Karlsruher Schriften
zur Anthropomatik

Band 28

Erik Ludwig Krempel

Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen

KIT Scientific Publishing

Erik Ludwig Krempel

Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen

Karlsruher Schriften zur Anthropomatik
Band 28
Herausgeber: Prof. Dr.-Ing. Jürgen Beyerer

Eine Übersicht aller bisher in dieser Schriftenreihe erschienenen Bände finden Sie am Ende des Buchs.

Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen

von
Erik Ludwig Krempel

KIT Scientific Publishing

Dissertation, Karlsruher Institut für Technologie (KIT)
Fakultät für Informatik, 2016

Impressum

Karlsruher Institut für Technologie (KIT)
KIT Scientific Publishing
Straße am Forum 2
D-76131 Karlsruhe

www.ksp.kit.edu

Print on Demand 2017

ISSN 1863-6489
ISBN 978-3-7315-0598-3
DOI 10.5445/KSP/1000060610

Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen

zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften

von der KIT-Fakultät für Informatik
des Karlsruher Instituts für Technologie (KIT)

genehmigte

Dissertation

von

Erik Ludwig Krempel

aus Karlsruhe

Tag der mündlichen Prüfung:	11.07.2016
Erster Gutachter:	Prof. Dr.-Ing. habil. Jürgen Beyerer
Zweiter Gutachter:	Univ.-Prof. Dipl.-Ing. Dr. techn. Bernhard Rinner

Inhaltsverzeichnis

Abkürzungsverzeichnis und Glossar

ACLU	American Civil Liberties Union.
AVE	Average Variance Extracted.
BDSG	Bundesdatenschutzgesetz.
BMBF	Bundesministerium für Bildung und Forschung.
BSI	Bundesamt für die Sicherheit in der Informationstechnik.
CNIL	Commission Nationale de l'Informatique et des Libertés.
DIN	Deutsches Institut für Normung.
DSFA	Datenschutz-Folgenabschätzung.
DSGVO	Datenschutzgrundverordnung.
EFUS	European Forum for Urban Security.
ENISA	European Union Agency for Network and Information Security.
FIP	Fair Information Practice Principles.
IKT	Informations- und Kommunikationstechnologie.
ISO	International Organization for Standardization.
Item	In der empirischen Sozialforschung versteht man unter dem Begriff *Item* ein einzelne Frage aus einem Fragebogen.
KASTEL	BMBF-Kompetenzzentrum für angewandte Sicherheitstechnologie.

KIT	Karlsruher Institute für Technologie.
Konstrukt	Ein alternativer Name für latente Variable. Der Name Konstrukt verdeutlicht die Eigenschaft, dass latente Variablen durch verschiedene gemessene Items konstruiert sind.
Latente Variable	In der empirischen Sozialforschung versteht man unter dem Begriff latente Variable eine Variable, die nicht direkt durch eine einzige Frage, sondern nur indirekt über mehrere Items abgefragt werden kann. So kann beispielsweise die Intelligenz nicht über eine einzelne Frage abgedeckt werden, sondern wird typischerweise aus den Dimensionen räumlich-mathematische Intelligenz, Sprachintelligenz und abstraktes Denken gebildet.
NEST	Network Enabled Surveillance and Tracking.
OECD	Organisation for Economic Cooperation and Development.
PbD	Privacy by Design.
PET	Privacy Enhancing Technologies.
PIA	Privacy Impact Assessment.
PLS	Partial Least Squares.
PLS-SGM	Partial Least Square-Strukturgleichungsmodellierung.
RFID	Radio-Frequency Identification.
ROI	Region of Interest. Bezeichnung für Regionen im Bild, die für die weitere Verarbeitung wichtig sind. Im Kontext vom Schutz der Privatsphäre werden damit typischerweise Gesichter, Nummernschilder oder andere Merkmale gemeint, die eine Identifikation von Personen erlauben.

SGM	Strukturgleichungsmodellierung (SGM) (engl.: Structural Equation Modeling (SEM)).
TAM	Technology Acceptance Model. Ein 1989 in der Dissertation von Davis veröffentlichtes Modell, um Aussagen darüber zu treffen, warum Personen eine Technologie akzeptieren. TAM war die Grundlage für eine ganze Reihe weiterer Modelle zur Erklärung von Technikakzeptanz.
TAM-VS	Technology Acceptance Model-Video Surveillance. Ein für die Videoüberwachung entworfenes Akzeptanzmodell basierend auf TAM.
TAM-VS2	Technology Acceptance Model-Video Surveillance. Ein für die Videoüberwachung entworfenes Akzeptanzmodell basierend auf TAM in seiner erweiterten Version 2.
TPM	Trusted Platform Module.
TRA	Theorie of Reasoned Action.
UTAUT	Unified Theory of Acceptance and Use of Technology.
ZAR	Zentrum für Angewandte Rechtswissenschaften.

1 Einleitung

Die Videoüberwachung öffentlicher Plätze wird in Deutschland divers diskutiert. Seit Jahren sprechen sich Initiativen gegen eine Ausweitung der Videoüberwachung aus [Zei13]. Es werden sowohl datenschutzrechtliche Probleme, als auch Zweifel an der Effektivität der Videoüberwachung geäußert, die beide gegen einen Einsatz sprechen [Hei07]. Im Gegensatz dazu wird nach schweren Straftaten in öffentlichen Räumen, beispielsweise die Übergriffe auf Frauen in der Silvesternacht 2015/2016 in Köln, sowohl von politischer Seite [WDR16] als auch von den Betroffenen selbst, mehr Videoüberwachung gefordert [Die16]. Diese ersten, oft sehr emotionalen Reaktionen bilden keine geeignete Grundlage, um über die Akzeptanz der Videoüberwachung zu urteilen. Sie zeigen jedoch, in welchem gespaltenen Verhältnis die Deutschen zur Videoüberwachung stehen. Auch wenn ihr eine Steigerung der Sicherheitslage zugesprochen wird, ist sie keinesfalls ein gerngesehener Teil des öffentlichen Lebens. An diesem Punkt greift die vorliegende Arbeit das Thema auf. Es wird untersucht, welche Faktoren die Akzeptanz der Videoüberwachung beeinflussen, um mit diesem Wissen gezielt Systeme mit mehr Akzeptanz zu bauen.

Bisher hatte lediglich die sozialwissenschaftliche Forschung das Thema Akzeptanz der Videoüberwachung untersucht. Viele existierende Studien befragen Betroffene zu ihrer Meinung zu konkret installierten Videoüberwachungsanlagen. Diese Akzeptanz korreliert stark mit sozioökonomischen Faktoren wie Alter, Bildung und politischer Einstellung der Befragten. Zusätzlich beeinflussen aktuelle Terroranschläge oder in den Medien präsente Verbrechen die Akzeptanz. Die überwiegende Mehrheit der Befragten gibt an, dass die Videoüberwachung ihrer Meinung nach geeignet ist, die Sicherheit im überwachten Gebiet zu steigern.

Dieser Sicherheitszuwachs skaliert nicht mit der Anzahl der Kameras, sondern nur mit der Anzahl des Personals. Um schnell eingreifen zu können, muss jedes Video von einem Operator ausgewertet werden, der in Notlagen Sicherheitskräfte zum Einsatzort schickt. In Zeiten knapper öffentlicher Kassen werden jedoch die wenigsten Kameras dauerhaft ausgewertet, sie zeichnen lediglich auf. Kommt es zu Anzeigen, können die Aufnahmen nachträglich ausgewertet und als Beweismittel genutzt werden. Das primäre Ziel der Videoüberwachung, kritische Situationen frühzeitig zu erkennen und zu verhindern, kann so nicht erreicht werden.

Dieser Herausforderung versucht man mit der sogenannten *intelligenten Videoüberwachung* zu begegnen. Während bei der konventionellen Videoüberwachung die von Kameras erfassten Daten zur Auswertung einem Operator angezeigt werden, versucht man in der intelligenten Videoüberwachung durch Algorithmen ein Verständnis über die beobachtete Szene zu bilden. Auch wenn die algorithmische Bildauswertung im Allgemeinen noch hinter der Leistung eines menschlichen Operators liegt, gibt es gute Gründe für den Einsatz. So ermüden Algorithmen nicht und können, entsprechende Hardware vorausgesetzt, fast beliebig viele Kameras gleichzeitig überwachen. Die algorithmische Szenenanalyse lässt sich dann in die weitere Verarbeitung der Videodaten einbinden. Idealerweise übernehmen Algorithmen eine Vorauswahl und der Operator bekommt bevorzugt die Szenen angezeigt, in denen besondere Vorkommnisse erkannt wurden.

Während die Entwicklung neuer Algorithmen zur Szenenanalyse seit Jahren sehr stark im wissenschaftlichen Fokus steht, fand die Frage der Akzeptanz bisher wenig Beachtung. Dies ist umso überraschender, da die intelligente Videoüberwachung auch in Bereiche vordringt, die bisher nicht videoüberwacht waren. Sie soll zukünftig die Patientensicherheit in Pflegeheimen oder Krankenhäusern gewährleisten und bis in die Privatwohnung Dienste für die Bewohner anbieten. Die heftige Kritik am EU-Forschungsprogramm INDECT ist nur ein Beispiel dafür, dass Betroffene einen deutlichen Unterschied zwischen der konventionellen Videoüberwachung und der intelligenten sehen [Stu12]. Gelingt es

nicht, die Systeme so zu gestalten, dass sie durch Betroffene akzeptiert werden, erscheint eine Nutzung der entwickelten Verfahren unwahrscheinlich.

1.1 Zielsetzung der Arbeit

Die bisher vernachlässigte Frage nach Akzeptanz der Videoüberwachung wird mit dieser Arbeit aufgegriffen. Ausgehend von der Akzeptanzforschung in der Informations- und Kommunikationstechnologie (IKT) wird ein Akzeptanzmodell für die (intelligente) Videoüberwachung erstellt. Als mögliche Einflussfaktoren auf die Akzeptanz sollen aber nicht sozioökonomische Faktoren, wie etwa das Alter, untersucht werden, sondern Faktoren, die direkt aus der technischen Ausgestaltung einer Videoüberwachung entstehen. Es ist beispielsweise wahrscheinlich, dass ein hohes Maß an technischem Datenschutz einen positiven Effekt auf die Akzeptanz hat. Wenn solche Faktoren bestimmt und durch Befragungen bestätigt sind, wird ein Katalog an beispielhaften technischen Veränderungen für Videosysteme erstellt und ausgewählte Techniken implementiert. Ziel ist es, für jeden der identifizierten Faktoren technische Lösungen anzubieten, die die Akzeptanz steigern.

Getrieben durch ein ausgewähltes Szenario, der datenschutzfreundlichen Sturzerkennung und Alarmierung für Krankenhäuser, wird ein Prototyp erstellt, der möglichst viele der entwickelten Technologien vereint. Dieser soll dazu dienen, die erstellten Technologien anschaulich zu präsentieren und gleichzeitig die abschließende Evaluation des Akzeptanzmodells erlauben. In dieser soll das erstellte Akzeptanzmodell und die gefundenen Faktoren noch einmal bestätigt werden. Weiter soll direkt am Prototyp eine gesteigerte Akzeptanz nachgewiesen werden.

Am Anfang der Arbeiten stehen somit drei Hypothesen:

Hypothese 1 Technologieakzeptanzforschung kann einen wichtigen Beitrag leisten, um zu verstehen, welche Faktoren die Akzeptanz von intelligenter Videoüberwachung beeinflussen.

Hypothese 2 Es können gezielt *technische* Komponenten entwickelt werden, die einen positiven Einfluss auf einen oder mehrere Akzeptanzfaktoren haben.

Hypothese 3 Durch entsprechendes Design können Videoüberwachungssysteme mit höherer Akzeptanz, bei mindestens gleichbleibender Funktionalität, entwickelt werden.

1.2 Eigene wissenschaftliche Beiträge

Akzeptanztreiber intelligenter Videoüberwachung Ausgehend von der Akzeptanzforschung der IKT wird ein Akzeptanzmodell für die (intelligente) Videoüberwachung erstellt [KB14]. Als Einflussfaktoren werden keine sozioökonomischen Faktoren, wie etwa das Alter, untersucht, sondern Faktoren, die direkt aus der technischen Ausgestaltung eines Überwachungssystems folgen. Es wird gezeigt, dass die Akzeptanz eines Videoüberwachungssystems maßgeblich durch die Faktoren *Nützlichkeit*, *Transparenz* und dem *Missbrauchsrisiko* geprägt ist. Diese Faktoren sind der Ausgangspunkt für die Entwicklung von technischen Komponenten, die die Akzeptanz eines Gesamtsystems steigern.

Interaktive Überwachung Die intelligente Videoüberwachung bietet ein hohes Potential, um Sicherheitsaufgaben zu erledigen. Gerade diese hohe Leistungsfähigkeit der Datenverarbeitung stellt ein Risiko für die Akzeptanz dar. Betroffene fühlen sich zunehmend als reines Subjekt einer automatisierten Auswertung und sehen Gefahren für den Datenschutz. Mit der interaktiven Überwachung wurde ein generischer Ansatz geschaffen, um die intelligente Videoüberwachung in ihrer Mächtigkeit und ihren Eingriffen in die Privatsphäre zu regulieren. Erweitere Verfahren für die Videoauswertung werden nur dann freigeschaltet, wenn die aktuelle Sicherheitslage dieses erfordert. Damit wird verhindert, dass der Operator durch die große Menge an Funktionalität überfordert wird und eine Grundlage für Verfahren der Transparenz und der Risikominimierung geschaffen.

Maßnahmen zur Steigerung der Transparenz Transparenz über die Datenverarbeitung kann auf mehreren Ebenen hergestellt werden. Je nach Überwachungszweck können den Betroffenen Informationen über das gesamte System, einzelne Sensoren oder den Operator gegeben werden. Die entwickelten Ansätze lassen sich dabei in zwei Gruppen einteilen. Zum einen sind Verfahren entstanden, bei denen ein Videoüberwachungssystem mittels Displays aktiv auf seine Betroffenen zugeht und über die aktuelle Datenverarbeitung informiert. Betroffene werden damit viel zeitgemäßer auf eine vorhandene Videoüberwachung hingewiesen als dies mit statischen Hinweisschildern möglich ist. Zum anderen wurden Verfahren entwickelt, wie interessierte Betroffene über ihr Smartphone mit einem Videoüberwachungssystem interagieren können. Dank eigens dafür entwickelter Apps können sich Betroffene über einzelne Kameras, das System und die eigene Beobachtung informieren.

Vor dem Einsatz muss sichergestellt werden, dass die Transparenz nicht im Konflikt mit dem Einsatzzweck steht. Eine Gegenüberstellung verschiedener Werkzeuge zu möglichen Zwecken hilft hier bei der Auswahl.

Privacy Score Gerade dann, wenn Endanwender in neue Systeme zur Videoüberwachung investieren, haben sie keine einfache Möglichkeit den Datenschutz angebotener Systeme zu vergleichen. Mit Privacy Score wurde ein Verfahren geschaffen, um eine breite Palette an Überwachungstechnik auf ihren Datenschutz hin zu bewerten [KB15]. Der Endanwender kann somit innerhalb weniger Stunden alle ihm verfügbaren Systeme vergleichen und eine fundierte Auswahl treffen.

Datenschutz-Folgenabschätzung Um ein Videoüberwachungssystem auf sein Risikopotential für den Datenschutz zu untersuchen, bietet eine Datenschutz-Folgenabschätzung (DSFA) das richtige Werkzeug. Wie das Werkzeug zu nutzen ist und welche Schritte nacheinander durchgeführt werden, ist in sogenannten Rahmenwerken dokumentiert. Das große Angebot an vorhandenen Rahmenwerken macht eine Auswahl jedoch für Nicht-Experten sehr schwer. Bei einer Bewertung vieler der vorhandenen Verfahren, wurde weiter festgestellt,

dass sich keines ideal für den Einsatz in der intelligenten Videoüberwachung eignet. Deshalb wurde mit der Kombination verschiedener bereits vorhandener Rahmenwerke ein neues Rahmenwerk für die (intelligente) Videoüberwachung geschaffen. Dieses ermöglicht eine methodische Sammlung, Bewertung und Behandlung von Risiken für die IT-Sicherheit und den Datenschutz.

Angreiferanalyse für die intelligente Videoüberwachung Ein Teil der Datenschutz-Folgenabschätzung (DSFA) besteht darin, die Bedrohungen für das untersuchte System zu sammeln und zu bewerten. Je nach Technologie kann dabei auf umfassende Bedrohungskataloge zurückgegriffen werden. Da für die (intelligente) Videoüberwachung kein solcher Bedrohungskatalog existiert, muss mit einer Angreiferanalyse begonnen werden. Es ist offensichtlich, dass ein intelligentes Videoüberwachungssystem aus Sicht der IT-Sicherheit ein vernetztes System mit erweiterten Funktionen darstellt. Da Bedrohungen und Angriffe gegen vernetzte Systeme bereits gut untersucht sind, konnte hier auf den Stand der Technik zurückgegriffen und lediglich für die erweiterten Funktionen die Bedrohungen untersucht werden. Das Ergebnis ist ein Katalog von insgesamt sechs neuen Bedrohungen, stark geprägt durch den Missbrauch durch einen Operator, die bei der intelligenten Videoüberwachung zusätzlich in die DSFA aufgenommen werden müssen.

Gesamtprototyp NurseEye Getrieben durch ein ausgewähltes Szenario, der datenschutzfreundlichen Sturzerkennung und Alarmierung für Krankenhäuser, wurde ein Prototyp erstellt, der ein Höchstmaß an Akzeptanz zum Ziel hat. Dieser soll dazu dienen, die erstellten Technologien anschaulich zu präsentieren und gleichzeitig die abschließende Evaluation des Akzeptanzmodells erlauben. NurseEye vereint eine algorithmische Detektion von Stürzen mit der schnellen und unkomplizierten Alarmierung von nahen Pflegekräften über mobile Endgeräte. Um maximale Transparenz für die Betroffenen zu erreichen, wurden Kameras durch Displays erweitert. Sie stellen damit einen bidirektionalen Kanal zwischen den Patienten und den Pflegern dar. Dank diesem *„Ich sehe, wer mich sieht"-Prinzip*, können Betroffene sofort erkennen, wenn ein Pfleger Zugriff auf

ihre Videodaten hat. Die begleitende Datenschutz-Folgenabschätzung (DSFA) stellt sicher, dass Risiken für den Datenschutz und damit Risiken für Missbrauch minimiert werden und kommuniziert dies an die Betroffenen.

1.3 Aufbau der Arbeit

Die vorliegende wissenschaftliche Arbeit ist in sieben inhaltliche Kapitel gegliedert. Kapitel 2 fasst die für das Verständnis der Arbeit wichtige Grundlagen zusammen. Da nicht davon ausgegangen werden kann, dass der Leser mit dem Themengebiet der *intelligenten Videoüberwachung* vertraut ist, beginnt die Arbeit mit der Abgrenzung verschiedener Systeme. Weiter wird ein grundlegendes Verständnis über die Arbeitsweise der algorithmischen Bildauswertung erarbeitet. Ein zusammenfassendes Einsatzszenario verdeutlicht anschließend, wie Technik und Algorithmen zu intelligenten Systemen kombiniert werden. Am Ende der Grundlagen wird der Begriff der Akzeptanz untersucht..

Im Kapitel 3 wird ein Überblick über den aktuellen Stand der Forschung gegeben. Das Thema „Akzeptanz der Videoüberwachung“ wird in verschiedenen wissenschaftlichen Disziplinen betrachtet, die wichtige Beiträge leisten können. Die Ergebnisse verschiedener Arbeitsgruppen der Sozial-, Recht- und Ingenieurwissenschaften werden vorgestellt und in ihrer Bedeutung für die Arbeit bewertet.

Kapitel 4 markiert den Start der eigenen wissenschaftlichen Arbeiten. Zur Untersuchung der erstellen Forschungshypothesen wird ein Akzeptanzmodell für die intelligente Videoüberwachung erstellt. Diese orientiert sich an den Arbeiten der Wirtschaftsinformatik und überträgt die Forschungsmethode auf das neue Gebiet der intelligenten Videoüberwachung. Das neu entwickelte Modell ist sowohl in der Lage, bestehende Theorien über die Akzeptanz zu bestätigen als auch neue Ansätze für die Akzeptanz der Videoüberwachung aufzuzeigen.
Kapitel 5, 6 und 7 greifen die Erkenntnisse aus dem Akzeptanzmodell auf und untersuchen, wie die einzelnen identifizierten Akzepterztreiber positiv beeinflusst werden. Dazu werden der Reihe nach Ansätze untersucht, wie die

empfundene Nützlichkeit (vgl. Kapitel 5), das Missbrauchsrisiko (vgl. Kapitel 6) und die Transparenz (vgl. Kapitel 7) durch technische Details so beeinflusst werden können, dass die Akzeptanz steigt.

Kapitel 8 greift die entwickelten Technologien auf und setzt sie in einem konkreten Einsatzszenario um. Ausgehend von dem Ziel, Stürze auf Gängen und Außenbereichen von Krankenhäusern zu detektieren und durch entsprechende Alarmierung die Versorgung zu verbessern, wird ein intelligentes Videoüberwachungssystem entworfen. In diesem werden die Erkenntnisse der Akzeptanzforschung aufgegriffen, um ein System zu entwickeln, dass für maximale Akzeptanz durch die Betroffenen optimiert ist. Eine prototypische Implementierung prüft die Machbarkeit der Ansätze.

In Kapitel 9 erfolgt eine abschließende Evaluierung des Gesamtsystems. Hier werden zwei Elemente betrachtet. Zum einen soll sichergestellt werden, ob die allgemeinen Theorien über die Akzeptanz von Videoüberwachung auch für das gewählte Einsatzgebiet Krankenhaus gültig sind. Zum anderen soll untersucht werden, ob, wie durch das Akzeptanzmodell prognostiziert, eine gesteigerte Akzeptanz erreicht werden konnte. Ein abschließendes Fazit in Kapitel 10 fasst die Ergebnisse der Arbeit zusammen und gibt einen Ausblick auf zukünftige Forschungsthemen.

2 Grundlagen

Zur Schaffung einer gemeinsamen Grundlage wird das folgende Kapitel zuerst verschiedene Formen der *Überwachung* genauer eingrenzen und ein typisches Einsatzszenario darstellen. Weiter wird der Begriff der Akzeptanz und seine Bedeutung für die Videoüberwachung untersucht.

2.1 Formen der Videoüberwachung

Der Begriff intelligente Videoüberwachung (engl.: smart video surveillance) ist in der Literatur weit verbreitet. Die wissenschaftliche Datenbank Scopus [SCOPUS] listet im Zeitraum ab 2010 über 400 Publikationen zu dem Schlagwort „smart video surveillance“. Umso überraschender ist es, dass bisher eine einheitlich akzeptierte Grenze zwischen konventioneller und intelligenter Videoüberwachung fehlt. Diese Arbeit greift die Definition von Videoüberwachungssystemen nach Moniri und Chibelushi auf [MC05]. Sie definieren drei unterschiedliche Formen der Videoüberwachung: konventionelle, automatisierte und intelligente Videoüberwachung. Dabei sind die Übergänge zwischen den einzelnen Systemarten fließend und können nicht an harten Kriterien festgemacht werden.

2.1.1 Konventionelle Videoüberwachung

Konventionelle Videoüberwachungssysteme haben ihre Ursprünge in den frühen vierziger Jahren des vergangen Jahrtausends. Ihr grundlegender technischer Aufbau ist in Abbildung 2.1 dargestellt. Ihr Ziel ist es, einer Sicherheitskraft zu ermöglichen, einen größeren Bereich gleichzeitig im Auge zu behalten, als dies ohne Technik möglich wäre. Als *Sensoren* kommen Kameras zum Einsatz, um entweder weit entfernte Areale oder Bereiche, zu denen der Blick bauartbedingt

beschränkt ist, sichtbar zu machen. Die *Infrastruktur* ist typischerweise auf analoge Signalübertragung aufgebaut. Häufig werden hier proprietäre Verfahren eingesetzt, was Systeme unterschiedlicher Hersteller zueinander inkompatibel macht. In späteren Entwicklungsschritten wurden Videorekorder integriert, um mit dem Videoarchiv auch im Nachhinein ein Ereignis nachvollziehen oder Beweismittel vorlegen zu können. Die *Bediengeräte* der Systeme sind stark eingeschränkt. Die Videodaten der Kameras werden dem Operator auf Monitorwänden angezeigt, auf denen er diese auswerten muss. Einfache Bedienkonsolen erlauben das Ein- und Ausschalten des Systems, den Zugriff auf ein optionales Videoarchiv und steuern eventuell vorhandene Schwenk-/Neige-Kameras.

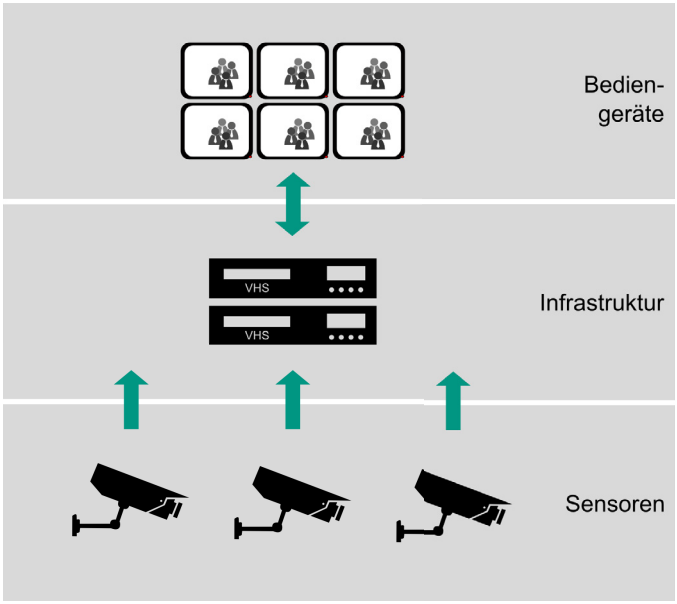


Abbildung 2.1: Konventionelle Videoüberwachung

2.1.2 Automatisierte Videoüberwachung

An der Grenze zwischen konventioneller und intelligenter Überwachung unterscheidet sich die Definition von Moniri und Chibelushi von anderen. Sie führen die *automatisierte Überwachung* als Zwischenstufe ein. Systeme zur automatisierten Videoüberwachung versuchen die Arbeitsbelastung des Operators zu reduzieren. Anstatt dem Operator die Daten der Kameras nur auf einer Monitorwand anzuzeigen, wird versucht, seine Aufmerksamkeit auf Videos mit erkannter Bewegung zu lenken. Die eingesetzten Methoden zur Bildauswertung sind jedoch primitiv und sind nicht in der Lage, die Semantik einer Szene zu erfassen. Es wird nur die Bewegung detektiert und nicht unterschieden, ob es sich um einen Menschen, um Autos oder einen sich im Wind bewegenden Ast handelt.

Der typische Aufbau eines automatisierten Videoüberwachungssystem ist in Abbildung 2.2 zu sehen. Als *Sensoren* werden Kameras genutzt. Diese sind bereits vielmals digital. Die *Infrastruktur* baut häufig auf digitaler Signalübertragung auf, die automatisierte Bildauswertung wird typischerweise auf handelsüblichen Servern ausgeführt. Die optionale Archivierung von Videodaten erfolgt typischerweise ebenfalls digital auf Festplattenservern. Durch die voranschreitende Standardisierung der Protokolle und Formate können Komponenten unterschiedlicher Hersteller eingeschränkt kombiniert werden. Die *Bediengeräte* sind ein Mix von Monitorwänden, einfachen Konsolen, wie bei konventionelle Systemen, und handelsüblichen PCs.

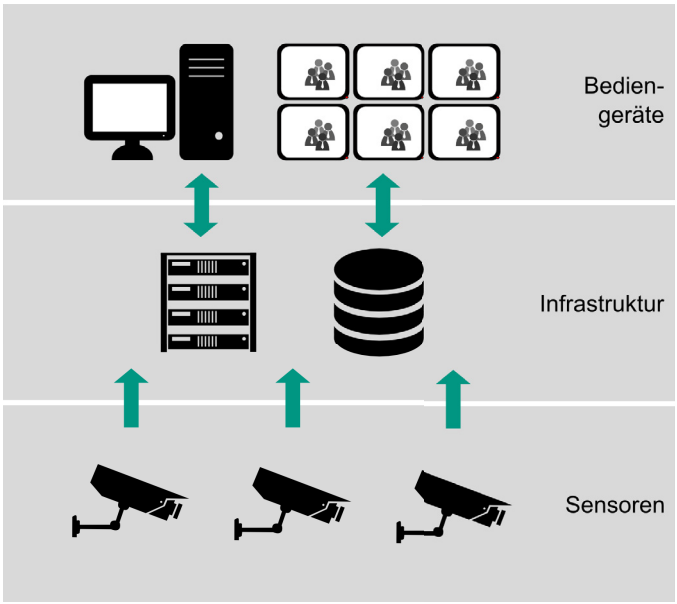


Abbildung 2.2: Automatisierte Videoüberwachung

2.1.3 Intelligente Videoüberwachung

Bei der *intelligenten Videoüberwachung*, im Englischen entweder smart oder intelligent video surveillance genannt, werden ebenfalls Algorithmen zur Bildauswertung eingesetzt, um dem Operator bei der Auswertung der erfassten Szenen zu unterstützen. Diese Algorithmen sind jedoch im Vergleich zu automatisierten System leistungsfähiger und versuchen die Semantik einer Szene zu erfassen. Szenen werden in mehreren Schritten ausgewertet und für die weitere Verarbeitung abstrahiert. Typische Verarbeitungsschritte sind das Detektieren, Klassifizieren und Verfolgen von Objekten. Viele Systeme klassifizieren zusätzlich das Verhalten von Objekten und können so beispielsweise zwischen stehenden, laufenden und rennenden Personen unterscheiden.

Abbildung 2.3 zeigt den typischen technischen Aufbau eines Systems. Als *Sensoren* kommen bei intelligenten Videoüberwachungssystemen digitale Kameras

zum Einsatz, teilweise werden Stereokameras eingesetzt. Diese erlauben, durch ihre dreidimensionale Erfassung der Umgebung, dass auch komplexe Handlungsabläufe erfasst werden. Zunehmend werden sogenannte Smart-Kameras angeboten, die neben der reinen Erfassung auch erste Auswerteaufgaben übernehmen [Bel10]. Neben Kameras lassen sich weitere Sensoren, wie beispielsweise Mikrofone [Zha+11] oder Radio-Frequency Identification (RFID)-Lesegeräte [HVL08], integrieren. Die *Infrastruktur* ist ausschließlich digital. Häufig kommen IP-basierte Netzwerke zum Einsatz. Die intelligente Bildauswertung erfolgt auf handelsüblichen Servern. Die optionale Archivierung von Videodaten erfolgt rein digital auf Festplattenservern. Die hohe Standardisierung aller eingesetzten Komponenten erlaubt es, dass fast beliebig Komponenten unterschiedlicher Hersteller miteinander kombiniert werden. Die *Bediengeräte* werden durch komplexe Softwareanwendungen gebildet. Mit ihnen kann der Operator das Verhalten des Systems bestimmen und erhält die benötigen Rückmeldungen über die Bildauswertung. Typischerweise erfolgt die Interaktion zwischen Operator und dem System über handelsübliche PCs. Einige Systeme setzen mobile Endgeräte ein, um mit dem Operator oder mobilen Sicherheitskräften zu interagieren [BK14].

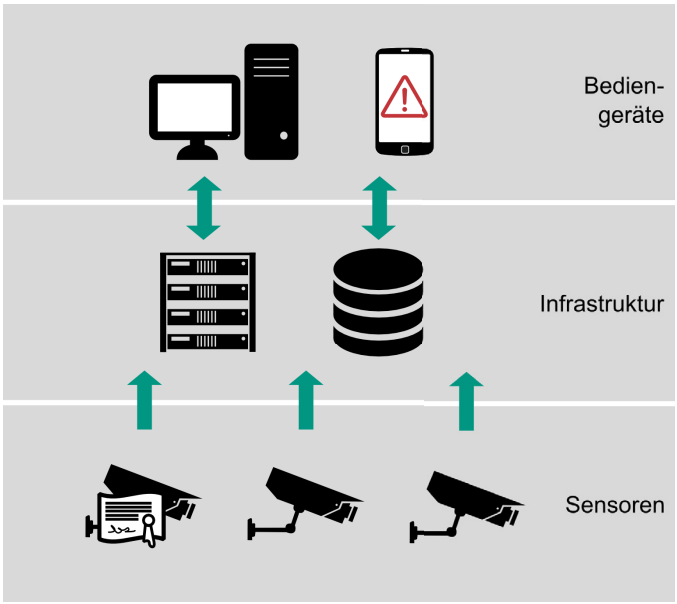


Abbildung 2.3: Intelligente Videoüberwachung

2.1.4 Die NEST-Referenzarchitektur

Network Enabled Surveillance and Tracking (NEST) ist eine seit 2010 am Fraunhofer IOSB entwickelte Referenzarchitektur für die intelligente Videoüberwachung [MRV10]. Die Besonderheit der in Abbildung 2.4 gezeigten Architektur liegt in der starken Entkopplung der einzelnen Verarbeitungsschritte. Dies wird durch die Trennung der Datenverarbeitung in *Signalverarbeitung*, *Informationsverwaltung* sowie *Informationsverwertung* erreicht.

Alle erfassten Rohdaten werden über den *Multiplexbus* für die verschiedenen Module zur *Signalverarbeitung* bereitgestellt. Eine nachträgliche Integration von leistungsfähigeren Algorithmen zur Signalauswertung ist sogar zur Laufzeit möglich. Ein typisches Modul in der Signalverarbeitung ist ein Algorithmus zur Personendetektion. Dieser durchsucht das ihm bereitgestellte Videomaterial nach Objekten, die er als Personen klassifizieren kann. Das Ergebnis

der Module zur Signalverarbeitung wird über den *Ereignisbus* in die Stufe der *Informationsverwaltung* transportiert.

Neben einem klassischen Videoarchiv ist auf dieser Ebene die *Modellwelt* angesiedelt. Sie wird zur Speicherung aller Nicht-Videodaten genutzt und verwaltet abstrakte Informationen, wie beispielsweise die Detektion einer Person an einer bestimmten Raumkoordinate. Des Weiteren ist sie für die Fusion von Daten aus unterschiedlichen Quellen oder Zeitpunkten zuständig. Wird die gleiche Person in aufeinanderfolgenden Zeitpunkten an unterschiedlichen Orten detektiert, fusioniert die Modellwelt diese Daten in einen Datensatz mit der aktuellen Position und einer Bewegungshistorie über die vergangenen Positionen. Wurde in einem der erfassten Zeitpunkte zusätzlich erkannt, dass die Person einen Koffer trägt, wird diese Information mit dem bereits vorhandenen Objekt fusioniert und ist in der weiteren Verarbeitung bekannt. Die Modellwelt speichert zusätzlich gegebenenfalls vorhandenes a-priori-Wissen, wie etwa den Gebäudeplan, für die spätere Verwertung.

Auf der höchsten Stufe der Architektur arbeiten Module zur *Informationsverwertung*, die über den *Dienstebus* die benötigten Informationen aus der Modellwelt oder dem Videoarchiv abrufen. Die Module der Informationsverwertung erfüllen konkrete Sicherheitsaufgaben im Überwachungssystem und bilden die Schnittstelle zum Operator. Um beispielsweise einen bestimmten Bereich in einem Gebäude vor Überfüllung zu schützen, würde man ein Modul zur Informationsverwertung entwickeln, dass die in der Modellwelt gespeicherten Detektion von Personen überwacht. Übersteigt die aktuelle Anzahl an Personen die maximale Belegung eines Raums, wird der Operator benachrichtigt. Module zur Informationsverwertung können dabei sowohl dauerhaft aktiv sein oder auch nur bei Bedarf, beispielsweise als Ergebnis eines anderen Moduls zur Informationsverwertung, aktiviert werden.

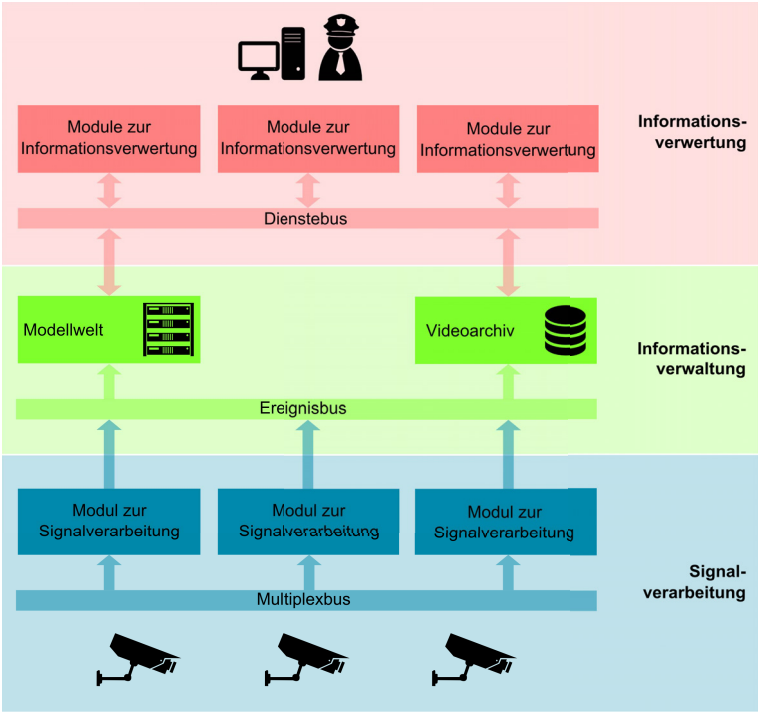


Abbildung 2.4: NEST-Architektur

2.2 Algorithmen zur Bildauswertung in der Videoüberwachung

Die algorithmische Auswertung von Videodaten ist ein grundlegender Baustein für die intelligente Videoüberwachung. Ziel ist es, dass nicht der Operator allein eine kritische Situation erkennen muss, sondern ein Algorithmus diese erkennt und dann die Aufmerksamkeit des Operators darauf lenkt. Auch wenn die Entwicklung von Algorithmen zur Videoauswertung nicht Bestandteil dieser Arbeit ist, soll kurz eine Übersicht über typische Verfahren gegeben werden.

Eine ausführlichere Studie über den aktuellen Stand, bieten die Arbeiten von Hu et al. [Hu+04] und Wang [Wan13].

Die *Objektdetektion* bildet die Grundlage für fast alle weiteren algorithmischen Verarbeitungsschritte in der Videoauswertung. Algorithmen zur Objektdetektion sind in der Lage, in einem Bild oder Szene die relevanten Objekte im Vordergrund vom Hintergrund zu trennen. Mittels *Objektklassifikation* werden die als relevant erkannten Objekten verschiedenen Klassen, wie Person, Auto, Koffer etc., zugeordnet. In der Videoüberwachung spricht man häufig von Verfahren zur *Personendetektion*, die in einer Szene Objekte erkennt und nur weiterverarbeitet, wenn sie als Person klassifiziert wurden.

Objektverfolgung wird genutzt, um ein einmal erkanntes und klassifiziertes Objekt über mehrere Bilder in einer Szene zu verfolgen. Ziel ist es, zu verstehen, wie sich das Objekt in der Szene bewegt. Die besondere Herausforderung liegt hier in der Wiedererkennung bereits bekannter Objekte, wenn diese, beispielsweise durch Überdeckung mit anderen Objekten, (teilweise) nicht mehr zu sehen waren. Die *Multi-Kamera Personenverfolgung*, die gerade für Überwachungsaufgaben sehr wichtig sein kann, ist ein Sonderfall dieser Klasse von Algorithmen. Eine einmal erkannte Person soll hierbei, über den Erfassungsbereich mehrerer Kameras, verfolgt werden. Beim Wechsel zwischen den Erfassungsbereichen mehrerer Kameras oder wenn eine Person verdeckt war, soll eine Wiedererkennung eine durchgängige Verfolgung erlauben. Ihre Leistungsfähigkeit lässt sich in die drei Klassen *Erkennen*, *Wiedererkennen* und *Identifizieren* einteilen. Beim *Erkennen* ist ein Videoüberwachungssystem in der Lage, in einer Szene das Objekt Person zu detektieren. *Wiedererkennen* bedeutet, dass ein Videoüberwachungssystem eine Person, die den Erfassungsbereich einer Kamera verlassen hat und wieder betritt, als dieselbe Person wiedererkennt. Häufig wird die Farbe der Kleidung, die Gangart oder andere soft-biometrische Merkmale für die Wiedererkennung genutzt. Verlassen Personen für eine längere Zeit den Erfassungsbereich aller Kameras oder wechseln ihre Kleidung, werden sie typischerweise nicht mehr wiedererkannt. *Identifizieren* ist die höchste Stufe der Personendetektion. Hier wird die Identität einer Person, beispielsweise durch den Abgleich mit einer Datenbank von biometrischen Gesichtsdaten,

eindeutig erkannt. Im Gegensatz zum Wiedererkennen geht man davon aus, dass die genutzte Methode zur Identifikation robust ist und man sich ihr nicht durch einfache Veränderungen, beispielsweise durch einen Wechsel der Kleidung, entziehen kann. Wiederkennen oder Identifizieren ist im Allgemeinen eine Voraussetzung für eine Mutli-Kamera Personenverfolgung.

Das Überwachen von Personenströmen ist ebenfalls eine häufig zu lösende Aufgabe für die Videoüberwachung. Bei einer sehr hohen Personendichte ist es nicht mehr möglich, einzelne Personen zu detektieren. In diesem Fall wird die Detektion von Gruppen mit geschätzten Personenzahlen genutzt.

Aufbauend auf den Ergebnissen der Objekterkennung und -verfolgung arbeiten weitere Algorithmen zur *Verhaltensanalyse*. Hier kann algorithmisch beispielsweise Gewalt [NAT98], das Sprühen von Graffiti [Ang+05], zurückgelassenes Gepäck [SR00] oder der Sturz einer Person [Tao+05], erkannt werden. Eine Sonderklasse dieser Algorithmen versucht *abnormales Verhalten* zu detektieren [DSC07]. Damit ist gemeint, dass ein Algorithmus das typische Verhalten von Personen an einem bestimmten Ort lernt und erkennt, wenn das aktuelle Verhalten von diesem stark abweicht. Mit dieser Klasse von Algorithmen versucht man Ereignisse, wie beispielsweise eine eintretende Panik zu erkennen, ohne genau spezifizieren zu können wie solche Ereignisse aussehen.

Eine letzte Klasse der Algorithmen arbeitet nicht auf den erkannten Objekten, sondern detektiert spezifische Muster in den Bildern. Beispiele hierfür sind die algorithmische Detektion von Feuer oder Rauch [LA04] oder die Manipulationserkennung an Geldautomaten.

2.3 Einsatzszenario für die intelligente Videoüberwachung

Um die Arbeitsweise von NEST im Speziellen und der intelligenten Videoüberwachung im Allgemeinen weiter zu verdeutlichen, wird hier ein 2014 umgesetztes Überwachungsszenario beschrieben. Im Szenario „Flughafensicherung“ wird ein großer Flughafenbetreiber bei typischen Sicherheitsaufgaben unterstützt. Das entworfene System nutzt zwei Algorithmen zur Signalverarbeitung, um aus den erfassten Rohdaten abstrahierte Informationen abzuleiten.

Personendetektion ist für die Erkennung von Personen im Videomaterial zuständig, während *Objektdetektion* Objekte erkennt und in verschiedene Klassen, wie etwa KOFFER, ROLLSTUHL oder PUTZWAGEN, einteilt. Die erfassten Daten werden in der *Modellwelt* fusioniert und gespeichert.

