigt und dessen fehlende Räume ergänzt. Aufbauend werden die Projekte Tonstudio und Fotolabor als Testprototypen mit den Modellen ausgerüstet. Zusätzlich werden die Räume mit einer Kür ausgestattet, um das Spiel attraktiver zu gestalten. Vorausblickend wird das Gebäude 9 komplett auf Unity basierend laufen.

5 Ausblick

Das Projekt hat zum Ziel, das Gebäude 9 virtuell erkundbar zu machen. Die Game-Engine Unity bietet in diesem Zusammenhang Support für zukünftige VR-Technologien. Daher werden bereits aktuelle Head-Mounted Displays unterstützt, wie die HTC Vive oder Oculus Rift. Über die Einbindung von Aufgaben innerhalb des Gebäudes können Interaktionen mit den HMDs verbunden werden. Dadurch lassen sich verschiedene Szenarien im VR-Bereich realisieren. Auch eine Einbindung von Motion Tracking Geräten ist vorstellbar, wie des Perception Neuron, mit welchem Neue Welt 9 durchlaufen werden kann oder mit Gegenständen aus der Umgebung interagiert werden kann. Des Weiteren gibt es in Hinblick auf Googles Daydream auch die Möglichkeit das Gebäude 9 mobil mit Smartphones begehbar zu machen. Dafür bietet Unity Unterstützung von Android an. Das begehen und interagieren des Gebäude 9 mit neuen Technologien ist ein Ziel des Projektes. Unity dient dazu als eine aktuelle Plattform, in welcher die Möglichkeiten gegeben sind.

Das Masterprojekt *CaMed* - Computerassistierte Medizin

Lukas Brand
Reutlingen University
Lukas_Klaus.Brand@Student.Reutlingen-University.DE

Sina Frommer
Reutlingen University
Sina_Mailin.Frommer@Student.Reutlingen-University.DE

Simone Hanisch
Reutlingen University
Simone.Hanisch@Student.Reutlingen-University.DE

Lea Keil
Reutlingen University
Lea.Keil@Student.Reutlingen-University.DE

Julija Rusinov
Reutlingen University
Julija.Rusinov@Student.Reutlingen-University.DE

Josia Scheytt
Reutlingen University
Josia.Scheytt@Student.Reutlingen-University.DE

Maxim Stoljar
Reutlingen University
Maxim.Stoljar@Student.Reutlingen-University.DE

Abstract

Das Projekt *CaMed* des Masterstudiengangs Human-Centered Computing bewegt sich im Umfeld der computerassistierten Medizin. Im Rahmen dessen entstehen unterschiedliche Projekte zur Unterstützung des klinischen Personals und der Prozesse vor, während und nach einer OP. In diesem Artikel werden die aktuellen Projekte, ein präoperatives Informationssystem, ein perioperatives Workflowmanagement-System und die Instandsetzung des DaVinci-Operationsroboters und ein dies bezügliches präoperatives Planungssystem vorgestellt.

Schlüsselwörter

Computerassistierte Medizin, Intelligenter OP, Perioperative Prozesse, Situationserkennung, Informationssysteme, Prozessunterstützung, Datenspeicherung, Planungssysteme, Ähnlichkeitsbestimmung

---

Betreuer Hochschule: Prof. Dr.-Ing. Oliver Burgert
Hochschule Reutlingen
Oliver.Burgert@Reutlingen-University.DE

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

CR-Kategorien

• **Information systems ~ Process control systems** • **Human-centered computing ~ HCI theory, concepts and models** • *Information systems ~ Network attached storage* • *Information systems ~ Expert systems* • *Information systems ~ Data analytics* • General and reference ~ Empirical studies

1 Einleitung

Das *CaMed*-Masterprojekt ist, neben dem VRLab, IOT und Neue Welt 9, eines der möglichen Wahloptionen für die Studierenden des Masterstudiengangs Human-Centered Computing. Es bietet den Studierenden die Möglichkeit sich über zwei Semester mit einem medizininformatischen Projekt zu beschäftigen, innovative Ideen zu entwickeln und Systeme umzusetzen, die eine Unterstützung des klinischen Personals und der Prozesse im Operationssaals bieten. *CaMed* verbindet damit aktuelle Informationstechnologien mit medizin-technischen Geräten und klinischen Abläufen im Kontext eines intelligenten OPs.