Auf den damit zur Verfügung stehenden Daten arbeiten mehrere Algorithmen zur Informationsverarbeitung. Die *Multi-Kamera Personenverfolgung* kann bei Bedarf eine Person auf ihrem Weg verfolgen. Für das Szenario ist besonders der Algorithmus zur *Erkennung von zurückgelassenem Gepäck* von Bedeutung. Wenn zu einem KOFFER keine Person in der Modellwelt zugeordnet werden kann, weil ein KOFFER abgestellt wurde und die Person sich davon entfernt hat, alarmiert das System den Operator. Die weitere Alarmbehandlung gliedert sich wie folgt: Da zwischen dem Abstellen eines Gepäckstücks und der Alarmierung eine gewisse Wartezeit liegt, nutzt der Operator das Videoarchiv, um die Person zu finden, die das Gepäckstück als letztes bewegt hatte. Sobald die Person gefunden wurde, können zwei unterschiedliche Verfahren genutzt werden. Bei der biometrischen Personensuche wird das Bild der abstellenden Person aus dem Videoarchiv zu einer biometrischen Personensuche im gesamten Flughafengelände genutzt. Wird die Person gefunden, wird der Operator über den aktuellen Aufenthaltsort informiert und kann über weitere Schritte entscheiden.

Nicht immer, kann die Person in den aktuellen Videodaten gefunden werden. Das kann den Grund haben, dass die Person den Flughafen verlassen hat, oder einfach nur daran liegen, dass sie sich aktuell in einem nicht von Kameras überwachten Bereich befindet. *Multi-Kamera Personenverfolgung* nutzt das Videoarchiv und die letzte bekannte Position der Person für eine automatische Suche. Sollte die Person dabei den Erfassungsbereich aller Kameras verlassen, sucht das System automatisch in den Videodaten aller angrenzenden Kameras, ob die Person dort wieder erscheint. Das Ergebnis ist der zeitliche und räumliche Pfad der Person, ab dem Start der Personenverfolgung bis zum aktuellen Zeitpunkt. Diesen kann der Operator nutzen, um über weitere Schritte zu entscheiden. Sollte die Person nur wenige Meter entfernt an einem Kiosk stehen, würde man sie vermutlich über den vergessenen Koffer informieren. Sollte sie

aber nach dem Abstellen des Koffers sofort den Flughafen verlassen haben, würde man vermutlich den Bereich des Flughafens sperren.

Dieses Szenario zeigt eines der angedachten Einsatzgebiete der intelligenten Videoüberwachung. Die Systeme sollen einen menschlichen Operator bei der Erkennung und Behandlung von Sicherheitsvorfällen unterstützen. Dabei wird die überlegene menschliche Lageneinschätzung mit der Informationsaufbereitung durch Algorithmen vereint, die nicht ermüden oder sich ablenken lassen.

2.4 Akzeptanz

Der letzte Punkt, über den Klarheit geschaffen werden soll, ist der Begriff *Akzeptanz* an sich. Schon alleine der Begriff „Akzeptanz“ wirft im Umfeld von Videoüberwachung Fragen auf. Das Wörterbuch der Soziologie definiert Akzeptanz als „die Eigenschaft einer Innovation, bei ihrer Einführung positive Reaktionen der davon Betroffenen zu erreichen“ [ETB89]. Ist man mit dieser Definition nicht zufrieden, beispielsweise weil nur die Einführung einer Innovation betrachtet wird und nicht die spätere Nutzung, hilft ein Blick auf den Wortursprung. Akzeptanz ist die Substantivierung des Verbs akzeptieren und stammt von dem lateinischen Wort „accipere“ ab. Dieses bedeutet so viel wie gutheißen, annehmen oder billigen. Möchte man also die Akzeptanz der Videoüberwachung durch technische Maßnahmen steigern, wie es die vorliegende Arbeit tut, verfolgt man das Ziel Videoüberwachungssysteme so auszugestalten, dass möglichst viele der Betroffenen dieses System annehmen.

Endruweit beschreibt den Begriff Akzeptanz als „die Eigenschaft einer Innovation, bei ihrer Einführung positive Reaktionen der davon Betroffenen zu erreichen“ [End02]. Die wissenschaftliche Diskussion, ob es sich bei Akzeptanz um eine passive Haltung handelt, bei der man besser zwischen der passiven Akzeptanz und der aktiven Akzeptabilität unterscheidet, wird hier nicht weiter aufgegriffen. Zwei wichtige Aspekte des Begriffs sollen aber näher betrachtet werden.

In zahlreichen Arbeiten, hier sei als Stellvertreter die Arbeit von Quiring [Qui06] genannt, wird die Akzeptanz in die drei Dimensionen *kognitive*, *af-*

fektive und *konative* Akzeptanz aufgeteilt. Die kognitive Akzeptanz adressiert den Verstand und zielt auf die Gegenüberstellung von Kosten und Nutzen einer Innovation ab. Die affektive Akzeptanz adressiert eine subjektive emotionale Einstellung, die die Wahrnehmung einer Innovation prägt. Die konative Dimension ist handlungsbezogen und beschreibt die Nutzung der Innovation durch die Betroffenen. Auch wenn die konative Dimension für die Akzeptanzforschung von Videoüberwachung keine Rolle spielt, ist die Trennung zwischen kognitiver und affektiver Akzeptanz hoch interessant. Sie erklärt, warum Betroffene zwar einerseits den Einsatz von Videoüberwachung zur Verbrechensbekämpfung und Beweissicherung befürworten, aber gleichzeitig in Bereichen mit Videoüberwachung ein unbestimmtes Unbehagen empfinden können.

Der zweite wichtige Aspekt ist die Akzeptanz-Skala von Sauer et al. [Sau+05]. Diese, ursprünglich für die Akzeptanz von Naturschutzgebieten entwickelte Skala, ist auch für die Technikakzeptanz interessant. Die in Tabelle 2.1 dargestellte Skala verdeutlicht, dass Akzeptanz nicht als eine binäre Entscheidung für oder gegen eine Innovation verstanden werden darf, sondern sich auf verschiedenen Stufen, zwischen den beiden Extremen der *Aktiven Gegnerschaft* und dem *Engagement* für eine Innovation, bewegt.

Inakzeptanz	*Stufe 1:* **Aktive Gegnerschaft** gegen die Sache bzw. das Akzeptanzobjekt. Sie entspricht einer sehr stakten Inakzeptanz und äußert sich in Handlungen. *Stufe 2:* **Ablehnung** entspricht einer starken Inakzeptanz, die verbal oder nonverbal geäußert wird.
Übergang	*Stufe 3:* **Zwiespalt** kann innerlich (innerhalb einer Person) oder intern (innerhalb einer Organisation) auftreten. *Stufe 4:* **Gleichgültigkeit**: Keine subjektive Betroffenheit, weder Akzeptanz noch Inakzeptanz.
Akzeptanz	*Stufe 5:* **Duldung:** Sehr geringe Akzeptanz, entsteht aufgrund von Machteingriffen. *Stufe 6:* **Konditionelle Akzeptanz:** Geringe Akzeptanz, die auf rationalen Überlegungen basiert und an Bedingungen gekoppelt ist. *Stufe 7:* **Zustimmung, Wohlwollen** entspricht hoher Akzeptanz, bei der das Akzeptanzobjekt vom Akzeptanzsubjekt aus innerer Überzeugung positiv bewertet wird. *Stufe 8:* **Engagement** für die Sache: sehr hohe Akzeptanz, die sich in Handlungen aufgrund innerer Überzeugung äußert.

Tabelle 2.1: Akzeptanz-Skala nach [Sau+05]

3 Verwandte Arbeiten

Eine erste Literaturrecherche zum Thema Akzeptanz der Videoüberwachung verleitet zum Eindruck, dass das Thema bereits sehr gründlich untersucht wurde. Bei genauer Prüfung entdeckt man jedoch, dass die Arbeiten sehr viel Redundanz aufweisen und alles andere als vollständig sind.

Grundsätzlich lassen sich verwandte Arbeiten in drei Gruppen einteilen, die im weiteren Verlauf dieses Kapitel betrachtet werden:

1. Sozialwissenschaftliche Arbeiten, die die Auswirkungen von Videoüberwachung auf die Gesellschaft untersuchen.

2. Rechtswissenschaftliche Arbeiten, die bestehende und neue Systeme zur Videoüberwachung auf ihre Rechtmäßigkeit prüfen.

3. Ingenieurwissenschaftliche Arbeiten, zur konkreten Ausgestaltung von Systemen zur Videoüberwachung.

3.1 Sozialwissenschaftliche Arbeiten

Die sozialwissenschaftlichen Arbeiten bilden den, für die Öffentlichkeit am meisten sichtbaren, Block. Sie beschäftigen sich mit der Frage, ob und wie Videoüberwachung einen Beitrag zur Sicherheit in öffentlichen Räumen leisten kann und soll. Besonders der *chilling effect* und seine negativen Auswirkungen auf die Gesellschaft, wird intensiv untersucht [Gra86]. Der aus dem anglo-amerikanisch-kanadischen Sprachraum stammende Begriff beschreibt, wie sich Bürger durch das bloße Vorhandensein von Videokameras (oder auch nur Attrappen) einer Art Selbstzensur unterziehen. Dieser Effekt sorgt dafür, dass es in den überwachten Bereichen zu weniger Straftaten kommt, da sich Bürger immer einer direkten Beobachtung durch den Staat und Strafbehörden ausgesetzt

sehen. Gleichzeitig kann aber auch beobachtet werden, dass Bürger sich in ihren Freiheiten stark eingeschränkt fühlen und auch ihre demokratischen Rechte zur freien Meinungsäußerung, Versammlungsrecht oder Demonstrationsrecht nur noch eingeschränkt ausüben. Bekannte Arbeiten in diesem Bereich sind beispielsweise Robb [Rob79], Askin [Ask72] und Starr et al. [Sta+08] wobei mit Ryberg [Ryb07] auch Kritiker der Theorien genannt werden sollen.

Eine weitere Dimension, die in der Sozialwissenschaft oft beachtet wird, ist die Frage nach der Wahrnehmung von Videoüberwachung durch die Betroffenen. Bereits unzählige Studien wurden erstellt, in denen verschiedene Personengruppen zu ihrer Meinung zur Videoüberwachung befragt wurden. Als ein Vertreter dieser Studien soll das Urban Eye Projekt als wohl umfassendste Studie der letzten Jahre genannt werden [UrbanEye]. Im Abschlussbericht fassen Hempel und Töpfer die Ergebnisse der über 1000 Befragungen in der Bevölkerung und 93 Experteninterviews zusammen [HT04]. Die Studie zeigt, wie auch viele ähnliche Untersuchungen, dass es große Schwankungen in der Wahrnehmung und Akzeptanz von Videoüberwachungssystemen gibt. Die Unterschiede stehen häufig in einem Zusammenhang mit Geschlecht, Alter und Bildung der Befragten sowie aktuellen Medienberichten zu Gewalttaten oder den Ländern, in denen die Studien durchgeführt werden.

In seiner Dissertation „Akzeptanz von Videoüberwachung – Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen“ greift Dominic Kudlacek die aktuelle sozialwissenschaftliche Forschung auf [Kud15]. Mit seiner Arbeit möchte er eine Lücke in der Erklärung der Akzeptanz von Videoüberwachung schließen. So ist es zwar mittlerweile größtenteils akzeptiert, dass die Akzeptanz sehr stark mit sozioökonomischen Faktoren, wie beispielsweise dem Alter variieren, an diese Stelle enden jedoch die meisten Erklärungen. Welche Hintergründe dafür verantwortlich sind, dass junge Menschen der Videoüberwachung eher kritisch gegenüberstehen, wird bisher nur unzureichend untersucht, so Kudlacek.
Er kommt zu dem Ergebnis, dass Videoüberwachung von der Bevölkerung überwiegend positiv aufgenommen wird und ihr eine hohe kriminalpräventive Wirkung zugesprochen wird. In einem Vergleich mit den Ergebnissen früherer

Studien, scheint die Akzeptanz der Videoüberwachung jedoch in den letzten Jahren etwas nachgelassen zu haben. Besonders interessant sind weiter die Erkenntnisse über die Gründe für eine ablehnende Haltung. Personen, die in der Arbeit von Kudlacek als Kritiker der Videoüberwachung identifiziert wurden, tun dies nicht aus diffusen Ängsten vor Totalüberwachung, sondern vielmehr aus Zweifeln an deren kriminalpräventiven Wirkung.

Weiter lassen die Ergebnisse von Kudlacek vermuten, dass die Bevölkerung viel aufgeklärter über die tatsächliche Wirkung ist, als vielmals angenommen wird. So gibt es keine allgemeine Erwartung, dass die Videoüberwachung einen effektiven Schutz von Affektstraftaten oder alkoholisierten Straftätern bietet. Über die Hälfte der Befragten geht jedoch davon aus, dass Videoüberwachung dazu beiträgt, Straftaten wie Diebstahl, Raub und Körperverletzung, aber auch terroristische Anschläge zu verhindern.

Anders als in vielen anderen Studien konnte die Befragung von Kudlacek keine signifikanten Unterschiede in der Akzeptanz zwischen Männern und Frauen feststellen. Allerdings zeigen sich hinsichtlich des Alters und des Bildungsstands signifikante Unterschiede. Ältere Menschen befürworten den Einsatz von Videoüberwachung häufiger und sind ebenso eher von ihrer kriminalpräventiven Wirkung überzeugt. Personen mit geringer Bildung beurteilen den Einsatz häufiger positiv als Personen mit hoher formaler Bildung. Diese zweifeln eher an der positiven Wirkung und scheinen seltener um ihre Sicherheit besorgt zu sein. Soweit decken sich die Ergebnisse von Kudlacek mit der überwiegenden Mehrzahl der Studien. Besonders interessant ist jedoch, dass er die Unterschiede auf zwei Einflüsse, das *Empfinden von Kriminalitätsfurcht* und die *Angst vor terroristischen Anschlägen*, zurückführen konnte. Diese beiden Faktoren alleine können, so argumentiert Kudlacek, einen sehr hohen Anteil der Varianz der Wahrnehmung erklären, die bei unterschiedlicher Bildung oder unterschiedlichem Alter festgestellt wird.
Der aktuelle Stand der Forschung in den Sozialwissenschaften gibt damit Aufschluss über die Akzeptanz der Videoüberwachung, jedoch keine Anhaltspunkte, wie diese durch technisches Design gezielt positiv zu beeinflussen ist.

3.2 Rechtswissenschaftliche Arbeiten

Im rechtswissenschaftlichen Bereich existiert eine Vielzahl an Veröffentlichungen zum Thema Videoüberwachung. Dabei handelt es sich fast ausschließlich um die rechtliche Untersuchung von konventionellen Systemen, die für die vorliegende Arbeit keinen wichtigen Beitrag liefern können und deshalb nicht weiter betrachtet werden. Zwei richtungsweisende Arbeiten aus dem rechtswissenschaftlichen Bereich, die sich mit der Frage der intelligenten Videoüberwachung beschäftigen, werden jedoch ausführlicher betrachtet.

Bier und Spieker gen. Döhmann sehen in der intelligenten Videoüberwachung ein hohes Risiko für einen Eingriff in die informationelle Selbstbestimmung, das durch geeignete technische Mittel und rechtliche Vorgabe kontrolliert werden muss [BD12]. Gleichzeitig machen sie auf das hohe Potential der Technologie für einen gestärkten Datenschutz in der Videoüberwachung aufmerksam. Gerade die Arbeitsweise der Systeme erlaubt eine bessere Berücksichtigung datenschutzrechtlicher Vorgaben und durch die geeignete Auswahl von Sensoren sind Sicherheitsaufgaben mit einem vergleichsweise geringeren rechtlichen Eingriff als bei konventionellen Systemen möglich. Protokollierungsfunktionen und automatische Benachrichtigungen in Verbindung mit modernen Smartphones erlauben laut den Autoren eine Steigerung der Transparenz und Nachvollziehbarkeit. Die Herausforderung für die Zukunft sehen sie darin, dass Überwachungssysteme so ausgestaltet werden, dass Möglichkeiten zum Datenschutz umgesetzt und dadurch die mögliche höhere Eingriffsintensität ausgeglichen wird.

In ihrer Arbeit „Gestufte Kontrolle bei Videoüberwachungsanlagen“ stellen Roßnagel, Desoi und Hornung ein Gesamtkonzept für eine rechtskonforme intelligente Videoüberwachung vor [RDH11]. Die Autoren argumentieren dort, dass intelligente Videoüberwachung, besonders durch mögliche Funktionen, wie dem automatischen Verfolgen von Personen über mehrere Kameras oder biometrischer Personenerkennung, potentiell einen viel schwereren Eingriff in die Privatsphäre darstellen als konventionelle Systeme. Trotzdem sehen sie das hohe Potential der Technik für die Gewährleistung von Sicherheit in über-

wachten Bereichen. Um einen angemessenen Ausgleich zwischen Sicherheit und Freiheit zu erreichen, schlagen sie ein Drei-Stufen-Modell vor.

In der ersten Stufen ist das System in seiner Mächtigkeit stark beschränkt und dem Operator stehen nur grundlegende Funktionen zur Beobachtung des überwachten Bereichs zur Verfügung. Ziel dieser Stufe ist es, dem Operator einen möglichst guten Überblick zu verschaffen, ohne in die Rechte der Beobachteten, ganz besonders in das Recht auf informationelle Selbstbestimmung, einzugreifen. Zum Schutz der Privatsphäre können die dem Operator angezeigten Videos durch geeignete Verfahren der Bildmanipulation, wie etwa Verpixeln, geschützt werden. Der Wechsel in die zweite Stufe geschieht entweder automatisch, also wenn ein Algorithmus zur Bildauswertung ein verdächtiges Verhalten beobachtet oder auf direkten Wunsch des Operators.

In der zweiten Stufe wird eine Straftat oder die Anbahnung einer solchen vermutet, weshalb nun intrusivere Verfahren zur Situationsbewertung bereitstehen. Der Operator kann nun beispielsweise Kameras nach Belieben zoomen und Gebrauch von erweiterten Algorithmen, etwa einer automatischen Personenverfolgung, machen. Auch in dieser Stufe soll das Recht auf informationelle Selbstbestimmung des Beobachteten so weit wie möglich gewahrt werden. Das System vermeidet es weiterhin das Gesicht der Betroffenen anzuzeigen und erlaubt keine Extraktion von biometrischen Templates, die für eine spätere Personenwiedererkennung genutzt werden könnten. Der Wechsel in die dritte Stufe kann wiederum durch einen Algorithmus oder auf Wunsch des Operators erfolgen.

In der dritten Stufe ist mit sehr hoher Wahrscheinlichkeit davon auszugehen, dass eine Straftat vorliegt oder eine konkrete Gefahr besteht, die nur durch das Eingreifen von Sicherheitspersonal abgewendet werden kann. Sie dient in erste Linie der Beweissicherung und der Koordination mit Einsatzkräften vor Ort. Das Videoüberwachungssystem zeigt nun auch die Gesichter der Betroffenen und erlaubt dem Operator ein biometrisches Template zu extrahieren. Dieses kann, sollte der Verdächtige fliehen, später zur Personenwiedererkennung eingesetzt werden.

Der von Roßnagel, Desoi und Hornung vorgeschlagene Einsatz zeigt anschaulich, wie die Mächtigkeit des Systems und damit auch sein potentieller Eingriff in die Rechte Betroffener, mit der aktuelle Situation abgeglichen werden kann. Droht eine Situation zu eskalieren, rechtfertigt sie tiefere Eingriffe, was aber nur für eine beschränkte Zeit und einen kleinen Personenkreis notwendig ist.

3.3 Ingenieurwissenschaftliche Arbeiten

Rund um das Thema intelligente Videoüberwachung existieren viele ingenieurwissenschaftliche Arbeiten. Sie haben ihren Fokus häufig bei der Erfassung und Auswertung von Bilddaten oder skalierenden Systemarchitekturen. Die Frage, wie die Akzeptanz dieser Systeme gesteigert werden kann, wird nur von wenigen Gruppen untersucht, wobei dies fast immer durch eine gesteigerte Anonymisierung erreicht werden soll. Dies ist zwar naheliegend, immerhin ist der größte Kritikpunkt an (intelligenter) Videoüberwachung ihr Eingriff in die Privatsphäre, deckt aber nicht die volle Bandbreite an Möglichkeiten ab, die im weiteren Verlauf der vorliegenden Arbeit untersucht werden.

Die ingenieurwissenschaftlichen Arbeiten erlauben noch einmal eine Trennung in zwei Untergruppen. Zum einen Arbeiten, die sich mit dem Schutz der Videodaten beschäftigen, und zum anderen Arbeiten, die den Entwurf, Entwicklung und Einsatz von Gesamtsystemen betrachten.

3.3.1 Arbeiten zum Schutz der Videodaten

Eine häufig genutzte Möglichkeit, um die Privatsphäre der Betroffenen zu schützen, liegt in der Manipulation der Videodaten. Hierfür werden die für die Privatsphäre kritischen Bildbereiche (engl.: Region of Interest (ROI)), wie beispielsweise Gesichter, ganze Personen oder Nummernschilder, anonymisiert. Die nun aufgeführten Ansätze stellen keine vollständige Untersuchung dar, sondern sollen vielmehr einen Überblick über die verschiedenen Herangehensweisen bieten.

Schiff et al. nutzen ein System, welches Bauarbeiter mittels ihrer Helme und farbigen Westen erkennt [Sch+09]. Die Bereiche dazwischen und damit auch das Gesicht der Mitarbeiter, werden anschließend mit farbigen Balken überdeckt. Cheung et al. gehen mit ihrem Ansatz noch etwas weiter [CZV06]. Sie anonymisieren ROIs indem sie diese vollständig mit dem Hintergrund der Szene ersetzen. Wird das Verfahren für den gesamten Körper und nicht nur das Gesicht angewendet, werden Personen in einer Szene praktisch unsichtbar. Diesen Verfahren ist gemeinsam, dass die in den ROIs enthalten Informationen komplett verloren gehen.

Sony hält das Patent auf ein Verfahren, dass bei der Erfassung von Videodaten den Hautton einer Person erkennt und durch einen anderen ersetzt [Ber00]. Damit soll eine rassistische Diskriminierung verhindert werden, wobei die Gesichter und damit auch die Mimik für die Auswertung erhalten bleiben. Wann ein solches Verfahren verfügbar sein wird und wie hoch der benötigte Rechenaufwand dafür sein wird, ist jedoch unklar. Vergleicht man die Ansprüche des Patents mit den aktuell vorhandenen Verfahren, erscheint eine Umsetzung innerhalb der nächsten fünf Jahre unwahrscheinlich.

Bereits verfügbare Verfahren zur Bildmanipulation, wie etwa Verpixeln oder Gaußsche Unschärfe, sind in der Lage, Informationen über die Farbe und Form der überdeckten ROIs zu erhalten. Mit dem KiwiVision® Privacy Protector® ist bereits ein Produkt auf dem Markt erhältlich, das in Echtzeit bewegte Bereiche anonymisiert [Kiw]. Mit diesen Ansätzen soll sichergestellt werden, dass geschütztes Videomaterial für den Operator auswertbar bleibt, er jedoch weniger Rückschluss auf die Identität der beobachteten Personen ziehen kann [BRB15]. Dufaux und Ebrahimi stellen ein alternatives Verfahren vor, indem sie Bildblöcke innerhalb der ROIs zufällig vertauschen und neu anordnen [DE06]. Weiter zeigen sie, dass ihr Verfahren deutlich robuster gegen Angriffe mit automatisierter Gesichtserkennung ist, als die üblichen Verfahren [DE10].
Andere Autoren haben ihre Verfahren absichtlich so aufgebaut, dass sie bei Bedarf und entsprechenden Berechtigungen umgekehrt werden können. Baaziz et al. nutzen ein System, in dem sie sich bewegende Bildbereiche markieren und anschließend anonymisieren [Baa+07]. Das Verfahren kann bei Bedarf, jedoch

mit erhöhtem Rechenaufwand, teilweise rückgängig gemacht werden. Boult schlägt ein Verfahren vor, in dem die ROIs verschlüsselt und nur bei Besitz des geheimen Schlüsselmaterials wiederhergestellt werden können [Bou05]. Cheung et al. präsentieren ein System, bei dem Personen in einer intelligenten Umgebung erkannt und anschließend das erfasste Videomaterial mit dem kryptographischen Schlüsselmaterial der erkannten Person verschlüsselt werden [CPN08]. Der Zugriff auf die erfassten Daten ist somit nur noch in Kooperation mit der sichtbaren Person möglich.

3.3.2 Arbeiten für Gesamtsysteme

Neben den bereits vorgestellten Arbeiten zum Schutz von Bildmaterial gibt es noch eine Reihe von weiteren Arbeiten, die Vorschläge für privatsphärengerechte Gesamtsysteme machen. Senior et al. präsentiert wohl eines der bekanntesten Systeme dieser Art [Sen+05]. Erfasste Videodaten werden bereits auf der Kamera verschlüsselt und so geschützt an das System übermittelt, wo sie durch Algorithmen aufbereitet werden. Jede Interaktion mit dem System geschieht anschließend ausschließlich über die sogenannte Privacy Console. An ihr können sich Personen oder auch Dienste anmelden und haben anschließend, entsprechend ihrer Zugriffsrechte, Zugang zu den vorhandenen Informationen. Senior et al. schlagen hier drei verschiedene Level vor: Auf dem Statistiklevel können Anfragen über die Anzahl an Personen in einem bestimmten Raum oder allgemeine Informationen über durchschnittliche Besuchermengen an Tagen gestellt werden. Dieser Level ist für Gebäudedienste, wie etwa eine adaptive Klimaanlage, konzipiert. Nutzer mit höheren Zugriffsrechten können zusätzlich auf ein Level mit gerenderten Videos zugreifen. Der Detailgrad der gerenderten Video kann dabei von primitiven Blöcken, die anstelle von Personen gezeigt werden, bis hin zu exakten Personenmodellen, auf die Anforderungen angepasst werden. Benutzer mit den höchsten Zugriffsrechten erhalten Zugang zum Videolevel und damit den erfassten Videodaten. Dieser Level sollte laut Senior et al. für Strafverfolgungsbehörden reserviert sein.

Fleck und Straßer präsentieren eine Arbeit zur Überwachung von Pflegeheimen [FS08]. Durch den Einsatz von Smart-Kameras, also Kameras, die sofort nach der Erfassung der Videodaten eine Verarbeitung durchführen, ist es möglich, eine privatsphärengerechte Überwachung zu etablieren. Anstatt durchgängig Videos zu verschicken, sendet eine Smart-Kamera nur dann Informationen über das Netzwerk, wenn von ihr ein Sturz erkannt wurde. Somit werden weniger sensitive Daten übertragen, was neben dem erhöhten Datenschutz zusätzlich das Netzwerk entlastet. Wenn ein Sturz erkannt wurde, wird dies dem Pflegepersonal auf einer Übersichtskarte dargestellt. Das System ist damit vollständig entkoppelt von den Aufnahmen der Kameras und nutzt diese nur zur Situationserkennung.

Winkler und Rinner präsentieren eine generische Arbeit zum Schutz von intelligenten Videoüberwachungssystemen [WR14]. Sie untersuchen, welche Sicherheitseigenschaften ein Kamerasystem erfüllen muss, um als sicher gelten zu können. Dabei betrachten sie sowohl den Schutz des Gesamtsystems vor Angreifern, wie auch die Qualität und Authentizität der erfassten Videodaten. Ähnlich wie bei Fleck und Straßer werden erfasste Videodaten bereits auf der eigens entwickelten TrustCAM verschlüsselt. Dabei setzen Winkler und Rinner auf ein mehrschichtiges Verfahren. So werden ROIs erkannt und aus dem Originalbild ausgeschnitten. Sowohl der Ausschnitt als auch eine mit Bildmanipulation geschützte Kopie werden verschlüsselt verschickt. Somit ist es, je nach aktueller Situation und Berechtigung des Betrachters möglich, ein individuelles Bild anzuzeigen. Ohne entsprechende Berechtigungen erhält ein Betrachter nur das Bild ohne ROIs. Nach einer erfolgreichen Authentifizierung ist es möglich, ihm selektiven Zugriff auf die geschützten ROIs oder sogar die unveränderten Bildinhalte zu geben. Winkler verfolgt den Ansatz der vertrauenswürdigen intelligenten Kameras und zeigt auf, wie sie einen wichtigen Bestandteil modernen Videoüberwachung bereitstellen [Win11]. Dank eines Trusted Platform Module (TPM), einem Mikrochip, der Sicherheitsfunktionen bereitstellt, kann gewährleistet werden, dass eine Kamera und die darauf installierte Software nicht manipuliert wurde. Dies kann sowohl vom Operator in der Zentrale als auch von Beobachteten vor Ort mittels einer Handy Software überprüft werden.

Dies ist für mögliche Zertifizierungen und dem Vertrauen der Überwachten in das System besonders wichtig.

Die Arbeit, die sich wohl am umfassendsten mit dem Datenschutz in der intelligenten Videoüberwachung beschäftigt, ist die Dissertation von Hauke Vagts [Vag13]. Vagts gliedert die Datenerfassung durch intelligente Videoüberwachung in die vier Phasen: Erhebung, Speicherung, Verarbeitung und Nutzung, denen er passende Privacy Enhancing Technologies (PET) zuordnet. Vagts gestaltet seine Architektur nach dem von Ann Cavoukian definierten Privacy by Design (PbD) [Cav09a] und erfüllt gleichzeitig die durch das Bundesdatenschutzgesetz (BDSG) gestellten Anforderungen an eine Videoüberwachung. Damit zeigt er, wie intelligente Videoüberwachung ausgestaltet werden kann, um eine Balance zwischen Sicherheit und Datenschutz zu gewährleisten.

In der gleichen Forschungsgruppe sind auch die Arbeiten von Pascal Birnstill entstanden. In seiner 2016 erscheinenden Dissertation „Privacy-Respecting Smart Video Surveillance Based on Usage Control Enforcement“ schlägt er ein konzeptionelles Rahmenprogramm vor, wie die intelligente Videoüberwachung in ihrer Leistungsfähigkeit reguliert werden kann [Birn16ch]. Seine Arbeit stellt ein System vor, bei dem die Zugriffs- und Nutzungsberechtigungen nicht ausschließlich von den Berechtigungen des Nutzers abhängen, sondern ebenfalls an die aktuelle Bedrohungssituation angepasst sind. Weiterhin ermöglicht das Rahmenwerk, dass Datenschutz-Privilegien auf die beobachteten Personen und Gruppen zugeschnitten werden. Das vorgeschlagene System könnte damit die Besucher in einem Museum deutlich intensiver überwachen als die Angestellten. Beide Verfahren ermöglichen damit, die Verhältnismäßigkeit der Videoüberwachung zu verbessern, indem nur bei kritischen Situationen oder bei unbekannten Personen genauer überwacht wird, während im Normalfall oder bei Personen, die täglich von der Videoüberwachung betroffen sind, mehr Privatsphäre sichergestellt wird.

4 Empirische Untersuchung der Akzeptanz

Nachdem in Kapitel 3 untersucht wurde, wie Akzeptanz von Videoüberwachung bisher betrachtet wurde, fasst dieses Kapitel die eigenen Überlegungen zusammen. Es werden die, in der IKT bereits seit vielen Jahren erfolgreich verwendeten Akzeptanzmodelle für die eigene Forschung genutzt. Diese erklären, wie unterschiedliche Faktoren, beispielsweise die empfundene Nützlichkeit oder Einfachheit der Nutzung, die Adaption neuer Technologie erklären. Das Ergebnis der eigenen Forschung ist ein neues Akzeptanzmodell, entwickelt für die Begebenheiten der intelligenten Videoüberwachung. Gänzlich neu ist dabei dessen Ausrichtung. Das Ziel hinter der Forschung ist es nicht, die Akzeptanz vollständig zu erklären, sondern Faktoren nachzuweisen, die durch die technische Ausgestaltung des Systems beeinflusst werden. Bekannte starke Faktoren, wie Alter oder die individuelle Angst Opfer von Straftaten zu werden, werden zugunsten von neuen Faktoren ignoriert, welche durch technische Gegebenheiten definiert sind.

Das entwickelte Modell wird anschließend empirisch getestet, um seine Bedeutung für die zukünftige technische Ausgestaltung von Videoüberwachungssystemen zu bestimmen.

4.1 Exkurs: Einführung in die Strukturgleichungsmodellierung

Im folgenden Kapitel werden verschiedene theoretische Modelle zur Erklärung der Akzeptanz vorgestellt und entwickelt. All diese Modelle der Akzeptanzforschung basieren auf dem Prinzip der *Strukturgleichungsmodellierung (SGM) (engl.: Structural Equation Modeling (SEM)) (SGM).* SGM bezeichnet ein statistisches Verfahren, um korrelative Zusammenhänge zwischen mehreren Variablen

zu testen oder zu finden. Sie wird den strukturprüfenden multivariaten Verfahren zugerechnet.

Bei der SGM ist es besonders, dass es sich bei den Variablen um sogenannte latente, also nicht direkt beobachtbare Variablen handeln kann. Ein gutes Beispiel für eine *latente Variable*, häufig auch *Konstrukt* genannt, ist die Intelligenz einer Person. Sie kann nicht direkt, sondern muss über mehrere Teilfragen, die sogenannten *Items*, indirekt abgefragt werden. Dabei decken verschiedene Items die unterschiedlichen Aspekte von Intelligenz, etwa sprachliches, rechnerisches und räumliches Denken, ab.

In dem später vorgestellten Akzeptanzmodell werden die Konstrukte: EMPFUNDENE NÜTZLICHKEIT, EMPFUNDENES RISIKO, TRANSPARENZ, EMOTIONALE EINSTELLUNG und AKZEPTANZ betrachtet. Dabei steht hinter jedem Konstrukt jeweils eine Menge an Items, die genutzt werden, um das Konstrukt zu erfassen. Es werden beispielsweise die Items *Erleichterung der Arbeit*, *Steigerung der Sicherheit*, *Erkennen von Straftaten* und *Sichern großer Bereiche* abfragt, um die latente Variable EMPFUNDENE NÜTZLICHKEIT zu messen (vgl. Tabelle B.1). Die Items bilden zusammen die *Skala* zur Erfassung der Konstrukte.

In der SGM wird weiter zwischen dem *Messmodell* und dem *Strukturmodell* unterschieden. Das Messmodell fasst ein erklärtes Konstrukt mit seiner Skala zusammen. Im Strukturmodell werden die Konstrukte und die Hypothesen bzgl. der Wirkung der Konstrukte aufeinander zusammengefasst. Da man sich bei der SGM primär für das Strukturmodell interessiert, werden die Messmodelle typischerweise zur besseren Übersicht nicht abgebildet. In Abbildung 4.1 werden die Begriffe und die Struktur der SGM noch einmal zusammengefasst.

Die Annahme, dass ein Konstrukt, hier als Beispiel die EMPFUNDENE NÜTZLICHKEIT, wirklich die empfundene Nützlichkeit der Betroffenen abdeckt, kann nicht einfach grundlos hingenommen werden. Zur Beurteilung einer Skala werden drei verschiedene Qualitätsmaße erfasst:

- AVE:
  Die durchschnittliche erklärte Varianz (engl.: Average Variance Extracted (AVE)) ist ein Maß für die Konvergenzvalidität eines Konstrukts. Sie misst

also, wie stark ein Konstrukt seine Items erklärt. Gute Skalen erreichen Werte oberhalb von 0,5, d.h. es werden mehr als 50 % der Varianz aller Items durch die Varianz des Konstrukts erklärt.

- Composite Reliability:
  Die Faktorreliabilität misst, wie hoch der Anteil systematischer gemeinsamer Varianz aller Items ist, die zur Schätzung eines Konstrukts verwendet wird. Gute Skalen erreichen Werte oberhalb von 0,7, d.h., dass somit weniger als 30 % der Varianz auf Konstruktebene durch unsystematische Fehlervarianzanteile entstehen.

- Cronbachs α:
  Das Cronbachs α misst, die interne Konsistenz einer Skala und bezeichnet das Ausmaß, in dem die Items einer Skala miteinander in Beziehung stehen. Ein hoher Wert lässt vermuten, dass alle Items der Skala dieselbe Eigenschaft erfassen.

Durch die wissenschaftliche Arbeit zur Erstellung, Evaluation und Verbesserung der verwendeten Skalen, sind heute für sehr viele Konstrukte geeignete Skalen vorhanden. In [Ros02] ist der Vorgang der Skalenentwicklung beschrieben und soll hier nicht weiter vertieft werden.

Werden gute Skalen verwendet, ist sichergestellt, dass tatsächlich ein gemeinsamer Wert, bzw. die Meinung der Probanden gemessen wird. Der Name des Konstrukts ist frei wählbar und sagt nicht darüber aus, was die dazugehörige Skala wirklich erfasst. In dieser Arbeit wurde immer versucht, einen möglichst aussagekräftigen Namen für die Konstrukte zu wählen. Ein Blick auf die verwendeten Items jeder Skala kann jedoch helfen, ein noch genaueres Bild über die erfasste Meinung zu bekommen. Um noch besser zwischen Konstrukten und Meinungen zu trennen, werden in der weiteren Arbeit Konstrukte immer als Kapitälchen geschrieben. Die EMPFUNDENE NÜTZLICHKEIT meint also das gemessene Konstrukt, während die empfundene Nützlichkeit ohne Kapitälchen die Meinung der Befragten zum Thema abbildet.

Die SGM kann sowohl für konfirmatorischen, also den bestätigenden Einsatz, als auch für den explorativen, also den entdeckenden Einsatz, genutzt werden. In dieser Arbeit wird sie als konfirmatives Werkzeug eingesetzt, um vermutete Zusammenhänge zwischen den Faktoren zu bestätigen. Dafür wurden Hypothesen darüber erstellt, wie sich die unterschiedlichen Faktoren gegenseitig beeinflussen. Zur statistischen Auswertung bieten sich zwei unterschiedliche Verfahren, der kovarianzbasierte und der varianzbasierte Ansatz, an. In dieser Arbeit wird der varianzbasierte Ansatz, häufig auch Partial Least Squares (PLS) genannt, genutzt. Die Entscheidung PLS zu nutzen geht zurück auf die Arbeiten von Peng und Lai [PL12] sowie Hair et al. [HRS11]. Beide Gruppen stimmen darin überein, dass PLS in einer ersten Untersuchung eines neuen Modells vorzuziehen ist. Es liefert schon mit kleineren Stichprobengrößen (> 50 Teilnehmer) stabile Ergebnisse und hat einen hohen erklärenden Faktor.

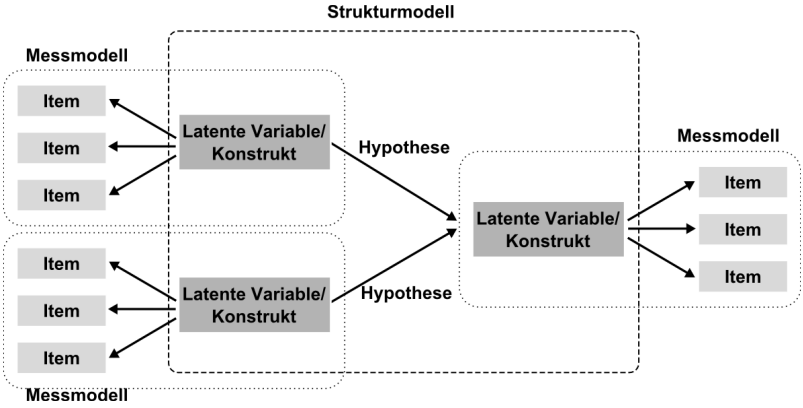


Abbildung 4.1: Strukturgleichungsmodellierung

4.2 Akzeptanzmodelle in der IKT

Das Technologieakzeptanzmodell (engl.: Technology Acceptance Model (TAM)) von Fred D. Davis ist der am weitesten verbreitete Ansatz im Bereich der IKT, um Akzeptanz durch die Anwender zu messen oder zu prognostizieren [Dav89].

Es erweitert die Theorie der begründeten Handlung (engl.: Theorie of Reasoned Action (TRA)) von Fishbein Martin [Fis79]. In TAM argumentiert Davis, dass zwei Konstrukte für die Akzeptanz von Technologie ausschlagend sind: Empfundene Nützlichkeit und empfundene Einfachheit der Nutzung. Die beiden Konstrukte versuchen den Grad zu messen, wie stark eine Person glaubt, dass eine bestimmte Technik ihre Arbeit verbessert und wie einfach sie zu benutzen ist. TAM ist als ein robustes Modell bekannt und wurde erfolgreich auf viele unterschiedliche Technologien angewendet, z.B. E-Mail, WWW und e-Health. Ein Artikel von Lee et al. erkennt TAM als das vorherrschende Modell für die Akzeptanzforschung und Google Scholar listest im Sommer 2015 insgesamt 24.582 Zitierungen für das ursprüngliche Paper von Davis [LKL03b].

Unterschiedliche Gruppen haben TAM erweitert, um besser Vorhersagen zu treffen, wie schnell eine Technologie Anwendung finden wird, nachdem sie in einer Domäne etabliert wurde. Venkatesh und Davis haben mit TAM2 ein Modell geschaffen, dass versucht zu erklären, wie empfundene Nützlichkeit von anderen Konstrukten, etwa Ergebnisqualität und Ruf, beeinflusst werden [VD00]. Venkatesh et al. schlagen mit Unified Theory of Acceptance and Use of Technology (UTAUT) ein noch komplexeres Modell vor, welches zusätzliche Faktoren, wie beispielsweise Geschlecht und sozialen Druck, berücksichtigt. Diese neuen Faktoren erlauben bessere Vorhersagen, aber die ursprüngliche Einfachheit von TAM ging verloren [Ven+03].

4.3 Akzeptanzmodell für die Videoüberwachung

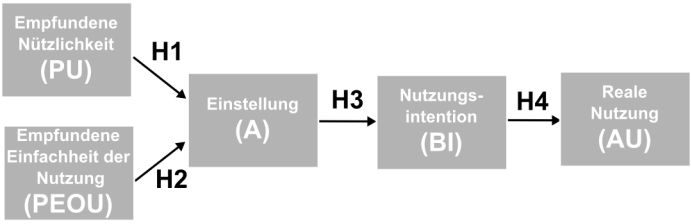


Abbildung 4.2: TAM: Das Akzeptanzmodell nach Davis [Dav89]

Um zu verstehen, wie TAM oder ähnliche Modelle genutzt werden können, um die Akzeptanz von Videoüberwachung zu erklären, muss man zuerst verstehen, wie TAM typischerweise genutzt wird. Die Arbeit von Davis und anderen Gruppen zielt auf folgendes Szenario ab: Mitarbeiter in einer Firma bekommen eine neue Technologie, beispielsweise die E-Mail, angeboten, die sie in ihrer täglichen Arbeit unterstützen soll. Für diese Technologie sollen Vorhersagen getroffen werden, wie stark die Mitarbeiter diese Technologie akzeptieren, also in ihrer täglichen Arbeit einsetzen werden. Wie in Abbildung 4.2 zu sehen ist, geht TAM von zwei Einflussfaktoren aus: Empfundene Nützlichkeit (engl.: Perceived Usefulness (PU)) und empfundene Einfachheit der Nutzung (engl.: Perceived Easy Of Use (PEOU)). Diese Faktoren beeinflussen die Einstellung (engl.: Attitude (A)) gegenüber einer neuen Technologie, die wiederrum die Nutzungsintention (engl.: Behavior Intention (BI)) beeinflusst. Am Ende des Modells steht die reale Nutzung (engl.: Actual Use (AU)), die von der Nutzungsintention beeinflusst wird. Die Trennung zwischen Nutzungsintention und realer Nutzung macht bei der Akzeptanz neuen Technologien durchaus Sinn. Es ist sehr gut möglich, dass Mitarbeiter einer Technologie sehr aufgeschlossen gegenüberstehen und gerne einsetzen möchten, aber beispielsweise Aufgrund von hohem Stress nicht in der Lage sind, sie in ihre Arbeit einzugliedern.
Folgende Hypothesen fassen die Effekte, die innerhalb TAM beobachtet werden, zusammen:

H1: Die empfundene Nützlichkeit (PU) hat einen *positiven* Einfluss auf die Einstellung (A).