2 Projekte

Aktuell wird im Rahmen von *CaMed* an Projekten in den drei Bereichen präoperative Informationssysteme, Komponenten eines OP-Workflowmanagementsystems und der

Instandsetzung und OP-Planung mit einem DaVinci-Operationsroboter gearbeitet.

2.1 Präoperatives Informationssystem

Bei dem präoperativen Informationssystem handelt es sich um ein System, das in einem Waschraum, in Form eines Spiegel-Displays, angebracht wird. Das Ziel des Systems ist es, während des präoperativen Waschvorgangs nützliche Informationen anzubieten und damit das OP-Personal zu unterstützen. Die angebotenen Informationen betreffen die Patienten- und OP-Daten, die Schritte des Waschvorgangs inklusive einer zeitlichen Begleitung, die Anzeige der Zeit bis zu einer OP, sowie den aktuellen Stand während einer OP. Durch das System wird es dem Nutzer ermöglicht über die OP besser informiert zu sein und wichtige Informationen unmittelbar vor der OP auffrischen zu können. Die Zielgruppe betrifft dabei das OP-Personal, zu dem die Chirurgen und die Assistenz gehören.

2.2 Der DaVinci-Operationsroboter

Das DaVinci-Operationssystem ist ein Teleoperationssystem für die computer-assistierte minimal-invasive Chirurgie, entwickelt von Intuitive Surgical. Über eine Konsole bedient der Operateur die drei Arme des Roboters und kann so operieren.

Im Rahmen des Masterprojektes *CaMed* wird die Inbetriebnahme und Reparatur des Operationssystems angestrebt. Dabei werden verschiedene Reverse-Engineering Methoden angewendet, um als Ziel ein funktionierendes System zu erhalten. Bislang wurden verschiedene Funktionstest der unterschiedlichen Komponenten des Systems durchgeführt und fehlerhafte Teile ersetzt.

Ein weiterer Schwerpunkt besteht in der präoperativen Operationsplanung für einen Eingriff mit dem DaVinci-Operationssystem. Hierzu wurde eine Simulation der Roboterbewegung erstellt, die es ermöglichen soll eine kollisionsfreie Roboterkonfiguration für die ausgewählten Zugangspunkte zu finden. Um diese Information für das Operationspersonal zu visualisieren, wird der Roboter mit der gefundenen Konfiguration als Hologramm in der Microsoft Hololens dargestellt.

2.3 Workflow-Management und Situationserkennung

Damit ein Workflow-Management-System automatisch entscheiden kann, inwieweit ein aktuell aktiver Prozessschritt abgeschlossen ist und wie es im Prozessmodell weitergeht, wird unter anderem eine Situationserkennung benötigt. Auf Basis von Daten aus heterogenen Datenquellen im Operationssaal, die durch Experten mit einer Beschreibung der aktuellen Situation versehen wurden, werden im Rahmen des Projekts Methoden zur Situationserkennung untersucht. Besonderer Fokus liegt dabei auf der Untersuchung von Methoden zur Datenauswahl, die aus der großen Menge an Daten nur die signifikanten Teile extrahieren sollen. Eine wichtige Informationsquelle sind dabei Videodaten der Endoskop-Kamera. Momentan werden diese Daten so verarbeitet, dass eine binäre Lokalisierung der Endoskopspitze (innerhalb/außerhalb des Patienten) möglich ist. Dies bietet einen potentiellen Parameter für die Situationserkennung und ermöglicht es beispielsweise Material von außerhalb des Patienten zu verwerfen oder Personen aus datenschutzrechtlichen Gründen unkenntlich zu machen.

Ein weiterer Bereich, welcher der operativen Unterstützung dienen soll, ist der Bereich der Ähnlichkeitsbestimmung bei Prozessen im OP. Hierbei geht es darum Ähnlichkeiten zwischen verschiedenen Prozessen einer OP-Art zu erkennen und zu messen. Mit diesen Erkenntnissen können etwa Vorhersagen über den Verlauf der OP gemacht werden. So kann beispielsweiße die zeitliche Planung im OP-Bereich angepasst werden und wertvolle Informationen zur OP- und Ressourcen-Planung gewonnen werden.

Masterprojekt Internet of Things

David Leisten
Reutlingen University
David.Leisten@Student.Reutlingen-University.DE

Vanessa Willenbrock
Reutlingen University
Vanessa.Willenbrock@Student.Reutlingen-University.DE

Clemens Weißenberg
Reutlingen University
Clemens_Oliver.Weissenberg@Student.Reutlingen-University.DE

Katharina Pavić
Reutlingen University
Katharina.Pavic@Student.Reutlingen-University.DE

Abstract

Das Masterprojekt Internet of Things (IoT) bildet eine der Projektgruppen, die man im Masterprojekt belegen kann. Hier werden in Gruppen von ein bis drei Personen Projekte bearbeitet, die in der Regel im Kontext des Internet of Things stehen. Im laufenden Projekt sTEP-R wird ein Prototyp eines rollstuhlgebundenen Bewegungstherapiesystems realisiert. Das Projekt MIND dient dazu einen Leitfaden und zugehörige Templates bezüglich einer Medizinproduktdokumentation zu erstellen. Während im Projekt HEATED eine Anwendung entwickelt wird, mit der Durchblutungsstörungen anhand von Wärmebildern detektiert werden sollen. Das interdisziplinäre Projekt IEP TSP entwickelt ein T-Shirt, mit dem es ermöglicht werden soll, EKG-Messungen am Patienten außerhalb des Krankenhauses zu machen.

---

*

Betreuer Hochschule: Prof. Dr. Sven Steddin
Sven. Steddin @Reutlingen-University.de
Prof. Dr. Natividad Martínez Madrid
Natividad.Martinez@Reutlingen-University.DE

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

Schlüsselwörter

Masterprojekt, Internet of Things, Human-Centered Computing, Rollstuhlgebundenes Bewegungstherapiegerät, Medizinproduktdokumentation, Wärmebildkamera, Textile Sensor Plattform

CR-Kategorien

Documentation, Design, Measurement, Human Factors, Experimentation

1 Masterprojekt Internet of Things

Das Masterprojekt bildet im Studiengang Human-Centered Computing ein Kernmodul. Es erstreckt sich über die ersten beiden Studiensemester und ermöglicht es den Studierenden, sich über einen längeren Zeitraum intensiv mit einem Projekt ihrer Wahl zu beschäftigen. Die hier vorgestellten Projekte aus der Projektgruppe Internet of Things (IoT) sTEP-R, MIND, HEATED und IEP TSP werden, mit Ausnahme von IEP TSP, jeweils von Einzelpersonen durchgeführt und befinden sich momentan in Phase zwei. Das bedeutet, dass die Planungsphase abgeschlossen ist und sie sich in der Umsetzungsphase befinden.

Das IoT ist sehr vielfältig und will in erster Linie Menschen bei ihren Tätigkeiten

unterstützen. Ein Ambient-Assisted-Living Labor bietet den Studenten die Möglichkeit an Projekten zu arbeiten, die ältere Menschen im täglichen Leben zu Hause unterstützen können. Diese elektronischen Assistenzsysteme sollen ein selbstbestimmtes, umgebungsunterstütztes Leben bieten.

2 sTEP-R

sTEP-R steht für die **TE**chnische Umsetzung eines **P**rototyps für ein **r**ollstuhlgebundenes Bewegungstherapiesystem. Im Rahmen des Projekts werden Übertragungsprotokolle zwischen den einzelnen Subsystemen (Motor, Microcontroller, User Interface) eines rollstuhlgebundenen Bewegungstherapiesystems definiert und umgesetzt, des Weiteren die Subsysteme physisch miteinander verbunden und die Geschwindigkeitsänderung des Motors über das User Interface (Smartphone-App) prototypisch umgesetzt.