H2: Das empfundene Einfachheit der Nutzung (PEOU) hat einen *positiven* Einfluss auf die Einstellung (A).

H3: Die Einstellung (A) hat einen positiven Einfluss auf die Nutzungsintention (BI).

H4: Die Nutzungsintention (BI) hat einen *positiven* Einfluss auf die reale Nutzung (AU).

Bis auf die reale Nutzung (AU) liegen latente Variablen (vgl. Abschnitt 4.1) vor, die nicht direkt gemessen, sondern über Items abgefragt werden müssen. Die Reale Nutzung kann durch einfaches zählen aller Personen die eine angebotene Technik einsetzen, ermittelt werden.

Wie an diesem Beispiel gut zu erkennen ist, unterscheiden sich die Einflüsse auf die Akzeptanz bei TAM stark von der Situation in der Videoüberwachung. Ziel der Forschung ist es, die Akzeptanz von Videoüberwachung durch die Bevölkerung zu verstehen. Die befragten Personen nutzen das System nicht selbst, sondern stehen unter seiner Beobachtung. Die empfundene Nützlichkeit ist zwar weiterhin ein interessanter Einflussfaktor, aber sie ist vielmehr aus dem Blickwinkel der eigenen Sicherheit, als der Arbeitserledigung zu betrachten. Da Beobachtete das System nicht bedienen, stellt die empfundene Einfachheit der Nutzung sehr wahrscheinlich keinen wichtigen Faktor dar.

Da sich weder TAM noch andere etablierte Modelle einsetzen lassen, um die Akzeptanz von Videoüberwachung umfassend zu verstehen, wurde ein neues geeigneteres Modell entwickelt. Als Grundlage wurde TAM genutzt, da es das am weitesten verbreitete Modell darstellt. Erweiterte Modelle, wie etwa UTAUT können zwar besser Erklärungen bilden, erscheinen aber zu kompliziert für eine erste modellgetriebene Untersuchung der Akzeptanz in der Videoüberwachung. Für das neue Modell wurde der Name Technology Acceptance Model-Video Surveillance (TAM-VS) gewählt, um den Ursprung deutlich zu machen [KB14].

In einem ersten Schritt wurden die möglichen Einflussfaktoren in Expertendiskussionen identifiziert. Wie bereits erwähnt, waren dabei nur Faktoren von Interesse, die sich später durch eine entsprechende Ausgestaltung der Technik positiv beeinflussen lassen. Die erste Version des Modells ist in Abbildung 4.3 zu sehen. Zu Beginn der Forschung wurde angenommen, dass es für die Akzeptanz (engl.: Acceptance (AC)) zwei entscheidende Einflüsse gibt. Zum einen die empfundene Nützlichkeit (engl.: Perceived Usefulness (PU)), die angibt, wie sehr Personen glauben, dass ein Videoüberwachungssystem dazu geeignet ist, ihre Sicherheit zu steigern. Zum andern kann bei der öffentlichen Diskussion eine sehr stark ausgeprägte emotionale Einstellung (engl.: Emotional Attitude (EA)) zu Thema Videoüberwachung beobachtet werden.

Die Trennung der Einflussfaktoren zwischen der EMPFUNDENEN NÜTZLICHKEIT und der EMOTIONALEN EINSTELLUNG spiegelt weiter die unterschiedlichen Dimensionen der Akzeptanz wider (vgl. Abschnitt 2.4). Die EMPFUNDENE NÜTZLICHKEIT soll den kognitiven Anteil, also die bewusste Bewertung der Vor- und Nachteile einer Videoüberwachung, messen. Die EMOTIONALE EINSTELLUNG misst den affektiven Anteil der Akzeptanz, also die subjektive emotionale Einstellung die Betroffene gegenüber dem System haben. Wie wichtig die EMOTIONALE EINSTELLUNG bei der Akzeptanz der Videoüberwachung genau ist, war eine der wichtigsten Forschungsfragen, die für die Erstellung von TAM-VS verantwortlich war.

Die Erkenntnisse aus TAM-VS sollen später gezielt dafür genutzt werden, Überwachungssysteme so zu entwickeln, dass eine möglichst hohe Akzeptanz bei der Bevölkerung erreicht wird. Daher ist es wichtig, auch die EMOTIONALE EINSTELLUNG zu verstehen und zu wissen, welche Faktoren diese beeinflussen. Viele in der Theorie bereits bekannte Faktoren, wie etwa Alter, Angst vor Gewaltverbrechen oder Misstrauen gegenüber Autorität, können nicht durch die technische Ausgestaltung beeinflusst werden und sind deshalb für das hier entwickelte Modell uninteressant. Faktoren, die direkt aus den technischen Merkmalen abgeleitet werden können sind: Das EMPFUNDENE RISIKO (engl.: Risk (RI)), dass durch ein Überwachungssystem einem Betroffenen Nachteile entstehen und die TRANSPARENZ (engl.: Transparency (TR)) bei der Datenverarbeitung. Folgende Hypothesen fassen die Effekte, die in TAM-VS vermutet werden, zusammen:

H1: Die EMPFUNDENE NÜTZLICHKEIT (PU) hat einen *positiven* Einfluss auf die AKZEPTANZ (AC).

H2: Das EMPFUNDENE RISIKO (RI) hat einen *negativen* Einfluss auf die EMOTIONALE EINSTELLUNG (EA).

H3: Die wahrgenommene TRANSPARENZ (TR) hat einen *positiven* Einfluss auf die EMOTIONALE EINSTELLUNG (EA).

H4: Die EMOTIONALE EINSTELLUNG (EA) hat einen *positiven* Einfluss auf die AKZEPTANZ (AC).

Neben dem Modell und den zu testenden Hypothesen werden zusätzlich Skalen (vgl. Abschnitt 4.1) zur Datenerhebung benötigt. Dabei wurde auf bestehende Skalen zurückgegriffen und diese für TAM-VS adaptiert. Die Zustimmung zu den einzelnen Aussagen der Items wurde mit einer fünfstufigen Zustimmungsskala mit „*(+2) ich stimme zu*“, „*(+1)*“, „*(0) ich bin neutral*“, „*(-1)*“, „*(-2) ich stimme nicht zu*“, gemessen. Die verwendete Skala entspricht damit einer Likert-Skala. Der verwendete Fragebogen ist vollständig in Anhang A zu finden.

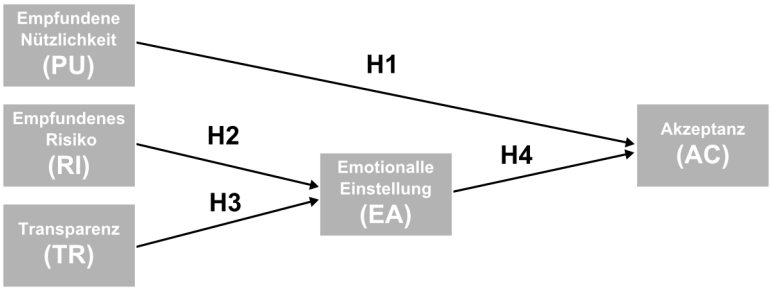


Abbildung 4.3: TAM-VS1: Ein Akzeptanzmodell für die Videoüberwachung

4.4 Evaluierung des neuen Akzeptanzmodells TAM-VS

Nach Abschluss der Modellbildung wurde mit einer ersten Befragung empirische Daten gesammelt und ausgewertet. Nur wenn das Modell an sich als stabil betrachtet werden kann, ist es für die weitere Entwicklung nutzbar.

4.4.1 Datenerhebung

Nachdem TAM-VS und ein geeigneter Fragebogen erstellt war, wurde es in einer ersten Befragung getestet. Die Datenerhebung wurde als Stift und Papierumfrage mit kurzen Präsentationen der zu untersuchenden Technologien

durchgeführt. Diese erste Erhebung erfolgte absichtlich nicht am eigenen Institut oder dem Karlsruher Institute für Technologie (KIT), da dort mit zu vielen stark technikaffinen Probanden zu rechnen war. Deshalb wurde die Befragung an der Berliner Universität der Künste (UdK) durchgeführt, die diverse Studiengänge anbietet. Die Teilnehmer wurden über mehrere Mailinglisten und soziale Netzwerke rekrutiert und mussten sich eine Woche vor den ersten Termin anmelden. Eine Teilnahme ohne eine vorherige Anmeldung war nicht möglich.

Es wurden zwei Szenarien mit unterschiedlich ausgestalteten Videoüberwachungssystemen an einem Flughafen evaluiert. Dieser stellt eine Umgebung dar, die typischerweise videoüberwacht und den meisten Probanden bekannt ist. Wie in Abbildung 4.4 gezeigt, wurde ein Modell eines Flughafens gebaut, um die Szenarien möglichst anschaulich visualisieren zu können.

Bevor die Szenarien vorgestellt wurden, hatten die Probanden Zeit das Modell zu besichtigen und allgemeine Fragen zum Aufbau zu stellen.

Das Modell besteht aus allen Elementen, die typischerweise auf einem Flughafen vorhanden sind: öffentlicher und privater Nahverkehr auf der linken Seite, eine Sicherheitskontrolle und Check-In Schalter in der Mitte, Abflughalle und Gates auf der rechten Seite, sowie ein Gepäckband und Zollkontrolle oben auf dem Gelände. Zusätzliche, nicht funktionale Elemente, wie etwa Toiletten und Cafes wurden ergänzt um einen typischen Flughafenaufbau zu erhalten. In diesem Modell wurden farbige Zylinder verwendet, um die Personen auf dem Flughafengelände zu visualisieren. Die beiden blauen Zylinder stellen Sicherheitspersonal dar, während alle anderen Figuren individuelle Besucher des Flughafens darstellen. Ein Monitor über dem Aufbau zeigt in den unterschiedlichen Szenarien, wie das Sicherheitspersonal das Videoüberwachungssystem nutzen kann.

Abbildung 4.4: Flughafenmodell

Szenario 1: Konventionelle Videoüberwachung im Flughafen Im konventionellen Szenario wurde der Monitor genutzt, um die Videozentrale zu demonstrieren. Wie in Abbildung 4.5 zu sehen ist, wurden verschiedene Videoströme des Flughafens auf dem Monitor angezeigt. Hier wurde eine einzige Kamera mit einem Top-Down Blick genutzt, deren Bild in kleinere Abschnitte geschnitten und anschließend umgeordnet wurden, um den Eindruck vieler Kameraströme zu erreichen. Dies entspricht den heute weit verbreiteten Videoüberwachungssystemen, die an einer zentralen Stelle ausgewertet werden.
Um die Nutzung zu verdeutlichen wurde ein Sicherheitsvorfall durchgespielt. Im Mittelpunkt stand ein Überfall an dem zwei Personen beteiligt sind (Täter und Opfer). Es wurde angenommen, dass der Operator den Vorfall im Videostrom detektieren würde, um entsprechend reagieren zu können. Nach kurzer Zeit floh der Täter und wurde von mobilem Sicherheitspersonal verfolgt, das vom Operator in der Zentrale koordiniert wurde. In diesem Szenario wird dabei

besonders deutlich, wie komplex die Aufgabe ist, eine flüchtende Person über mehrere Videoströme zu verfolgen.

Am Ende der Präsentation wurden die Fragebögen an die Probanden ausgeteilt und sie bekamen ausreichend Zeit, um ihn zu beantworten.

Abbildung 4.5: Monitorausgabe Szenario 1:
Konventionelle Videoüberwachung am Flughafen

Szenario 2: Intelligente Videoüberwachung im Flughafen Nachdem die Teilnehmer den ersten Teil des Fragebogens ausgefüllt hatten, wurde das zweite Szenario mit intelligenter Videoüberwachung vorgestellt. Hier wurde viel Zeit darauf verwendet zu erklären, dass es sich bei dem vorgestellten System, um einen Forschungsprototypen handelt, der so noch nicht eingesetzt werden kann, aber in Zukunft vermutlich in gleicher oder ähnlicher Form eingesetzt werden könnte.

Das vorgestellte System unterstützt den Operator, indem es einige Aufgaben übernimmt. Anstatt eines Monitors mit vielen Videoströmen wird dem Operator das Übersichtsbild des Geländes angezeigt (Abbildung 4.6).

In der Übersichtsdarstellung werden dem Operator alle Personen auf dem Flughafen als schwarze anonyme Figuren visualisiert. Die Position der mobilen Kollegen wird durch Sicherheitskräfte visualisiert. Das System ist in der Lage, Personen automatisch über mehrere Kameras zu verfolgen. Weiterhin ist das System in der Lage, besondere Ereignisse, wie etwa Gewalt, automatisch zu detektieren und den Operator darauf aufmerksam zu machen. Wenn das System ein solches Ereignis erkennt, färbt es den Marker der auslösenden Person violett und die der umstehenden Personen rot, ein. Der Operator kann nun gezielt den Videostrom untersuchen, in dem das Ereignis erkannt wurde und die Situation schnell bewerten.

Zur weiteren Verdeutlichung der Arbeitsweise wurde der gleiche Sicherheitsvorfall wie im klassischen Szenario durchgespielt. Eine Person wurde überfallen und dieser Vorfall vom System erkannt. Auch in diesem Szenario floh der Täter und wurde von den mobilen Sicherheitskräften verfolgt. Der Operator kann sich jedoch nun vollständig auf die Koordination der Kollegen konzentrieren, da die Verfolgung des Fliehenden automatisch vom System übernommen wurde. Am Ende der Demonstration hatten die Befragten Gelegenheit Fragen zur Funktionsweise intelligenter Überwachungssysteme zu stellen, um Missverständnisse zu vermeiden. Alle Fragen zu ethischen oder moralischen Themen wurden jedoch auf das Ende der Befragung verschoben, um eine Beeinflussung der Befragten zu verhindern.

Am Ende der Präsentation wurden die Fragebögen an die Probanden ausgeteilt und diese bekamen ausreichend Zeit, um diese zu beantworten.

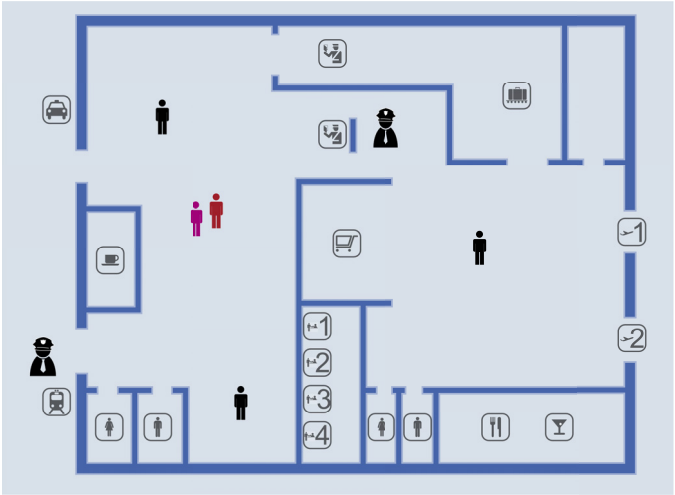


Abbildung 4.6: Monitorausgabe Szenario 2:
Intelligente Videoüberwachung am Flughafen

4.4.2 Analyse der Daten

Insgesamt wurden fünf Befragungsrunden durchgeführt, mit durchschnittlich ca. 15 Personen pro Runde. Im Ausgleich für die Befragung von einer Stunde bekam jeder Teilnehmer ein Incentive von 20€ angeboten, um einen durchgehend hohe Motivation der Teilnehmer zu erreichen.

In Tabelle 4.1 ist die sozioökonomische Analyse der Stichprobe zusammengefasst. Insgesamt wurden 82 gültige Fragebogen ausgefüllt. Die Technikaffinität wurde verdeckt über die Frage „Wenn sie technische Probleme mit beispielsweise ihrem PC oder Handy haben, können sie diese:“ *„Fast immer selbst lösen“*, *„Manchmal selbst lösen“*, *„Fast niemals selbst lösen“* erhoben. Es ist eine deutliche Verschiebung der Stichprobe zur deutschen Gesamtbevölkerung zu erkennen. Die Stichprobe besteht insgesamt aus einem zu hohen Anteil an Frauen, weist einen sehr hohen Bildungslevel auf und ist sehr technikaffin. Rückschlüsse auf die Gesamtbevölkerung sollten also nur mit Vorsicht gezogen werden.

	Anzahl	Anteil in %
Geschlecht		
Weiblich	51	62
Männlich	28	34
Keine Angabe	3	4
Alter		
20-29	51	62
30-39	21	26
40-49	6	7
50-59	2	2
60-69	0	0
70+	0	0
Keine Angabe	2	2
Höchster Schulabschluss		
Mittlere Reife (Realschulabschluss, Polytechnische Oberschule 10. Klasse)	2	2
Fachhochschulreife, Abitur, Erweiterte Oberschule	28	34
Abgeschlossenes Studium	49	60
Weiß nicht	1	1
Keine Angabe	2	2
Technikaffinität		
hoch	42	51
mittel	30	37
gering	8	10
weiß nicht	1	1
Keine Angabe	1	1

Tabelle 4.1: Erste Analyse der Probanden

Test des Messmodells

Das Modell und die darüber aufgestellten Hypothesen wurde statistisch mit der Partial Least Square-Strukturgleichungsmodellierung (PLS-SGM) überprüft [Chi98]. SmartPLS wurde für die Auswertung der Daten genutzt [RWW05].

Nach dem PLS-SGM Ansatz, beginnt die Prüfung des Gesamtmodells mit der Prüfung des Messmodells. In diesem Schritt soll sichergestellt werden, dass die Items, die zusammen beispielsweise den Faktor EMPFUNDENE NÜTZLICHKEIT messen sollen, dieses auch erreichen. Dazu schlägt Chin eine Reihe von Qualitätskriterien vor [Chi98].

Tabelle 4.2 zeigt die Faktorreliabilität (engl.: Composite Reliability) an, der die Eignung eines Faktors zur Erklärung aller ihm zugeordneten Items misst. Alle Werte sind oberhalb des von Chin geforderten Schwellwertes von 0,7. Dies bedeutet, dass weniger als 30% der Varianz auf Konstruktebene durch unsystematische Fehlervarianzanteile begründet ist.

Die durchschnittlich erklärte Varianz (engl.: Average Variance Extracted (AVE)) ist für alle Items größer als 0,5, was für eine gute Konvergenzvalidität spricht. Die ebenfalls in Tabelle 4.2 dargestellten Werte für das Cronbachs α sprechen für eine hohe interne Konsistenz. Die bekannte Faustregel zur Interpretation der Werte [GM10], bezeichnet Werte größer als 0,7 als akzeptabel und Werte größer als 0,8 als gut. Der Wert von 0,42 für das EMPFUNDENE RISIKO im konventionellen Szenario wird hingegen als inakzeptabel bezeichnet. Leider konnte nicht geklärt werden, wie es zu diesem Ausreißer kam. Da er weder im intelligenten Szenario, noch im später betrachteten Szenario intelligente Videoüberwachung im Krankenhaus (vgl. Kapitel 9) auftritt, wird von einem Fehler bei der Datenerhebung ausgegangen. Trotzdem sollte vor einer Wiederverendung der Skala, diese gründlich untersucht werden.

Tabelle 4.3 zeigt die äußeren Gewichte aller Items. Diese stellen ein Maß für die Korrelation zwischen einzelnen Items und den ihnen zugeordneten Faktoren dar. Im Szenario der konventionellen Videoüberwachung am Flughafen liegt dieses zweimal unterhalb des von Chin vorgeschlagenen optimalen Schwellwerts von 0,7. Nach Hulland [Hul99] ist selbst der niedrigste Wert von

0,6 noch weit über dem kritischen Schwellwert von 0,4 der bei einer ersten explorativen Untersuchung erreicht werden sollte. Im Szenario der intelligenten Videoüberwachung wird der Schwellwert nach Chin nie unterschritten. Dies unterstreicht weiterhin die Vermutung eines brauchbaren Messmodels.

Das dritte allgemein in der Forschungsgemeinde akzeptierte Qualitätskriterium eines PLS-SGM-Messmodels ist das Fornell-Larcker Kriterium [FL81]. Es fordert, dass die Quadratwurzel der AVE höher ist als der Betrag der gegenseitigen Korrelation der Konstrukte. Das Konstrukt soll also stärker mit seinen eigenen Items korrelieren als mit anderen Konstrukten. In Tabelle 4.4 sind jeweils die Kreuzkorrelationen der Konstrukte dargestellt sowie die Quadratwurzel der AVE auf der Diagonalen. Es ist zu erkennen, dass das Fornell-Larcker Kriterium für jedes Konstrukt im Messmodell erfüllt ist. Damit ist am Ende der Prüfung kein Hinweis für ein ungültiges Messmodell zu erkennen.

	AVE	Composite Reliability	Cronbachs α
Szenario konventionelle Videoüberwachung			
PU	0,64	0,88	0,82
RI	0,63	0,77	0,42
TR	0,68	0,86	0,76
EA	0,67	0,86	0,75
AC	0,71	0,88	0,79
Szenario intelligente Videoüberwachung			
PU	0,68	0,89	0,84
RI	0,77	0,87	0,70
TR	0,67	0,86	0,75
EA	0,66	0,85	0,74
AC	0,75	0,90	0,83

Tabelle 4.2: Qualitätskriterien Messmodell

Item	Konventionelle Videoüberwachung	Intelligente Videoüberwachung
PU1	0,81	0,74
PU2	0,85	0,84
PU3	0,64	0,80
PU5	0,89	0,90
RI1	0,78	0,90
RI3	0,81	0,85
TR2	0,91	0,81
TR3	0,92	0,86
TR4	0,60	0,78
EA1	0,83	0,85
EA4	0,79	0,77
EA5	0,83	0,81
AC1	0,92	0,93
AC2	0,76	0,78
AC4	0,83	0,87

Tabelle 4.3: Äußere Gewichte der Items

	AC	EA	PU	RI	TR
Konventionelle Videoüberwachung					
AC	0,84				
EA	0,80	0,82			
PU	0,54	0,60	0,80		
RI	-0,34	-0,36	-0,26	0,79	
TR	0,47	0,45	0,33	-0,11	0,82
Intelligente Videoüberwachung					
AC	0,87				
EA	0,85	0,81			
PU	0,69	0,69	0,82		
RI	-0,43	-0,47	-0,29	0,88	
TR	0,54	0,51	0,45	-0,42	0,82

Tabelle 4.4: Fornell-Larcker Kriterium

Test des Strukturmodells

Nachdem die Prüfung des Messmodells keine kritischen Mängel aufgezeigt hat, wurde das Strukturmodell geprüft. Das erste entscheidende Kriterium für die Qualität des Strukturmodells ist R^2 der Konstrukte, da es ein Maß für die Aussagequalität des Modells ist. Je höher der Wert von R^2 ist, desto mehr kann ein Modell die Varianz eines Konstrukts, beispielsweise der Akzeptanz, durch die beobachtete Varianz der Einflussfaktoren, beispielsweise empfundene Nützlichkeit und emotionale Einstellung, erklären. Was die kritischen Schwellwerte von R^2 sind, ist stark vom Einsatzzweck des Modells abhängig. Chin definiert Werte von R^2>0,67 als substantiell, R^2>0,33 als moderat und R^2>0,19 als schwach [Chi98]. Andere Quellen, etwa Schwaiger argumentieren, dass kleinere Werte von R^2 auftreten können, ohne dass dadurch das Modell als unwichtig identifiziert werden sollte [SM11]. Dies kann gerade dann auftreten, wenn die Modellentwicklung noch nicht abgeschlossen ist und manche Einflussfaktoren (absichtlich) nicht berücksichtigt wurden.

Die bestimmten Werte von R^2 für die Akzeptanz: 0,64 im konventionellen Szenario und 0,74 im intelligenten Szenario, erfüllen das Kriterium von Chin um als moderat bzw. substantiell erkannt zu werden. Sie bedeuten, das immerhin 64%, bzw. 60% der beobachteten Varianz im Konstrukt Akzeptanz, durch die Varianz in den beiden Konstrukten empfundene Nützlichkeit und emotionale Einstellung erklärt werden.

Die Werte von R^2 für die emotionale Einstellung: 0,30 im konventionellen Szenario und 0,34 im intelligenten Szenario, sind nach Chin beide als moderat zu bewerten. Sie bedeuten, dass immerhin 30%, bzw. 34% der beobachteten Varianz im Konstrukt emotionale Einstellung durch die Varianz in den beiden Konstrukten empfundenes Risiko und Transparenz erklärt werden.

Die nicht erklärte Varianz kann die Folge eines oder mehrerer nicht erfassten Faktoren oder zufälliger Effekte sein. Zumindest für die emotionale Einstellung kann vermutet werden, dass noch weitere wichtige Einflussfaktoren existieren.

Zur Prüfung der Hypothesen wurden abschließend noch die Pfadkoeffizienten und ihre jeweilige Signifikanz bestimmt. Die Ergebnisse werden in Abbildung 4.7 für das Szenario der konventionellen und in Abbildung 4.8 für das Szenario der intelligenten Videoüberwachung am Flughafen dargestellt. Dort sind ebenfalls die Werte für R^2 der jeweiligen Konstrukte notiert.

Die Pfadkoeffizienten wurden mittels Bootstrapping bestimmt, wie es beim Einsatz von PLS-SGM empfohlen wird [HRS11]. Auch für die Mindestmaße der absoluten Werte der Pfadkoeffizienten gibt es unterschiedliche Aussagen. Sellin und Keeves fordern Werte von mindestens 0,1, um einen Zusammenhang als wichtig zu identifizieren [SK94]. Andere Quellen besagen, dass alle Werte wichtige Zusammenhänge darstellen, solange die Wirkrichtung wie vorhergesagt ist und die Werte signifikant sind. In beiden Szenarien entspricht die Wirkrichtung der prädizierten Richtung und ist größer als der von Sellin und Keeves vorgeschlagene Wert von 0,1.

Wie erwartet hat das EMPFUNDENE RISIKO einen negativen Effekt (Pfadkoeffizienten mit negativem Vorzeichen) auf die EMOTIONALE EINSTELLUNG und die TRANSPARENZ einen positiven Effekt. Der Einfluss der EMPFUNDENEN NÜTZLICHKEIT auf die AKZEPTANZ ist wie zu erwarten positiv. Im Szenario der konventionellen Videoüberwachung scheitert der Pfadkoeffizient jedoch an der Signifikanz. Somit kann ein positiver Einfluss der EMPFUNDENEN NÜTZLICHKEIT auf die AKZEPTANZ nur im Szenario der intelligenten Videoüberwachung nachgewiesen werden.

Wichtig bei der Bewertung der Ergebnisse ist, dass die zugrundeliegende Skala nicht metrisch ist und somit keinen prozentualen Vergleich der Effekte erlaubt. Trotzdem ist klar zu erkennen, dass der Einfluss der EMPFUNDENEN NÜTZLICHKEIT auf die AKZEPTANZ deutlich geringer ist, als der Einfluss der EMOTIONALEN EINSTELLUNG. Diese Wirkzusammenhänge werden im nächsten Kapitel genauer untersucht.

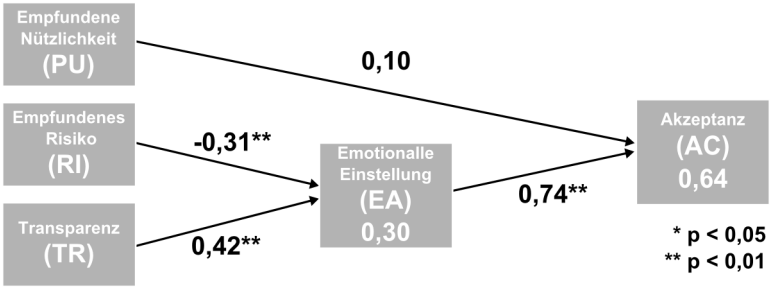


Abbildung 4.7: Auswertung Strukturmodell im konventionellen Szenario

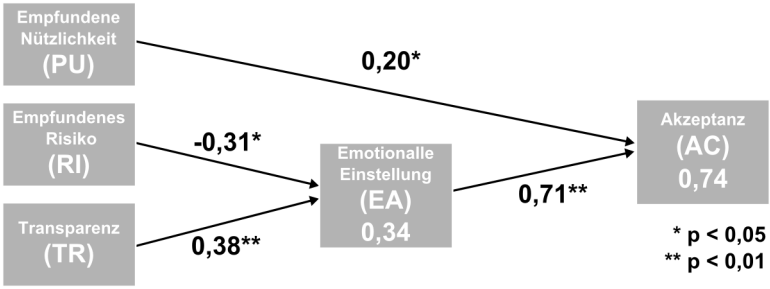


Abbildung 4.8: Auswertung Strukturmodell im intelligenten Szenario

4.5 Bedeutung des Modells

Mit der ersten Evaluierung mit den Daten aus Berlin konnte gezeigt werden, dass das Modell stabil ist. Es ist damit das erste modellgetriebene Verfahren, um die Akzeptanz von Videoüberwachung zu untersuchen.

4.5.1 Erwarteter Einfluss des Modells in der Akzeptanzforschung

Mit TAM-VS wurde ein erstes Modell geschaffen, um die Akzeptanz von Videoüberwachung strukturiert untersuchen zu können. Es orientiert sich stark an der bisher geleisteten Arbeit zur Akzeptanz und portiert das Gelernte auf das neue Gebiet der Videoüberwachung. Ein solches Modell hatte vorher, trotz

der großen Menge an Studien zur Videoüberwachung, nicht existiert. Weniger als ein Jahr nach der ersten Veröffentlichung zum Modell, sind bereits zwei Forschungsgruppen bekannt, die das Modell für ihre Arbeit verwenden wollen [KB14]. Eine an der Fachhochschule Graz kobetreute Arbeit „Acceptance of Video Surveillance Among Younger and Elder Generations in Graz“ von Serra et al., mit einer Stichprobe von über 400 Probanden, konnte 2015 ganz ähnliche Effekte nachweisen [Ser+15]. Es ist wahrscheinlich, dass TAM-VS als Ausgangspunkt für zukünftige Forschung, zu einem deutlich besseren Verständnis der Akzeptanz von Videoüberwachung beitragen kann. Ebenfalls könnte das Modell durch weitere Forschung zukünftig auf den gesamten Bereich von Sicherheitstechnologien angewendet werden.

4.5.2 Bedeutung der Ergebnisse für den Entwurf von Videoüberwachungssystemen

Nach der ersten Studie und der Validierung des Akzeptanzmodells lassen sich Ergebnisse für die Entwicklung von neuen bzw. für das Neudesign existierender Überwachungssysteme festhalten. Auf den ersten Blick sind die Resultate der Studie wenig überraschend. Sowohl die EMPFUNDENE NÜTZLICHKEIT des Systems als auch die EMOTIONALE EINSTELLUNG haben einen Einfluss auf die AKZEPTANZ von Überwachungssystemen. Diese Abhängigkeit zwischen den Faktoren wurde bisher nur vermutet. Ein erstes wichtiges Ergebnis ist, dass diese Abhängigkeit bestätigt wurde.

Ein tieferer Blick in die Ergebnisse dieser Arbeit führt zu einer überraschenderen Erkenntnis. Die EMOTIONALE EINSTELLUNG hat einen höheren Einfluss auf die Akzeptanz als die EMPFUNDENEN NÜTZLICHKEIT. Im konventionellen Überwachungsszenario ist der Pfadkoeffizient der Wirkung der EMPFUNDENEN NÜTZLICHKEIT nur geringfügig größer als der Schwellwert, der von Sellin und Keevens vorgeschlagen wurde. Im Szenario der intelligenten Überwachung ist der Effekt der EMPFUNDENEN NÜTZLICHKEIT größer, aber in beiden Fällen ist die EMOTIONALE EINSTELLUNG wesentlich wichtiger. Das bestätigt die These, dass die Akzeptanz von Videoüberwachung primär einen emotionalen Hintergrund

hat. Auch wenn Sicherheit für einen Teil der Akzeptanz verantwortlich ist, scheint es, dass eine alleinige Verbesserung der Sicherheit nicht zu hochgradig akzeptierten und gewollten Systemen führt.

Die EMOTIONALE EINSTELLUNG stellt einen starken Faktor für die Akzeptanz von Systemen dar und Entwickler sollten versuchen, diese zu verbessern. Die Ergebnisse zeigen, dass das EMPFUNDENE RISIKO einen negativen Einfluss auf die EMOTIONALE EINSTELLUNG hat. Gelingt es also, das empfundene Missbrauchspotential einer Videoüberwachung zu reduzieren, sollte daraus eine gesteigerte Akzeptanz folgern. Ob und wie dies bei einem sehr subjektiven und individuellen Faktor wie dem Missbrauchspotential möglich ist, wird die zukünftige Forschung zeigen.

Die Steigerung der Transparenz von Systemen scheint hier der vielversprechendere Faktor zu sein. Wenn Entwickler darauf abzielen, die Transparenz zu verbessern, z.B. durch eine Offenlegung und Erklärung der Funktionsweise, bieten intelligente Überwachungssysteme ein großes Potential die Akzeptanz zu verbessern.

Schon hier wird deutlich, dass sich die Akzeptanz nicht isoliert verbessern lässt, sondern sehr stark vom gesamten Systemaufbau abhängig ist. Beispielsweise wird eine Senkung des Missbrauchsrisikos nur dann einen positiven Effekt auf die Akzeptanz erreichen können, wenn dies durch geeignete Verfahren transparent für die Betroffenen ist.

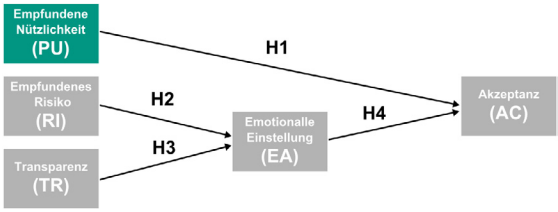
Weitere Forschung ist notwendig um herauszufinden, welche weiteren Faktoren die EMOTIONALE EINSTELLUNG beeinflussen. Die ermittelten Werten für R^2 lassen vermuten, dass mindestens ein weiterer starker Einflussfaktor existiert, der bis jetzt unbekannt ist. Ob es sich dabei ausschließlich um sozioökonomische Variablen, oder vielleicht auch um Elemente handelt, die technisch beeinflusst werden können, ist bisher noch unklar.

Eine Beschränkung der ersten Studie stellt die erfassten Befragten dar. Im Vergleich zur Gesamtbevölkerung, ist die Gruppe der Befragten besser gebildet und jünger, als ein repräsentativer Querschnitt. Wie stark die Meinung der Gesamtbevölkerung mit der Meinung der Stichprobe korreliert bleibt ungeklärt. Auf Grund der offenen Auswahl der befragten Kandidaten lässt sich

aber vermuten, dass die Teilnehmer der Studie ein gesteigertes Interesse an der Entwicklung von Sicherheitstechnologie haben. Es kann somit angenommen werden, dass die Befragten eine gesteigerten Einfluss auf die Meinung von Freunden, Verwandten und Arbeitskollegen ausüben. Gleichzeitig steigt die Wahrscheinlichkeit, dass die Befragten, beispielsweise über ein politisches Engagement oder als Mitglieder von Betriebsräten, zukünftig Einfluss auf die Ausgestaltung von Videoüberwachung ausüben.

Die Faktoren EMPFUNDENE NÜTZLICHKEIT, EMPFUNDENES RISIKO und TRANSPARENZ werden in den folgenden drei Kapiteln einzeln betrachtet und Technologien, Methoden und Ansätze entwickelt, um sie vorteilhaft zu beeinflussen.

5 Empfundene Nützlichkeit



TAM-VS1: Wirkung der empfundenen Nützlichkeit

Obwohl die Ergebnisse von TAM-VS vermuten lassen, dass der Faktor EMPFUNDENE NÜTZLICHKEIT weniger Einfluss auf die Akzeptanz hat, als die Faktoren EMPFUNDENES RISIKO oder TRANSPARENZ, darf seine Wichtigkeit nicht unterschätzt werden. Die Arbeiten von Sara Degli Esposti deuten darauf hin, dass die Nützlichkeit eine notwendige, aber nicht hinreichende Bedingung für die Akzeptanz darstellt [Deg14]. Diese Vermutung deckt sich mit den Ergebnissen von Gill et al. [GBA07]. Das würde bedeuten, dass Videoüberwachung, die keinerlei Beitrag zur Sicherheit leistet, auch dann nicht akzeptiert wird, wenn die anderen Akzeptanzfaktoren voll erfüllt sind. Auch wenn TAM-VS diese Aussage weder belegt noch verwirft, erscheint sie zumindest plausibel.

Videoüberwachung ist immer mit einem gewissen Eingriff in die Privatsphäre der Betroffenen verbunden. Diese lässt sich nur dann rechtfertigen, wenn die Videoüberwachung diesen Eingriff erfordert, um eine bestimmte Nützlichkeit zu erreichen. Im folgenden Kapitel soll diese Nützlichkeit näher betrachtet werden. Dazu werden zuerst die unterschiedlichen Schutzziele der Videoüberwachung betrachtet, wobei für die intelligente Videoüberwachung eine Erweiterung der klassischen Schutzziele vorgeschlagen wird. Der Kern des Kapitels ist dann der Ansatz der interaktiven Videoüberwachung. Dieser generische Ansatz wurde entwickelt, um die Mächtigkeit, also die Nützlichkeit aber auch die

Eingriffe in die Privatsphäre, von Überwachungssystemen zu regulieren. Wird er genutzt, bieten sich bisher nicht genutzte Ansätze für Sicherheitskräfte und Betroffene mit einem solchen System zu interagieren. Beispiele für diese Interaktion schließen das Kapitel ab.

5.1 Nützlichkeit als Zielvorgabe

Nach §6 b Abs. 1 BDSG ist der Einsatz von Videoüberwachung nur dann zulässig, wenn sie für die Erfüllung des Einsatzzwecks erforderlich ist. An dieser Stelle soll keine Betrachtung der Rechtslage erfolgen, da dies bereits ausführlich an anderen Stellen geschehen ist. Es existieren beinahe für beliebige Anwendungsfelder, beispielsweise für den öffentlichen Nahverkehr [Hil09], den Arbeitsplatz [Bay05] oder den öffentlichen Raum [Kla06], ausführliche rechtliche Untersuchungen. Die Arbeiten stimmen alle darin überein, dass die Zulässigkeit einer Videoüberwachung immer an die Erfüllung eines konkreten Zwecks gebunden ist. Dies formuliert somit die elementare Grundanforderung für die weitere Arbeit: **Eine Veränderung einer Videoüberwachung auf eine Art und Weise, die die Erfüllung des Ziels gefährdet, muss ausgeschlossen werden.**

Im weiteren Verlauf werden zunächst die Schutzziele der Videoüberwachung betrachtet, um ein Verständnis darüber zu bekommen, für welche Zwecke Systeme eingesetzt werden.

5.1.1 Ziele der intelligenten Videoüberwachung

Das primäre Ziel von konventioneller Videoüberwachung besteht in der Bereitstellung oder Erhöhung von Sicherheit. Doch schon mit dem Begriff *Sicherheit* bestehen Unklarheiten in der Definition. Klassisch werden unter dem deutschen Wort Sicherheit die beiden englischen Schutzziele *Safety* und *Security* zusammengefasst. In der intelligenten Videoüberwachung ist es zudem sinnvoll, noch ein drittes Ziel *Services* einzuführen. Damit lassen sich folgende Ziele für den Einsatz von intelligenter Videoüberwachung definieren:

- **Safety:**
  Videoüberwachungsanlagen die der Bereitstellung von *Safety* zuzuordnen sind, zielen auf die Erhaltung der *körperlichen Unversehrtheit* vor zufälligen Ereignissen ab. Das Schutzgut ist mindestens ein Mensch, der vor zufälligem Schaden durch eine Maschine oder andere Menschen geschützt werden soll.

- **Security:**
  Wenn eine Videoüberwachungsanlage das Schutzziel *Security* verfolgt, zielt sie auf den Schutz vor *mutwilligem* und zugleich *schadhaftem Verhalten* ab. Das Schutzgut ist mindestens ein Mensch oder Objekt, der/das vor *mutwilligem* Schaden durch *einen Menschen* geschützt werden soll.

- **Services:**
  Services folgen der Definition nach Vagts [Vag13]. Hierbei handelt es ich um Dienste, die nicht mit einer Safety- oder Security-Aufgabe betraut sind, sondern mit einer von der Videoüberwachung betroffenen Person interagiert. Services sind bisher eher in der Forschung untersucht und nur sehr wenig auf dem Markt vorhanden.

In Abbildung 5.1 sind die drei Schutzziele und ihre gegenseitige Abgrenzung dargestellt. Wie man leicht erkennen kann, sind die Grenzen zwischen ihnen nicht scharf. Die Überschneidungen ergeben sich sowohl aus der Tatsache, dass ein System mehrere Aufgaben wahrnehmen kann als auch, dass eine Aufgabe mehreren Zielen zugeordnet werden kann. Die Überschneidungsbereiche werden im Folgenden anhand von Beispielen verdeutlicht:

(a) Dies ist wohl die typischste Überschneidung von Schutzzielen. Viele Videoüberwachungssysteme verfolgen gleichzeitig Safety- und Security-Ziele. So sind beispielsweise Anlagen auf öffentlichen Plätzen fast immer zum Schutz vor Unfällen (Safety) und zum Schutz vor Gewalt (Security) im Betrieb.

(b) Security-Dienste die gleichzeitig Services sind, können als „Security on Demand“ verstanden werden. Ein Beispiel ist der Forschungsprototyp

„Watch My Car“. Hier gibt eine Person dem Videoüberwachungssystem im Parkhaus den Auftrag, sofort die Polizei zu alarmieren, wenn das bewachte Auto von einer anderen Person weggefahren wird.

(c) Äquivalent zu (b) können Dienste, die Safety und Services vereinen, als „Safety on Demand“ verstanden werden. Ein Beispiel ist ein System, in dem Patienten mit Kreislaufproblemen das System auffordern, sofort Hilfe zu alarmieren, wenn sie eine besondere Pose einnehmen.

(d) Intelligente Videoüberwachungssysteme werden in der Zukunft auch in private Haushalte Einzug halten. Eine Kamera im Kinderzimmer, die die Eltern alarmiert, wenn fremde Personen den Raum betreten, Rauch zu erkennen ist oder das Kind aufgewacht ist, deckt gleichzeitig Safety, Security und Services ab.

Betrachtet man die Fragen, die genutzt wurden, um die EMPFUNDENE NÜTZLICHKEIT zu messen (vgl. Tabelle B.1 und Tabelle E.1), fällt auf, dass eine echte Steigerung der Sicherheit und die EMPFUNDENE NÜTZLICHKEIT nicht zwingend zusammenhängen müssen. Anstatt statistische Aussagen über die Sicherheit an einem Ort zu treffen, oder zu messen, wie viele Sicherheitsvorfälle durch ein Videoüberwachungssystem gelöst wurden, fragt TAM-VS danach, wie sehr Betroffene glauben, dass sich ein bestimmtes System eignet, um die Sicherheit in einem überwachten Gebiet zu steigern.

Diese Einstellung könnte auf verschiedene Arten positiv beeinflusst werden. Der von Bruce Scheier geprägte Begriff „Security Theater“ beschreibt Maßnahmen, die dafür gedacht sind, die gefühlte Sicherheit zu steigern, jedoch keinen nennenswerten Effekt auf die tatsächliche Sicherheit nachweisen können [Sch06]. Da solche Maßnahmen zumindest moralisch verwerflich erscheinen und ein positiver Effekt vermutlich nur vorübergehend wäre, werden sie in dieser Arbeit nicht entwickelt.

Es ist stark davon auszugehen, dass eine gesteigerte Sicherheit spätestens mittelfristig einen positiven Effekt auf die empfundene Nützlichkeit der Systeme haben wird. Die tatsächliche Steigerung der Sicherheit stellt ein Forschungs-

gebiet dar, das sehr aktiv untersucht wird. Unzählige Forschungsgruppen und Projekte arbeiten an besseren Verfahren zur automatischen Situationserkennung und Gefahrenprävention. Die Weiterentwicklung bestehender Verfahren wird den Experten der algorithmischen Bildauswertung überlassen und in dieser Arbeit nicht aufgegriffen.

Intelligente Videoüberachtungssysteme bieten deutlich verbesserte Möglichkeiten zur Interaktion von Mensch und System. Darauf aufbauend können Dienste entstehen, die direkt von den Betroffenen genutzt werden. So stellen sie technische Änderungen dar, die nicht nur mittelbar über die gesteigerte Sicherheit auf die Akzeptanz wirken können, sondern auch ganz direkt wahrgenommen werden.

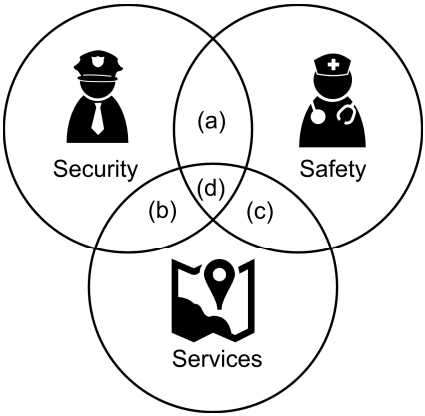


Abbildung 5.1: Schutzziele der intelligenten Videoüberwachung

5.2 Interaktive Überwachung

Der gesteigerten Funktionalität der intelligenten Videoüberwachung können keineswegs nur positive Effekte auf die Akzeptanz zugeordnet werden. Die heftige Kritik am Forschungsprojekt INDECT macht deutlich, dass die hohe Mächtigkeit der Systeme bei den Betroffenen ein Gefühl des Kontrollverlustes und damit einhergehende Ängste auslösen [Stu12]. Eine reine Steigerung der

Mächtigkeit alleine erscheint deshalb nicht sinnvoll. Diese muss in ein entsprechendes Regelwerk eingebunden sein, um eine Balance zwischen Sicherheit und Datenschutz zu erreichen.

Die Arbeiten von Roßnagel, Desoi und Hornung stellen mit der gestuften Kontrolle der Videoüberwachung bereits eine Architektur dar, mit der die Mächtigkeit eines Überwachungssystems an die aktuelle Sicherheitslage angepasst werden kann [RDH11]. Sie stellt nicht nur für den Datenschutz einen wichtigen Ansatzpunkt dar, sondern bildet die Grundlage vieler weitere Arbeiten zur Interaktion, Risikominimierung und Transparenz. Für den direkten Einsatz ist das beschriebene Verfahren aber noch zu abstrakt. Zusammen mit Pascal Birnstill wurde sie deshalb zum Konzept der *interaktiven Überwachung* als generischem Ansatz zur maßgeschneiderten Funktionalität in der intelligenten Videoüberwachung verfeinert [KBB16a; BK14].

Die interaktive Überwachung bindet die Funktionalität eines Überwachungssystems an definierte Zustände, die an die aktuelle Sicherheitslage angepasst sind. Übergänge zwischen den Zuständen erfolgen, wie bei einem endlichen Automaten, durch die Verarbeitung von Ereignissen.

In Abbildung 5.2 ist ein Beispiel mit drei Zuständen und vier Ereignisse dargestellt. Ausgehend vom Startzustand *Bereitschaftsmodus* verarbeitet das System alle eingehenden Ereignisse. Der Übergang zwischen zwei Zuständen kann entweder durch die direkte Interaktion des Operators erfolgen oder durch eine automatische Detektion durch einen Algorithmus. Beruht ein Zustandswechsel auf der automatischen Detektion, kann es rechtlich notwendig sein, diesen Wechsel durch einen Operator bestätigen zu lassen, bevor weitere Schritte eingeleitet werden (mehr dazu in Abschnitt 8.2.2). Die jeweiligen Zustände sind in Anlehnung an die Arbeit von Roßnagel, Desoi und Hornung mit unterschiedlicher Funktionalität verbunden. Im Bereitschaftsmodus erlaubt das System lediglich einen stark anonymisierten Zugriff auf das System.

Wurde eine potentiell kritische Situation erkannt, wechselt das System in den *Beurteilungsmodus* und erlaubt dem Operator Zugriff auf erweiterte Funktionen. Der bestehende Anfangsverdacht rechtfertigt hier Funktionalität mit einem tieferen möglichen Eingriff in die Privatsphäre und gibt dem Operator

somit Zugriff auf Funktionen zur interaktiven Situationsbewertung. Kann das Eintreten des Ereignisses im Beurteilungsmodus nicht bestätigt werden, wird es verworfen und das System wechselt wieder in den Bereitschaftsmodus. Wird das Ereignis hingegen bestätigt, wechselt das System in seinen dritten Zustand *Bearbeitungsmodus*. In diesem liegen Hinweise für eine konkrete Bedrohung vor, die nur durch rechtzeitiges Eingreifen durch das Sicherheitspersonal abgewendet werden können. Das System erlaubt dem Operator hierzu eine Nutzung auch stark in die Privatsphäre der Betroffenen eingreifender Funktionen. Wenn die Bearbeitung erfolgreich abgeschlossen ist, wechselt das System wieder in den Bereitschaftsmodus und bietet maximalen Datenschutz für die Betroffenen.

Die interaktive Überwachung zeichnet sich durch die beiden Prinzipien *Mensch im Mittelpunkt* und die *zweckgebundene Funktionalität* aus. Mensch im Mittelpunkt bedeutet, dass alle Zustandsübergange entweder direkt durch den Operator ausgelöst werden oder bei automatischen Übergängen unter seiner Kontrolle stehen. So kann der Operator jederzeit eine automatische Detektion verwerfen und das System wird niemals eine Zustandsübergang auslösen, der nicht vom Operator überwacht werden kann. Zweckgebundene Funktionalität bedeutet, dass der Operator in jedem Zustand eine geeignete Menge an Operationen nutzen kann. Ohne dass ein begründeter Anfangsverdacht vorliegt, müssen die Betroffenen nicht mit einem Eingriff in ihre Privatsphäre rechnen. Für den Operator ergibt sich der Vorteil, dass die Komplexität des Systems reduziert wird und er immer nur genau die Funktionalität angeboten bekommt, die er benötigt.

Im Allgemeinen kann ein interaktives Überwachungssystem beliebig, aber endlich viele unterschiedliche Ereignisse verarbeiten und auch beliebig, aber endlich viele Zustände haben. Dabei können im gleichen System für unterschiedliche Ereignisse, beispielsweise der Detektion von Gewalt oder der Detektion eines zurückgelassenen Koffers, ganz unterschiedliche Zustände mit unterschiedlichen Funktionen genutzt werden. Zustände müssen dabei nicht zwingend für das gesamte System gelten, sondern können auch nur für solche Bereiche aktiv sein, in denen Ereignisse detektiert wurden. Birnstill und Pretschner zeigen wie sich mittels Usage Control Zustände auch an einzelne

Personen binden lassen [BP13]. Damit wird es möglich, die benötigten Eingriffe in die Privatsphäre noch selektiver zu gestalten. Wird beispielsweise in einem bestimmten Bereich Gewalt erkannt, wechselt das System nicht global in einen anderen Zustand, sondern nur für die Personen, die an der erkannten Gewalthandlung beteiligt waren.

Abbildung 5.2: Grundsatz der interaktiven Überwachung

5.3 Koordination mobiler Sicherheitskräfte

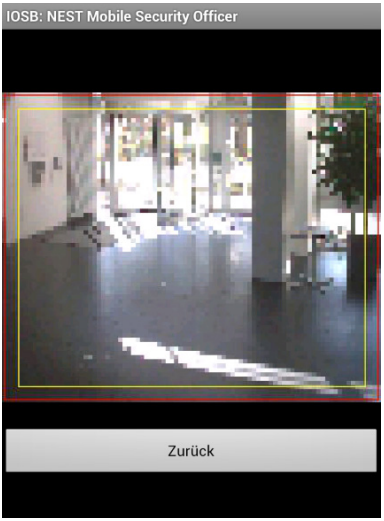
Nicht nur die Erkennung von kritischen Situationen, auch deren Weiterverarbeitung kann so ausgestaltet werden, dass die Nützlichkeit des Systems steigt. Lange Zeit war es technisch bedingt, dass alle Videodaten in einer Zentrale zusammenlaufen und dort von einem Operator ausgewertet werden. Wurde ein kritisches Ereignis erkannt, hat der Operator Einsatzkräfte vor Ort über Funk verständigt.

In der intelligenten Videoüberwachung wird eine gezielte Alarmierung von Mitarbeitern möglich. Dazu werden die mobilen Einsatzkräfte mit Smartphones ausgestattet, die ihre Position in regelmäßigen Abständen an das System übermitteln. Das Videoüberwachungssystem hat zusätzlich Wissen über das

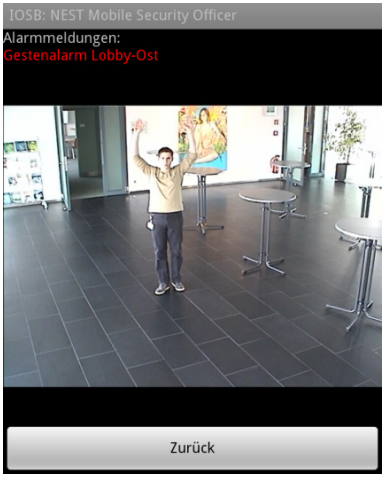
eigene Gelände und kann bestimmen, wo sich mobile Einsatzkräfte befinden. Kommt es zu kritischen Situationen, kann der Operator die Position der Teams in einer Karte einsehen und die mobilen Sicherheitskräfte koordinieren.

In Abbildung 5.3 ist eine weitere Möglichkeit der Interaktion mit mobilen Einsatzkräften gezeigt. Durch eine Software auf ihren Smartphones können mobile Sicherheitskräfte auf Teile des intelligenten Überwachungssystems zugreifen. Sie haben Zugriff auf die Kameras in ihrer Nähe und werden über aktuell im System vorhandene Alarme informiert (vgl. Abbildung 5.3a). Der Zugriff auf Daten kann auch in diesem Fall durch die aktuelle Sicherheitssituation beeinflusst werden. Greift ein Wachmann auf eine Kamera zu, für die aktuell kein Alarm vorliegt, bekommt er nur ein anonymisiertes Videobild (vgl. Abbildung 5.3b), wohingegen der Zugriff auf eine Kamera mit vorliegendem Alarm in voller Auflösung erfolgt (vgl. Abbildung 5.3c). Die entwickelte Anwendung kann weiter dazu genutzt werden, einem mobilen Wachmann zusätzliche Informationen, beispielsweise Bilder von aktuell gesuchten Verdächtigen, zuzuspielen (vgl. Abbildung 5.3d).

(a) Übersicht über Kameras und Alarme



(b) Zugriff auf eine Kamera ohne Alarm



(c) Zugriff auf eine Kamera mit Alarm

(d) Suche nach Verdächtigem

Abbildung 5.3: Interaktion für mobile Einsatzkräfte

5.4 Nutzerdienste

Nutzerdienste bilden eine weitere Möglichkeit, um die empfundene Nützlichkeit eines Videoüberwachungssystems zu steigern. Dabei lassen sich die Ansätze in zwei unterschiedliche Gruppen einteilen.

Systeme die *Safety on Demand* oder *Security on Demand* als Services haben, bieten den Betroffenen optionale Sicherheitsdienste. Die gemeinsame Arbeit mit Vagts untersucht Systeme, die den Nutzern Sicherheit als Dienstleistung anbietet [VKB12]. Neben der bereits erwähnten Gestendetektion, die genutzt werden kann, um Sicherheitspersonal auf wichtige Ereignisse hinzuweisen, können diese Services auch komplexere Sicherheitsaufgaben übernehmen. Die entwickelte Funktion *WatchMe* ermöglicht einem Beobachteten, auf eignen Wunsch, den Grad an Überwachung in einer bestimmten Situation zu steigern. Somit könnte eine Person, die nachts alleine in der U-Bahn unterwegs ist, dass System auffordern, sie besonders aufmerksam zu überwachen. Das entsprechende Überwachungssystem wird dann den Operator benachrichtigen, wenn sich andere Personen in der ansonsten leeren Straßenbahn sehr nahe an die überwachte Person annähern. Zur Umsetzung wurde eine Anwendung für Smartphones und ein entsprechend konfiguriertes intelligentes Überwachungssystem genutzt. Um die gesteigerte Überwachung zu starten, stellt die Person eine entsprechende Aufforderung an das System. Das System reagiert, indem es dem Smartphone eine optische Marke übermittelt, die anschließend auf dem Display des Smartphones angezeigt wird. Sobald der Nutzer diese Marke der nächsten Kamera zur Detektion vorgehalten hat, ist das System aktiv. Die Person wird nun mit erhöhter Priorität überwacht und der Operator wird auf besondere Situationen, beispielsweise Personen, die sich sehr nahe an die überwachte Person annähern, aufmerksam gemacht werden. Auf Wunsch des Beobachteten können solche Dienste jederzeit beendet werden, wodurch wieder auf die normale Schutzstufe reduziert wird.

Die zweite Gruppe der Services wurde ebenfalls in der Arbeit mit Vagts behandelt. Dabei handelt es sich um Dienste, die keinen Safety- oder Security-Hintergrund haben, sondern reine Komfortdienste darstellen. Auch hier wird

der Ansatz genutzt, dass Nutzer dem System erlauben, gezielt mehr Daten über sie zu erfassen. Die so erhobenen Daten können anschließend mit anderen Nutzern geteilt werden.

Ein solcher Nutzerdienst ist der exemplarisch implementierte *BuddyFinder*.

Mit der entwickelten App können zwei oder mehr Personen auf einem weitläufigen Gelände, beispielsweise einem Flughafen, den aktuellen Aufenthaltsort ihrer Freunde einsehen. Die Einwilligung in die Datenerfassung wird wiederum durch das Zeigen von Marken umgesetzt. Das intelligente Überwachungssystem im Hintergrund erfasst die Positionen der angemeldeten Nutzer und teilt sie entsprechend der konfigurierten Einstellungen. Die Nutzer können das System nutzen, um sich ohne aufwändige Absprache auf dem Gelände zu finden.

BuddyFinder und andere Dienste, die reine Services darstellen, veranschaulichen damit die vermutete Entwicklung bei intelligenten Videoüberwachungssystemen. Die Gewährleistung von Sicherheit wird durch das Angebot weiterer Dienste ergänzt. Eine ähnliche Entwicklung ist beispielsweise rund um das Smart Home zu beobachten in dem ehemals passive Umgebungen neue Dienstleistungen für die Bewohner anbieten.

5.5 Fazit: Steigerung der empfundenen Nützlichkeit

Die Steigerung der Nützlichkeit und Sicherheit intelligenter Videoüberwachung ist ein primäres Forschungsthema. Daher ist es wenig überraschend, dass bereits sehr viel Arbeit in die Weiterentwicklung der algorithmischen Bildauswertung und dem Bau gesamter Systeme erfolgt ist. Es ist zu erwarten, dass diese Anstrengungen zur Steigerung der Nützlichkeit beitragen und spätestens mittelfristig einen positiven Effekt auf die Akzeptanz haben werden.

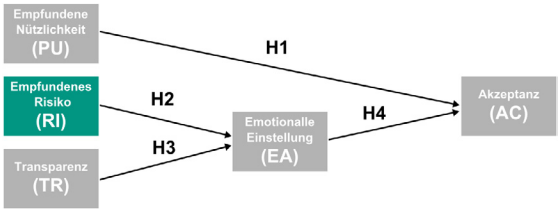
In der vorliegenden Arbeit wurde mit der interaktiven Überwachung ein Konzept vorgestellt, wie die Mächtigkeit einer intelligenten Videoüberwachung an die aktuelle Sicherheitslage gekoppelt werden kann. Der Operator hat damit immer genau die Funktionalität, die er zur Bearbeitung der aktuellen Situation braucht und Eingriffe in die Privatsphäre der Betroffenen wird minimiert. Gleichzeitig trägt die interaktive Überwachung dazu bei, der Angst des Kontroll-

verlustes von Betroffenen entgegenzuwirken. Zur Steigerung der Akzeptanz ist es jedoch wichtig, die vorgestellten Verfahren auch für die Betroffenen transparent zu machen, dies wird in Kapitel 7 behandelt.

Die bereits 2011 entwickelten Ansätze, um mobile Sicherheitskräfte zu koordinieren, sind mittlerweile bereits teilweise auf dem Markt angekommen. Gerade der mobile Zugriff auf Videos durch Smartphones ist weit verbreitet, wird typischerweise jedoch nicht an die Position der Sicherheitskraft oder der aktuellen Sicherheitssituation gekoppelt.

Die vorgestellten Ansätze, um intelligente Videoüberwachungssysteme für Services zu nutzen, ermöglichen den Betroffenen direkt mit dem System zu interagieren. Lediglich die Arbeiten von Winkler und Rinner verflogenen ähnliche Ansätze, um intelligente Videoüberwachung mehr an den Bedürfnissen der Betroffenen auszurichten [WR12].

6 Risikominimierung



TAM-VS1: Wirkung des empfundenen Risikos

Die individuelle Einschätzung, ob von einem Videoüberwachungssystem ein Risiko ausgeht, hat einen starken Einfluss auf die Akzeptanz (intelligenter) Videoüberwachung. Dabei können aus den Ergebnissen von TAM-VS keine Rückschlüsse daraus gezogen werden, ob die Risikoeinschätzung der Befragten realistisch ist.

Betrachtet man die Fragen des Messinstruments (siehe dazu Tabelle B.2 und Tabelle E.2), das für die Erfassung des Konstrukts EMPFUNDENES RISIKO genutzt wurde, wird schnell klar, was die Befragten unter ihrem Risiko verstehen. Es geht um die unerlaubte oder fehlerhafte Verwendung der erfassten Daten, entweder durch den Operator selbst oder einen Angreifer.

Dieses Kapitel wird zuerst betrachten, welche rechtlichen und andere Anforderungen an eine Risikominimierung bisher existieren. Danach werden zwei Ansätze untersucht, um das Missbrauchsrisiko der intelligenten Videoüberwachung zu senken. Zuerst wird das Werkzeug Privacy Score betrachtet, dass einen Betreiber in der *Planungsphase* unterstützt, für sein Sicherheitsproblem ein System mit möglichst geringem Missbrauchspotential zu wählen. Anschließend wird mit den DSFA ein Werkzeug betrachtet, dass im *Betrieb* einer Anlage sicherstellt, dass keine unnötigen Eingriffe in die Privatsphäre durch den Operator entstehen und das System vor Angriffen geschützt ist.

Es kann beobachtet werden, dass die Risikoeinschätzung der einzelnen Personen stark unterschiedlich ist und dass mit einer höheren Risikoeinschätzung eine geringere Akzeptanz einhergeht. Die individuelle Risikoeinschätzung ist das Resultat viele unterschiedlicher Faktoren, unter anderem auch davon, wie über ein bestimmtes Thema kommuniziert wird und wie viele Fälle von Missbrauch bekannt werden. Die American Civil Liberties Union (ACLU) beschreibt fünf Arten des Missbrauchs von Videoüberwachungsanlagen [Ame]:

- **Krimineller Missbrauch:**
  Diese Missbrauchsart subsumiert die nachfolgenden Arten größtenteils und deckt zusätzlich beispielsweise den Missbrauch durch eine einzelne Person ab, welche darauf abzielt, anderen zu schaden, ohne einen persönliche Nutzen daraus zu ziehen.

- **Institutioneller Missbrauch:**
  Neben dem Missbrauch durch einzelne oder wenige Personen ist auch eine illegale Verwendung durch ganze Institutionen möglich. Als Beispiel sei hier der Missbrauch durch Geheimdienste aufgeführt.

- **Missbrauch für persönliche Zwecke:**
  Hinsichtlich des Missbrauchs für persönliche Zwecke führt die ACLU Fälle auf, in denen Polizeibeamte Überwachungsinformationen nutzten, um beispielsweise Frauen nachzustellen, um Autofahrern nach Verkehrsstreitigkeiten zu drohen oder um ehemalige Kollegen zu verfolgen.

- **Diskriminierende Zielauswahl:**
  Bei dem Einsatz von Videoüberwachungsanlagen besteht die Gefahr, dass Minderheiten überproportional häufig fokussiert werden [Nor97], was ebenfalls eine Form von Missbrauch darstellt.

- **Voyeurismus:**
  Ein weiteres Missbrauchspotential von Videoüberwachung besteht darin, dass der Operator das System zu voyeuristischen Zwecken nutzt.

Will man als Betreiber einer Videoüberwachungsanlage verhindern, dass es zu Missbrauch durch das installierte System kommt, sind zwei zeitlich getrennte Phasen entscheidend. Während der *Planungsphase* muss ein System gewählt werden, dass eine bestimmte Aufgabe mit einem minimalen Eingriff in die Privatsphäre erfüllt. Dies ist schwierig, da der Markt an Systemen bereits bei konventioneller Videoüberachtung sehr groß ist und durch die intelligente Videoüberwachung eine Vielzahl neuer Systeme entstehen.

Vor dem *Betrieb*, muss initial eine Bewertung der Datenverarbeitung vorgenommen werden. Diese sollte regelmäßig geprüft und muss unter Umständen bei Änderungen am System wiederholt werden.

6.1 Risikominimierung als Zielvorgabe

Die Ergebnisse von TAM-VS sind ein klares Zeichen dafür, dass die Reduzierung des Missbrauchsrisikos von Videoüberwachungssystemen für die Akzeptanz wichtig ist. Auf gesetzlicher Seite findet sich in Deutschland das BDSG [BDSG] ebenso wie die europäische Datenschutzrichtlinie 95/46/EC [95/46/EC]. Ebenso sollte für Deutschland der Entwurf der europäischen Datenschutzgrundverordnung (DSGVO) beachtet werden [DSGVO].

- **Technische und organisatorische Maßnahmen:**
  Nach §9 BDSG sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und/oder organisatorische Maßnahmen zu treffen, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind.

- **Security of processing:**
  Nach Artikel 17 der europäische Datenschutzrichtlinie 95/46/EC sind Mitgliedstaaten verpflichtet sicherzustellen, dass eine Verarbeitung von personenbezogenen Daten unter Einhaltung von IT-Sicherheit erfolgt.

Ebenso kann im aktuellen Entwurf DSGVO eine Erweiterung der geforderten IT-Sicherheit beobachtet werden. Zusätzlich zur von Artikel 17 geforderten IT-

Sicherheit fordert der neue Gesetzentwurf die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) und dass die Systeme nach Privacy by Design entworfen wurden.

Neben den vorgestellten gesetzlichen Anforderungen existieren noch eine Reihe freiwilliger Verhaltensprinzipien, die für die intelligente Videoüberwachung relevant sind. So fordern beispielsweise die Fair Information Practice Principles (FIP) für jede Form der automatischen Datenverarbeitung, Integrität der Daten und Sicherheit der verarbeitenden Systeme.

Im Folgenden werden zwei entwickelte Ansätze beschrieben, um das Risiko des Datenmissbrauchs bei der intelligenten Videoüberwachung zu reduzieren. Privacy Score ist dabei für die Planungsphase entworfen und das entwickelte Verfahren für eine DSFA ist für den Betrieb der Anlage gedacht.

6.2 Privacy Score

Als Betreiber einer Videoüberwachungsanlage ist man für dessen Datensicherheit und Datenschutz verantwortlich. Gerade die große Menge an verfügbaren Systemen mit deutlichen Unterschieden in Datenschutz macht diese Aufgaben für Nichtexperten im Datenschutz schwer. Das folgende Szenario verdeutlicht die Schwierigkeit:

Ein Sicherheitsexperte ist für die Sicherheit auf einem öffentlichen Gelände verantwortlich. Anhaltende Sicherheitsvorfälle bringen ihn zu der Entscheidung, ein Sicherheitssystem installieren zu wollen. Hier treffen viele Anforderungen aufeinander. Das System muss in der Lage sein, das vorliegende Sicherheitsproblem zu lösen, es darf den Budgetrahmen nicht überschreiten, sollte einfach zu bedienen sein und soll den Eingriff in die Privatsphäre der Betroffenen auf ein Minimum reduzieren.
Während Kosten relativ einfach zu vergleichen sind, existierte bisher keine einfache Möglichkeit, um zwischen Systemen mit unterschiedlichen Datenschutzeigenschaften zu wählen. Um für solche Fälle eine Entscheidungshilfe anzubieten wurde Privacy Score entworfen [KB15]. Es wurde für einen schnellen Vergleich von *Systemen*, auch über Technologiegrenzen hinweg, entworfen. Es

ist durchaus möglich, dass nicht nur Videoüberwachungssysteme verschiedener Hersteller für eine geforderte Sicherheitsaufgabe nutzbar sind, sondern neben der Videoüberwachung auch andere Sicherheitstechnologien, beispielsweise Metalldetektoren, geeignet sind.

Privacy Score soll keinesfalls ein Ersatz für eine DSFA, die später in diesem Kapitel betrachtet wird, verstanden werden. Vielmehr ist es ein ergänzendes Werkzeug für einen anderen Anwenderkreis. Während für eine DSFA ein Team von Experten die Bewertung vornimmt und dafür typischerweise mehrere Wochen braucht, kann eine Bewertung nach Privacy Score vom Betreiber selbst durchgeführt werden und dauert pro System nur ca. eine Stunde. Ein typisches Vorgehen ist es deshalb, mit Privacy Score die Menge der vorliegenden Systeme zu vergleichen und mit einer abschließenden DSFA dieses System zu untersuchen.

Privacy Score bietet dazu eine nummerische ausgeprägte Bewertung von Systemen zwischen 0 und 21 Punkten. Dabei ist zu beachten, dass die Bewertung nur ordinal ausgeprägt ist. Das bedeutet insbesondere, dass Vergleiche zwischen Systemen in ihrer Aussage eingeschränkt sind. Hat beispielsweise System A 5 Punkte und System B 10 Punkte, so ist System B nach Datenschutzgesichtspunkten vorzuziehen, es ist jedoch keineswegs doppelt so gut.

6.2.1 Vorbereitung

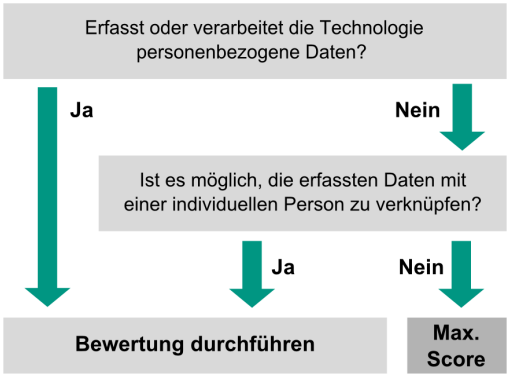


Abbildung 6.1: Vorprüfung zu Privacy Score

Vor der eigentlichen Bewertung mit Privacy Score müssen einige Grundlagen geschaffen werden. Der Auditor sollte ein grundlegendes Verständnis über die zu bewertenden Systeme und genaue Informationen über das Szenario haben. Er muss wissen, welche Sensoren Daten erfassen, wie diese verarbeitet werden und wie das System benutzt wird. Im Gegensatz zu einer DSFA muss er jedoch kein Verständnis über die internen Vorgänge des Systems haben. Am Ende der Vorbereitungen wird eine initiale Prüfung vorgenommen, ob eine Analyse mit Privacy Score notwendig ist (vgl. Abbildung 6.1).

Wenn ein System personenbezogene Daten erfasst oder verarbeitet, ist eine vollständige Prüfung immer notwendig. Ist dies nicht der Fall, beispielsweise bei einen Gas-Chromatographen zur Drogenfahndung, ist die zweite Frage, ob Daten erfasst oder verarbeitet werden, die einer Person zugeordnet werden können. Dies ist beispielsweise der Fall für eine GPS-Wanze. Die Wanze an sich speichert oder übermittelt nur in regelmäßigen Abständen den eigenen Ort. Kann diese Information aber mit einer Person verknüpft werden, beispielsweise weil die Wanze am Wagen eines verdächtigen installiert wurde, muss eine vollständige Prüfung vorgenommen werden.

6.2.2 Prüfung

Um die eigentliche Prüfung vorzunehmen, muss ein Auditor neun Fragen über die Technologie und die Datenverarbeitung beantworten. Die Antworten sind entweder ja/nein oder er kann zwischen einer Menge vordefinierter Antwortmöglichkeiten wählen. Neben den Punkten, die durch die vom Auditor gewählten Antworten entstehen, hat jede Frage eine spezifische Gewichtung. Dieses ist vorgegeben und repräsentiert wie wichtig die abgefragte Eigenschaft für den Datenschutz ist. Da beispielsweise die Selektivität der Datenerfassung für den Datenschutz eine höhere Rolle spielt, als ob ein Sensor Daten verschlüsselt abspeichert, hat sie ein höheres Gewicht.

Die Fragen sind in die Blöcke *Datenerfassung*, *Datenzugang und -nutzung* sowie *technischer Datenschutz* unterteilt.

Datenerfassung Tabelle 6.1 zeigt die Fragen von Privacy Score, die sich mit der Erfassung von Daten beschäftigen. Für die Datenerfassung ist gerade die Selektivität der Datenerfassung wichtig. Im Idealfall sind nur die Personen von der Überwachung betroffen, die für die Erfüllung der konkreten Sicherheitsaufgabe notwendig sind. Dies ist der Fall für eine gezielte Überwachung von Telefonortsdaten. Lediglich die Position von Verdächtigen wird erfasst, während alle anderen Personen, selbst in nächster Umgebung, davon nicht betroffen sind. Im Gegensatz zur Selektivität beschäftigt sich die Frage der Datenminimierung damit, welche Daten von Betroffenen erfasst werden. Die letzte Frage im Block Datenerfassung deckt ab, ob die Datenerfassung heimlich oder öffentlich stattfindet. Während es in Fällen wie der Videoüberwachung für die Überwachungsaufgabe von Vorteil ist, sichtbar zu sein, kann eine Telefonüberwachung nur heimlich eingesetzt werden, wenn sie sinnvolle Ergebnisse bringen soll.

Nr.	Frage	Skala	Gewicht
C1	Erfolgt die Erfassung selektiv?	0 = nein, alle Anwesenden sind betroffen 1 = teilweise selektiv 2 = Nur Subjekt(e) werden erfasst	3
C2	Ist die Menge der erfassten Daten minimal?	0 = nein 1 = ja, nur benötige Daten werden erfasst	1
C3	Erfolgt die Erfassung heimlich oder offen?	0 = heimlich 1 = offen	1

Tabelle 6.1: Privacy Score: Fragen zur Datenerfassung

Datenzugang und -nutzung Die Fragen in Tabelle 6.2 untersuchen, wie die erfassten Daten genutzt werden. Wichtig ist die Frage, wie der Zugriff auf die erfassten Daten geregelt ist. Ist der Zugriff auf eine vernünftige Gruppe von Personen begrenzt oder sind die Daten frei zugänglich? Besonders die Idee, Videodaten frei zugänglich zu machen und Privatpersonen einen kleinen Bonus für gemeldete Straftaten zu bezahlen [Sch13], hat verheerende Auswirkungen für die Privatsphäre. Auch wenn der Zugriff auf bestimmte Personen beschränkt ist, bleibt die Frage, wie die Nutzung der Daten geregelt ist. Im besten Fall existieren klare Richtlinien, wie die erfassten Daten verwendet werden dürfen, die auch technisch erzwungen werden. In einer weniger strikten Version existieren diese Richtlinien, werden aber lediglich durch Verfahrensanweisungen durchgesetzt. Ein Schutz vor *Function Creep*, also die schleichende Ausweitung der Zweckbestimmung, stellt im Bereich von Datenzugang und -nutzung den effektivsten Schutz der Privatsphäre dar, ist jedoch auch nur schwer zu erreichen. So lassen sich Ansätze wie die interaktive Überwachung (vgl. Abschnitt 5.2) nur

schwer nachträglich in ein System integrieren, sondern müssen von Anfang an im Design berücksichtigt werden.

Nr.	Frage	Skala	Gewicht
A1	Wer hat Zugriff auf die Daten?	0 = freier Zugriff auf Daten 1 = Zugriff ist auf legitime Teilnehmer begrenzt	2
A2	Existieren klare Anweisungen, wer Zugriff auf die Daten hat?	0 = nein 1 = Organisatorische Regeln sind vorhanden 2 = Regeln werden technisch erzwungen	1
A3	Existiert ein Schutz gegen Function Creep?	0 = nein 1 = ja	3

Tabelle 6.2: Privacy Score: Fragen zu Datenzugang und -nutzung

Datenschutz Tabelle 6.3 deckt den Bereich des technischen Datenschutzes ab. Im technischen Datenschutz ist es wichtig zu prüfen, ob die erfassten Daten verschlüsselt oder auf andere Weise vor unberechtigtem Zugriff geschützt sind. Weiter wird bewertet, ob Maßnahmen vorhanden sind, um die Daten vor Manipulation zu schützen. Dieser Schutz sollte sowohl gegen interne Angreifer, also bösartige Mitarbeiter, als auch externe Angreifer, also gezielte Angriffe durch Hacker, ausgestaltet sein. Für mobile Sensoren, beispielsweise versteckte Kameras, die Daten auf einem internen Speicher ablegen, ist eine weitere Prüfung wichtig. Die erfassten Daten müssen gegen einen Angreifer geschützt sein, der Sensoren stiehlt und so versucht Zugang zu den erfassten Informationen zu erhalten.

Nr.	Frage	Skala	Gewicht
P1	Sind die erfassten Daten verschlüsselt oder anders zugriffsgeschützt?	0 = nein, kein Zugriffsschutz 1 = ja, Verschlüsselung oder andere Maßnahme vorhanden	1
P2	Sind die Daten vor Manipulation geschützt?	0 = nein; 1 = Schutz gegen externe Manipulation 2 = Schutz gegen externe und interne Manipulation	2
P3	Ist der Sensor vor Datendiebstahl geschützt?	0 = nein; 1 = ja oder nicht zutreffend	1

Tabelle 6.3: Privacy Score: Fragen zum technischen Datenschutz

6.2.3 Beispiel: Bewertung eines konventionellen Videoüberwachungssystem

Tabelle 6.4 zeigt die beispielhafte Bewertung eines Videoüberwachungssystems für die Überwachung eines öffentlichen Platzes. Die Bewertung ist Teil der Arbeit des bereits erwähnten Sicherheitsverantwortlichen, der Systeme unterschiedlicher Hersteller in ihren Datenschutzeigenschaften vergleichen will. Er bewertet alle ihm angebotenen Systeme und nutzt die Ergebnisse für seine Entscheidung.

Das beispielhaft untersuchte System weißt, wie für konventionelle Videoüberwachungssysteme üblich, einen gewissen Grad der Selektivität auf. Von der Überwachung sind nicht alle Bürger betroffen, aber sobald man sich auf dem videoüberwachten Platz befindet, ist man betroffen. Die erfassten Daten sind nicht minimal, es findest keine Anonymisierung der Bilder statt. Da es sich um eine Videoüberwachung an einem öffentlichen Platz handelt, hat die

Erfassung der Daten sichtbar zu erfolgen. Der Zugang zu den erfassten Daten ist limitiert auf die Mitarbeiter der Sicherheitsfirma, ein freier Zugang zu den Daten ist nicht vorgesehen. Richtlinien, wann die erfassten Daten verwendet werden dürfen, existieren, werden aber nicht technisch, sondern nur durch Verhaltensanweisungen durchgesetzt. Wie für konventionelle Videoüberwachungssysteme typisch existiert in dem hier bewerteten System kein Schutz vor Function Creep. Es ist nicht zu verhindern, dass ein entsprechend motivierter Operator das System außerhalb des gedachten Überwachungszwecks nutzt.

Die bis hier betrachteten Punkte, Datensammlung, Datenzugriff und -nutzung, wären bei einer vergleichenden Bewertung konventioneller Videoüberwachungssysteme verschiedener Hersteller, vermutlich für alle Systeme identisch. Die Bewertung ist neben der Technologie besonders auch vom Einsatzszenario und der Organisation der Sicherheitskräfte abhängig. Unterschiedliche Bewertungen im gleichen Szenario sind zu erwarten, wenn unterschiedliche Technologien, beispielsweise konventionelle und intelligente Videoüberwachung, verglichen werden. Hier unterscheidet sich der Punkt Datensicherheit deutlich von den beiden vorherigen.

Das beispielhaft bewertete System nutzt entsprechende Verfahren, um die erfassten Daten bei der Übertragung von der Kamera zur Infrastruktur zu verschlüsseln. Die Datenspeicherung erfolgt ebenfalls verschlüsselt. Durch die geeignete Verschlüsselung sind die Daten im Speicher vor externer Manipulation geschützt, Schutz vor Manipulation durch interne Angreifer besteht jedoch nicht. Da die Kameras erfasste Daten sofort an die Infrastruktur schicken und nicht auf der Kamera selbst speichern, bekommt das System hier den Punkt automatisch.

Um nach der Bewertung den eigentlichen Privacy Score eines Systems zu erhalten, müssen lediglich die Punkte in den neun Fragen mit den entsprechenden Gewichten multipliziert und aufaddiert werden. Das beispielhafte System erhält somit einen Privacy Score von **11 Punkten**.

Nr.	Frage	Punkte	Gewicht	Ergebnis
Datenerfassung				
C1	Erfolgt die Erfassung selektiv?	1	3	3
C2	Ist die Menge der erfassten Daten minimal?	0	1	0
C3	Erfolgt die Erfassung heimlich oder offen?	1	1	1
Datenzugang und -nutzung				
A1	Wer hat Zugriff auf die Daten?	1	2	2
A2	Existieren klaren Anweisungen, wer Zugriff auf die Daten hat?	1	1	1
A3	Existiert ein Schutz gegen Function Creep?	0	3	0
Technischer Datenschutz				
P1	Sind die erfassten Daten verschlüsselt oder anders Zugriffsgeschütz?	1	1	1
P2	Sind die Daten vor Manipulation geschützt?	1	2	2
P3	Ist der Sensor vor Datendiebstahl geschützt?	1	1	1
Summe				11

Tabelle 6.4: Privacy Score: Bewertung einer Videoüberwachung im öffentlichen Raum

6.2.4 Zusammengefasste Ergebnisse

Tabelle 6.5 zeigt das Ergebnis einer breiten Studie über Überwachungstechnologie mit Privacy Score. Diese Bewertung entstand innerhalb des EU-Projektes SURVEILLE [SUR]. Ziel von SURVEILLE war es, verschiedene Überwachungssysteme vergleichbar zu machen, in dem die sozialen, ethischen, rechtlichen und finanziellen Kosten mit dem Nutzen der Technologie verglichen wurden. Deliverable 3.3b System Effectiveness and Efficiency-Data Protection [KG13] geht tiefer in die Bewertung ein. Hier soll nur ein Überblick gegeben werden.

Privacy Score zeigt seine Stärke darin, dass sehr viele und unterschiedliche Überwachungstechnologien damit verglichen werden können. Besonders die Möglichkeit Systeme auch über Technologiegrenzen hinweg zu vergleichen, ist für einen breiten Überblick entscheidend. Leider war es in Rahmen von SURVEILLE nicht möglich, alle vom Konsortium gewählten Technologien vollständig zu analysieren. Beispielsweise war es nicht möglich zu bewerten, ob und wie Daten auf einen Abhörgerät der Polizei, vor Zugriff und Veränderung geschützt sind, da dem Konsortium der Zugang verweigert wurde. Somit konnte für diese Technologien kein Privacy Score ermittelt werden. In diesen Fällen wurden die Privacy Score-Intervalle zwischen dem besten und schlechtesten möglichen Ergebnis angegeben. Für den eigentlichen Anwendungszweck von Privacy Score, nämlich einen Betreiber bei der Wahl zwischen unterschiedlichen ihm angebotenen Systemen zu unterstützen, sollte es kein Problem darstellen, alle benötigten Informationen von den Anbietern zu erfahren.

Tabelle 6.5 zeigt einige interessante Ergebnisse. Die Technologie mit dem schlechtesten Wert ist das Automatic Identification System (AIS) das eingesetzt wird, um Schiffe zu lokalisieren. Alle Positionsdaten der Schiffe sind öffentlich einsehbar [AIS] und das genutzte Protokoll bietet keinerlei Schutz vor Missbrauch oder Manipulation der Daten. Dies ist insofern nicht verwunderlich, als AIS für die Kollisionsvermeidung in der beruflichen Schifffahrt entworfen wurde und selbst keinerlei persönliche Daten beinhaltet. Gleichzeitig verdeutlicht es sehr schön das Risiko für den Datenschutz, wenn es möglich ist Daten mit einer individuellen Person zu verknüpfen (vgl. Abbildung 6.1). Ist bekannt,

wer sich auf einem bestimmten Schiff aufhält, kann seine Bewegung präzise nachvollzogen werden.

Ein weiteres interessantes Ergebnis ist der Privacy Score des gewählten Security Scanners, in deutschen Medien auch oft als „Nacktscanner“ bezeichnet. Das gewählte Modell konnte mit einem Privacy Score von 18 Punkten ein sehr gutes Ergebnis erreichen. Das ist insbesondere nach der schlechten öffentlichen Reaktion auf die Technologie etwas verwunderlich. Auch wenn die Untersuchung, warum die Akzeptanz der Security Scanner so schlecht ist, weit über diese Arbeit hinausgeht, bietet TAM-VS erste Anhaltspunkte. Es sollen deshalb ein paar Vermutungen dazu angestellt werden, warum die Akzeptanz so schlecht ist und wie sie zu verbessern wäre.

Eine erste Erklärung der Ergebnisse ist zumindest darin zu sehen, dass viele der im bewerteten System vorhandenen Techniken zum Schutz der Privatsphäre erst nach der schlechten öffentlichen Reaktion integriert wurden. Die Systeme bieten also heute weit mehr Datenschutz, als in der öffentlichen Diskussion angenommen wird. Man kann den Herstellern zumindest eine Teilschuld geben, da Datenschutz nicht proaktiv implementiert wurde, sondern erst auf starken öffentlichen Druck nachgebessert wurde. Diese Erklärung deckt aber nur Teile des Problems ab. Schon der in den Medien genutzte Name „Nacktscanner“ zeigt, wie emotional das Thema diskutiert wurde. Hier ist bestimmt eine Teilschuld in der Berichterstattung der Medien zu sehen, die nicht darin unterschieden haben, welche Bilder die Technologie machen könnte und welche Daten wirklich genutzt werden. Auch wenn ein modernes System lediglich eine abstrakte Silhouette eines Menschen und darauf erkannte Gegenstände zeigt, bleibt eine gefühlte Verletzung der Intimsphäre in der Öffentlichkeit. Hier werden die Hersteller und Nutzer viel Öffentlichkeitsarbeit investieren müssen, um Vertrauen herzustellen. Grundsätzlich kann festgestellt werden, dass durch eine begleitende DSFA proaktiv auf die Datenschutz- und Akzeptanzprobleme reagiert hätte werden können. Diese werden im nächsten Kapitel betrachtet.