Das rollstuhlgebundene Bewegungstherapiesystem ermöglicht es einem Rollstuhlfahrer seine Beine jederzeit und an jedem Ort aktiv oder passiv zu trainieren. Dadurch sollen Folgeerkrankungen des Bewegungsmangels vorgebeugt werden und/oder die Beinmuskulatur rehabilitiert werden.

3 MIND

Im Projekt MIND geht es um die **M**ediz**IN**produkt **D**okumentation. Um ein Medizinprodukt zulassen zu können, müssen diverse Schritte durchlaufen und verschiedene Normen und Richtlinien eingehalten werden. Hat man sich mit dieser Thematik noch nie auseinandergesetzt, ist der Einstieg schwer. Es sind kaum Dokumente vorhanden, mit denen ein Überblick gegeben wird. Ziel dieses Projektes ist es daher einen Leitfaden zu erstellen, anhand dessen Schritt für Schritt erklärt wird, welche Dokumente wie angelegt, befüllt und gepflegt werden müssen. Zur Veranschaulichung werden einige dieser Dokumente bereits am Beispiel des rollstuhlgebundenen Bewegungstherapiesystems befüllt. So kann der Nutzer die Vorgehensweise besser nachvollziehen und die dargestellten Inhalte auf sein eigenes Produkt übertragen.

4 HEATED

Die Applikation HEATED ermöglicht den Einsatz eines mobilen wärmebilderzeugenden Kamerasystems, das die Wärmeabstrahlung, hervorgerufen durch Blutgefäße im menschlichen Körper, aufzeichnet. Mit HEATED können Abweichungen der Körpertemperatur berührungslos sichtbar gemacht werden bevor sich deren mögliche Auswirkungen oberflächlich manifestieren. HEATED soll dazu genutzt werden, Therapien mit Bezug zu Durchblutungsstörungen (bspw. PAVK) in den unteren Extremitäten zu dokumentieren und graphisch aufzubereiten. HEATED dient in erster Linie der Verlaufskontrolle und kann somit einen visuellen Nachweis für die individuelle Wirksamkeit der angewandten Therapie liefern.

5 IEP TSP

Im Rahmen eines **I**nterdisziplinären **E**ntwicklungs **P**rojekts (=IEP) von fünf Studenten aus den Fachbereichen Informatik und Textil & Design wird eine **T**extile **S**ensor **P**lattform (=TSP) entwickelt. Der Leitgedanke für das Projekt ist die (Langzeit-) EKG-Messung am Patienten außerhalb des Krankenhauses per Ferndiagnose. Dazu sollen Sensoren und Recheneinheiten in einem tragbaren, textilen Kleidungsstück eingearbeitet werden, sodass die Diagnose beispielsweise durch tragen eines alltagstauglichen T-Shirts ermöglicht wird. Ziel ist die Entwicklung eines Prototyps für ein Medizinprodukt. Die Kommunikation von TSP zum Krankenhaus soll mittels Smartphone-App stattfinden.

Reinigungsroboter mit LEGO Mindstorms “T-Clean 1.0”

Justin Spohn
Ferdinand-von-Steinbeis-Schule
Reutlingen

Celina Breiter
Kerschensteinerschule Reutlingen

Abstract
Das Ziel war es, einen Roboter zu entwerfen. Er soll eine für uneingeschränkte einfache, aber für eingeschränkte Personen schwere Arbeit erledigen: das Putzen. Hierzu wurde ein Prototyp mit LEGO Mindstorms konstruiert und programmiert. Die prototypische Putzfläche ist eine Tischplatte.

Schlüsselwörter
Reinigungsroboter, Haushaltshilfe, Lego Mindstorms, Automatisierung, Smart Home

CR-Kategorien
C.5.3 [Microcomputers]

1 Einführung
Dieses Projekt der Gewerblichen Schulen in Reutlingen wurde von Schülerinnen und Schülern der technischen Gymnasien selbstständig entwickelt und durchgeführt. Schüler der Klasse 12 an der Ferdinand-von-Steinbeis-Schule erarbeiteten die vorgestellten Systeme, Schülerinnen der Klasse 11 an der Kerschensteinerschule waren für Grafik und Postergestaltung zuständig.