Ein letzter Punkt betrifft die empfundene Nützlichkeit der Systeme. Bei Kontrollen durch staatliche und private Stellen werden immer wieder Mängel, sowohl bei der klassischen Sicherheitsüberprüfung mit Metalldetektoren

als auch bei Security Scannern gefunden. In der öffentlichen Wahrnehmung werden aber ganz besonders die Mängel der Security Scanner diskutiert. Ein wissenschaftlicher Vergleich der Effizienz der beiden Systeme könnte hier ein erster Schritt sein, um die Vor- und Nachteile der beiden Systeme deutlich zu kommunizieren.

Technologie	SC_1	SC_2	SC_3	SA_1	SA_2	SA_3	SP_1	SP_2	SP_3	Summe
Videoüberwachungssystem auf einem öffentlichen Platz	3	0	1	2	1	0	1	2	1	11
NEST-System mit Personentracking	6	1	1	2	1	3	1	2	1	18
NurseEye	6	1	1	2	2	3	1	2	1	19
Verdeckte Observation	6	1	0	2	1	3	0	4	0	17
Abhörgerät im Haus eines Verdächtigen	3	0	0	2	1	0	1	[0, 4]	1	[8, 12]
Abhörgerät im Fahrzeug eines Verdächtigen	3	0	0	2	1	0	1	[0, 4]	1	[8, 12]
Abhören von Mobiltelefonen	6	0	0	2	1	0	1	[0, 4]	1	[8, 12]
Minidrohne mit Kamera	6	1	0	2	1	3	0	4	0	17
Positionsbestimmung von Mobiltelefonen	6	1	0	2	1	0	1	2	1	14
AIS Schiffspositionsbestimmung	0	1	1	0	0	0	0	0	0	2
Sprengstoffdetektor am Hafen	-	-	-	-	-	-	-	-	-	21
Gaschromatographie zur Drogenerkennung	-	-	-	-	-	-	-	-	-	21
Röntgen von Fluggepäck	-	-	-	-	-	-	-	-	-	21
Security Scanner (Bodyscanner)	3	1	1	2	2	3	1	4	1	18

Tabelle 6.5: Privacy Score: Bewertung verschiedener Überwachungstechnologien

6.3 Datenschutz-Folgeabschätzung

Mit Privacy Score wurde ein Werkzeug geschaffen, um verschiedene Systeme rein ordinal auf ihre Datenschutzeigenschaften hin zu vergleichen. Es bietet jedoch keine tiefere Analyse der Datenverarbeitung.

Durch die zunehmende Bedeutung von Datenschutz hat sich international der Wunsch nach methodischen Verfahren zur Datenschutzbewertung etabliert. Im anglo-amerikanisch-kanadischen Sprachraum haben sich dafür die Begriffe Privacy Impact Assessment (PIA) oder Privacy Risk Assessment durchgesetzt. Die französische Datenschutzbehörde spricht hingegen vom Privacy Risk Management. Da es keine Abgrenzung zwischen den Verfahren gibt, wird in dieser Arbeit der im Deutschen geläufige Begriff Datenschutz-Folgenabschätzung (DSFA) verwendet. Eine DSFA beschreibt eine methodische Überprüfung, ob der Einsatz einer Technologie dem geltenden Datenschutz entspricht und zu Eingriffen in die Privatsphäre führen kann.

6.3.1 Begrifflichkeiten, Methodik und Rahmenwerke

Methodisch kann eine DSFA mit dem Risikomanagement nach dem Verfahren IT-Grundschutz (Bundesamt für die Sicherheit in der Informationstechnik (BSI)) oder International Organization for Standardization (ISO) 27005 verglichen werden. Deshalb ist es kaum überraschend, dass größtenteils ähnliche Begriffe genutzt werden. Gegenstand der Untersuchung ist ein *Projekt*, also ein technisches System zur Datenverarbeitung mit seinen definierten Schnittstellen. *Ereignisse* führen zu negativen Konsequenzen oder Schäden im Projekt. Das *Risiko* ist eine, einem Ereignis zugeordnete Kennzahl, die sich aus der *Eintrittswahrscheinlichkeit* und der *Höhe* der zu erwarteten Schäden zusammensetzt. *Stakeholder* sind alle Gruppen oder Personen, die direkt oder indirekt durch das Projekt betroffen sind. Im Gegensatz zum Risikomanagement ist bei einer DSFA der besondere Fokus beim Datenschutz. Es wird sowohl überprüft, welche Datenschutzgesetze bei der Umsetzung beachtet werden müssen und welche Risiken für die Privatsphäre der Betroffenen existieren.

Zum 12.05.2009 veröffentlichte die Europäische Kommission eine Empfehlung, dass für RFID-basierte Technologien eine PIA durchgeführt werden sollte. Im aktuellen Entwurf der DSGVO wird die Erstellung einer PIA für alle Technologien empfohlen, die personenbezogene Daten verarbeiten. Diese konkrete Erwähnung in Gesetzen und Empfehlungen verleitet zum Eindruck, dass es sich bei einer DSFA um ein einsatzbereites festes Verfahren handeln würde. Dies ist jedoch nicht der Fall. Ähnlich wie beim Risikomanagement gibt es auch bei den DSFA viele verschiedene *Rahmenwerke*. Ein Rahmenwerk stellt die konkrete Durchführung einer DSFA dar.

6.3.2 Ziele der DSFA

DSFA umfasst methodische Maßnahmen, um Datenschutzprobleme in Projekten frühzeitig zu erkennen und behandeln. Werden sie begleitend während der Entwicklung genutzt, können sie dabei helfen, Schutzmaßnahmen zu treffen, bevor erheblicher Schaden entstanden ist, der nur durch hohe Aufwände zu beheben ist. Im Gegensatz zum Risikomanagement betrachtet eine DSFA ein Projekt auch deutlich umfassender und versucht alle relevanten Stakeholder in den Prozess einzubinden. Hier ist es das Ziel, alle Interessen der Betroffenen in das Endsystem einfließen zu lassen. Eine DSFA, bzw. die entstehenden Berichte, sind weiterhin der Öffentlichkeit zugänglich und schaffen damit Transparenz und Vertrauen in das System. Das EU-Projekt PIAF liefert weitere Gründe, die für die Durchführung einer DSFA sprechen:

Erfüllung von gesetzlichen Anforderungen Für einige Technologien, beispielsweise RFID-basierte Systeme, ist die Durchführung einer DSFA in europäischen Raum verpflichtend. Weiter dient sie zur Identifizierung von gesetzlichen Anforderungen, um Strafen und Sanktionen zu vermeiden. Hier müssen nicht nur Datenschutzaspekte, sondern ebenfalls bereichsspezifische Regelungen betrachtet werden.

Identifizierung und Behandlung von Risiken Die Ergebnisse einer DSFA fließen direkt in das Risikomanagment mit ein. Diese hilft Risiken für das Unternehmen, Betroffene und das Projekt zu identifizieren, zu bewerten und zu behandeln. Gleichzeitig schafft sie Aufmerksamkeit bei den Mitarbeitern bezüglich der Sicherheits- und Datenschutzaspekten.

Kostenreduktion Werden Risiken frühzeitig in einem Projekt erkannt und behandelt, lassen sie sich meist viel einfacher und günstiger beseitigen als zu einem späteren Zeitpunkt. Werden Risiken erst dadurch erkannt, dass Schaden eintritt, können Folgekosten für Firmen existenzbedrohend sein. Weiterhin kann bereits zu Beginn eines Projekts erkannt werden, wenn die Kosten für die Behandlung erkannter Risiken den Nutzen des Projektes übersteigt und damit für ein Unternehmen unattraktiv machen.

Entwicklung von effektiven und effizienten Lösungen Nachträglich integrierte Lösungen bieten meist weniger Schutz und sind weniger effizient, als Mechanismen, die bereits im Design beachtet wurden.

Vermeidung von Reputations- und Vertrauensverlust Wird öffentlich über Schadensereignisse berichtet, kann dies mit einem hohen Imageverlust für die betroffenen Firmen verbunden sein. Wenn Technologien oder Firmen einmal mit einem schlechten Image belegt sind, kann es sehr lange dauern, bis das Vertrauen der Kunden wieder aufgebaut werden kann.

Verbesserung der Kommunikationsstrategie Der Einfluss der verschiedenen Stakeholder auf den Erfolg von Projekten wird immer noch häufig unterschätzt. Eine DSFA stellt sicher, dass die Bedürfnisse aller Stakeholder erkannt wurden und hoffentlich in das Systemdesign mit einfließen.

Sensibilisierung und Transparenz für Betroffene Nicht nur die Unternehmen, sondern auch die Betroffenen profitieren von der Auseinandersetzung

mit dem Thema DSFA. Betroffene werden implizit darüber aufgeklärt, wie ihre persönlichen Daten weiterverarbeitet werden, welche Schutzmechanismen existieren und welche Gefahren bei der Nutzung der Technologie akzeptiert werden müssen. Gerade der letzte Punkt gewinnt zunehmend an Bedeutung. Da negative Folgen für die Privatsphäre nicht immer ausgeschlossen werden können, müssen Betroffene darüber aufgeklärt werden, welche Folgen mit der Technologie verbunden sind.

Sicherheit Die Identifizierung und Behandlung von Risiken für den Datenschutz verbessert fast automatisch die IT-Sicherheit eines Systems.

Einbindung in den Entwicklungsprozess Gerade bei Überwachungssystemen besteht eine sehr strikte Trennung zwischen Nutzern und Betroffenen. Eine DSFA stellt sicher, dass ihre Bedürfnisse stärker in die Entwicklung des Systems einbezogen werden.

6.3.3 Durchführung einer DSFA

Sollte für die eigene Technologie bereits ein Rahmenwerk vorgeben sein, wie dies für RFID-basierte Systeme mit dem BSI-Rahmenwerk der Fall ist, wird dieses genutzt [Bun11]. Dies ist jedoch für die intelligente Videoüberwachung nicht der Fall. Die Arbeit von Koch und Krempel untersucht deshalb viele der vorhandenen Rahmenwerke und prüft ihre Einsatzfähigkeit für die intelligente Videoüberwachung [Koc13]. Leider hat sich gezeigt, dass keines der untersuchten Rahmenwerke gut geeignet ist, um ein intelligentes Videoüberwachungssystem zu bewerten. Sie sind entweder für andere Technologien entworfen oder sehr allgemein gehalten, womit der Einsetzende zu wenig Unterstützung bei der Erkennung und Behandlung von Risiken bekommt. Deshalb wird eine Kombination der vorhandenen Rahmenwerke vorgeschlagen und erkannte Lücken geschlossen. Die Struktur folgt dabei dem Verfahren des Bundesstaats Victoria in Australien [Off05]. Dieses für Behörden verpflichtende Verfahren ist sehr gut strukturiert und kann auch von Unternehmen genutzt werden. Es

wurde gewählt, da es neben dem Datenschutzrecht auch auf die körperliche Privatsphäre und den Schutz der Kommunikation der Betroffenen eingeht.

Abbildung 6.2 gliedert die einzelnen Phasen des neu kombinierten Verfahrens. Die Abbildung zeigt schon deutlich, dass eine DSFA, ganz ähnlich wie die meisten Werkzeuge der IT-Sicherheit, einen Prozess beschreiben. Nach der initialen Bewertung einer Technologie sollte eine DSFA periodisch und nach allen größeren Änderungen neu durchgeführt werden.

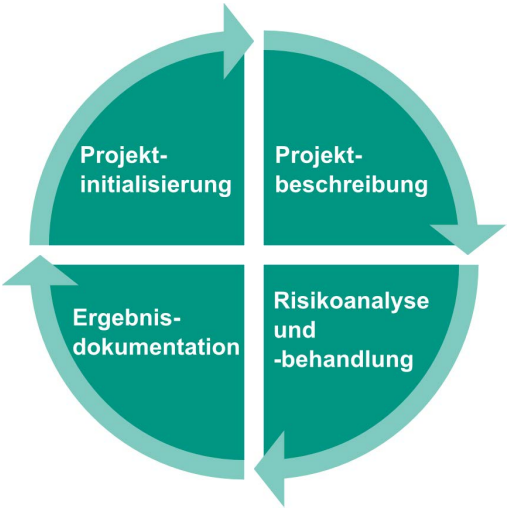


Abbildung 6.2: Übersicht über die Schritte einer DSFA

Projektinitialisierung In der Projektinitialisierung werden verantwortliche Personen für die Durchführung festgelegt sowie der Zeit- und Budgetrahmen der Prüfung definiert. Um gute Ergebnisse zu erzielen, ist darauf zu achten, dass sowohl technische als auch rechtliche Experten Teil des Bewertungsteams sind. Weiterhin werden die relevanten Stakeholder identifiziert. Ein initialer Fragebogen (vgl. Anhang C) klärt weiter, ob für das betrachtete Projekt die Durchführung einer DSFA notwendig ist. Dies ist der Fall, wenn mindestens eine der Fragen mit „Ja“ beantwortet wird.

Projektbeschreibung Die Beschreibung des Projektes ist ein wesentlicher Teil einer DSFA, da Risiken nur für bekannte Funktionen, Prozesse und Daten ermittelt werden können. Die Projektbeschreibung ist der Ausgangspunkt, um Schnittstellen und Abhängigkeiten zu anderen Projekten zu identifizieren. Idealerweise werden die Bedürfnisse der Stakeholder durch die Befragung einer repräsentativen Gruppe erhoben. Neben der Technologie ist weiterhin das genaue Einsatzszenario zu spezifizieren. Am Ende dieser Phase sollte das Team folgende Fragen beantworten können:

- Welche primären Assests (Software, Hardware, Netzwerke, Geschäftsprozesse, Daten, etc.) werden genutzt und von welchen anderen Assets sind diese abhängig?
- Welche Datenflüsse liegen im System vor?
- An welchen Verarbeitungsvorgängen sind die primären Assets beteiligt und welche Arten personenbezogener Daten werden verarbeitet?
- Wer wird von den Verarbeitungsvorgängen beeinflusst und wer sind die Verantwortlichen?
- Welche Vorteile haben die Betroffenen von der Verarbeitung?
- Welche rechtlichen Regelungen müssen beachtet werden?
- Welche spezifischen Regelungen (z.B. Betriebsvereinbarungen) müssen beachtet werden?
- Welche Risikoquellen kommen in Betracht?

Risikoanalyse und -behandlung Ist das Projekt umfassend beschrieben, werden mögliche Risiken für das Projekt und die Privatsphäre der Betroffenen analysiert. Hier erhält das DSFA-Team, je nach gewähltem DSFA-Rahmenwerk, Unterstützung durch umfassende Gefährdungskataloge. Beispielsweise erhält das RFID-Rahmenprogramm desBSI umfassende Gefährdungen für eben diese

Applikationen [Bun11]. Wichtige Punkte in dieser Phase sind es, alle möglicherweise vorhandenen Risiken zu sammeln und zu dokumentieren.

Anschließend werden Risiken in ihrer Schwere und der Eintrittswahrscheinlichkeit eingestuft. Dazu wird das Schema der französischen Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) genutzt. Der Schweregrad eines Risikos wird in zwei Dimensionen, die in Tabelle 6.6 dargestellt sind, bewertet. Zuerst wird geschätzt, wie einfach eine Person identifiziert werden kann und danach wie drastisch die Auswirkungen sind. Die Klasse des Schweregrads ist dann die Summe der beiden Elemente und wird den Stufen: <5 *geringfügig*, =5 *begrenzt*, =6 *erheblich* und >6 *maximal* zugeteilt.

Nach der Bewertung des Schweregrads wird die Eintrittswahrscheinlichkeit bewertet. Dies erfolgt analog zum Schweregrad nach Tabelle 6.7. Zuerst wird das Schadenspotential und danach die Ressourcen der Schadenquelle bewertet. Handelt es sich bei der Schadensquelle nicht um einen menschlichen Angreifer, sondern und ein Zufallsereignis, wird anstelle der Ressourcen der Quelle die Eintrittswahrscheinlichkeit des Zufallsereignisses bewertet. Die Eintrittswahrscheinlichkeit des Risikos ist danach wieder die Summe der beiden Elemente und wird den Stufen: <5 *geringfügig*, =5 *begrenzt*, =6 *erheblich* und >6 *maximal* zugeteilt.

Um zu entscheiden, welche der erkannten Risiken behandelt werden müssen, nutzt man eine Einteilung in Risikoklassen, wie es in Abbildung 6.3 dargestellt ist. Alle Risiken, die einen Schweregrad von erheblich oder höher und eine Eintrittswahrscheinlichkeit von erheblich oder höher haben, müssen unbedingt durch geeignete Maßnahmen behandelt werden. Der Prozess iterativ und wird so lange wiederholt, bis alle erkannten Risiken durch geeignete Maßnahmen auf ein annehmbares Maß reduziert werden konnten.

Wertung	Identifizierung	Auswirkung
1	Die Identifizierung einer Person ist nahezu unmöglich.	Keine oder geringe Auswirkungen.
2	Die Identifizierung einer Person ist unter gewissen Umständen möglich.	Unannehmlichkeiten, die mit geringen Mitteln bewältigt werden können.
3	Die Identifizierung einer Person ist mit einfachen Mitteln möglich.	Erhebliche Schäden, die mit ausreichenden Mittel bewältigt werden können.
4	Die Identifizierung einer Person ist problemlos möglich.	Untragbare, gegebenenfalls irreversible Schäden.

Tabelle 6.6: Ermittlung des Schweregrads nach CNIL

Wertung	Schadenspotential	Ressourcen der Quelle
1	Es ist nahezu unmöglich, eine Schwachstelle der betroffenen Assets auszunutzen	Die Quelle verfügt nicht über die nötigen Ressourcen.
2	Es ist schwierig, eine Schwachstelle der betroffenen Assets auszunutzen.	Die Ressourcen der Quelle sind begrenzt.
3	Es ist möglich, eine Schwachstelle der betroffenen Assets auszunutzen.	Die Ressourcen der Quelle sind erheblich.
4	Es ist einfach, eine Schwachstelle der betroffenen Assets auszunutzen.	Die Quelle verfügt über unbegrenzte Ressourcen.

Tabelle 6.7: Ermittlung der Eintrittswahrscheinlichkeit nach CNIL

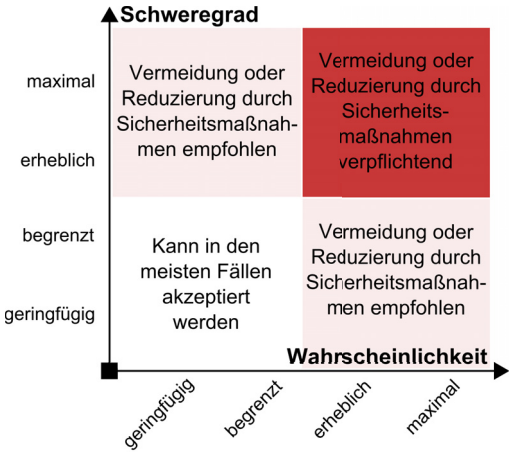


Abbildung 6.3: Risikoklassen und Behandlung nach CNIL

Ergebnisdokumentation Die DSFA geht nach Abschluss der Risikoanalyse und -behandlung in ihren letzten Schritt, der Ergebnisdokumentation über. Hier wird ein abschließender öffentlicher Report verfasst. Dazu wird ein Register geführt, welches die Problembeschreibung, mindernde oder vermeidende Maßnahmen sowie Änderungen am Projekt enthält. Besonders wichtig sind ebenfalls eine Auflistung der Risiken für die Privatsphäre, die nicht behandelt wurden und die damit verbleibenden Restrisiken, die akzeptiert werden. Je nach gewähltem Rahmenwerk kann an dieser Stelle ein externes Audit genutzt werden, um den DSFA-Prozess auf Vollständigkeit und Richtigkeit zu prüfen.

6.3.4 Ergebnisse der DSFA

Da eine DSFA erst endet, wenn alle Risiken auf eine definierte Eintrittswahrscheinlichkeit und Schweregrad reduziert wurden, ist das Ergebnis mehr als nur ein Abschlussbericht. Wird das Verfahren korrekt durchgeführt, erhält man ein technisches System zur Datenverarbeitung mit einem hohen Datenschutzstandard. Im Gegensatz zu beispielsweise dem BSI-IT-Grundschutz oder der ISO 27005 werden nicht nur Anforderungen an die IT-Sicherheit umgesetzt,

sondern auch die Wünsche und Anforderungen aller beteiligten Stakeholder berücksichtigt. Werden die Stakeholder korrekt identifiziert, befragt und beim Design berücksichtigt, trägt die DSFA aktiv dazu bei, ein System zu entwickeln, für das hohe Akzeptanz zu erwarten ist. Dies amortisiert den hohen Personal-, Kosten- und Zeitaufwand, der für die Durchführung benötigt wird.

6.4 Risikominimierung und die Schutzziele

In Abschnitt 5.1.1 wurden die Schutzziele der (intelligenten) Videoüberwachung betrachtet und gefordert, dass die zu entwickelnden Verfahren zur Risikominimierung nicht mit diesen in Konflikt stehen dürfen.

Beide vorgestellten Verfahren, Privacy Score und DSFA, haben keinen direkten negativen Einfluss auf die Erreichung der Schutzziele. Unter Umständen kann es sinnvoll sein, den Abschlussbericht der DSFA vor Veröffentlichung zu prüfen, um nicht versehentlich Schwachstellen in der Sicherheit für Angreifer zugänglich zu machen. Es sei jedoch angemerkt, dass solche Risiken in Allgemeinen im Rahmen einer DSFA behandelt und beseitigt werden.

Insgesamt stellen damit Verfahren zur Risikominimierung ein sehr gutes Werkzeug zur Steigerung der Akzeptanz bereit. Neben dem direkten positiven Effekt auf die Akzeptanz kann außerdem festgestellt werden, dass eine DSFA häufig die IT-Sicherheit eines Systems steigert und damit ebenfalls einen positiven Effekt auf den Betrieb hat.

6.5 Fazit: Risikominimierung

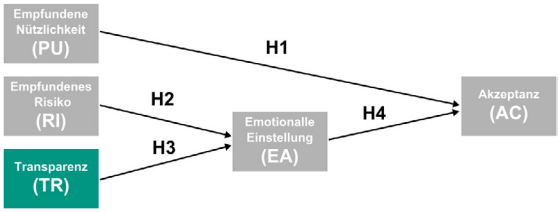
Insgesamt stellt es sich als große Herausforderung dar, die Angst vor Missbrauch zu senken. Auch wenn die hier beschriebenen Verfahren genutzt werden, ist dies vielmals für die Betroffenen nicht ersichtlich und hat somit nur einen geringen Effekt. Um die Wirkung zu erhöhen, bieten sich zwei Ansätze an. Zum einen eine Steigerung der Transparenz, die im nächsten Abschnitt betrachtet wird und die Zertifizierung von Systemen. Da die Wirkung der Zertifizierung direkt vom Vertrauen in die zertifizierende Instanz anhängig ist, wurde sie in

dieser Arbeit nicht als mögliches Werkzeug genutzt. Es soll jedoch zur Vollständigkeit erwähnt werden, dass mit dem European Privacy Seal bereits ein Zertifikat für guten Datenschutz existiert, dass auch für Sicherheitstechnik nutzbar ist [EuroPrise]. Gleichzeitig wurden 2015 im Deutsches Institut für Normung (DIN) in Zusammenarbeit mit der European Union Agency for Network and Information Security (ENISA) Arbeiten für eine Zertifizierung für Sicherheitstechnik begonnen. Diese sollten durch die große Bekanntheit einen hohen Beitrag zur Senkung des Missbrauchsrisikos leisten.

Ähnlich wie bei der Steigerung der Sicherheit wird vermutet, dass durch Systeme mit geringem Missbrauchspotential spätestens mittelfristig die Angst vor Missbrauch gesenkt werden kann. Um das Missbrauchsrisiko der intelligenten Videoüberwachung zu reduzieren, wurden zwei Methoden untersucht. Privacy Score ist als Hilfsmittel für Betreiber entwickelt und soll diesen helfen, für ihren Sicherheitsfall die Überwachungstechnologie mit dem geringsten Eingriff in die Privatsphäre zu wählen. Dank dem einfachen Vorgehen mit einem Fragebogen, können auch Nicht-Datenschutzexperten Technologien in ihrem Einsatzszenario einfach bewerten. Das einfache Ergebnis von Privacy Score, ein Zahlenwert zwischen 0 und 21 Punkten, lässt schnelle, jedoch nur ordinale Vergleiche zwischen Systemen zu.

Ist ein passendes System gewählt, bietet eine DSFA ein methodisches Vorgehen, um Datenschutzprobleme zu identifizieren, zu vermeiden und zu dokumentieren. Leider hat sich gezeigt, dass keines der vorhandenen Rahmenwerke für die Bewertung von Überwachungstechnologie ideal ist. Es wurde eine alternative Kombination existierender Rahmenwerke vorgeschlagen, die sich besser für den Einsatz eignet. In Kapitel 8 wird diese genutzt, um die Entwicklung eines Prototyps zu begleiten.

7 Transparenz



TAM-VS1: Wirkung der Transparenz

Transparenz bildet die Grundlage dafür, dass Betroffene sich ein fundiertes Meinungsbild über ein vorliegendes System machen können. Natürlich gilt dabei, dass eine gesteigerte Transparenz nur dann positiv für die Akzeptanz ist, wenn das System entsprechend gestaltet ist. Methoden zur Sicherstellung des Datenschutzes, Regulierung der Datennutzung oder Reduzierung des Missbrauchsrisikos sind Voraussetzungen dafür, dass die Transparenz die Akzeptanz steigern kann. Dieses Kapitel betrachtet zuerst, welche rechtlichen und anderen Anforderungen für Transparenz bereits bestehen. Anschließend untersucht es verschiedene Ansätze, um die Arbeitsweise von Videoüberwachungssystemen für die Betroffenen transparent zu gestalten. Es werden zum einen Methoden untersucht, die bereits vorhandene Informationen, beispielsweise den verantwortlichen Betreiber, für die Betroffenen zugänglicher machen. Zum anderen werden auch völlig neuartige Ansätze untersucht, um beispielsweise den Betroffenen eine direkte Rückmeldung zu geben, wenn sie unter Beobachtung durch einen Operator stehen.

Auch für das durch TAM-VS erklärte Konstrukt Transparenz lohnt es sich, einen Blick auf die genutzten Fragen der Erhebung zu werfen (vgl. Tabelle B.3 und Tabelle E.3). Das Konstrukt deckt ab, wie stark Betroffene verstehen, welche Daten erfasst werden, wie diese von einem Überwachungssystem verarbeitet

werden und was der eigentliche Einsatzzweck der Videoüberwachung ist. Das in der Videoüberwachung ein hoher Bedarf für Transparenz herrscht, ist alleine schon durch das starke *Informationsungleichgewicht* zwischen Beobachteten und Beobachtern gegeben. Die Beobachter erhalten durch das System eine hohe Dichte an Informationen über die Beobachteten, von Aussehen und Position über Verhalten und Interaktion mit anderen Personen. Die Beobachteten selbst erhalten neben einem Hinweisschild auf die Überwachung keine Informationen. Dieses Ungleichgewicht wird durch die fortschreitende Entwicklung der intelligenten Überwachung stärker. Mehr Transparenz ist der Weg, um die Informationsverteilung wieder auszugleichen. Senior et al. sehen in der Transparenz in der Videoüberwachung als „watch the watchers" einen Demokratisierungsprozess [Sen+05]. Die Arbeiten von Rajamäki et al. bestätigen die positive Wirkung der Transparenz auf die Akzeptanz weiter [Raj+12]. In einer Studie wurde untersucht, ob Studenten in Finnland bereit sind, ihrer Exekutive mehr Überwachungsbefugnisse zu erteilen. Wenn diese mit mehr Möglichkeiten zur Transparenz und Kontrolle verbunden waren, war die Zustimmung deutlich höher.

7.1 Transparenz als Zielvorgabe

Die Ergebnisse von TAM-VS sind ein klares Zeichen dafür, dass die Transparenz von Videoüberwachungssystemen gesteigert werden muss, um die Akzeptanz zu steigern. Dies deckt sich ebenso mit der Forderungen nach mehr Transparenz aus verschiedenen Quellen, die sowohl geltendes Recht als auch freiwillige Verhaltensprinzipien abdecken.

7.1.1 Transparenz als gesetzliche Forderung

Auf gesetzlicher Seite findet sich in Deutschland das BDSG ebenso wie die europäische Datenschutzrichtlinie 95/46/EC [95/46/EC]. Zudem sollte für Deutschland der Entwurf der europäischen DSGVO beachtet werden. Die Arbeiten von Vagts [Vag13], Bier und Spieker gen. Döhmann [Bie10] sowie Laubis und Krem-

pel [Lau14] untersuchten die rechtlichen Anforderungen für Transparenz in der intelligenten Videoüberwachung intensiv. An dieser Stelle werden die zusammengefassten Transparenzansprüche aufgeführt, um die später entwickelten technischen Systeme zur Transparenzsteigerung zu motivieren:

- **Hinweispflicht:**
  Nach §6b BDSG muss bei der Beobachtung öffentlich zugänglicher Räume durch Kameras mit geeigneten Maßnahmen auf die Beobachtung und die verantwortliche Stelle hingewiesen werden.

- **Auskunftspflicht:**
  Nach §§19, 34 BDSG ist einem von der Überwachung Betroffenen auf Antrag Auskunft zu erteilen. Diese Auskunft umfasst neben den Daten auch deren Herkunft, deren potentielle Empfänger und den Zweck der Speicherung.

- **Benachrichtigungspflicht:**
  Wird ein Betroffener ohne dessen Kenntnis durch eine Überwachungsanlage erfasst – und kann daher keinen Antrag auf Auskunft stellen – ist er nach §§19, 34 BDSG über diesen Umstand zu benachrichtigen. Des Weiteren ist er über die Speicherung, die verantwortliche Stelle, den Zweck und – zumindest erstmals – über Empfänger zu unterrichten, soweit er nicht mit ihnen als Empfänger rechnen muss.

- **Meldepflicht:**
  Bei intelligenten Videoüberwachungsanlagen, welche eine automatische Verarbeitung im Sinne des §4d BDSG durchführen, muss die Anlage vor Inbetriebnahme bei einer entsprechenden Behörde beziehungsweise einer entsprechenden Institution gemeldet werden.

- **Prüfpflicht:**
  Entstehen durch eine automatische Verarbeitung besondere Risiken für die Rechte der Betroffenen gemäß §4d BDSG, muss vor Inbetriebnahme eine Prüfung durch den Datenschutzbeauftragten durchgeführt werden, welcher sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden hat.

- **Datenschutzaudit:**
  §9a BDSG sieht die Möglichkeit von Datenschutzaudits und deren Veröffentlichung vor. Die Veröffentlichung kann als Mittel der Transparenz erachtet werden.

Bei der *Melde-* und *Prüfpflicht* sowie dem *Datenschutzaudit* handelt es sich dabei um rein organisatorische Verfahren, mit denen ein intelligentes Überwachungssystem gegenüber Behörden transparent gemacht wird. In Abschnitt 6.3 wurden bereits untersucht, wie eine DSFA für ein intelligentes Überwachungssystem ausgestaltet werden kann und damit eine Ausgangslage für eine Auditierung darstellen.

7.1.2 Transparenz als freiwilliges Verhaltensprinzip

Neben den vorgestellten gesetzlichen Forderungen existieren noch eine Reihe freiwilliger Verhaltensprinzipien, die auch für die intelligente Videoüberwachung herangezogen werden können, und die Transparenz fordern. Auch wenn diese keine rechtsverbindlichen Forderungen darstellen, verdeutlichen sie die Bedeutung der Transparenz:

- **FIP:**
  Die Fair Information Practice Principles (FIP) stellen durch die Organisation for Economic Cooperation and Development (OECD) erlassene, unverbindliche, internationale Richtlinien dar, welche eine hohe Akzeptanz genießen und zuletzt 2013 in den „Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“ verfasst wurden [Org13]. Die FIP fordern hier *Offenheit* über die Verarbeitung von Daten, die wie folgt definiert wird:

  > „Das Offenheitsprinzip kann als Voraussetzung für das Einbeziehungsprinzip angesehen werden; Für die Wirksamkeit des Letzteren muss es praktisch möglich sein, Informationen über die Erhebung, die Speicherung oder die Verwendung von

> personenbezogenen Daten zu erhalten. Das regelmäßige Informieren durch die Erheber von Daten auf einer freiwilligen Basis, Veröffentlichungen in offiziellen Registern über die Beschreibung der Verarbeitungstätigkeiten und die Anmeldung bei Behörden sind ein paar Wege, dies eventuell gewährleisten zu können."

- **PbD:**
  Das PbD-Konzept wurde in den 90er Jahren von Ann Cavoukian entwickelt und besagt, dass Datenschutzaspekte bereits ab der Designphase eines Systems berücksichtigt werden müssen [Cav09a]. Eines der sieben Grundprinzipien von PbD *Sichtbarkeit und Transparenz* fordert, dass:

  > „Privacy by Design will allen Beteiligten die Sicherheit geben, dass das System unabhängig von Geschäftspraktiken oder Technologien wirklich die angekündigten Maßnahmen und Ziele verfolgt und sich einer unabhängigen Prüfung unterwirft. Seine einzelnen Komponenten und Verfahren bleiben sichtbar und transparent, und zwar gleichermaßen für Nutzer und Anbieter. Denken Sie daran, Vertrauen ist gut, Kontrolle ist besser."

- **EFUS-Charta zur Videoüberwachung:**
  Die vom European Forum for Urban Security (EFUS) erstellte Charta „Städte, Bürger und Videoüberwachung: Für eine demokratische und verantwortliche Nutzung von Videoüberwachung" fordert gezielt die Transparenz der Systeme [Eur10]. In ihr wird der *„Grundsatz der Transparenz"* definiert und entsprechende Handlungsempfehlungen gegeben:

  > „Während des gesamten Projektes lautete eine der wesentlichen Fragen der Partner, wie sich die Videoüberwachungssysteme für die Bürger transparent gestalten lassen und wie sich der Schutz ihres Privatlebens und ihrer Grundrechte sicherstellen lässt?"

- **Erweiterte Schutzziele nach Rost und Bock** [RB11]:
  Nach Rost und Bock sind die klassischen IT-Sicherheitsschutzziele *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* alleine nicht ausreichend, um guten Datenschutz zu gewährleisten. Sie fordern zusätzlich noch drei neue Schutzziele: *Transparenz*, *Intervenierbarkeit* und *Nicht-Verkettbarkeit*. Rost und Bock definieren dazu Transparenz wie folgt:

  > „Das Schutzziel Transparenz, das mehr als nur ‚Prüfbarkeit' meint, ist mit solchen Maßnahmen herzustellen, die gewährleisten, dass die Erhebung und Verarbeitung von Daten in Verfahren und deren Nutzung mit zumutbarem Aufwand geplant, nachvollzogen, überprüft und bewertet werden können."

7.2 Gewährleistung von Transparenz

Organisatorische Maßnahmen, wie etwa das Erstellen und Veröffentlichen von Audits, erlauben es, die eigene Datenverarbeitung systematisch zu protokollieren und Auskunftspflichten gegenüber Behörden zu erfüllen. Mit der DSFA wurde dies bereits behandelt. Trotz des hohen Aufwand dieser Dokumentation bleibt es fraglich, ob die erstellten Berichte für interessierte Bürger verständlich sind und damit auch Transparenz gegenüber dieser Gruppe erreicht werden kann. Deshalb wurde eine Reihe weiterer Verfahren, die dazu gedacht sind, die Auskunftspflichten gegenüber den Bürgern zu erfüllen, entwickelt. Dabei lassen sich die Ansätze hinsichtlich ihres Informationsgegenstands, also danach worüber informiert wird, gruppieren.

- Systemtransparenz: Wer hat ein System gebaut, wer ist verantwortlich, warum ist das System im Einsatz?
- Sensortransparenz: Wie werden Daten durch das System erfasst?
- Operatortransparenz: Wer wertet die erfassten Daten aus?
- Beobachtungstransparenz: Wann steht man unter Beobachtung durch das System?

Auch wenn die Trennung nicht scharf ist und Ansätze häufig mehr als einen Gegenstand abdecken, lässt sich damit eine grobe Struktur erreichen.

7.2.1 Systemtransparenz

Zur einfachsten Form der Transparenz gehören jene Formen, die über die Existenz einer Videoüberwachung informieren. Nach §6b BDSG müssen Hinweisschilder auf eine Videoüberwachung hinweisen und mindestens die verantwortliche Stelle und einen verantwortlichen Datenschutzbeauftragten nennen.

Neben bereits bei konventionellen Systemen bekannten Problemen, wie zum Beispiel, dass blinde Personen sie nicht wahrnehmen können, oder dass Betroffene nicht erkennen können, ob Videomaterial gespeichert wird, kommen weitere hinzu. Betroffene können aus einem einfachen Hinweisschild nicht ableiten, welche Verfahren zur Videoauswertung durch das System genutzt werden und wie sie die ihnen zustehenden Informationsrechte einfordern können. Mit zunehmender Leistungsfähigkeit der Systeme, erscheint ein Hinweisschild, dem Anspruch von Transparenz nicht mehr gerecht zu werden [HD11].

Bereits seit einigen Jahren gibt es Bestrebungen, die genutzten Hinweisschilder zu standardisieren und zusätzliche Informationen auf ihnen darzustellen. Clement und Ferenbok schlagen dazu ein System vor, dass Betroffene deutlich besser aufklärt. Ihr Hinweisschild informiert beispielsweise auch darüber, wie lange Daten gespeichert werden, ob das System die Daten anonymisiert oder verschlüsselt und ob das System erweitere Funktionen wie etwa eine Gesichtserkennung nutzt [CF11].

Wenn sich der Trend zu mehr Nutzerdiensten fortsetzt, ist es auch anzunehmen, dass zukünftig Flyer oder andere Werbemittel über installierte Systeme und deren Funktionalität hinweisen. Diese bieten auch eine gute Möglichkeit Betroffene vor Ort umfassend über ein installiertes System zu informieren.

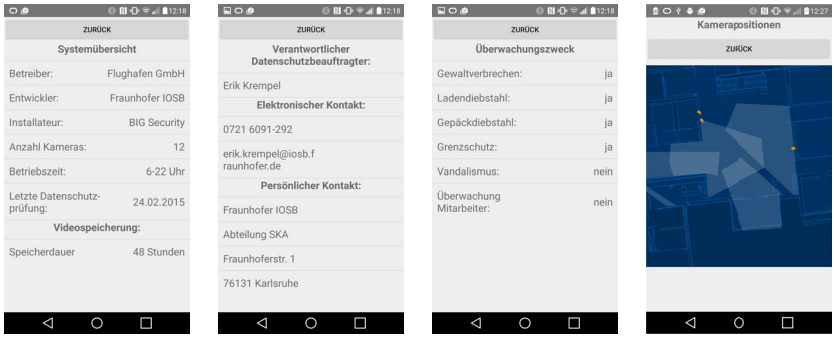
Smartphones bieten einen weiteren Weg für Betreiber und Betroffene miteinander in Kontakt zu treten und damit das Informationsungleichgewicht aufzulösen. In Abbildung 7.1 ist eine App gezeigt, die für eine Probeinstallation im Fraunhofer IOSB entwickelt wurde. Das Szenario sieht vor, dass Besucher

weiterhin mittels Hinweisschild auf das installierte System hingewiesen werden. Zusätzlich zu den gesetzlich geforderten Informationen über den Betreiber hat das neue Hinweisschild noch eine QR-Marke. Wenn ein Besucher diese scannt, wird ihm angeboten, die zum installierten Überwachungssystem zugehörige App zu installieren. In dieser kann er dann Informationen über das System (vgl. Abbildung 7.1a), den verantwortlichen Datenschutzbeauftragten (vgl. Abbildung 7.1b), den Überwachungszweck (vgl. Abbildung 7.1c) und den genau überwachten Bereich (vgl. Abbildung 7.1d) einsehen. Gleichzeitig kann die App genutzt werden, um dem verantwortlichen Datenschutzbeauftragten eine Nachricht zukommen zu lassen.

Die bisher betrachteten Verfahren eigenen sich dafür, über ein System vor Ort Informationen einzuholen. Interessierte müssen dafür aber bereits im Bereich sein, der videoüberwacht wird. Eine Information aus der Ferne ist nicht möglich. Ebenfalls fehlte eine verlässliche Übersicht darüber, wie viele Kamerasysteme überhaupt weltweit oder zumindest in Deutschland installiert sind. Um hier mehr Klarheit zu bekommen, wurde das Projekt CCTV Map [KK15] gestartet. Das Projekt basiert auf der Abschlussarbeit von Markus Nägelin [Näg13] und wurde im September 2015 fertigstellt. Die Idee hinter CCTV Map ist einfach: Selbst für staatliche Stellen oder private Organisation ist es fast unmöglich einen Überblick über installierte Videoüberwachungssysteme zu bekommen. Dies gilt für interessierte Privatpersonen umso mehr. Selbst wenn aufwendige manuelle Datenerhebungen stattfinden, sind diese bereits nach kurzer Zeit veraltet. Gleichzeitig haben erfolgreiche Projekte im Internet, hier sei nur die Wikipedia als Beispiel genannt, gezeigt, dass es möglich ist mit kollaborativen Projekten eine hohe Datenqualität zu erreichen. Wichtige Voraussetzung für den Erfolg ist jedoch, dass sich Freiwillige für das Thema interessieren und Systeme einfach zu bedienen sind. Aus diesem Grund wurde eine möglichst einfach zu bedienende Webseite geschaffen, die in Abbildung 7.2 zu sehen ist.

Die Karten von CCTV Map und auch die darin angezeigten Videokameras basieren auf den Daten von OpenStreetMap [Ope]. Das Eintragen neuer oder das Korrigieren bestehender Kameras wurde deutlich vereinfacht und dauert nun nur noch wenige Sekunden. Die Hoffnung ist, dass sich mit dieser einfa-

chen Übersicht genügend Freiwillige motivieren lassen, um den Datenbestand zu pflegen. Einen Monat nach der Veröffentlichung des Projektes waren in CCTV Map 207 Kameras im Stadtgebiet von Karlsruhe eingetragen. Sobald eine Übersicht geschaffen ist, sollen im nächsten Schritt weitere Informationen über die Systeme erhoben werden. Denkbar ist, dass Systeme mit gutem Datenschutz oder zertifizierte Systeme in der Webseite markiert werden und damit als vertrauenswürdige Systeme erkennbar sind.



(a) Übersicht **(b)** Datenschutz **(c)** Einsatzzweck **(d)** Gelände

Abbildung 7.1: Informationen über ein Überwachungssystem in einer App

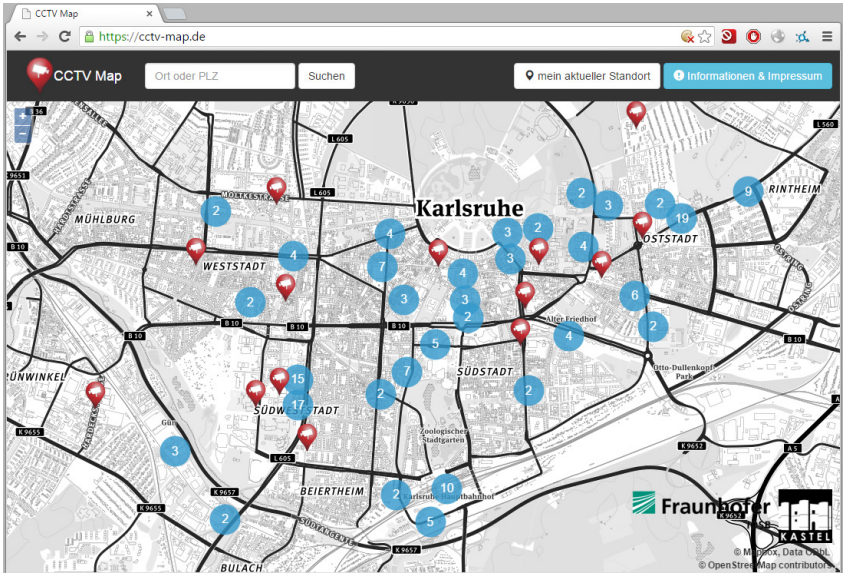


Abbildung 7.2: Webseite von CCTV Map

7.2.2 Sensortransparenz

Eine weitere Möglichkeit, um Vertrauen und Transparenz herzustellen, bezieht sich auf konkrete Sensoren. Denn auch wenn Kameras nur in seltenen Fällen verdeckt installiert werden, ist es für einen Laien kaum möglich, den Erfassungsbereich einer Kamera abzuschätzen. In Abbildung 7.3 wird das Problem verdeutlicht. Es zeigt den Erfassungsbereich derselben Kamera einmal mit einem Teleobjektiv (links) und einem Weitwinkelobjektiv (rechts) aufgenommen.