Betreuer Schule: Bernhard Thiersch
Ferdinand-von-Steinbeis-Schule
Kerschensteinerschule
Reutlingen

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

2 Funktionsweise
Der Roboter erkennt mit Hilfe eines Farbsensors, welcher die Stärke des reflektierenden Lichts misst, die Grenzen der Tischplatte. Entfernungen werden aus den Umdrehungen der Räder errechnet. So erkennt T-Clean die Maße des Tisches. Durch Dividieren von Länge und Breite wird die Mitte der Tischplatte ermittelt. Da sich T-Clean dort nicht an Linien orientieren kann, versucht er sich beim Anfahren möglichst gerade mithilfe zweier Infrarot-Sensoren auszurichten. T-Clean fährt nur so lange nach vorne bis ihm vom Ultraschallsensor das Ende des Tisches gemeldet wird. Der M-Motor ermöglicht es ihm das Trockenputztuch vor und zurück zu bewegen. Der Tisch ist nach Ablauf des Programms trocken.

3 Programmlogik
Zu Beginn wird geprüft, ob T-Clean richtig auf dem Tisch platziert wurde. Diese Platzierung muss der Nutzer selbst vornehmen. Als Hilfe zeigt T-Clean die aktuellen Sensorwerte auf dem Display. Ist die Platzierung richtig, gibt T-Clean visuelle Rückmeldung durch Häkchen hinter dem Sensorwert. Schlägt die Positionsüberprüfung fehl, gibt T-Clean akustische Rückmeldung und beendet das Programm. Sind allerdings alle Sensorwerte wie gewünscht, wartet T-Clean nach drücken der Starttaste fünf Sekunden. Dann bewegt sich T-Clean an der Tischkante entlang nach vorne, bis er am Ende des Tisches angelangt ist. Nun rechnet T-Clean die gemessenen

Umdrehungen mal den Umfang seiner Reifen. Im Anschluss wird noch seine eigene Länge dazu addiert. Anschließend dreht sich T-Clean. Nun wird der Programm-Code wiederholt. Hierbei wird die Breite des Tisches gemessen und auf dem Display ausgegeben. Das selbe wird weitere zwei Male ausgeführt, ohne die Abmessungen des Tisches zu bestimmen. Nun befindet sich T-Clean am Anfangspunkt. Die als Zweite gemessene Länge wird nun durch T-Cleans Breite dividiert. So wird ermittelt, wie viele Bahnen er fahren muss, um die Tischfläche zu Reinigen. Er fährt nun die Breite dividiert durch die Anzahl der Bahnen, dividiert durch seinen Reifenumfang zurück. Von der Anzahl der benötigten Bahnen wird nun eine Bahn abgezogen. T-Clean dreht sich dann senkrecht zur Tischbreite und richtet sich möglichst gerade aus. Anschließend wird eine Bahn gefahren. Am Ende dreht er sich um 180 Grad. Da sich vorne am Roboter das Nassputztuch befindet, muss er sich drehen um die Bahn trocknen zu können. Der Roboter richtet sich erneut möglichst gerade aus, fährt zurück und stellt sich wieder parallel zur Tischbreite auf. Sind noch Bahnen übrig, fährt er erneut zurück und wiederholt den Vorgang. Haben die benötigten Bahnen die Zahl “0” erreicht, fährt der Roboter an der Tischkante nach vorne und dreht sich am Ende des Tisches um 90 Grad. T-Clean befindet sich nun wieder in der Ausgangsposition. Das Programm wird beendet.

Lichtsteuerung für Pflanzen mit Raspberry Pi

Tobias Schulz
Ferdinand-von-Steinbeis-Schule
Reutlingen

Celina Breiter
Kerschensteinerschule Reutlingen

Abstract
Das vorliegende Paper beschreibt ein Schülerprojekt. Das Ziel des Projekts war, "ideale" Lichtverhältnisse für eine Pflanze an jedem Ort im Haus herzustellen.

Schlüsselwörter
Raspberry Pi, Lichtsteuerung, Smart Home

CR-Kategorien
C.5.3 [Microcomputers]

1 Einleitung
Dieses Projekt der Gewerblichen Schulen in Reutlingen wurde von Schülerinnen und Schülern der technischen Gymnasien selbstständig entwickelt und durchgeführt. Schüler der Klasse 12 an der Ferdinand-von-Steinbeis-Schule erarbeiteten die vorgestellten Systeme, Schülerinnen der Klasse 11 an der Kerschensteinerschule waren für Grafik und Postergestaltung zuständig.

Betreuer Schule: Bernhard Thiersch
Ferdinand-von-Steinbeis-Schule und Kerschensteinerschule Reutlingen

Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

2 Idee
Um einer dunklen Ecke ein wenig Farbe zu verleihen, wird sie häufig mit Pflanzen geschmückt. Da diese aber häufig viel Licht benötigen, hält die Pflanzenpracht meist nicht lange an und die Pflanze geht ein. Damit dieser Lichtmangel kein Problem mehr darstellt, gibt es sogenannte "Sonnenergänzungslampen". Diese versorgen die Pflanze mit infrarotem und ultraviolettem Licht, welches Pflanzen benötigen. Nun ist es aber lästig, die Lampen die ganze Zeit ein und aus zu schalten wenn es dunkel oder hell wird. Damit man dies auch steuern kann, wenn man mal nicht daheim ist oder dies sogar automatisch gesteuert wird, wurde dieses Projekt entwickelt.

3 Aufbau und Funktion
Das System besteht aus einem Raspberry Pi 3 Model B, einer Micro-SD-Karte, einem 5V-Netzteil und einem 433-MHz-Sendemodul. Eine Funksteckdose kann dessen Signale empfangen. Zur Einrichtung und Programmierung werden zusätzlich noch Bildschirm, Tastatur und Maus benötigt. Das 433MHz-Sendemodul wird mit den drei Anschlüssen an die GPIO-Pins des Raspberry Pi für die Spannungsversorgung, die Datenleitung und Masse angeschlossen. Für größere Reichweite kann auch eine zusätzliche Antenne an das Sendemodul angeschlossen werden. Auf der Mikro-SD-Karte befindet sich das freie Betriebssystem Raspbian. Nach der Installation von WiringPi und Raspberry-Remote kann man

die Funksteckdosen schon manuell steuern. Um diese Steuerung zu erweitern, wird ein Apache2-Webserver eingerichtet. Eine HTML-Datei stellt Buttons zur Verfügung, denen via PHP die Befehle zum Ein- und Ausschalten der Funksteckdosen zugewiesen werden. Durch Cronjobs kann eine Zeitschaltuhr eingerichtet werden, die für eine Konstante oder variable Anzahl "Sonnenstunden" sorgt. Je nach Pflanzenart können so Klimazonen und Jahreszeiten simuliert werden. Zudem kann manuell über das Webinterface geschaltet werden. Die Verbindung zum Webinterface wird über den Browser und die IP-Adresse des Raspberry Pi aufgebaut.

4 Weitere Ideen

Mit dieser Steuerung lassen sich nicht nur Sonnenergänzungslampen steuern, sondern alle Geräte die an Steckdosen anschließbar sind. Man kann zum Beispiel Weihnachtsbeleuchtung fernsteuern oder die Zeitschaltfunktion dafür nutzen. Dieses System kann man auch mit einem Luxmeter koppeln der die Steckdosen mit den Lampen automatisch einschaltet, wenn es dunkel wird und sie auch wieder automatisch ausschaltet. Man könnte außerdem Luxmeter und Zeitschaltuhr miteinander koppeln, so dass die Lampe sich in einem bestimmten Zeitfenster immer dann einschaltet, wenn es der Pflanze zu dunkel ist.

Gestensteuerung mit einem Microcomputer und einer Kamera

Sören Gutbrod
Ferdinand-von-Steinbeis-Schule
Reutlingen

Brenda Duebeck
Kerschensteinerschule Reutlingen

Abstract
Der Microcontroller Raspberry Pi 2 [1] wurde mit einer Kamera für die Gestensteuerung ausgestattet. Die Programmierung wurde in C++ mit Hilfe des Frameworks OpenNI [2] umgesetzt. Die Gestensteuerung soll die ergonomischen Möglichkeiten von Computersystemen im Alltag, zum Beispiel in den Bereichen Smart-Home oder Automotive-Systems, erweitern.