Klassische Ansätze, um den Erfassungsbereich von Kameras sichtbar zu machen, kennt man aus dem Einzelhandel. Am Eingang der Geschäfte gibt es hier große Monitore, die die Bilder der installierten Kameras anzeigen. Auch wenn der Sinn hinter diesen Systemen typischerweise ein Hinweis auf die Videoüberwachung und damit eine Abschreckung vor Ladendiebstahl ist, bietet es für die Betroffenen Transparenz. Sie können erkennen, welche Qualität

die Bilder der Kameras haben, wie der Blickwinkel ist und welche Bereiche videoüberwacht sind. Natürlich können sie dabei nicht überprüfen, ob auch alle installierten Kameras auf dem Monitor angezeigt werden.

Dieser einfache Ansatz lässt sich derart weiterentwickeln, da es mittels preisgünstiger Displays möglich ist, jede Kamera mit einem solchen auszustatten. Wenn unter jeder Kamera ein Display installiert ist, können interessierte Personen sich schnell ein Bild davon machen, wohin eine Kamera gerichtet ist und ob möglicherweise sensible Bereiche wie Toiletten von der Videoüberwachung betroffen sind.

Eine Alternative dazu stellen Kameras dar, auf die direkt aus dem Internet zugegriffen werden kann. Beispielsweise an Flughäfen oder Cafeterien existieren solche Kameras, die die Länge der Warteschlangen zeigen. Der eigentliche Sinn dieser Kameras ist auch hier nicht die Bereitstellung von Transparenz, sondern eher ein Zusatznutzen, um schon aus der Ferne die ungefähre Wartezeit abschätzen zu können. Kritisch bei diesem Ansatz ist jedoch, dass es zu einem Konflikt zwischen Transparenz und Schutz der Privatsphäre kommen kann. Es ist unbedingt darauf zu achten, dass das verfügbare Videomaterial durch geeignete Verfahren zur Bildmanipulation (vgl. Abschnitt 3.3.1) geschützt ist. Sonst könnte ein Angreifer aus der Ferne erkennen, welche Personen sich im Erfassungsbereich der Kamera befinden.

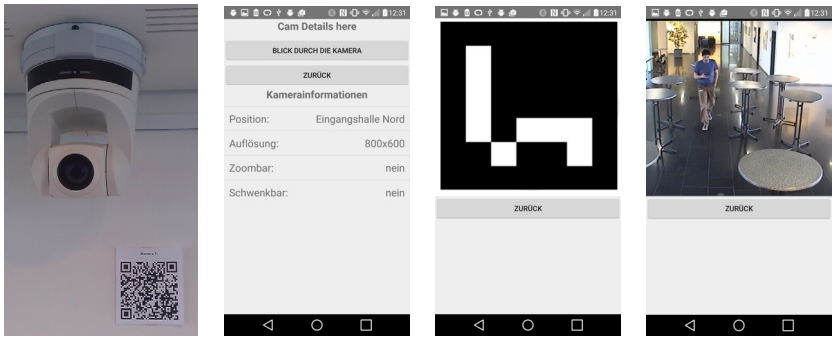
Der Einsatz einer App bietet sich ebenfalls an, um Informationen über einen einzelnen Sensor zu bieten. Als Erweiterung zum bereits erwähnten Experimentalsystem am Fraunhofer IOSB wurde ebenfalls eine Möglichkeit geschaffen, um Transparenz für Sensoren bereitzustellen.

Kameras im System sind mit QR-Marken ausgestattet (vgl. Abbildung 7.4a). Wenn diese mit der App für das Überwachungssystem gescannt werden, erhält man Basisinformationen (vgl. Abbildung 7.4b) zu diesem Sensor. Weiter kann man einen Blick durch die Kamera anfordern. Hier gibt es zwei verschiedene Möglichkeiten, wie der Zugriff auf die Daten geschützt werden kann. Im einfachen Fall werden Verfahren zur Bildmanipulation eingesetzt, um zu verhindern, dass es zu einem Eingriff in die Privatsphäre anderer kommt. Ist das Bildmaterial ausreichend verfremdet, ist es egal, ob der Zugreifende sich wirklich beim

Sensor befindet. Das Bild ist aber auch weniger geeignet einen echten Eindruck von der Datenerfassung durch den Sensor zu vermitteln.

Im aufwendigeren Fall möchte man dem Benutzer das Originalbild der Kamera zeigen, muss dazu aber sicherstellen, dass er wirklich im Erfassungsbereich der Kamera ist. Dazu spielt man ihm mit der App eine zufällig erzeugtes Muster zu und fordert ihn auf, dieses vor die Kamera zu halten (vgl. Abbildung 7.4c. Wenn das System die Marke erkannt hat, darf er für 15 Sekunden auf die Livedaten (vgl. Abbildung 7.4d) der Kamera zugreifen. Damit wird sichergestellt, dass niemand auf die Livedaten einer Kamera zugreifen kann, wenn er sich nicht selbst im Erfassungsbereich dieser Kamera befindet.

Abbildung 7.3: Vergleich des Erfassungsbereichs zwischen Tele- und Weitwinkelobjektiv, ©Axis Communications



(a) QR-Marke **(b)** Basisinformation **(c)** Markenprüfung **(d)** Kamerabild

Abbildung 7.4: Informationen über einen Sensor in einer App

7.2.3 Operatortransparenz

Betrachtet man klassische und intelligente Videoüberwachung, fällt auf, dass über einen Aspekt der Datenverarbeitung gar keine Transparenz herrscht. So ist es zwar gesetzlich gefordert, dass die verantwortliche Firma für eine Videoüberwachung genannt wird, der Mensch hinter der Kamera bleibt aber unbekannt. Will man dieses Informationsungleichgewicht auflösen und ein *„Ich sehe, wer mich mich sieht“*-Prinzip etablieren, hat man verschiedene Möglichkeiten.

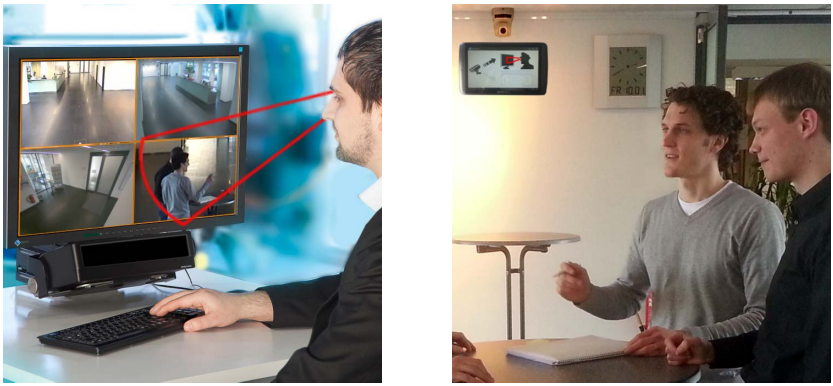
Die einfachste Form der Transparenz wäre es, wenn man das Sicherheitsteam den Beobachteten vorstellt. Diese Praxis, die eigenen Mitarbeiter an einer zentralen Stelle wie den Kassen im Einzelhandel oder der Firmenwebseite mit Namen und Bild vorzustellen, kann ebenfalls auf ein Sicherheitsteam ausgeweitet werden. Dies wäre ein erster Schritt, um zu verdeutlichen, dass hinter der anonymen Kamera ein Mensch sitzt, der im Notfall helfen und eingreifen kann. Ebenso eigenen sich einfache Methoden der Interaktion mit dem Operator, um die Transparenz zu steigern. Ist es möglich den Operator per Telefon oder sogar Videochat zu kontaktieren, können erkannte Sicherheitsprobleme einfach kommuniziert werden.

Das Prinzip das Informationsungleichgewicht aufzulösen lässt sich ausweiten, indem die Betroffenen die Möglichkeit haben, ihrerseits auf ein Video des Operators zuzugreifen. Ein einfaches Videobild der Überwachungszentrale könnte dafür im Internet erreichbar sein oder auf Displays vor Ort für die Überwachten sichtbar gemacht werden. Im Extremfall könnte sogar an jeder Kamera ein Display montiert sein, das den Operator bei seiner Arbeit zeigt. Die Idee hinter diesem *„Ich sehe wer mich mich sieht"*-Prinzip darf jedoch nicht missverstanden werden.

Es ist nicht das Ziel das Recht auf informationelle Selbstbestimmung bei Beobachtetem und Beobachter zu verletzen und damit ein ungerechtes Gleichgewicht zu erreichen. Vielmehr soll gerade durch die Balance der Informationen auch der Datenschutz gestärkt und transparent gemacht werden. Ist zum Beispiel ein System so konfiguriert, dass der Operator nur ein anonymisiertes Bild der Kameras sehen kann, haben die Beobachteten auch ein ebenso anonymisiertes Bild des Operators. Muss die Anonymisierung kurzzeitig aufgehoben werden, beispielsweise weil eine Situation nicht eindeutig zu erkennen ist, dann geschieht dies auch bei den Bildern des Operators.

Eine weitere Form der Operatortransparenz wird in Abschnitt 8.3.3 beschrieben. Dort wird ein System für Krankenhäuser vorgestellt, in dem Videos nicht von einem Operator in einer Sicherheitszentrale ausgewertet werden, sondern algorithmisch erkannte Notfälle direkt von einer Pflegekraft bearbeitet werden. Sobald das System erlaubt, dass eine Pflegekraft auf eine der installierten Kameras zugreift, baut es gleichzeitig einen Audio- und Videochat zwischen der betroffenen Person und der Pflegekraft auf. Das erlaubt eine sehr hohe Transparenz darüber, wer Zugriff auf Daten hat und erlaubt der Pflegekraft, wenn es sich wirklich um einen Notfall handelt, direkt beruhigend auf die verunglückte Person einzuwirken.

7.2.4 Beobachtungstransparenz



(a) Blickerfassung des Operators

(b) Visualisierung für die Beobachteten

Abbildung 7.5: Visualisierung der Beobachtung durch den Operator

Ein weiter Aspekt über den nur sehr wenig Transparenz herrscht, ist die Frage, wann Videos ausgewertet werden und wann eine Person unter Beobachtung steht. Diese Intransparenz ist häufig Absicht, da eine zu hohe Transparenz im Gegensatz zum eigentlichen Überwachungszweck stehen kann (vgl. auch Abschnitt 7.3).

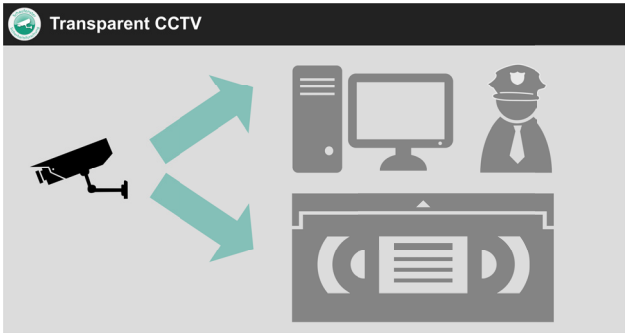
Selbst bei konventionellen Systemen kann nicht mehr davon ausgegangen werden, dass Videomaterial dauerhaft durch einen Operator ausgewertet wird. Gerade in Bussen und Bahnen wird häufig nur ausgewertet, wenn ein konkreter Verdacht oder eine Beschädigung vorliegt. Aber selbst bei Systemen, die in einer Sicherheitszentrale live ausgewertet werden, ist die Beobachtung durch den Operator unklar. In einer großen Sicherheitszentrale laufen die Video von vielen verschiedenen Kameras auf. Teilweise wechseln die Monitore dabei zwischen den Videos von verschiedenen Kameras, sodass ein Teil der Videos nicht mehr angezeigt wird. Selbst wenn alle Videos angezeigt werden, ist es unsicher, ob ein Operator eine bestimmte Kamera beobachtet. Dies wird dann zum Problem,

wenn Personen einen Notfall oder ein Verbrechen beobachten, aber selbst nicht eingreifen und sich auf die Videoüberwachung verlassen.

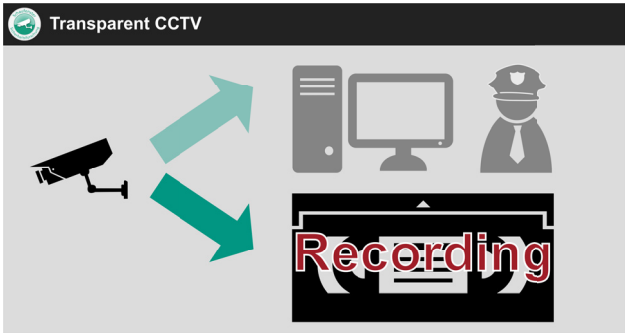
Um diesem Problem zu begegnen, wurde ein System entwickelt, das den Beobachteten direkte Auskunft darüber gibt, wann eine Kamera ausgewertet wird [Lau14]. Das System funktioniert dabei, wie in Abbildung 7.5 gezeigt. In der Sicherheitszentrale wird ein Gerät installiert, dass den Blickwinkel des Operators erfasst (vgl. Abbildung 7.5a). Damit kann das System feststellen, welchen Monitor und auch welchen Bildausschnitt der Operator aktuell beobachtet. Die Visualisierung der Daten erfolgt auf Displays, die an den Kameras installiert werden (vgl. Abbildung 7.5b). Für die Visualisierung auf den Displays wurden Symbole gewählt, die ein intuitives Verständnis der Betroffenen erlauben. In Situationen in denen es zu *keiner Beobachtung* kommt, also die Videodaten weder durch den Operator ausgewertet noch gespeichert werden, zeigt das System lediglich eine Kamera an. Alle weiteren Symbole, die eine Auswertung kennzeichnen, sind verblasst (vgl. Abbildung 7.6a).

Findet hingegen eine *Speicherung* durch das System statt, wird den Betroffenen dies durch ein leicht verständliches Symbol signalisiert (vgl. Abbildung 7.6b). Sieht ein Betroffener, dass Daten zwar gespeichert aber nicht live ausgewertet werden, kann er sein Verhalten entsprechend anpassen. Wenn er eine Notlage beobachtet, wird er sich nun nicht mehr auf Hilfe durch den Operator verlassen, sondern selbst die notwendigen Schritte ergreifen.

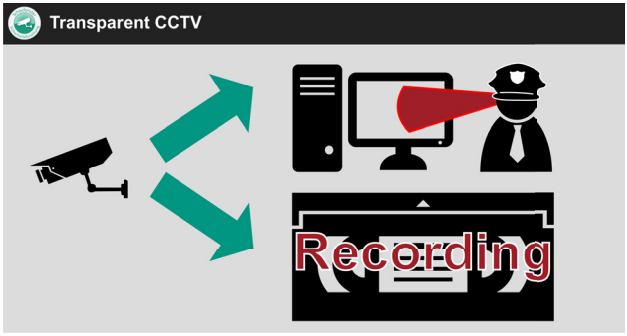
Richtet der Operator seinen Blick auf eine Szene und lässt ihn auch dort, nimmt das System an, dass er eine wichtige Szene auf dem Monitor beobachtet. Die *Beobachtung* unterscheidet sich von der normalen Auswertung durch den Operator darin, dass er seinen Blick längere Zeit auf einen Videostrom gerichtet hält und diesen nicht wie üblich zwischen den verschiedenen Szenen wechselt. Den Betroffenen wird dies durch eine entsprechendes Symbol signalisiert (vgl. Abbildung 7.6c). Je nach Einsatzszenario kann der Betroffene nun beruhigt sein, dass eine kritische Situation erkannt wurde und sich auf die Hilfe durch den Operator verlassen.



(a) Keine Auswertung



(b) Videodaten werden aufgezeichnet



(c) Videodaten werden aufgezeichnet und durch den Operator ausgewertet

Abbildung 7.6: Visualisierungsmöglichkeiten auf den Kameradisplays

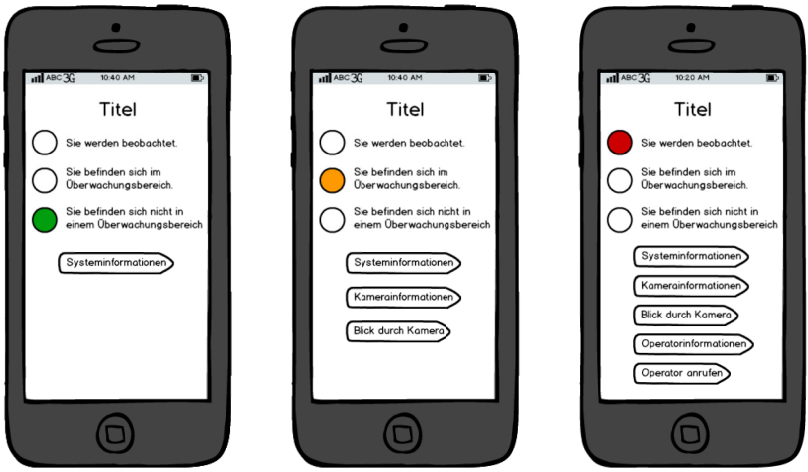
Dieser Ansatz, die Beobachtung durch den Operator zu visualisieren, lässt sich auch auf intelligente Systeme übertragen. Gerade wenn intelligente Überwachungssysteme so eingesetzt werden, dass eine Vorauswertung durch das System geschieht und der Operator nur in besonderen Situationen benachrichtigt wird (vgl. Abschnitt 5.2), ist die Transparenz der Auswertung besonders wichtig. Ohne diese hätten die Betroffenen nämlich keine Möglichkeit zu erkennen, wann Videodaten lediglich durch einen Algorithmus auswertet werden, sie also relativ unbeobachtet sind und wann ein menschlicher Operator auf die Daten zugreift. Auch für diese Visualisierung können Displays an den Kameras eingesetzt werden. Dieses Szenario wird ausführlich in Kapitel 8 behandelt.

Gerade bei intelligenten Videoüberwachungssystemen, in denen neben sichtbaren Sensoren, wie Kameras, auch zusätzliche unsichtbare Sensoren, wie beispielsweise Bewegungsmelder oder Bodendrucksensoren, denkbar sind, ist es wünschenswert, eine proaktive Benachrichtigung über solche Systeme direkt an den Beobachteten zu senden. Der Einsatz von Smartphones ist hier naheliegend. Abbildung 7.7 zeigt einen Entwurf, wie eine solche Smartphone Anwendung aussehen könnte, die gleichzeitig die Beobachtung durch den Operator visualisiert und einige der vorgestellten Verfahren zur System- und Sensortransparenz integriert.

In Abbildung 7.7a befindet sich der Nutzer nicht innerhalb des überwachten Bereichs. Er kann jedoch statische Informationen über das System, wie etwa die verantwortliche Stelle, abrufen.

In Abbildung 7.7b befindet sich der Nutzer nun innerhalb des überwachten Bereichs. Dies wird in der App visualisiert und könnte durch zusätzliche Benachrichtigungen, wie einen Signalton oder einer Vibration, verdeutlicht werden. Sobald ein Nutzer innerhalb des überwachten Bereichs ist, kann er zusätzliche Informationen über die ihn erfassenden Sensoren erhalten und beispielsweise auch einen Blick durch die Kamera werfen.

In Abbildung 7.7c kommt es nun zu einer direkten Beobachtung durch den Operator. Dies wird in der App visualisiert und der Benutzer hat die Möglichkeit, Informationen über den Operator zu bekommen oder ihn zu kontaktieren.



(a) Außerhalb des überwachten Bereichs

(b) Innerhalb des überwachten Bereichs

(c) Beobachtung durch den Operator

Abbildung 7.7: Visualisierungsmöglichkeiten für die Erfassung

7.3 Transparenz und die Schutzziele

In Abschnitt 5.1.1 wurden die Schutzziele der (intelligenten) Videoüberwachung betrachtet und gefordert, dass die zu entwickelnden Verfahren zur Steigerung der Akzeptanz nicht mit diesen in Konflikt stehen dürfen. Gerade die Methoden zur Steigerung der Transparenz haben jedoch einen möglichen negativen Einfluss. Ist das primäre Schutzziel *Security*, also möchte man sich vor mutwilligem und zugleich schadhaftem Verhalten eines Angreifers schützen, kann Transparenz nachteilig sein. So ist es nicht sinnvoll, einem Angreifer genau mitzuteilen, wann ein Operator einen bestimmten Bereich beobachtet, wenn man verhindern möchte, dass der Angreifer diesen Bereich betritt. Erlaubt man den Überwachten direkt mit dem Operator in Kontakt zu treten, könnte ein Angreifer diesen ablenken, während ein Komplize eine Straftat begeht.

Ist das primäre Ziel einer Videoüberwachung *Safety*, also der Schutz vor zufälligen Ereignissen, darf das System beliebig transparent sein, ohne die Erreichung des eigentlichen Schutzzieles zu gefährden. Dies wird in Kapitel 8 am Beispiel des Prototypen NurseEye deutlich. Neben einer gesteigerten Akzeptanz kann die Transparenz sogar zum Erreichen des Schutzziels beitragen, indem Beobachtete erkennen können, wann das System einen Notfall erkannt hat.

Für die *Services* ergibt sich leider wieder die wenig befriedigende Situation, dass für jeden Anwendungsfall genau abgewogen werden muss, ob Schutzziel und Transparenz miteinander im Konflikt sehen. Die ursprüngliche Hoffnung, dass die verschiedenen Transparenzarten pauschal für verschiedene Schutzziele eingesetzt werden können, wurde nicht erreicht. Hier bedarf es genauer Abwägung, welche Informationen man mit den Betroffenen teilen kann, ohne das Schutzziel zu gefährden. Zur Steigerung der Akzeptanz wird damit auch weiterhin umfangreiches Expertenwissen benötigt, um nicht durch eine falsche Wahl der Transparenzmethode das eigentliche Schutzziel zu gefährden.

7.4 Fazit: Transparenz

Zusammenfassend ist die Transparenz eines Videoüberwachungssystems ein sehr spannender Ansatzpunkt, um die Akzeptanz zu steigern. Überraschenderweise wurden bei der Recherche fast keine anderen Forschergruppen gefunden, die sich mit dem vielversprechenden Thema beschäftigen. Clement und Ferenbok haben untersucht, wie Hinweisschilder mehr Transparenz über die Datenverarbeitung erzeugen können. Auch erwähnt werden sollten die Arbeiten von Winkler und Rinner [WR10]. Sie präsentieren Arbeiten zu vertrauenswürdigen Kameras, die erfasste Bilder bereits auf dem Gerät anonymisieren und verschlüsseln. Betroffene können mit einem Smartphone überprüfen, welche Schritte der Datenverarbeitung die TrustCAM vornimmt und ob die Software auch korrekt arbeitet [WR14].

Mit den selbst entwickelten Transparenzmethoden wurde diese Lücke in den vorhandenen Forschungsarbeiten geschlossen. Es wurde gezeigt, wie auf verschiedenen Ebenen der Datenverarbeitung Transparenz erreicht werden

kann. Gerade der Einsatz von Smartphones konnte hier für viele neue Ansätze genutzt werden. Betroffene können sich somit über das System, die verwendeten Sensoren, den Operator und teilweise sogar über die eigene Beobachtung informieren. Für Personen, die selbst kein Smartphone haben oder es nicht nutzen möchten, wurden Displays in intelligente Videoüberwachungssysteme integriert. Diese informieren Betroffene über die Auswertung des Videos und ob der Operator Notsituationen erkannt hat.

8 NurseEye – Intelligente Sturzerkennung und -alarmierung

Nachdem in den letzten drei Kapiteln ein ausführlicher Katalog an Methoden vorgestellt wurde, um die in TAM-VS erkannten Akzeptanzfaktoren positiv zu beeinflussen, soll ein Prototyp einer intelligenten Videoüberwachung geschaffen werden, der auf maximale Akzeptanz durch die Betroffenen ausgerichtet ist. Die Umsetzung dieses Prototypen *NurseEye* wurde im Rahmen des BMBF-Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) bearbeitet. KASTEL hat sich zur Aufgabe gemacht, eine datenschutzfreundliche Videoüberwachung für den Einsatz in Pflegeheimen oder Krankenhäusern zu entwickeln. Da gerade in diesem Bereich die Frage der Akzeptanz kritisch ist, stellt es ein spannendes Umfeld für die erste Anwendung der durch TAM-VS gelernten Zusammenhänge dar.

Die Forscher am Fraunhofer IOSB haben sehr viel Erfahrung darin, wie Systeme ausgestaltet werden können, dass sie neben der Funktionalität ebenfalls den Datenschutz berücksichtigten [Fis+14; Bir+15; Gre+13; BK12; VKB10]. Da nicht alle Entwickler auf einen so umfassenden Erfahrungsschatz zurückgreifen können, wurde der Versuch unternommen, die datenschutzfreundliche Entwicklung anhand einer DSFA zu strukturieren. Es wird das in Abschnitt 6.3 entwickelte Rahmenwerk verwendet.

Der Prozess beginnt mit der Fixierung der Aufgabenstellung und geht dann in eine ausführliche Anforderungsanalyse mit allen wichtigen Stakeholdern über. Im weiteren Schritt Systementwurf, wird das System skizziert, bevor es im Schritt Risikoanalyse und Behandlung untersucht wird. In dieser Phase wird auch eine ausführliche Angreiferanalyse für die intelligente Videoüberwachung durchgeführt. Die Implementierung schließt den Prozess ab.

Eingerahmte Blöcke am Anfang der Kapitel werden jeweils kurz die Ziele der aktuellen Phase in der DSFA beschreiben, bevor die eigentlichen Projektergebnisse zusammengefasst werden. Dies soll weniger erfahrenen Entwicklern als Vorlage dienen, um Datenschutz und Akzeptanz in ihr Design einzubetten.

8.1 Aufgabenstellung

DSFA: Projektinitialisierung In der Projektinitialisierung werden verantwortliche Personen für die Durchführung festgelegt, sowie der Zeit- und Budgetrahmen der Prüfung definiert. Um gute Ergebnisse zu erzielen ist darauf zu achten, dass sowohl technische als auch rechtliche Experten Teil des Bewertungsteams sind. Weiterhin werden die relevanten Stakeholder identifiziert. Ein initialer Fragebogen (vgl. Anhang C) klärt weiter, ob für das betrachtete Projekt die Durchführung einer DSFA notwendig ist. Dies ist der Fall, wenn mindestens eine der Fragen mit „Ja“ beantwortet wird.

Der Projektverantwortliche für die Entwicklung von NurseEye ist Erik Krempel, Budget- und Zeitrahmen werden durch das umschließende Forschungsprojekt KASTEL vorgegeben. Die rechtliche Analyse wird zusammen mit Sebastian Bretthauer, Jurist und wissenschaftlicher Mitarbeiter am Zentrum für Angewandte Rechtswissenschaften (ZAR) am KIT durchgeführt. Des Weiteren soll die unschätzbare Zusammenarbeit mit dem St. Franziskus-Hospital in Münster mit Herrn Dr. med. Peter Kleinekemper hervorgehoben werden. Weitere wichtige Stakeholder sind Betreiber von Krankenhäusern, Mitglieder der Belegschaft und die betroffenen Patienten.

Im initialen Fragebogen zur Vorprüfung müssen sechs der 17 Fragen mit „Ja“ beantwortet werden. Die Notwenigkeit einer DSFA ist damit bestätigt.

8.2 Anforderungserhebung

DSFA: Projektbeschreibung In der Projektbeschreibung sollen alle Prozesse, Funktionen und Daten ermittelt werden, die vom späteren System genutzt werden. Sie ist der Ausgangspunkt, um Schnittstellen und Abhängigkeiten zu anderen Projekten zu identifizieren. Idealerweise werden die Bedürfnisse der Stakeholder durch die Befragung einer repräsentativen Gruppe erhoben. Neben der Technologie ist das Einsatzszenario zu spezifizieren.

Zur Festlegung der Anforderungen wurden mehrere Workshops mit externen Partnern durchgeführt sowie Expertengespräche auf Messen und Veranstaltungen geführt. Herr Dr. med. Peter Kleinekemper stand dabei als zentraler Ansprechpartner für die Anforderungen der Krankenhäuser zu Verfügung. Zudem wurden medizinische Mitarbeiter des Städtischen Klinikums Karlsruhe zu ihren Anforderungen an NurseEye befragt. Ihre Meinung vertritt sowohl die späteren Nutzer des Systems als auch Personen, die lediglich durch die Videoüberwachung betroffen sind. Die Ergebnisse dieser Analyse werden kurz vorgestellt. Dabei werden die Anforderungen nummeriert (→ Req[i]) und später in Abschnitt 8.2.4 zusammengefasst.

8.2.1 Einsatzszenario – Funktionale Anforderungen

Ein grundlegendes Problem für Krankenhäuser stellt der zunehmende Mangel an Personal dar. Im Gegensatz zu gängigen Vorurteilen lässt sich dieser nicht nur durch höhere Budgets erfüllen, da zu wenig geschultes Personal auf dem Arbeitsmarkt vorhanden ist. Insbesondere nachts und in den späten Abendstunden wird dieser Mangel an Personal kritisch, da nicht mehr genügend Pflegekräfte anwesend sind, um das gesamte Krankenhausgelände zu beaufsichtigen. Gerade wenn Patienten auf den langen und unübersichtlichen Wegen zwischen Stationen oder auf den Wegen von ihren Zimmern ins Freie verunglücken, kann es lange dauern, bis ein Unfall erkannt wird. In diesen halböffentlichen Bereichen wäre eine technische Unterstützung wünschenswert, um Notlagen schneller zu

erkennen. Typisch sind Stürze als Folge von Kreislaufzusammenbrüchen oder Herzinfarkten (→ Req[01]).

Patientenzimmer und insbesondere die angeschlossenen Badezimmer stellen einen besonders sensiblen Bereich dar, was das Risiko für die Privatsphäre erhöht. Eine Alarmierung bei Notlagen ist typischerweise durch andere Patienten im gleichen Zimmer oder Notfallmelder an den Betten und im Badezimmer möglich. Daher werden sie in der ersten Version des Systems nicht beachtet.

Grundsätzlich drängt sich die Frage auf, welches Verfahren zur Sturzdetektion geeignet ist. Technisch lassen sich Systeme zur Sturzdetektion grob in drei verschiedene Klassen einteilen [Nou+07]. Erstens: Systeme, bei denen die zu überwachenden Personen Sensoren am Körper tragen, welche Stürze erkennen und weiterleiten. Zweitens: Systeme, die Sensoren direkt im Fußboden oder in Teppichen verbauen und damit Stürze detektieren. Drittens: Systeme, die mittels optischer Sensoren – meist Farb- oder Infrarotkameras – Videodaten erfassen und algorithmisch auswerten.

Die optische Erfassung hat dabei einige Vorteile gegenüber den anderen Klassen. Da keine Sensoren am Körper getragen werden müssen, ist die Bewegungsfreiheit nicht eingeschränkt. In einem Gespräch mit Pflegepersonal wurde der Vorteil erkannt, dass bei einem System, welches ohne am Körper getragene Sensoren auskommt, keine Auswahl der „Risikopatienten“ erfolgen muss. Dies stellt für das Pflegepersonal eine hohe Entlastung dar, da die Vergabe von Sensoren nicht mehr als Diskriminierung aufgefasst werden kann. Weiter können mit einem kamerabasierten System nicht nur Stürze von überwachten Patienten, sondern auch von Besuchern oder Mitarbeitern erkannt werden. Im Vergleich zu den Sensoren im Boden ist der Aufwand, ein kamerabasiertes System zu installieren, geringer und damit günstiger. Geht durch Sensoren im Boden oder am Körper ein Alarm ein, muss eine Pflegekraft den entsprechenden Ort aufsuchen und vor Ort überprüfen, ob wirklich ein Notfall vorliegt. Die Kameras der bildbasierten Verfahren haben hier einen entscheidenden Vorteil: Sie lassen eine Bewertung aus der Ferne zu (→ Req[06]).

Das System soll eine Safety-Aufgabe (vgl. Abschnitt 5.1.1) im Krankenhaus übernehmen und bei Stürzen nahes Pflegepersonal alarmieren (→ Req[02]).

Dabei muss das System so einfach zu bedienen sein, dass das Pflegepersonal nicht von anderen Aufgaben abgehalten wird → Req[03]. Ein System mit einer klassischen Zentrale, in die die Videoströme aller Kameras wiedergeben werden, ist für das Krankenhaus aus folgenden Gründen unbrauchbar:

1. Datenschutzanforderungen: Die permanente Beobachtung von Patienten und Mitarbeitern durch Sicherheitspersonal ist aus Datenschutzgründen nicht tragbar (→ Req[07], → Req[08]).

2. Situationsbewertung: Erkannte Notlagen können nur durch medizinisches Personal korrekt bewertet werden. Wenn ein Mitarbeiter des Sicherheitspersonals einen Notfall sieht, ist er womöglich nicht in der Lage, diesen korrekt einzuschätzen.

3. Situationsbehandlung: Die Notfallbearbeitung muss durch medizinisches Personal erfolgen. Mitarbeiter des Sicherheitspersonals haben nicht das benötigte Fachwissen, um einer verunglückten Person zu helfen.

4. Alarmierung: Wenn ein Notfall in der Zentrale erkannt wurde, ist es unklar, wie passendes medizinisches Personal verständigt werden kann. Dieses ist typischerweise in den zugeteilten Stationen unterwegs. Selbst wenn sie mit mobilen Telefonen ausgestattet sind, ist nicht immer klar, ob sie verfügbar sind (→ Req[04]). Es kann gut sein, dass ein Mitarbeiter medizinische Notfälle bearbeitet und nicht auf einen vom Sicherheitspersonal gemeldeten Alarm reagieren kann (→ Req[05]).

5. Qualität der Versorgung: Wird das medizinische Personal durch die Zentrale an einen Unfallort gerufen, kann erst vor Ort die genaue Situation bewertet werden. Unter Umständen kann der Mitarbeiter erst vor Ort erkennen, dass eine weitere Ausrüstung notwendig ist.

8.2.2 Rechtliche Anforderungen – Nicht-Funktionale Anforderungen

Die rechtlichen Anforderungen wurden zusammen mit Sebastian Bretthauer innerhalb von KASTEL erarbeitet. Im Rahmen dieser Arbeit entstanden vier interdisziplinäre Arbeiten [BK14; BKB15; Bir+13; Bir+15] zur datenschutzfreundlichen Videoüberwachung, deren Ergebnisse hier aufbereitet und zusammengefasst werden.

Das Bundesdatenschutzgesetz (BDSG) und der Entwurf der europäischen Datenschutzgrundverordnung (DSGVO) stellen relevante rechtliche Rahmenwerke dar. Das BDSG stellt nationales Recht dar, das ein hohes Maß an Datenschutz fordert. Zusätzlich ist es das in Deutschland geltende Datenschutzrecht, wenn es nicht von Landesrecht oder bereichsspezifischen Gesetzen überschrieben wird. Das DSGVO wird betrachtet, da es ein verpflichtendes Mindestmaß an Datenschutz darstellt, wie es in gesamt Europa eingeführt werden soll.

Erforderlichkeit Nach §6 b Abs 1 BDSG existieren drei Gründe, warum die Nutzung von Videoüberwachung im öffentlichen Raum zulässig sein kann:

1. Aufgabenerfüllung öffentlicher Stellen
2. Wahrnehmung des Hausrechts
3. Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

Entscheidend ist dabei, dass keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dies ist jedoch nur eine notwendige, keine hinreichende Bedingung für die Zulässigkeit des Einsatzes. Vielmehr muss die Videoüberwachung erforderlich sein und keine alternative weniger instruktive Methode denselben Zweck erfüllen können. Diese Erforderlichkeit des BDSG erscheint nach Gesprächen mit den Anwendern erfüllt und wird deshalb nicht mehr als eigenständige Anforderung aufgenommen.

Datenvermeidung und Datensparsamkeit Nach §3 a BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf ein Minimum zu reduzieren (→ Req[13]). Systeme sind so zu gestalten, dass immer möglichst wenige Daten zur Erfüllung des eigentlichen Zwecks benötigt werden. Gemäß Art. 5 c DSGVO müssen personenbezogene Daten dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein.

Transparenz Nach §6 b Abs 2 BDSG ist die Videoüberwachung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen (→ Req[10]). Mit welchen technischen Mittels diese Transparenz zu erreichen ist, wird vom Gesetzgeber aber nicht näher spezifiziert. Ähnliche Anforderungen werden auch von Art. 5 a) DSGVO an das System gestellt.

Zweckbindung Nach §6 b Abs 5 BDSG sind erfasste Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen (→ Req[14]). Dies deckt sich ebenfalls mit Art. 5 e) DSGVO, die eine sofortige Löschung personenbezogener Daten fordert, sobald diese nicht mehr erforderlich sind. Weiter wird gefordert, dass Daten, die von NurseEye für eine Sturzerkennung erfasst wurden, nicht für andere Zwecke verarbeitet werden (→ Req[09]).

Automatisierte Verarbeitung personenbezogener Daten Nach §6 a Abs. 1 BDSG ist es nicht zulässig, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt sind (→ Req[11]). Der Betroffene soll nicht zum bloßen Objekt von Computeroperationen degradiert werden. Letztendlich soll ein Mensch die persönliche Verantwortung für die zu treffende Entscheidung übernehmen. Es ist aber zulässig, die Aufmerksamkeit eines Mitarbeiters durch NurseEye entsprechend zu lenken. Zu vergleichbaren Anforderungen kommt man, wenn

man die DSGVO betrachtet. Hier verbietet Art. 20 DSGVO ebenfalls eine rein automatische Auswertung der erfassten persönlichen Daten.

Datenschutzfolgen-Abschätzung Art. 33 no. 3 des Entwurfs einer europäischen DSGVO fordert, dass für alle Technologien, die Daten über Bürger im öffentlichen Raum erfassen oder verarbeiten, ein DSFA erstellt werden muss (→ Req[12]). Dies deckt sich ebenfalls mit den Forderungen nach §9 a BDSG zur Durchführung eines Datenschutzaudits. Auch wenn diese Anforderung schon im Rahmen einer laufenden DSFA erkannt wurde, wird es als eigenständige Anforderung aufgenommen, um die Erfüllung alle Anforderungen zu protokollieren.

8.2.3 Privacy by Design – Nicht-Funktionale Anforderungen

Im Laufe der rechtlichen Untersuchungen zu NurseEye wurde erkannt, dass die technische Entwicklung der intelligenten Videoüberwachung deutlich schneller ist, als die Anpassung der rechtlichen Vorgaben. Es bedarf also einer gewissen Voraussicht, um ein System zu entwerfen, dass auch zukünftiger Gesetzgebung entspricht. In seiner Dissertation „Privatheit und Datenschutz in der intelligenten Überwachung: Ein datenschutzgewährendes System, entworfen nach dem ‚Privacy by Design' Prinzip" hat Hauke Vagts gezeigt, welch hohes Datenschutzpotential in PbD steckt [Vag13].

Das von Ann Cavoukian formulierte *Privacy by Design* beschreibt sieben Privacy-Prinzipien, die Systeme einhalten sollen, um optimale Ergebnisse zu erhalten [Cav09a]. Im Gegensatz zu einer DSFA, die ein methodisches Verfahren beschreibt, um Datenschutzprobleme während der Entwicklung zu erkennen und zu behandeln, handelt es sich bei den sieben Prinzipien um Grundanforderungen, die durch ein System zu erfüllen sind. Damit ist eine direkte Umsetzung der PbD-Prinzipien von Nicht-Datenschutzexperten schwierig. Dieses Schwäche wurde in zwei Veröffentlichungen untersucht und der Versuch unternommen, die Prinzipien mehr für den Einsatz von Entwicklern anzupassen [Bie+12a; Bie+12b].

Für die Entwicklung von NurseEye wurde dieses neue Konzept angewendet. PbD wird innerhalb der Entwicklung von NurseEye als Stakeholder der DSFA betrachtet. Dies garantiert somit, dass alle Anforderungen von PbD umgesetzt werden und gleichzeitig die Vorteile der DSFA genutzt werden. Hier werden die sieben Prinzipien von PbD kurz aufgelistet und gezeigt, wie sie innerhalb von NurseEye als Anforderung aufgenommen werden. Die deutschen Zitate der sieben Prinzipien sind der offiziellen Übersetzung von Ann Cavoukian entnommen und an den gekennzeichneten Stellen gekürzt [Cavo9b].

1. Proaktiv und nicht reaktiv; als Vorbeugung und nicht als Abhilfe

> „PbD ist von proaktiven und nicht reaktiven Maßnahmen geprägt. Es sieht Gefahren für die Privatsphäre voraus und verhindert sie bevor sie eintreten können. PbD bietet keine Abhilfe im Falle von datenschutzrechtlichen Verletzungen, wenn sie erst einmal eingetreten sind – es verhindert vielmehr deren Auftreten. [...]"

Der gesamte Systementwurf von NurseEye verfolgt einen proaktiven Datenschutz. Die begleitende DSFA, die ausführliche Angreiferanalyse und die rechtliche Analyse bezeugen diese Grundhaltung. Proaktiver Datenschutz wird als eigenständige Anforderung aufgenommen, um die Erfüllung aller Anforderungen zu protokollieren (→ Req[17]).

2. Datenschutz als Standardeinstellung

> „Wir können uns alle einer Sache gewiss sein – die Standardeinstellungen sind entscheidend! Privacy by Design soll den größtmöglichen Schutz der Privatsphäre bringen, indem sichergestellt wird, dass personenbezogene Daten automatisch in jedem IT-System und bei allen Geschäftspraktiken geschützt werden. Wenn eine Person nichts unternimmt, bleibt der Schutz ihrer Privatsphäre immer noch intakt. Einzelpersonen sind nicht gefordert, selbst etwas für den Schutz ihrer Privatsphäre zu unternehmen – der Schutz ist bereits systemimmanent, als Standardeinstellung."

Bei Prinzip Nummer 2 werden Schwächen von PbD für Sicherheitstechnologie sichtbar. Bei NurseEye sind die Betroffenen und die Nutzer des Systems zwei unterschiedliche Gruppen. Um die Trennung deutlicher zu machen, werden die beiden Gruppen zukünftig Betroffene und Bediener genannt. Die Betroffenen können nicht beeinflussen, ob und wann welche ihrer Daten genutzt werden. Von daher erscheint das Prinzip unpassend. Kennt man jedoch die Motivation hinter dem Prinzip, erkennt man, dass es auch für NurseEye eine Bedeutung hat. PbD möchte nicht verbieten, dass Nutzer, beispielsweise über soziale Netzwerke, persönliche Daten teilen. Das System muss jedoch so konfiguriert sein, dass dieses Teilen nur auf ausdrücklichen Wunsch der Nutzer geschieht und nicht die Standardeinstellung ist. Für NurseEye kann man dies so interpretieren, dass die Grundeinstellungen des Systems die Betroffenen optimal schützen. Daraus kann die Forderung abgeleitet werden, dass Bediener nicht in der Lage sein dürfen, die Datenschutzeinstellungen zum Nachteil der Betroffenen zu verändern (→ Req[15]).