Schlüsselwörter
Raspberry Pi, Microcontroller, Smarthome, Gestensteuerung, OpenNI

CR-Kategorien
C.5.3 [Microcomputers]

1 Einleitung
Dieses Projekt der Gewerblichen Schulen in Reutlingen wurde von Schülerinnen und Schülern der technischen Gymnasien selbstständig entwickelt und durchgeführt. Schüler der Klasse 12 an der Ferdinand-von-Steinbeis-Schule erarbeiteten die vorgestellten Systeme, Schülerinnen der Klasse 11 an der Kerschensteinerschule waren für Grafik und Postergestaltung zuständig.

Betreuer Schule: Bernhard Thiersch
Ferdinand-von-Steinbeis-Schule
Kerschensteinerschule Reutlingen
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

Der Kontakt zwischen Mensch und Maschine wird zunehmend enger. Wir blicken in eine Zukunft, in der in unseren Träumen selbstfahrende Autos die Straßen beherrschen, Drohnen Einkäufe liefern und Maschinen selbst Material nachbestellen. Von der Ära der Lochkarten, über die Hardkeys zum Touchscreen hat sich vieles verändert. Die verbreiteten Arten der Mensch-Maschine-Interaktion erfordern einen direkten physischen Kontakt zur Benutzungsoberfläche. Anders ist es bei der Gestensteuerung. Bei dieser werden Bewegungen mit einer Kamera aufgezeichnet, vom System erkannt und mit vordefinierten Bewegungsmustern verglichen.

2 Zielsetzung und Nutzen
Ziel des Projektes war es, eine fortschrittliche Steuerung zu entwickeln. Hierbei wurde viel Wert auf eine einfache Gestaltung der Benutzungsoberfläche gelegt, die es jedem ermöglicht, ohne Vorkenntnisse die Gestensteuerung zu nutzen.

3 Aufbau des Projekts
Abbildung 1 zeigt den Microcontroller Raspberry Pi mit der Raspberry Pi Camera [1]. Die Gestensteuerung wird mit diesem umgesetzt. Zur Hilfe kommt dabei die Raspberry Pi Camera, welche mit dem Raspberry Pi 2 über ein Camera-Serial-Interface verbunden ist.

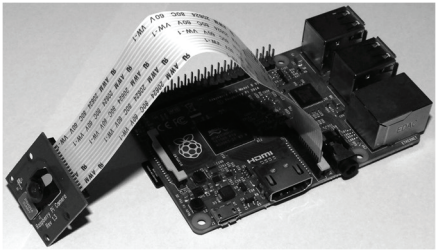

Abb.1 Raspberry Pi mit Raspberry Pi Camera

Eine Internetverbindung über den vorhandenen Ethernetport oder einen USB WLAN-Adapter ist nicht erforderlich, wenn der Raspberry Pi 2 als Front- und Backend der Gestensteuerung arbeitet. Bei Front-und-Backend-Betrieb des Mikrocontrollers müssen die zu steuernden Elemente, zum Beispiel Licht, über die vorhandenen GPIOs verbunden werden. Darauf zu achten ist dabei, dass die Ausgangsspannung 5 Volt und max. 16 Milliampere beträgt und somit in den meisten Fällen eine externe Stromquelle benötigt wird.

4 Vorteile und Nachteile

Ein Nachteil des Systems ist, dass das Gerät in der Gestenlernphase nicht einwandfrei bedient werden kann. Zudem kann es passieren, dass Gesten nicht erkannt werden. Manchmal können auch unbeabsichtigte Bewegungen als Gesten interpretiert werden. Die Kamera ist zudem immer aktiv und könnte die Privatsphäre beeinträchtigen. Ein Vorteil ist die erleichterte Steuerung, die durch neue Gesten und neue Funktionen erweitert werden kann. Bei der Gestensteuerung mittels Raspberry Pi 2 ist das System ortsgebunden, weil ein gleichbleibender Hintergrund benötigt wird.

An öffentlichen Orten bringt Gestensteuerung den Vorteil, dass durch das Wegfallen des physischen Kontakts keine Krankheitserreger verbreitet werden können.

5 Ausblick

Die Gestensteuerung mittels Microcontroller kann eine ernstzunehmende Alternative zu konventionellen Steuerungen werden. Hier kommen die geringen Anschaffungskosten und erleichterte Benutzung zur Geltung. Der Vorteil, dass keine direkte Berührung des Systems notwendig ist, lässt einen vielfältigen Einsatzbereich zu. Durch intensive Forschung und Verbesserung der Software und Kameratechnik, kann man viele Einsatzbereiche erschließen, zum Beispiel in der Medizintechnik oder Kernphysik.

6 Literaturverzeichnis

[1] Raspberry Pi Foundation, “Raspberry Pi Model B” https://www.raspberrypi.org/products/raspberry-pi-2-model-b/; Abgerufen am: 13.03.17.

[2] Apple Inc, “OpenNI” https://structure.io/openni; Abgerufen am 13.03.17.

[3] CHIP Communications GmbH, “Das ultimative Raspberry Pi Handbuch” http://blog.fraunhofer.de/Futurelog/wp-content/uploads/2016/05/Chip-Digital-Magazin-Spezial-Da-CHIP.pdf; S. 138f; Abgerufen am 12.03.17.

[4] Liu Yan, “Hand Gesture to control web browser”, (Video) https://www.youtube.com/watch?v=IMsBIJP5FTY; Abgerufen am 12.03.2017.

/GUT.ECHT.ANDERS

ADVANCED UNIBYTE

Die Datensurfer

Die Advanced UniByte GmbH (AU) gehört zu den führenden Systemhäusern für IT-Infrastruktur, Speicherlösungen sowie Cloud- und Managed Services. Das AU-Expertenwissen umfasst Storage-, Netzwerk-, Computing- und Virtualisierungs-Lösungen ebenso wie die IT-technische Integration weltweiter Niederlassungen. Im hochsensiblen Umfeld der Datensicherheit und Hochverfügbarkeit haben wir uns einen herausragenden Ruf erarbeitet, AU-Cloud- und Managed-Services sorgen für maximale Entlastung unserer Kunden. Mit unserem Know-how und dem Experten-Netzwerk aus Technologieführern unterstützen wir sie auf ihrem Weg der digitalen Transformation.

Im Mittelpunkt unserer Arbeit steht die vertrauensvolle und zukunftsorientierte Zusammenarbeit mit unseren Kunden, die uns mehrfach als „Bestes Systemhaus des Jahres“ ausgezeichnet haben.

Für diesen spannenden Zukunftsmarkt suchen wir Dich – Du bist neugierig auf neue Entwicklungen, übernimmst gerne Verantwortung, willst die Zukunft mitgestalten und identifizierst Dich mit unserer Firmenphilosophie, die **GUT / ECHT / ANDERS** ist.

An den Standorten **Metzingen, Gröbenzell und Denzlingen** vergeben wir nach Bedarf im Bereich Wirtschaftsinformatik sowie Medien- und Kommunikationsinformatik:

- Management-Traineeprogramme
- Bachelor- & Masterabschlussarbeiten
- Werkstudententätigkeiten & Praktika
- Auszubildendenstellen

Bewirb Dich bei:
Advanced UniByte GmbH
Abteilung Personal & Ausbildung
Paul-Lechler-Str. 8, 72555 Metzingen

Teresa Monopoli
Tel: +49 7123 9542-258

Elena Ciuffreda
Tel: +49 7123 9542-256

E-Mail: bewerbung@au.de
www.au.de

AUSGEZEICHNETE IT
GUT / ECHT / ANDERS

Hochschule Reutlingen
Reutlingen University

Reutlingen University
Fakultät Informatik
Human-Centered Computing
Alteburgstraße 150,
72762 Reutlingen

http://www.huc.reutlingen-university.de

Telefon: +49 7121 / 271-4002
Telefax: +49 7121 / 271-4042

E-Mail: infoinside@reutlingen-university.de
Internet: http://www.infoinside.reutlingen-university.de

ISBN 978-3-00-056455-0