3. Der Datenschutz ist in das Design eingebettet

> „PbD ist in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet. Es wird nicht nach dem Vorfall als add-on eingebaut. Das Ergebnis ist, dass der Datenschutz eine wesentliche Komponente der Kernfunktionalität wird. Datenschutz ist ein wesentlicher Bestandteil des Systems, ohne Abstriche bei der Funktionalität."

Prinzip Nummer 3 wird ebenfalls durch die Einbettung von Datenschutz in den Entwurf von NurseEye erfüllt. Trotzdem wird es als Anforderung aufgenommen, um die Erfüllung aller Anforderungen zu protokollieren (→ Req[18]).

4. Volle Funktionalität – eine Positivsumme, keine Nullsumme

> „Privacy by Design will allen berechtigten Interessen und Zielen entgegenkommen, und zwar durch eine Positivsumme, die ein zufriedenstellendes Ergebnis für beide Seiten erzielt, und nicht durch

> einen veralteten Nullsummenansatz, bei dem schließlich unnötige Kompromisse erforderlich werden. Durch Privacy by Design wird die Vortäuschung falscher Dichotomien wie Datenschutz versus Sicherheit vermieden. Privacy by Design zeigt, dass es möglich ist, beides zugleich zu erreichen."

Prinzip Nummer 4 zeigt deutlich, dass PbD nicht mit den besonderen Anforderungen von Sicherheitstechnologie formuliert wurde. Auch wenn Datenschutz eines der primären Ziele von NurseEye ist, bleibt ein gewisser Eingriff in die Privatsphäre unumgänglich. Ein gewisser Konflikt zwischen Sicherheit und Datenschutz bleibt also bestehen. Das Ziel von NurseEye muss jedoch sein, bei einem sehr geringen Eingriff in die Privatsphäre einen sehr hohen Grad an Funktionalität zu erreichen und damit die Positivsumme zu erfüllen. Dies wird als Anforderung aufgenommen (→ Req[16]).

5. Durchgängige Sicherheit – Schutz des gesamten Lebenszyklus

> „Nachdem Privacy by Design vor der Ersterfassung der Information in das System ‚eingebettet' wurde, erstreckt sich dessen Wirkung auf den gesamten Lebenszyklus der Daten - starke Sicherheitsmaßnahmen sind für den Datenschutz unerlässlich, und zwar von Anfang bis Ende. Dadurch wird erreicht, dass alle Daten sicher gespeichert und am Ende des Prozesses sicher und rechtzeitig vernichtet werden. So sorgt Privacy by Design von der Wiege bis zur Bahre durchgängig für eine sichere Datenverarbeitung."

Das Grundprinzip Daten auf dem gesamten Lebenszyklus vor Missbrauch zu schützen, ist bereits Teil der Anforderungen von NurseEye.

6. Sichtbarkeit und Transparenz – Für Offenheit sorgen

> „Privacy by Design will allen Beteiligten die Sicherheit geben, dass das System unabhängig von Geschäftspraktiken oder Technologien wirklich die angekündigten Maßnahmen und Ziele verfolgt

> und sich einer unabhängigen Prüfung unterwirft. Seine einzelnen Komponenten und Verfahren bleiben sichtbar und transparent, und zwar gleichermaßen für Nutzer und Anbieter. Denken Sie daran, Vertrauen ist gut, Kontrolle ist besser."

Transparenz ist ein Grundanspruch des Entwurfes von NurseEye. Das zeigt sich gerade in der bereits aufgenommenen Anforderung Req[10] zur Transparenz der Datenverarbeitung und Anforderung Req[12] zur Durchführung einer DSFA. Es müssen keine zusätzlichen Anforderungen zur Erfüllung oder Protokollierung von Prinzip Nummer 6 aufgenommen werden.

7. Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen

> „Privacy by Design erfordert vor allem von den Architekten und Betreibern (von IT-Systemen), dass für sie die Interessen der Einzelpersonen an erster Stelle stehen. Sie bieten Maßnahmen wie strenge datenschutzfreundliche Voreinstellungen und angemessene Benachrichtigungen an und eröffnen benutzerfreundliche Optionen. Sie sorgen für eine nutzerzentrierte Gestaltung."

Bei Prinzip Nummer 7 ist, ähnlich wie in Prinzip Nummer 4, zu beobachten, dass PbD nicht für Sicherheitstechnologie entworfen wurde. In NurseEye wird eine nutzerzentrierte Gestaltung dadurch erreicht, dass eine Sicherheitsaufgabe, das schnelle Erkennen und Bearbeiten von Stürzen, erfüllt wird. Der Datenschutz, zumindest im Falle eines vorliegenden Unfalls, ist zweitrangig zur Sicherheitsaufgabe. Trotzdem verfolgt NurseEye das Ziel, die Menge der erhobenen Daten minimal zu halten und nur in stark limitierten Ereignissen einen Eingriff in die Privatsphäre zu benötigen. Prinzip 7 wird somit von NurseEye und den gesammelten Anforderungen erfüllt werden, jedoch nicht auf die von PbD vorgesehene Art und Weise.

Fazit zu Privacy by Design für NurseEye

PbD bringt als eigenständiger Stakeholder neue Blickwinkel in den Prozess ein, der ganz besonders die datenschutzfreundliche Ausgestaltung der Technik abdeckt. Überraschenderweise konnten durch PbD Anforderungen erfasst werden, die nicht von den Betroffenen selbst formuliert wurden, aber den Schutz der Betroffenen erhöhen werden. Die Erfahrung eines Datenschutzexperten konnte also genutzt werden, um mehr Möglichkeiten für den Datenschutz zu identifizieren, als dies durch die Betroffenen alleine möglich war. So kann festgestellt werden, dass durch die Integration von PbD als eigenständigem Stakeholder innerhalb der DSFA ein noch vollständigeres Anforderungsprofil erstellt werden konnte.

8.2.4 Zusammengefasste Anforderungen

- □ Req[01]: NurseEye soll Stürze in entfernten Bereichen erkennen.
- □ Req[02]: NurseEye soll das Pflegepersonal effizienter zur Behandlung von Notlagen koordinieren.
- □ Req[03]: NurseEye muss einfach zu bedienen sein.
- □ Req[04]: NurseEye muss sich in die alltäglichen Arbeitsabläufe einpassen lassen.
- □ Req[05]: NurseEye darf laufende Arbeiten nicht unterbrechen.
- □ Req[06]: NurseEye muss eine Bewertung des Notfalls aus der Ferne zulassen.
- □ Req[07]: NurseEye darf nicht zur Mitarbeiterüberwachung nutzbar sein.
- □ Req[08]: NurseEye darf nicht zur permanenten Überwachung der Patienten führen.
- □ Req[09]: Videodaten von erkannten Stürzen dürfen das System nicht verlassen.

□ Req[10]: NurseEye muss ein hohes Level an Transparenz erreichen.

□ Req[11]: NurseEye darf keine automatische Einzelfallentscheidung treffen.

□ Req[12]: Es muss eine DSFA für NurseEye erstellt werden.

□ Req[13]: NurseEye muss die Menge der benötigten personenbezogenen Daten minimieren.

□ Req[14]: NurseEye muss alle erfassten Daten löschen, sobald sie nicht mehr benötigt werden.

□ Req[15]: Die Bediener von NurseEye können dessen Einstellungen zum Datenschutz nicht nachteilig beeinflussen.

□ Req[16]: NurseEye erreicht eine Positivsumme zwischen Privatsphäre und Funktionalität.

□ Req[17]: NurseEye verfolgt einen proaktiven Ansatz für Datenschutz.

□ Req[18]: Datenschutz muss tief in das Design des Systems integriert sein.

8.3 Systementwurf

Nach Abschluss der Anforderungsanalyse wurde NurseEye entworfen. Zentrale Bestandteile von NurseEye sind die algorithmische *Sturzerkennung und -bearbeitung*, die *Interaktion mit dem Pflegepersonal* bei erkannten Stürzen sowie die *Transparenz der Datenverarbeitung*. Abbildung 8.1 verdeutlicht das Grunddesign von NurseEye zusätzlich. Detektiert die algorithmische Auswertung keine besonderen Ereignisse (Stürze), werden die erfassten Daten sofort nach der algorithmischen Auswertung gelöscht. Nur im Falle eines Sturzes wird eine Pflegekraft alarmiert, die dann für die Bearbeitung zuständig ist.

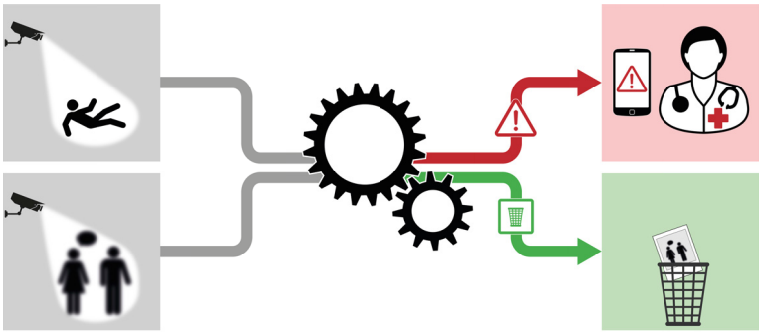


Abbildung 8.1: NurseEye-Prinzip

8.3.1 Sturzerkennung und -bearbeitung

Die Frage, welches bildbasierte Verfahren am besten geeignet ist, um Stürze zu erkennen, wird intensiv untersucht. Die wissenschaftliche Datenbank Scopus [SCOPUS] listet im Zeitraum ab 2010 über 130 Publikationen zu dem Schlagwort „fall detection video“ auf. NurseEye baut auf dieser Forschung auf und entwickelt keine eigenen Verfahren zur Sturzdetektion. Vielmehr richtet es seinen Fokus darauf, wie die weitere Verarbeitung einer algorithmischen Sturzerkennung ausgestaltet wird.
Zu den Nachteilen der kamerabasierten Lösung zählen potenziell hohe Eingriffe in die Privatsphäre aller Betroffenen. Um diesen zu begegnen, nutzt NurseEye das Prinzip der interaktiven Videoüberwachung (vgl. Abschnitt 5.2), um die Eingriffe minimal zu halten und arbeitet in den drei Betriebsmodi: *Bereitschaftsmodus*, *Beurteilungsmodus* und *Bearbeitungsmodus*.

Bereitschaftsmodus Im Bereitschaftsmodus arbeitet NurseEye unabhängig von menschlicher Interaktion oder Auswertung und erreicht maximalen Datenschutz. Wenn das System aktiviert ist, werden die von den installierten Kameras erfassten Bilddaten von Algorithmen ausgewertet. Es gibt keine zentrale Auswertung durch einen Operator und die Pflegekräfte haben keine Möglichkeit

auf die erfassten Daten zuzugreifen. Wenn ein Algorithmus mit einer gewissen Wahrscheinlichkeit einen Sturz detektiert hat, wechselt NurseEye in den Beurteilungsmodus.

Beurteilungsmodus Ziel des Beurteilungsmodus ist es, eine menschliche Bewertung eines erkannten Sturzes zu bekommen. Dies hat zum einen den Grund, dass algorithmische Sturzerkennung, oder die algorithmische Bildauswertung generell, immer einer gewissen Fehlerrate unterliegt. Dabei wird zwischen den sog. *false-positives* und den *false-negatives* unterschieden. Bei einem false-positive wird eine unkritische Situation, beispielsweise wenn sich eine Person bückt, um etwas vom Boden aufzuheben, fälschlicherweise als Sturz klassifiziert. Bei einem false-negativ wird ein echter Sturz nicht als solcher erkannt. Grundsätzlich ist es nicht möglich, beide Fehlerarten bei der Bildauswertung gänzlich zu vermeiden. Durch entsprechende Konfiguration kann jedoch das Verhältnis von false-negatives zu false-positives verändert werden. Da bei NurseEye ein false-negativ, also das Nichterkennen eines vorliegenden Sturzes, weitaus schlimmere Folgen haben würde als eine falsche Klassifikation eines Sturzes, wurde es entsprechend konservativ konfiguriert.

Der zweite Grund für den Beurteilungsmodus ist das Verbot der automatisierten Einzelfallentscheidung durch das BDSG und DSGVO. Detektiert in NurseEye ein Algorithmus einen Sturz, hat dies keine direkten Folgen für den Betroffenen. NurseEye lenkt lediglich die Aufmerksamkeit des Pflegepersonals auf das besondere Ereignis. Um einen unnötigen Eingriff in die Privatsphäre der Betroffenen so weit wie möglich zu reduzieren, werden die Videos vor der Anzeige anonymisiert. Hierzu wird das von Birnstill et al. entwickelte Verfahren verwendet [BRB15].

Anhand des Videos eines potentiellen Sturzes entscheidet eine Pflegekraft, ob es sich um einen echten Sturz handelt, oder ob ein false-positive vorliegt. Im Falle eines Fehlalarms wird das Ereignis zusammen mit allen dafür erfassten Daten gelöscht und das System wird wieder in den Bereitschaftsmodus gesetzt. Wenn die Pflegekraft das Ereignis als Sturz bestätigt, wechselt das System in den Bearbeitungsmodus.

Bearbeitungsmodus Im Bearbeitungsmodus wurde eine Detektion bereits als Sturz bestätigt. Dies bedeutet, dass sich eine Person in einem potentiell gefährlichen Zustand befindet und schnelle Hilfe benötigt wird. Aus diesem Grund werden im Bearbeitungsmodus tiefere Eingriffe in die Privatsphäre des Betroffenen erlaubt, wenn diese zu einer schnelleren Bearbeitung beitragen. Die zuständige Pflegekraft hat im Bearbeitungsmodus vollen Zugriff auf die erfassten Videodaten in der maximal zur Verfügung stehenden Auflösung. Dank diesem Videomaterial kann sie bereits aus der Ferne die Situation des Gestürzten einsehen und bewerten, ob sie eventuell weitere medizinische Ausrüstung benötigt oder direkt zum Unfallort geht. Es wäre auch denkbar, dass in diesem Schritt bereits zusätzliches medizinisches Personal benachrichtigt werden kann. Dies ist jedoch in NurseEye nicht umgesetzt.

Sobald ein Sturz von einer Pflegekraft behandelt wurde, wird das System wieder in den Bereitschaftsmodus versetzt und alle erfassten Daten gelöscht.

8.3.2 Interaktion mit dem Pflegepersonal

In der Anforderungserhebung wurde erkannt, dass es in einem Krankenhaus keine geeignete zentrale Stelle zur Bearbeitung von Sturzalarmen gibt. Die Bearbeitung der Alarme muss idealerweise innerhalb der betroffenen Station erfolgen, und wenn dies nicht möglich ist, in räumlicher Nähe. Weiter muss sich das System in die täglichen Arbeitsabläufe integrieren lassen. Damit scheidet eine Benachrichtigung der Pflegekräfte an einem festen Ort, beispielsweise dem Stationszimmer, aus. Die Interaktion mit dem Pflegepersonal erfolgt deshalb über mobile Endgeräte. Dazu wird angenommen, dass man alle Pflegekräfte, zumindest in der Abend- und Nachtstunden, wenn erfahrungsgemäß nur wenig Personal anwesend ist, mit mobilen Endgeräten ausstattet. Abbildung 8.2 zeigt die App, mit der das Pflegepersonal mit dem System interagiert.

So lange sich NurseEye im Bereitschaftsmodus befindet, braucht es keinerlei Interaktion mit dem Pflegepersonal. Wenn eine Pflegekraft auf die App zugreift, kann sie Informationen über den Zustand des Systems abfragen, also erkennen

ob NurseEye ein- oder ausgeschaltet ist, hat aber keinen Zugriff auf Livedaten (vgl. Abbildung 8.2a).

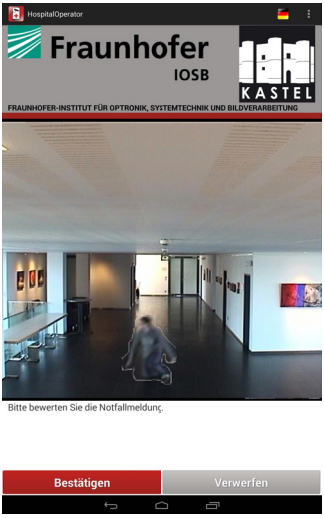
Wenn die Sturzerkennung meldet einen Sturz erkannt zu haben, wechselt NurseEye in den Beurteilungsmodus und sucht eine Pflegekraft, die den Vorfall bewerten kann. Dazu wird zuerst eine Alarmierung (vgl. Abbildung 8.2b) an das Endgerät geschickt, dass räumlich am nächsten am Unfallort ist. Sollte die alarmierte Pflegekraft keine Zeit haben, den Alarm zu bearbeiten (vgl. Req[05]: NurseEye darf laufende Arbeiten nicht unterbrechen) wird der Alarm an weitere Smartphones verteilt.

Sobald eine Pflegekräfte den Alarm bestätigt, wird sie vom System als Bearbeiter markiert und weitere Alarmierungen bei anderen Pflegekräften gelöscht. Der Bearbeiter kann mit seinem Smartphone die anonymisierte Videoszene sehen, die vom Algorithmus als Sturz erkannt wurde (vgl. Abbildung 8.2c).

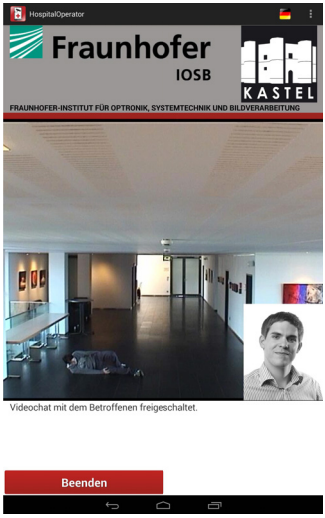
Wenn die Pflegekraft im Beurteilungsmodus den vermuteten Sturz bestätigt, wechselt das System in den Bearbeitungsmodus. In diesem hat die Pflegekraft Zugriff auf die nicht mehr anonymisierten Livedaten der Kamera. Dieses soll sie schon aus der Ferne mit den benötigten Informationen versorgen, um die optimale Versorgung des verunglückten Patienten sicherzustellen. Sobald der gestürzten Person geholfen wurde, wird dies in der App bestätigt und NurseEye wechselt wieder in den Bereitschaftsmodus.

(a) Bereitschaftsmodus

(b) Sturzalarm eingegangen



(c) Beurteilungsmodus



(d) Bearbeitungsmodus

Abbildung 8.2: Die NurseEye App für die Pflegekräfte

8.3.3 Transparenz der Datenverarbeitung

Für die Transparenz der Beobachteten bieten sich verschiedene Konzepte an. Grundsätzlich ist bei einer Entwicklung wie NurseEye nicht davon auszugehen, dass die Betroffenen die Arbeitsweise leicht verstehen können und somit in der Lage sind das System zu bewerten. Deshalb muss der erste Schritt sein, die Öffentlichkeit im Allgemeinen und Betroffene im Speziellen über die Arbeitsweise des Systems zu informieren. Klassische Printmedien, wie etwa ein Flyer, sind eine gute erste Möglichkeit, um Betroffene über ein System wie NurseEye zu informieren. Somit wird eine grundsätzliche Aufmerksamkeit der Betroffenen für die weitere Interaktion geschaffen.

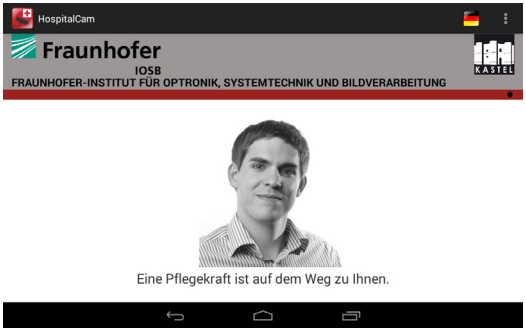
Zusätzlich wird die bereits in Abschnitt 7.2 vorgestellte Funktion zur Beobachtungstransparenz für das Krankenhausszenario angepasst. Dafür werden an den Kameras in den überwachten Gängen Tablets installiert, auf denen die NurseEye Transparenz App installiert ist. Diese ist in Abbildung 8.3 zu sehen. Wenn NurseEye aktiviert ist und die Daten der Kameras im Bereitschaftsmodus verarbeitet, wird dies den Betroffenen angezeigt (vgl. Abbildung 8.3a). Wechselt das System, weil ein Algorithmus meldet auf den Videodaten der Kamera einen Sturz erkannt zu haben, in den Beurteilungsmodus, signalisiert das Tablet dies entsprechend (vgl. Abbildung 8.3b). Sobald es zu einer Auswertung der Videodaten durch eine Pflegekraft kommt, folgt NurseEye dem sogenannten „Ich sehe, wer mich sieht“-Prinzip. Gleichzeitig dazu, dass eine Pflegekraft Zugriff auf Videodaten einer Kamera erhält, wird die Frontkamera ihres Smartphones aktiviert. Das durch die Kamera erfasste Bild der Pflegekraft wird dann an das Tablet der Kamera gesendet, durch die die Pflegekraft blicken kann (vgl. Abbildung 8.3c). Das hat zur Folge, dass immer, wenn ein Betroffener durch eine Pflegekraft beobachtet wird, dieser die Pflegekraft ebenfalls sehen kann. Neben der hohen Transparenz der Datenverarbeitung hat dies einen zusätzlichen medizinischen Grund.

Sollte sich die gestürzte Person verletzt haben, besteht die Gefahr, dass sie in Panik gerät und sich weitere Verletzungen zuzieht. Beispielsweise erleiden gerade ältere Patienten bei einem Sturz leicht eine Oberschenkelhalsfraktur.

Panische Bewegungen oder der Versuch alleine aufzustehen können schwerwiegende weitere Verletzungen zur Folge haben. Das „Ich sehe wer mich sieht"-Prinzip stellt hier sicher, dass die Pflegekraft schon aus der Ferne den Zustand des Gestürzten erkennen und schon auf dem Weg zum Unfallort beruhigend auf diesen einwirken kann. Dieser positive Effekt kann verstärkt werden, wenn neben dem Videosignal zusätzlich Audio zwischen dem Gestürzten und der Pflegekraft freigeschaltet wird.

(a) Bereitschaftsmodus

(b) Sturzalarm versendet



(c) Betrachtung durch eine Pflegekraft

Abbildung 8.3: Displays an den Kameras zeigen die Nutzung der Daten

8.4 Risikoanalyse und -behandlung

DSFA: Risikoanalyse und Behandlung Ist das Projekt umfassend beschrieben, werden mögliche Risiken für das Projekt und die Privatsphäre der Betroffenen analysiert. Wichtige Punkte in dieser Phase sind es, alle möglicherweise vorhandenen Risiken zu sammeln und zu dokumentieren. Anschließend werden Risiken in ihrer Schwere und der Eintrittswahrscheinlichkeit eingestuft und entschieden, welche Risiken getragen oder unbedingt vor der Einführung reduziert werden müssen.

Bisher existiert für die intelligente Videoüberwachung kein umfassender Bedrohungskatalog. Zu Beginn der Risikoanalyse und Behandlung wurde deshalb eine Angreiferanalyse erstellt. Diese betrachtet zuerst intelligente Videoüberwachungssysteme allgemein und geht später auf die speziellen Rahmenbedingungen von NurseEye ein.

Es werden die jeweiligen Begriffe verwendet, die der Definition in KASTEL folgen [KAS13]. Ein *Angreifer* ist demnach eine Person oder eine Personengruppe, die einen oder mehrere Angriffe durchführen. Ein *Angriff* ist die gezielte Realisierung einer Bedrohung. Eine *Bedrohung* eines Systems ist eine Möglichkeit, ein oder mehrere Sicherheitsziele gezielt zu beeinträchtigen. Ein *Sicherheitsziel* beschreibt eine Eigenschaft (…) eines Systems, die erfüllt werden muss, um bestimmte Güter vor bestimmten Bedrohungen zu schützen. Dabei deckt der Begriff Sicherheitsziel sowohl die klassischen Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit ab, sowie Datenschutz-Schutzziele die konkret auf technischen Datenschutz abzielen. *Güter* sind Ressourcen, die für mindestens einen Akteur einen realen oder ideellen Wert besitzen. Der Begriff der *Angreiferziele* ist nicht aus den KASTEL-Begriffsdefinitionen übernommen, sondern wurde neu definiert. Angreiferziele beschreiben, was einen Angreifer dazu bringt, bestimmte Angriffe gegen ein System vorzunehmen. Grundsätzlich ist davon auszugehen, dass ein Angreifer eine oder mehrere Bedrohungen für einen Angriff nutzt, um ein oder mehrere Sicherheitsziele zu verletzen und damit seine Angreiferziele zu erreichen. Die *Motivation* hinter

den Angreiferzielen kann sowohl der Angriff als Mittel sein, um beispielsweise mit gestohlenen Gütern einen Gewinn zu erzielen oder der Angriff kann der Zweck an sich sein, wenn der Angreifer nur das Ziel hat möglichst viel Chaos zu stiften. Die Arbeit von Beyerer und Geisler betrachtet Angreifer und ihre unterschiedlichen Motivationen genauer [BG15]. Abbildung 8.4 sammelt die *Angreifer*, welche *Bedrohungen* gegen das System sie darstellen und welche *Angreiferziele* sie verfolgen.

8.4.1 Bedrohungen

Videoüberwachungssysteme haben eine lange Geschichte. Frühe Installationen gehen zurück die 1940er Jahre. Für die meiste Zeit war der Einsatz analoger Technologie charakteristisch, die anderen Bedrohungen ausgesetzt ist, als die heutigen digitalen Systeme. Installateure von Videoüberwachungsanlagen haben häufig wenig Erfahrung im Umgang und Betrieb von IT-Systemen. Deshalb baut die Angreiferanalyse auf der Annahme auf, dass etablierte Verfahren zur IT-Sicherheit nicht durchgehend genutzt sind. Hingegen sind grundlegende Verfahren zur Bereitstellung physikalischer Sicherheit, wie Zugangskontrollen zur Zentrale, vorhanden. Geht man von dieser Annahme aus, können die Bedrohungen in sechs Gruppen eingeteilt werden:

- **Abhören: (engl.: tapping)**
  Diese Gruppe beinhaltet alle Angriffe, bei denen ein Angreifer die Kommunikation der Videoüberwachungsanlage abhört, aber kein eigenes Signal in das System einbringt. Angriffe dieser Art sind allgemein schwer zu erkennen, da sie das Verhalten des Systems nicht verändern. Wenn öffentlich zugängliche Informationen genutzt werden, um ein Angreiferziel zu erreichen, wird dies ebenfalls der Gruppe Abhören zugeordnet. Das wäre beispielsweise der Fall, wenn ein Supermarkt Monitore mit den Videoströmen ihrer Kameras installiert und ein Ladendieb diese Information nutzt, um zu lernen, in welchen Bereichen er unbeobachtet ist.
  Beispiele: Abhören von IP-Netzwerkverkehr, Mitscheiden von Daten aus dem WLAN-Verkehr

- **Signalmanipulation: (engl.: signal manipulation)**
  Grundsätzlich wäre jede Person, die sich in einem videoüberwachten Bereich befindet, in der Lage eine Reihe von Angriffen gegen die Signalverarbeitung des Systems durchzuführen. Typischerweise haben Angriffe dieser Gruppe größere Folgen für das System, lassen sich aber auch einfacher erkennen. Mögliche Angriffe variieren in Folgen und Aufwand zwischen dem einfachen Zerstören von Kameras bis hin zum Einspeisen manipulierter (Video-) Daten in das Kommunikationsnetzwerk.
  Beispiele: Beschädigung von Kameras, Manipulation der Kameraausrichtung, Einspeisen manipulierter Videoströme

- **Passiver Missbrauch: (engl.: passive misuse)**
  Missbrauch durch den Operator oder andere Personen die Zugriff auf das System erhalten, stellt durch die höhere Funktionalität der intelligenten Systeme eine große Gefahr dar. Unter passivem Missbrauch werden alle Angriffe gruppiert, in denen ein System gegen seinem eigentlichen Einsatzzweck genutzt wird, ohne dafür das System zu manipulieren.
  Beispiele: Bespitzelung von Personen, Voyeurismus

- **Aktiver Missbrauch: (engl.: active misuse)**
  Aktiver Missbrauch eines intelligenten Videoüberwachungssystems stellt eine viel höhere Gefahr für die Betroffenen dar, als dies bei konventionellen Systemen der Fall ist. Angreifer können hier erweiterte Systemfunktionalität, etwa das automatische Verfolgen von Personen über mehrere Kameras hinweg, benutzten, um ihre Zwecke zu erreichen. Als aktiver Missbrauch wird es auch verstanden, wenn absichtlich vom System erkannte Situationen verworfen werden.
  Beispiele: Missbrauch der Personenverfolgung, detektierte Notfälle absichtlich verwerfen

- **Archivmanipulation: (engl.: data manipulation)**
  Mit Zugang zum Videoarchiv kann ein Angreifer beliebig Daten in diesem verändern. Der Angreifer kann Daten vollständig löschen oder durch

manipulierte Versionen ersetzten. Außerdem kann er Daten vom System kopieren und für seine eigenen Zwecke missbrauchen. Da durch die Manipulation des Archivs das Verhalten des Systems nicht direkt beeinflusst wird, ist es schwer zu erkennen.
Beispiele: Löschen von Beweismitteln, Manipulieren von Beweismitteln

- **Sabotage: (engl.: sabotage)**
  Sabotage deckt alle Änderungen am Systemverhalten zum Vorteil eines Angreifers ab. Einfache Änderungen wären das Deaktivieren von einzelnen Kameras oder Algorithmen zur Videoauswertung. Aufwendige Angriffe können darin bestehen, eigene Algorithmen zur Videoanalyse in das System einzuschleusen. Im Gegenzug zur Signalmanipulation oder der Archivmanipulation wird bei der Sabotage das interne Arbeiten des Systems gestört und nicht die Sensoren oder deren Daten verändert.
  Beispiele: Deaktivierung von einzelnen Sensoren, Ändern oder Hinzufügen von Algorithmen zur Videoauswertung

8.4.2 Angreifer

Neben den unterschiedlichen Angriffsarten lassen sich auch die Angreifer klassifizieren. Es können drei Gruppen unterschieden werden:

- **Externer Angreifer**
  Jede Person in einem überwachten Bereich kommt als Angreifer gegen das System in Frage. Unter der Annahme, dass grundlegende Sicherheitsprinzipien, wie etwa Zugangskontrollen zu den Servern und Betriebsräumen, eingesetzt werden, sind externe Angreifer stark in ihrer Mächtigkeit beschränkt. Sie können zum Erreichen ihrer Ziele lediglich auf *Abhören* und *Signalmanipulation* zurückgreifen.

- **Böswilliger Operator**
  Intelligente Videoüberwachungssysteme bieten dem Operator eine breite Palette an Funktionen an. Diese Funktionen können, entweder aus Versehen, aus Langeweile oder motiviert durch inneren oder äußeren Druck,

missbraucht werden. Unabhängig von der Motivation kann ein böswilliger Operator auf die gleichen Angriffe zurückgreifen wie der externe Angreifer und zusätzlich *passiven Missbrauch* und *aktiven Missbrauch* des Systems nutzen. Um die Gruppen klarer zu trennen, wird angenommen, dass ein Operator zwar auf ein vorhandenes Videoarchiv zugreifen, dieses aber nicht verändern oder kopieren kann. Diese Möglichkeit ist nur Administratoren gegeben.

- **Böswilliger Administrator**
  Der böswillige Administrator hat die höchste Stufe an Zugangsberechtigungen und stellt damit den mächtigsten Angreifer gegen das System dar. Wie der externe Angreifer kann er auf Abhören und Signalmanipulation zurückgreifen. Es muss ebenfalls davon ausgegangen werden, dass ein Administrator Zugang zu den Bediengeräten des Operators hat. Er kann also ebenfalls passiven und aktiven Missbrauch des Systems einsetzen. Zusätzlich hat er durch den Zugang zu Rechner- und Serverräumen die Möglichkeit, *Archivmanipulation* zu begehen und das System sowie die Kommunikationsinfrastruktur durch *Sabotage* zu verändern.

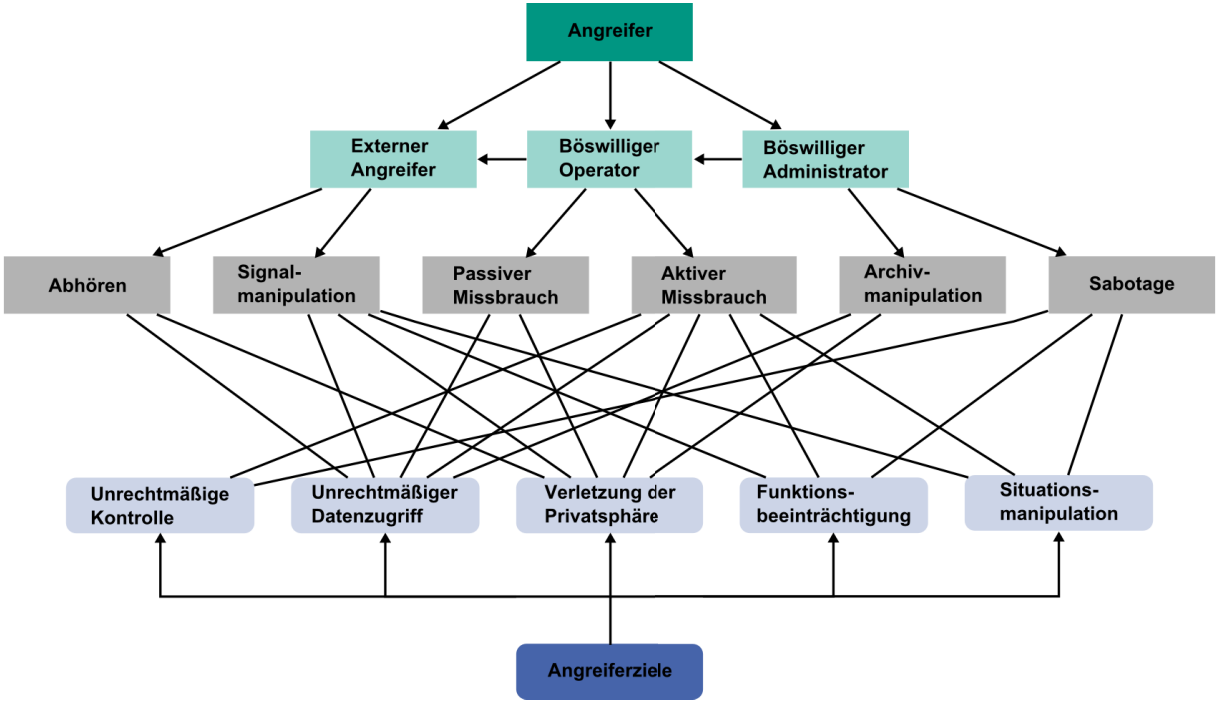


Abbildung 8.4: Angreiferanalyse

8.4.3 Angreiferziele

Wie die Bedrohungen und die Angreifer lassen sich auch die Angreiferziele in verschiedene Gruppen unterteilen. Diese sind nicht zwingend unabhängig voneinander. Es kann gut sein, dass ein Angreifer zuerst *unrechtmäßige Kontrolle* über ein System erhalten muss, um sein eigentliches Ziel *Situationsmanipulation* zu erreichen.

- **Unrechtmäßige Kontrolle**
  Wenn ein Angreifer in der Lage ist das System (teilweise) zu kontrollieren, kann er es seiner Vorstellung entsprechend manipulieren. So kann er gefälschte Steuerbefehle an eine PTZ-Kamera senden, um Bereiche einzusehen, die von besonderem Interesse für ihn sind oder umgekehrt eine Kamera so drehen, dass eine besondere Region nicht unter Kameraüberwachung steht.

- **Unrechtmäßiger Datenzugriff**
  Unrechtmäßig erlangte Daten können von einem Angreifer genutzt werden, um Bereiche auszukundschaften, während er selbst unbeobachtet bleibt. Immer wenn ein böswilliger Operator oder Administrator ein Videoüberwachungssystem außerhalb des definierten Zweckes nutzt, zählt dies ebenfalls als unrechtmäßiger Datenzugriff.

- **Verletzung der Privatsphäre**
  Auch wenn alle Überwachungssysteme in einem gewissen Rahmen einen Eingriff in die Privatsphäre darstellen, ist dieser notwendig, um den rechtlich geprüften Überwachungszweck zu erreichen und kann nicht ganz vermieden werden. Wenn die Verletzung der Privatsphäre das Angreiferziel ist, versucht der Angreifer den Eingriff auszuweiten und damit seine Zwecke zu verfolgen. Sein Nutzen daraus kann von einfachem Voyeurismus bis zu komplexen mehrstufigen Plänen reichen. In einem der bekannteren Angriffe wurde verheiratete Männern mit Videoaufnahmen erpresst, auf denen ersichtlich ist, dass sie bestimmte Nachtclubs besuchen [TL97].

- **Funktionsbeeinträchtigung**
  Funktionsbeeinträchtigung ist eines der einfachsten Angreiferziele, die ein Angreifer haben kann. Er möchte die Funktion des Systems beeinträchtigten, entweder um unbeobachtet zu sein oder aus reinem Vandalismus. In der intelligenten Videoüberwachung sind jedoch auch ausgefallenere Ziele vorstellbar. Ein Angreifer könnte nicht das Ziel haben, das gesamte System lahmzulegen, sondern gezielt einen einzelnen Algorithmus zur Gefahrendetektion zu stören. So könnte er beispielsweise den Algorithmus zur Gewaltdetektion in einem Bereich stören, in dem er plant jemanden zu überfallen.

- **Situationsmanipulation**
  Die Situationsmanipulation ist eng verwandt mit der Funktionsbeeinträchtigung, sie ist jedoch weniger offensichtlich. Ein Angreifer könnte dazu gefälschte Videodaten oder Ergebnisse eines Algorithmus zur Videoauswertung in das System einspeisen, um entweder zu verhindern, dass ein Ereignis korrekt erkannt wird oder den Operator durch eine hohe Anzahl an Fehlalarmen abzulenken. Situationsmanipulation kann ebenfalls als Teil aufwendiger Mehrparteienangriffe genutzt werden, die später im Kapitel betrachtet werden.

8.4.4 Zwischenfazit der Angreiferanalyse

Betrachtet man die gesammelten Bedrohungen, Angreifer, und Angreiferziele lassen sich diese in zwei Gruppen einteilen: Es gibt Angriffsszenarien, die bereits aus dem Bereich der IT-Sicherheit bekannt sind, und solche, die neu und spezifisch für die intelligente Videoüberwachung sind. Aus einem technischen Standpunkt handelt es sich bei intelligenten Videoüberwachungssystemen um verteilte IT-Systeme. Für diese Systeme existieren bereits vielfältige Verfahren, um Gefahren zu minimieren und abzuwehren. Beispielhaft seien der BSI-IT-Grundschutz [Buno6] und Common Criteria for Information Technology Security Evaluation [CC] als Verfahren genannt, die sich eignen, komplexe IT-Systeme und ihre Komponenten abzusichern. Werden bekannte IT-Sicherheitsstandards

konsequent umgesetzt, ist bereits eine Vielzahl der möglichen Angriffe deutlich erschwert. Um einen grundlegenden Schutz zu erreichen, sollten mindestens die folgenden Sicherheitsmaßnahmen genutzt werden:

- **Zugangskontrollen zur Infrastruktur**
  Zugang zu den Serverräumen ist auf die Administratoren zu beschränken. Nur Operatoren dürfen Zugang zu den Räumen haben, von wo das Überwachungssystem bedient wird.
- **Benutzerauthentifizierung**
  Das System lässt sich durch den Operator nur bedienen, wenn sich dieser zuvor an dem System angemeldet hat.
- **Verschlüsselung**
  Alle Sensoren müssen Daten direkt nach der Erfassung verschlüsseln und signieren, bevor diese über das Netzwerk übertragen werden.
- **Geräteauthentifizierung**
  Nur vertrauenswürdige Systeme erhalten Zugriff zum Netzwerk.
- **Netztrennung**
  Das Netzwerk des Überwachungssystems ist vollständig getrennt von anderen Netzen.

Da es sich bei diesen Methoden um den Stand der Technik handelt, wird nicht näher auf die Angriffe und Schutzmethoden eingegangen, sondern direkt spezifische Angriffe gegen intelligente Videoüberwachung untersucht.

8.4.5 Spezifische Angriffe gegen (intelligente) Videoüberwachung

Sind bekannte Angriffe gegen verteilte IT-Systeme behandelt, bleiben einige Angriffe übrig, die spezifisch für die (intelligente) Videoüberwachung sind. Diese werden im weiteren Verlauf des Kapitels kurz betrachtet und ein jeweils ein generischer Lösungsansatz präsentiert, weiter wird auf die Situation von NurseEye eingegangen.

Funktionsbeeinträchtigung durch falsche Ereignisse

Die Systemfunktionalität „kritische Ereignisse“ automatisch zu detektieren kann von einem Angreifer missbraucht werden. Wenn der Operator durch eine hohe Anzahl von vermeintlichen Fehlalarmen das Vertrauen in das System verliert oder indem der Operator durch gezielt ausgelöste Ereignisse von wichtigen Ereignissen abgelenkt wird, lässt sich die Funktion des Systems nachteilig beeinträchtigen.

Ähnlich wie das missbräuchliche Auslösen von Feuermeldern gibt es auf technischer Ebene keinen Schutz gegen solche Angriffe. Durch eine strikte Verfolgung und hohe Strafen für Personen, die absichtlich falsche Alarme erzeugen, lassen sich die Angriffe jedoch organisatorisch eingrenzen. Es kann jedoch vermutet werden, dass ähnlich wie bei Feuermeldern und Notbremsen in Zügen es nur zu wenigen Fällen von Missbrauch kommen wird.

Ein ähnliches Problem entsteht, wenn das System durch unzureichende Qualität der Daten von sich aus fehlerhafte Alarme versendet. Ab einer gewissen Menge an Fehlalarmen wird der Operator das Vertrauen in das System verlieren und Alarme nicht mehr mit der benötigten Sorgfalt bearbeiten. Im Zweifelsfall sollten Bereiche, in denen keine gute Qualität der Erkennung erreicht werden kann, deaktiviert werden, bevor dadurch das Vertrauen in das System sinkt.

NurseEye Szenario Das Argument, dass Notfallknöpfe bisher wenig missbraucht werden, gilt besonders für den Einsatz in Krankenhäusern. Trotz einer intensiven Recherche konnten keine dokumentierten Fälle gefunden werden, bei denen Notfallmelder in Krankenhäusern missbräuchlich genutzt wurden. Da bei NurseEye eine Alarmmeldung über einen Sturz nicht in einer Zentrale verarbeitet wird, sondern an räumlich nahe Pflegekräfte gesendet wird, ändert an der vermuteten Missbrauchswahrscheinlichkeit nichts.

Die Gefahr von Fehlalarmen durch unzureichende Datenqualität muss in NurseEye sorgfältig untersucht werden. Die Detektion von Stürzen stellt eine hohe Herausforderung für die Bildauswertung dar. Sind die Sensoren nicht performant oder das Umfeld schwierig, kann es leicht zur Situation kommen,

dass sehr viele Fehlalarme entstehen. Es sollte deshalb ausgewertet werden, ob und in welchen Kameras diese auftreten, um bei Bedarf nachzubessern.

Bewertung:

Schweregrad = begrenzt
Eintrittswahrscheinlichkeit = erheblich

Missbrauch von Livedaten

Wenn ein Operator Zugriff auf Livedaten hat, kann er diese auf unterschiedliche Art und Weise missbrauchen. Er kann sie zu voyeuristischen Zwecken nutzen, Bewegungsprofile von Personen erstellen oder die Videodaten zur Erpressung nutzen. Auch wenn solche Angriffe schon bei konventionellen Videoüberwachungssystemen möglich waren, nehmen sie zu Zeiten von hochauflösenden digitalen Videodaten an Bedeutung zu.

Zur gleichen Zeit bieten intelligente Videoüberwachungssysteme Methoden zur Bildmanipulation, die Angriffe verhindern oder zumindest deutlich erschweren. Videodaten sollten, wenn immer möglich, dementsprechend geschützt und dem Operator nur bei besonderen Ereignissen oder auf direkten Wunsch zur Verfügung gestellt werden. Durch Loggen und anschließende Audits können Angriffe stark eingeschränkt werden. Wenn die Detektion von kritischen Ereignissen ausreichend zuverlässig ist, ist es ebenfalls denkbar, dem Operator nur bei aktiven Alarmen Zugriff auf Livedaten zu gewähren und alternativ nur eine Übersicht über das Gelände anzubieten.

NurseEye Szenario In NurseEye wurde aus verschiedenen Gründen darauf verzichtet, den Pflegekräften uneingeschränkten Zugriff auf die Livedaten zu geben. Da bei NurseEye immer nur dann Zugriff erlaubt wird, wenn auf einer Kamera ein Sturz erkannt wurde, wird das Potential für Missbrauch stark eingeschränkt. Eine verbleibende Möglichkeit die Livedaten zu missbrauchen, liegt im absichtlichen Auslösen einer Sturzmeldung. So kann eine Pflegekraft absichtlich vor der Kamera stürzen, an deren Livedaten sie interessiert ist. Durch ihre räumliche Nähe zur Kamera ist sichergestellt, dass der Alarm zuerst an ihr

Smartphone gesendet wird. Wenn sie den Sturz bestätigt, hat sie anschließend Zugriff auf die Livedaten einer Kamera bis sie den Vorfall als beendet erklärt. Dieser Angriff ist jedoch leicht durch die Auswertung von Logdateien zu erkennen und in seinen Auswirkungen stark eingeschränkt. Da ein Smartphone in NurseEye immer nur einen Alarm bearbeiten kann, skaliert der Angriff nicht, und mit einem Smartphone kann die Pflegekraft nur Zugriff auf eine der Kameras bekommen. Weiter würde das zur Kamera gehörende Display alle Personen darüber informieren, dass gerade ein Zugriff auf die Livedaten stattfindet.

Bewertung:

Schweregrad = geringfügig
Eintrittswahrscheinlichkeit = begrenzt

Missbrauch des Videoarchivs

Der Missbrauch des Videoarchivs stellt potentiell schwere Folgen für die Betroffenen dar. Die gespeicherten Daten können von einem böswilligen Operator oder Administrator auf gleiche Art und Weise missbraucht werden wie die Livedaten. Verfügt das intelligente Überwachungssystem über erweiterte Funktionen, um das Archiv zu verarbeiten, beispielsweise einer biometrischen Personensuche, werden mögliche Folgen für die Privatsphäre schlimmer. Die Chance, den Angriff frühzeitig zu erkennen, erscheinen gering zu sein.

Als Schutz vor Angriffen ist deshalb zuerst zu prüfen, ob ein Videoarchiv notwendig ist. Langzeitarchive sollten nur angelegt werden, wenn die möglichen Vorteile einen potentiellen Eingriff in die Privatsphäre deutlich übertreffen. Diese Maßnahme ist sehr stark von Anwendungsszenario abhängig. Auf einem Flughafen kann die Möglichkeit schwere Straftaten im Nachhinein aufklären zu können, eine Speicherung über lange Zeiträume rechtfertigen. Ein Krankenhaus, das mit intelligenter Videoüberwachung Stürze erkennen will, kann sich jedoch entscheiden, gar keine Archivierung der Videodaten vorzunehmen. Wenn Videomaterial gespeichert wird, sollte es verschlüsselt sein und nur restriktiv genutzt werden können. Zugriff durch die Administratoren ist durch organisatorische Maßnahmen, beispielsweise dem Vier-Augen-Prinzip

einzuschränken. Zugriff durch die Operatoren sollte auf einen angemessenen Zeitrahmen reduziert und geloggt werden. Ein Audit der Zugriffe auf das Archiv kann auch hier helfen, um Angriffe zu erkennen und entsprechend zu reagieren.

NurseEye Szenario In seinem aktuellen Entwicklungsstand wird in NurseEye kein Langzeitarchiv angelegt. Zur algorithmischen Detektion von Stürzen existieren im System kurze Ringpuffer mit den Bildern der letzten 15 Sekunden für jede Kamera. Diese werden, so lange keine Sturzdetektion vorliegt, nicht gesichert, sondern immer das älteste Bild überschrieben. Wird ein Sturz erkannt, wird der Puffer kurzfristig gespeichert und der zuständigen Pflegekraft zur Bewertung zu Verfügung gestellt. Sobald eine Sturzmeldung vollständig bearbeitet wurde, wird dieser Puffer gelöscht. Zusammen mit Pascal Birnstill wurde außerdem ein System erarbeitet, damit die bewertende Pflegekraft keine Möglichkeit hat, die ihr zur Bewertung zur Verfügung gestellten Videodaten zu verbreiten [KBB16a]. Somit sollte ein Missbrauch des Videoarchivs ausgeschlossen sein.
Bewertung:
Schweregrad = geringfügig
Eintrittswahrscheinlichkeit = geringfügig

Missbrauch der Systemfunktionalität

Die höchste Gefahr für die Privatsphäre Betroffener entsteht durch die erweiterte Funktionalität von intelligenter Videoüberwachung. Funktionen, wie das automatische Verfolgen einer Person über mehrere Kameras hinweg, haben tiefe potentielle Eingriffe zur Folge. Durch die interaktive Überwachung (vgl. Abschnitt 5.2) können hier Risiken reduziert werden. Das Stufenmodell erlaubt es, erweiterte Funktionalität nur gezielt freizuschalten, wenn entweder ein Algorithmus ein verdächtiges Verhalten beobachtet hat oder wenn es direkt vom Operator angefordert und geloggt wird. Dies schränkt die Möglichkeiten eines Missbrauchst deutlich ein und erhöht gleichzeitig das Risiko für einen böswilligen Operator entdeckt zu werden. Zusätzlich stellten Birnstill und Pretschner ein Verfahren vor, das ein noch feingranulareres Regeln der Funktionalität zulässt [Bir13]. Ihr System erlaubt es nicht nur, auf unterschiedlichen

Stufen verschiedene Funktionalität anzubieten, sondern bindet die Freigabe an betroffene Personen.

NurseEye Szenario Im Krankenhausszenario ist keine Systemfunktionalität vorhanden, die hohes Missbrauchspotential bietet. Die algorithmische Sturzdetektion ist die einzige Form der automatischen Datenverarbeitung und erlaubt keinen bisher erkannten Missbrauch.

Bewertung:

Schweregrad = begrenzt

Eintrittswahrscheinlichkeit = geringfügig

Mehrparteienangriffe

Wenn ein Team von koordinierten Angreifern vorhanden ist, verlieren einige der vorgestellten Sicherheitsmaßnahmen ihre Wirkung.

Ein Beispiel eines solchen Angriffs ist ein System, das die automatische Verfolgung von Personen über mehrere Kameras hinweg nur dann erlaubt, wenn vorher Gewalt erkannt wurde. Ein Team aus einem Angreifer vor Ort und einem böswilligen Operator können diesen System wie folgt missbrauchen, um eine dritte Person zu verfolgen: Der Angreifer vor Ort löst in der unmittelbaren Umgebung der dritten Person die Gewaltdetektion aus. Der Operator nutzt die eintreffende Gewaltmeldung und markiert die dritte Person für die automatische Verfolgung. Nun kann das System genutzt werden, um die dritte Person über das Gelände zu verfolgen. Da die Verfolgung nach einer automatischen Gewaltdetektion und nicht durch den Operator angefordert wurde, wäre sie auch in Logdateien nicht auffällig.

Während dieser und ähnliche Angriffe theoretisch möglich sind, ist ihre Bedeutung für die intelligente Videoüberwachung unklar. Da es bisher erst wenige intelligente Videoüberwachungssysteme gibt und diese nicht durch den interaktiven Ansatz (vgl. Abschnitt 5.2) geschützt werden, ist unklar welche Bedeutung Mehrparteiangriffe haben werden.

NurseEye Szenario Im NurseEye Szenario konnte kein kritischer Mehrparteienangriffe identifiziert werden. Es ist zwar vorstellbar, dass ein Angreifer absichtlich einen Sturzalarm auslöst und so seinem Komplizen Zugang zu den erfassten Videodaten gibt. Da sich der Angreifer dazu aber unmittelbar in der Nähe der zu beobachteten Person befinden muss, ist der Angriff in seiner Wirkung sehr begrenzt.

Bewertung:

Schweregrad = begrenzt
Eintrittswahrscheinlichkeit = begrenzt

Komposition von anonymisierten Informationsquellen

Dass die Komposition von anonymisierten Datenquellen ein potentiellen Eingriff in die Privatsphäre zur Folgen haben kann, ist ein bekanntes Problem. So kann beispielsweise die Komposition zweier anonymisierter Datenbanken die Anonymisierung vollständig aufheben [GKS08]. Ähnliche Probleme können auftreten, wenn bereits datenschutzfreundliche Datenquellen einer intelligenten Videoüberwachung kombiniert werden.

Ein einfaches Beispiel ist wie folgt: Aus Sicherheitsgründen wird auf einem großen Firmengelände die Position der Mitarbeiter mittels Kameras erfasst. Die Videodaten werden dabei von Algorithmen verarbeitet, die lediglich die Position der Mitarbeiter extrahieren. Die Darstellung erfolgt auf einer Übersichtskarte des Geländes, auf dem anonyme Marker die Position der einzelnen Mitarbeiter darstellen. Der Operator hat niemals Zugriff zu den Videoströmen der Kameras. Diese Darstellung hat somit keinen signifikanten Einfluss auf die Privatsphäre der Mitarbeiter. Die zweite Informationsquelle ist eine Kamera am einzigen Eingang am Firmengelände. Der Operator nutzt diese Kamera, um zu prüfen, welche Personen Zugang zum Gelände haben. Da es sich nur um eine Kamera handelt und diese nur einen sehr kleinen Bereich abdeckt, ist auch hier kein großer Eingriff in die Privatsphäre zu beobachten. Trotzdem stellt die Komposition der beiden Informationsquellen einen großen Eingriff in die Privatsphäre dar. Betritt ein Mitarbeiter am Morgen das Gelände wird seine

Position mit einem Marker auf der Karte markiert. Der Operator kann den kurzen Moment am Eingang nutzen, um dem anonymen Marker des Mitarbeiters dessen Identität zuzuordnen. Auch wenn die Position fortan nur durch einen Marker dargestellt wird, weiß der Operator jederzeit, wo sich ein bestimmter Mitarbeiter befindet.

Im Gegensatz zu anonymisierten Datenbanken existieren bei Multimediadaten noch keine umfassenden Erfahrungen darüber, wann solche Eingriffe entstehen können.

NurseEye Szenario Das Problem der Komposition hat für das Design von NurseEye hohe Bedeutung. Ursprünglich war geplant, den Pflegekräften im Bereitschaftsmodus von NurseEye Zugriff zu einer Karte ihrer Station mit anonymen Markern für die detektierten Personen zu geben. Dies würde ihnen beispielsweise ermöglichen, Arbeiten in abgelegenen Vorbereitungsräumen zu verrichten und nur zu ihren Stationen zurückzukehren, wenn sich dort hilfesuchende Personen befinden. Die Idee wurde verworfen als erkannt wurde, wie einfach diese Anonymisierung aufgelöst werden kann und somit der Pflegekraft eine durchgängige Verfolgung von Patienten, Besuchern und anderen Mitarbeitern erlauben würde.

Bewertung:

Schweregrad = erheblich
Eintrittswahrscheinlichkeit = begrenzt

Hintergrundwissen des Operators

Die Gefahr, die durch das Hintergrundwissen entsteht, ist vergleichbar zu den Szenarien der Komposition anonymer Quellen. Der Operator hat eine oder mehrere anonyme oder pseudonyme Datenquellen und kann diese Dank seines Hintergrundwissens personalisieren.

Als einfaches Beispiel kann wieder das Szenario der Firma genutzt werden: Aus Sicherheitsgründen wird auf einem großen Firmengelände die Position der Mitarbeiter mittels Kameras erfasst. Die Videodaten werden dabei von

Algorithmen verarbeitet, die lediglich die Position der Mitarbeiter extrahieren. Die Darstellung erfolgt auf einer Übersichtskarte des Geländes, auf dem anonyme Marker die Position der einzelnen Mitarbeiter darstellen. Der Operator hat niemals Zugriff zu den Videoströmen der Kameras. Unter Umständen benötigt der Operator gar keine weitere externe Datenquellen, sondern kann rein mit seinem Hintergrundwissen zu den anonymen Markern eine Person zuordnen. Kennt er beispielsweise die Schichtpläne, kann er bereits stark einschränken, welche Personen auf dem Gelände sein können. Werden bestimmte Bereiche, beispielsweise Einzelplatzbüros oder bestimmte Maschinen, nur von einer Person genutzt, kann der Operator gut darauf schließen, welche Person sich hinter einem Marker verbirgt. Welche Schlüsse der Operator mit seinem Hintergrundwissen und den ihm zur Verfügung gestellten Datenquellen ziehen kann, ist dabei sehr schwer abzuschätzen und kann tiefe Eingriffe in die Privatsphäre nach sich ziehen. Hier besteht bisher sehr wenig Erfahrung darin, wie die Bedrohung zu bewerten ist und wie sie vermieden werden kann. Es wird deutlich, dass Sichten auf Daten nicht nur danach bewertet werden müssen, worauf sie Zugriff erlauben, sondern auch betrachtet werden muss, welches Hintergrundwissen der Betrachtende hat.

NurseEye Szenario Die ursprüngliche Idee, den Pflegekräften Zugriff auf eine Karte mit anonymen Markern der Personendetektionen zu geben, wurde bereits wegen der Gefahr der Komposition von Datenquellen verworfen. Diese Funktionalität wäre auch aufgrund von Angriffen mit Hintergrundwissen kritisch. Da Pflegekräfte genau wissen, welche Patienten in welchen Zimmern sind und ein Vorgesetzter die Mitarbeiter beispielsweise daran erkennen kann, dass diese ins Stationszimmer gehen, wäre der Schutz nur unzureichend gewesen.
Bewertung:
Schweregrad = erheblich
Eintrittswahrscheinlichkeit = geringfügig

Fazit: Risikoanalyse und Behandlung

In der Angreiferanalyse wurden eine Reihe möglicher Missbrauchsarten identifiziert, die für die intelligente Videoüberwachung relevant sind. Abbildung 8.5 fasst diese in dem Bewertungsschema nach CNIL zusammen. Die Funktionsbeeinträchtigung durch falsche Ereignisse und die Komposition von anonymen Quellen wurden als besonders kritisch erkannt und bereits erste Schritte unternommen, um ihnen zu begegnen. Damit liegt keines der identifizierten Risiken in einem Bereich, der nicht akzeptiert werden kann.

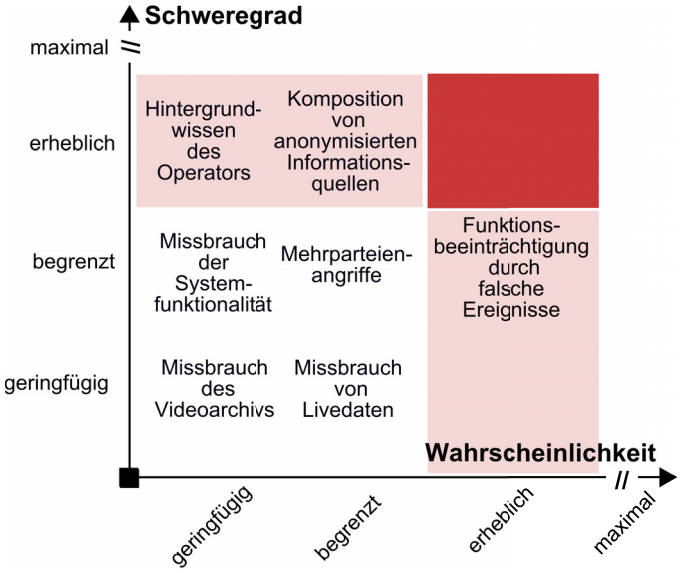


Abbildung 8.5: Identifizierte Missbrauchsrisiken für NurseEye

8.5 Implementierung Prototyp

Ergebnisdokumentation Nach der der Risikoanalyse und -behandlung geht eine DSFA in ihren letzten Schritt Ergebnisdokumentation über. Dazu wird ein Register geführt, welches die Problembeschreibung, mindernde oder vermeidende Maßnahmen sowie Änderungen am Projekt enthält. Weiter findet eine Auflistung der Risiken für die Privatsphäre statt, die nicht vollständig behandelt wurden und welche damit verbleibenden Restrisiken existieren.

Zum Abschluss der Entwicklung wurde ein Prototyp von NurseEye implementiert. Dieser wird zum einen dazu genutzt, die entwickelten Verfahren auf ihre Funktionalität zu testen und zum anderen für die abschließende Evaluation als Demonstrator eingesetzt. In diesem Abschnitt soll untersucht werden, wie die an NurseEye gestellten Anforderungen mit der NEST-Architektur (vgl. Abschnitt 2.1.4) erreicht werden können.

In Abbildung 8.6 wird die für das NurseEye Szenario konfigurierte NEST-Architektur dargestellt. Auf der Ebene der *Signalverarbeitung* sind drei Module aktiv. Eines ist für die Befüllung des Ringpuffers mit den letzten 15 Sekunden Videomaterial beauftragt. Er reicht automatisch für jede Kamera das aktuellste Bild vom Multiplexbus an das *Kurzzeitarchiv* weiter, wo es für die konfigurierte Zeit gespeichert wird.

Das zweite aktive Modul ist für die Lokalisation der mobilen Endgeräte zuständig. Da diese indirekt auf die Position des Pflegepersonals schließen lassen und somit zur Mitarbeiterüberwachung missbraucht werden könnten, sind diese Daten nur für das System lesbar. Andere Pflegekräfte oder gar die Vorgensetzen können diese Daten nicht einsehen (☑ Req[07]). Es erfasst periodisch die aktuelle Position aller in NurseEye aktiven Endgeräte und übermittelt die Position an die Modellwelt.

Das dritte aktive Modul ist die *Sturzdetektion*. Für die Videodaten jeder Kamera ist jeweils eine eigene Instanz der Sturzerkennung aktiv. Das erlaubt zum einen eine individuelle Konfiguration der Sturzerkennung und zum andern vermeidet es Leistungsprobleme auf den ausführenden Servern. Die Trennung

zwischen Signalverarbeitung und Informationsverwaltung erlaubt es, dass je Kamera ein eigener Rechner für die Auswertung zuständig ist und die Ergebnisse an einem zentralen Ort gesammelt werden.

Es fällt auf, dass in der vorliegenden Architektur keine Personendetektion vorhanden ist. Da die Gefahr für einen Missbrauch dieser Funktionalität als höher als ihr Nutzen eingeschätzt wurde, erfasst NurseEye nicht die aktuelle Position von Personen. Die Sturzerkennung prüft zwar im ersten Schritt der Bildauswertung, ob sich darin eine Person befindet, das Ergebnis dieser Beobachtung wird aber nicht an die Ebene zur *Informationsverwaltung* gesendet. Wenn kein akuter Sturz im System vorliegt, werden keine Informationen über Betroffene außerhalb der Signalverarbeitung gehalten (☑ Req[13]).

Detektiert ein Algorithmus einen Sturz, sendet er einen Tupel bestehend aus der ID der verarbeiteten Kamera und dem Ereignis über den Ereignisbus (☑ Req[01]). Die *Modellwelt* speichert die Sturzmeldungen und hält zusätzlich den aktuellen Zustand (Detektion, Bewertung, Bearbeitung, Beendet) und ggf. den zuständigen Bearbeiter eines Alarms vor. Die Sturzerkennung ist der einzige Grund, warum es in NurseEye zu einer Zustandsänderung kommen kann. Das Pflegepersonal hat keine Möglichkeit diese zu erzwingen (☑ Req[15]). Damit können sich Patienten sicher sein, dass es zu keinen ungerechtfertigten Eingriffen in ihre Privatsphäre kommt (☑ Req[08]).

Jeder Zustandsänderung eines Alarms wird über den *Dienstebus* kommuniziert. Sobald ein neuer Alarm über den Dienstebus kommuniziert wird, sichert das Kurzzeitarchiv den gesamten Ringpuffer der entsprechenden Kamera und alle weiteren Videodaten dieser Kamera bis der Alarm Abgeschlossen wird. Auf der Ebene der *Informationsverwertung* kommt es beim Eingehen neuer Alarme ebenfalls zu Zustandsänderungen. Der Dienst *Transparenz für Betroffene*, verarbeitet die Meldung des neuen Alarms und informiert auf dem der entsprechenden Kamera zugeordneten Display über den erkannten Sturzalarm (Req[10] teilweise erfüllt). Der Dienst *Alarmierung von Pflegekräften* ist ebenfalls von der Zustandsänderung betroffen. Wenn ein neuer Alarm eingeht, gleicht er die Position der Sturzmeldung und der mobilen Endgeräte ab. Es werden genau die mobilen Endgeräte alarmiert, die möglichst nahe am Unfallort sind und aktuell

noch für keinen Alarm zuständig sind (☑ Req[02], ☑ Req[04], ☑ Req[05]). Sollte bis zum Ablauf einer bestimmten Wartezeit keines der angesprochenen Geräte den Alarm bestätigt haben, werden auch weiter entfernte Geräte alarmiert.

Sobald eine Pflegekraft den Alarm auf ihrem mobilen Endgerät annimmt, wird dies wieder über den Dienstebus kommuniziert. Damit erlöschen die Alarme auf allen weiteren Endgeräten und die Modellwelt ändert den Status des Alarms zu Bewertung. Das mobile Endgerät kann nun auf die anonymisierten Daten aus dem Kurzzeitarchiv zugreifen.

Die Pflegekraft prüft nun auf ihrem mobilen Endgerät, ob tatsächlich ein Sturz vorliegt oder ob ein Fehler in der algorithmischen Bildauswertung aufgetreten ist (☑ Req[06]). Nur wenn die Pflegekraft die Sturzmeldung als korrekt bestätigt, wechselt das System in den Status Bearbeitung (☑ Req[11]). Die gemeinsame Arbeit mit Pascal Birnstill behandelt ausführlich, wie dabei sichergestellt wird, das keine Videodaten vom mobilen Endgerät exportiert werden (☑ Req[09]) [KBB16a]. Wenn eine Sturzmeldung in Bearbeitung ist, kann die Pflegekraft auf die Livedaten der Kamera zugreifen, die den Sturz gefilmt hat. Diese Daten sollen der Pflegekraft dabei helfen, den Zustand der gestürzten Person besser bewerten zu können und somit effektiver zu helfen. Mit dem Zugriff auf die Kamera aktiviert das mobile Endgerät ebenfalls seine eigene Frontkamera und gibt den Datenstrom für den Dienst Transparenz für Betroffene frei. Sobald die Pflegekraft Zugriff auf Livedaten einer Kamera hat, zeigt das Display für den Betroffenen das Gesicht der Pflegekraft an (☑ Req[10]).

Ist der gemeldete und bestätigte Sturz erfolgreich bearbeitet, oder wurde ein Alarm als Fehlalarm markiert, sendet das mobile Endgerät des Bearbeiters Beendet über den Dienstebus. Daraufhin wechselt das Display an der Kamera der Betroffenen wieder in den Ausgangszustand und informiert über die automatische Bildauswertung. Das Kurzzeitarchiv empfängt die Nachricht und löscht die gesamten für diese Sturzmeldung gespeicherten Daten (☑ Req[14]). Damit befindet sich NurseEye wieder im Ausgangszustand.

8.6 Fazit über den Prototyp NurseEye

Die Implementierung des Prototypen NurseEye setzt alle funktionalen Anforderungen an das System um. Es gibt jedoch noch Einschränkungen darin, wie gut die Anforderungen erreicht werden. Anforderung Req[07]: NurseEye darf nicht zur Mitarbeiterüberwachung nutzbar sein, wurde als erfüllt markiert. NurseEye lässt nicht zu, dass ein Vorgesetzter das System missbraucht, um die Position seiner Mitarbeiter zu ermitteln. Ob damit alle Möglichkeiten der Mitarbeiterüberwachung ausgeschlossen sind, ist unklar. Unter Umständen lassen sich Systemprotokolle über Anzahl der Sturzmeldungen, bearbeitendem Endgerät und Reaktionszeit zur Leistungsbewertung von Mitarbeitern missbrauchen. Ob dies eine echte Gefahr ist, kann erst untersucht werden, wenn NurseEye im täglichen Einsatz ist und mehr Daten vorliegen. Ebenfalls nur durch mehr Daten lässt sich beantworten, ob Req[03] – NurseEye muss einfach zu bedienen sein – erfüllt ist. Es wurde versucht, die Bedienung so einfach und intuitiv wie möglich zu gestalten, nur eine Erprobung in der Praxis kann zeigen, ob dies gelungen ist.

Die Nicht-Funktionalen Anforderungen Req[16], Req[17], Req[18], die aus der Aufnahme von PbD als Stakeholder folgen, sind ebenfalls erfüllt. Der proaktive Ansatz, Datenschutz tief in das Design des Systems zu integrieren, war damit erfolgreich. Gleichzeitig muss festgestellt werden, dass teilweise Wünsche einzelner Stakeholder nicht berücksichtigt werden konnten, da diese im direkten Konflikt mit dem Datenschutz stehen. So wurde von einigen Pflegekräften der Wunsch geäußert, auch ohne aktuellen Sturz Zugriff auf die Kameras erhalten zu können. Damit wollten sie überprüfen, dass keine nicht erkannten Notfälle in diesen Bereichen vorliegen. Da dies tief gegen das Design von NurseEye verstößt, wurde diese Funktion nicht integriert.

Am Ende der DSFA sind nur noch geringe Risiken verbleibend. Nur drei der identifizierten Bedrohungen waren in ihrer Schwere oder Wahrscheinlichkeit in der Stufe erheblich oder höher. Die höchste Gefahr für die Akzeptanz und die Einsatztauglichkeit von NurseEye wird in Funktionsbeeinträchtigung durch falsche Ereignisse gesehen. Es wurde bereits erwähnt, dass man lieber

weniger Bereiche überwachen sollte, als Kameras an Orten mit nur unzureichender Qualität der Detektion zu erlauben. Angriffe über die Komposition von anonymisierten Quellen oder mit dem Hintergrundwissen des Operators wurden insoweit behandelt, als dass NurseEye im Bereitschaftsmodus keinerlei Zugriff auf die erfassten Daten gewährt. Die verbleibenden geringen Eingriffe in die Privatsphäre und möglichen Angriffe sind sowohl in ihrem Schweregrad als auch der Eintrittswahrscheinlichkeit begrenzt und können hingenommen werden. Am Ende der DSFA kann somit festgestellt werden, dass alle gesetzten Ziele erreicht werden konnten und keine Risiken gegen eine erste Erprobung in der Praxis sprechen.

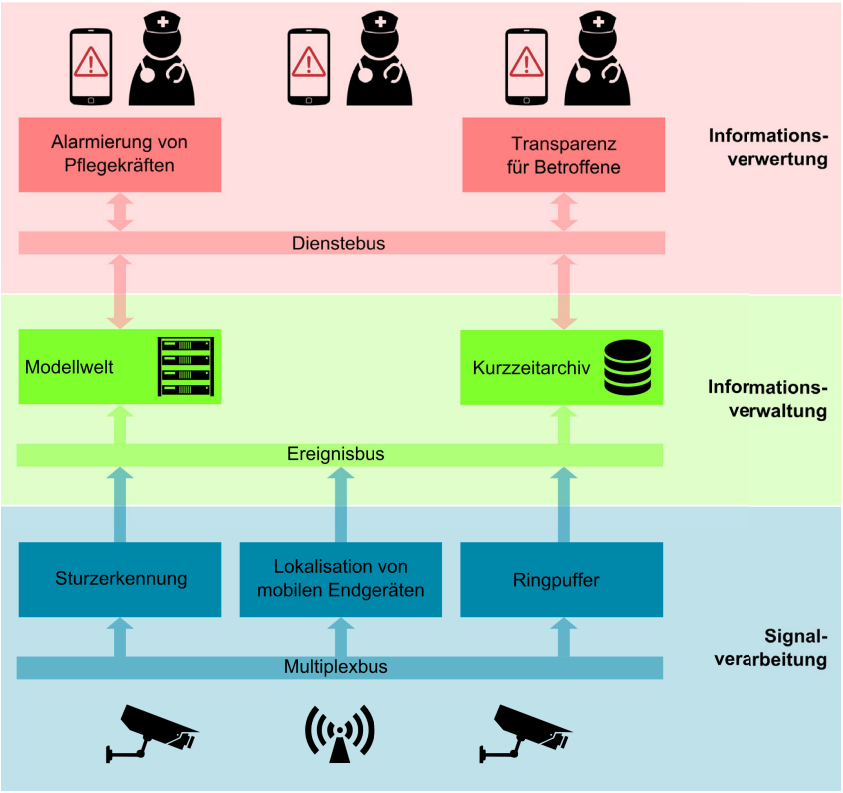


Abbildung 8.6: NEST-Architektur für das NurseEye-Szenario

9 Evaluation

Zum Abschluss der Arbeit wird das erstellte Akzeptanzmodell TAM-VS und der Prototyp NurseEye mit einer Evaluierung untersucht. Diese gliedert sich in zwei Teile. Zuerst wird untersucht, ob TAM-VS im NurseEye-Szenario vergleichbare Ergebnisse liefert, wie in den beiden bereits untersuchten Szenarien *Konventionelle Videoüberwachung* und *Intelligente Videoüberwachung* am Flughafen (vgl. Abschnitt 4.4.1 und Abschnitt 4.4.1). Anschließend werden einige Fragen zu Designentscheidungen im Prototyp NurseEye untersucht.

9.1 Datenerhebung und Analyse der Stichprobe

Die Daten für die Analyse wurden im Rahmen mehrerer Befragungsrunden erfasst. Diese wurden auf der CeBIT 2015 und einer Veranstaltung der Industrie und Handelskammer in Karlsruhe durchgeführt. Eine ursprünglich geplante weitere Datenerhebung im Sankt Franziskus Hospitals in Münster konnte leider nicht durchgeführt werden. Ergänzende Befragungen wurden im Haus des Fraunhofer IOSB durchgeführt.

In jeder Befragung bekam eine oder mehrere Personen NurseEye und den möglichen Einsatz in einem Krankenhaus oder einer Pflegeeinrichtung vorgestellt. Das Szenario beschreibt NurseEye in seinem Einsatz als halbautonomes System zur Sturzdetektion auf den Verkehrswegen und den Außenbereichen. Die Probanden bekamen die automatische Sturzdetektion, die Alarmierung der Pflegekräfte und die Displays zur Transparenz der Datenverarbeitung vorgestellt. Da die Probanden in der Befragung die Rolle der Betroffenen einnehmen, konnten sie die Bedienung von NurseEye nur beobachten, aber nicht selbst ausprobieren. Nach Abschluss der Präsentation hatten die Probanden Zeit, um den gedruckten Fragebogen (vgl. Anhang D) auszufüllen und bei Unklarheiten Fragen zu stellen.

In Tabelle 9.1 ist die sozioökonomische Analyse der Stichprobe zusammengefasst. Es wurden insgesamt 77 gültige Fragebogen ausgefüllt. Die Technikaffinität wurde verdeckt über die Frage „Wenn sie technische Probleme mit beispielsweise ihrem PC oder Handy haben, können sie diese:“ *„Fast immer selbst lösen“*, *„Manchmal selbst lösen“*, *„Fast niemals selbst lösen“* erhoben. Es ist eine deutliche Verschiebung der Stichprobe zur deutschen Gesamtbevölkerung zu erkennen. Die Stichprobe besteht insgesamt aus einem zu hohen Anteil an Männern, weißt einen sehr hohen Bildungslevel auf und ist sehr technikaffin. Rückschlüsse auf die Gesamtbevölkerung sollten also nur mit Vorsicht gezogen werden.

	Anzahl	Anteil in %
Geschlecht		
Weiblich	14	18
Männlich	63	82
Alter		
14-19	10	13
20-29	34	44
30-39	21	27
40-49	4	5
50-59	5	6
60-69	1	1
70+	2	3
Höchster Schulabschluss		
Sonderschulabschluss, Abschluss der Förderschule	0	0
Volks- oder Hauptschulabschluss / Polytechnische Oberschule 8. Klasse	0	0
Mittlere Reife (Realschulabschluss, Polytechnische Oberschule 10. Klasse)	5	6
Fachhochschulreife, Abitur, Erweiterte Oberschule	25	32
Abgeschlossenes Studium	47	61
Technikaffinität		
hoch	65	84
mittel	10	13
gering	2	3

Tabelle 9.1: Erste Analyse der Probanden

9.2 Erweiterung und Evaluierung von TAM-VS

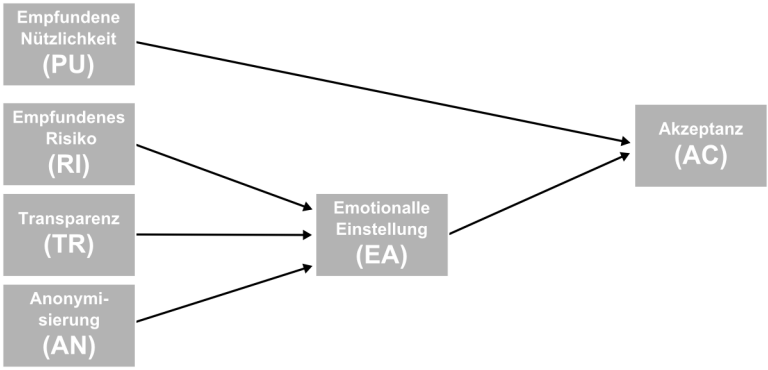


Abbildung 9.1: Erweitertes Akzeptanzmodell TAM-VS2

In der eingänglichen Untersuchung von TAM-VS (vgl. Abschnitt 4.4.2) konnten grundlegende Annahmen über die Akzeptanz von Videoüberwachung nachgewiesen werden. In Abbildung 9.1 ist die erste Version des Akzeptanzmodells TAM-VS mit einer Erweiterung dargestellt.
Die grundlegende Annahmen hinter TAM-VS besteht darin, dass es zwei Faktoren, die EMPFUNDENE NÜTZLICHKEIT (engl.: Perceived Usefulness (PU)) und die EMOTIONALE EINSTELLUNG (engl.: Emotional Attitude (EA)) gibt, die direkt auf die AKZEPTANZ (engl.: Acceptance (AC)) von Videoüberwachung wirken. In der ersten Version von TAM-VS wurde weiter angenommen, dass die zwei Faktoren EMPFUNDENES MISSBRAUCHSRISIKO (engl.: Risk (RI)) und TRANSPARENZ der Datenverarbeitung (engl.: Transparency (TR)) auf die EMOTIONALE EINSTELLUNG wirken. Dieses Modell bleibt so bestehen, es wird jedoch der neue Faktor ANONYMISIERUNG (engl.: Anonymity (AN)) eingeführt, welcher auf die EMOTIONALE EINSTELLUNG wirkt. Bei allen Faktoren handelt es sich um latente Variablen, die für Messung genutzten Skalen und ihre jeweiligen Items, sind im Anhang ab Tabelle E.1 zu finden. Es werden folgende Hypothesen aufgestellt:

H1: Die EMPFUNDENE NÜTZLICHKEIT (PU) hat einen *positiven* Einfluss auf die AKZEPTANZ (AC).

H2: Das EMPFUNDENE MISSBRAUCHSRISIKO (RI) hat einen *negativen* Einfluss auf die EMOTIONALE EINSTELLUNG (EA).

H3: Die TRANSPARENZ der Datenverarbeitung (TR) hat einen *positiven* Einfluss auf die EMOTIONALE EINSTELLUNG (EA).

H4: Die EMOTIONALE EINSTELLUNG (EA) hat einen *positiven* Einfluss auf die AKZEPTANZ (AC).

H5: Die ANONYMISIERUNG (AN) hat einen *positiven* Einfluss auf die EMOTIONALE EINSTELLUNG (EA).

Zur Auswertung der erhobenen Daten wurde das Werkzeug SmartPLS genutzt [RWW05]. Identisch zur ersten Untersuchung von TAM-VS (vgl. Abschnitt 4.4.2) beginnt die Analyse mit dem Test des verwendeten Messmodells.

Tabelle 9.2 fasst die Ergebnisse der Analyse des Messmodells zusammen, es werden die von Chin [Chi98] vorgeschlagenen Schwellwerte genutzt. Die durchschnittliche extrahierte Varianz (engl.: Average Variance Extracted (AVE)) ist für alle Items größer als 0,5, was für eine gute Konvergenzvalidität spricht. Die Faktorreliabilität (engl.: Composite Reliability) misst die Eignung eines Faktors zur Erklärung aller ihm zugeordneten Items. Alle Werte sind oberhalb des von Chin geforderten Schwellwertes von 0,7.

Die bekannte Faustregel zur Interpretation des Cronbachs α [GM10], bezeichnet Werte größer als 0,7 als akzeptabel und Werte größer als 0,8 als gut. Einer der Werte für das Cronbachs α liegen knapp unter dem von Chin vorgeschlagenen Schwellwert von 0,7. George [Geo03] und Churchill et al. [CP84] argumentieren jedoch, dass bei neu entwickelten Skalen Werte ab 0,6 akzeptiert werden können.

Tabelle 9.3 zeigt die äußeren Gewichte aller Items. Diese stellen ein Maß für die Korrelation zwischen einzelnen Items und den ihnen zugeordneten Faktoren dar. Dieses ist einmal unterhalb des von Chin vorgeschlagenen Schwellwerts

von 0,7. Nach Hulland [Hul99] ist selbst der niedrigste Wert von 0,68 noch weit über dem kritischen Schwellwert von 0,4, der bei einer ersten explorativen Untersuchung erreicht werden sollte.

Das letzte wichtige Qualitätskriterium für ein PLS-SGM Messmodell ist das Fornell-Larcker Kriterium [FL81]. Es fordert, dass die Quadratwurzel der AVE höher ist als die gegenseitige Korrelation der Konstrukte. In Tabelle 9.4 sind jeweils die Kreuzkorrelationen der Konstrukte dargestellt, sowie die Quadratwurzel der AVE auf der Diagonalen. Es ist zu erkennen, dass das Fornell-Larcker Kriterium für jeden Faktor im Messmodell erfüllt ist.

9.2.1 Test des Messmodells

	AVE	Composite Reliability	Cronbachs α
PU	0,65	0,84	0,73
RI	0,62	0,83	0,69
TR	0,83	0,91	0,81
AN	0,64	0,84	0,73
EA	0,67	0,86	0,75
AC	0,71	0,88	0,80

Tabelle 9.2: Qualitätskriterien Messmodell

Item	Äußeres Gewicht
PU1	0,68
PU6	0,89
PU7	0,83
RI2	0,73
RI4	0,82
RI5	0,80
TR1	0,96
TR2	0,87
AN1	0,83
AN2	0,77
AN3	0,78
EA1	0,80
EA2	0,86
EA4	0,79
AC1	0,89
AC4	0,82
AC8	0,82

Tabelle 9.3: Äußere Gewichte der Items

	AC	EA	AN	PU	RI	TR
AC	0,84					
EA	0,77	0,82				
AN	0,53	0,51	0,80			
PU	0,69	0,56	0,34	0,80		
RI	-0,36	-0,40	-0,36	-0,27	0,79	
TR	0,35	0,41	0,28	0,17	-0,26	0,91

Tabelle 9.4: Fornell-Larcker Kriterium

9.2.2 Test des Strukturmodells

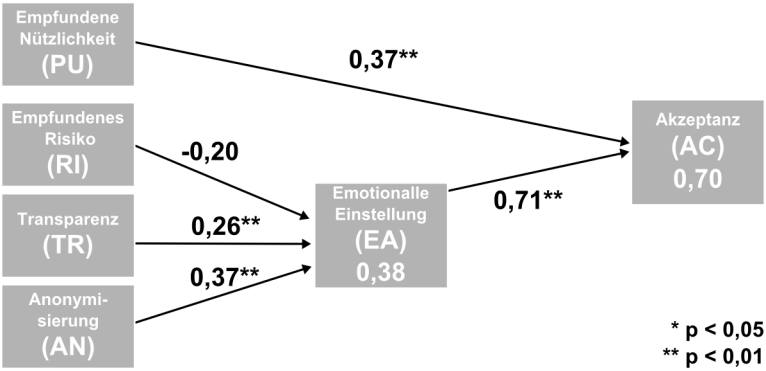


Abbildung 9.2: Auswertung des Strukturmodells für TAM-VS2

Nachdem die Prüfung des Messmodells keine kritischen Mängel aufgezeigt hat, wurde das Strukturmodell geprüft. Die Ergebnisse werden in Abbildung 9.2 zusammengefasst. Das erste entscheidende Kriterium für die Qualität des Strukturmodells ist R^2 der Faktoren, da es ein Maß für die Aussagequalität des Modells ist. Zuerst soll R^2 der Akzeptanz betrachtet werden. Dieser ist mit 0,70 über dem von Chin definiertet Schwellwert, sodass er als substantiell zu bezeichnen ist. Das bedeutet, dass 70% der beobachteten Varianz in der Akzeptanz durch die Varianz in den beiden Faktoren empfundene Nützlichkeit und emotionale Einstellung erklärt werden können. Die Varianz der emotionalen Einstellung ist mit einem R^2 von 0,38 deutlich weniger stark erklärt, liegt aber über dem Schwellwert von 0,33, ab dem man von einem moderaten Faktor spricht. In nächsten Abschnitt wird die Bedeutung dieser beiden Werte genauer betrachtet und auch eine Vermutung angestellt, warum die emotionale Einstellung mit dem Technology Acceptance Model-Video Surveillance (TAM-VS2) nicht zu einem höheren Grad erklärt werden kann.

Zur Prüfung der Hypothesen werden abschließend die Pfadkoeffizienten und ihre jeweilige Signifikanz bestimmt. Die Werte wurden mittels Bootstrapping bestimmt, wie es beim Einsatz von PLS-SGM empfohlen wird [HRS11].

Auch für die Mindestmaße der absoluten Werte der Pfadkoeffizienten gibt es unterschiedliche Aussagen. Der Betrag der Pfadkoeffizienten ist durchgehend größer als 0,1 und die Wirkrichtung entspricht der prädizierten Richtung. Damit kann nach Sellin und Keeves von einem wichtigen Zusammenhang gesprochen werden [SK94]. Allerdings scheitert der Pfadkoeffizient des EMPFUNDENEN RISIKOS knapp an der 5% Signifikanz. Damit kann der vermutete negative Einfluss anhand der vorliegenden Daten nicht bestätigt werden.

Wichtig bei der Bewertung der Ergebnisse ist weiter, dass die zugrundeliegenden Skalen nicht metrisch sind. Somit können keine Aussagen über Größenverhältnisse getroffen werden. Es ist lediglich eine Ordnung der unterschiedlichen Pfadkoeffizienten erlaubt. Es ist klar zu erkennen, dass der Einfluss der EMPFUNDENEN NÜTZLICHKEIT auf die AKZEPTANZ geringer ist als der Einfluss der EMOTIONALEN EINSTELLUNG.

9.2.3 Diskussion der Ergebnisse

Das erstellte Akzeptanzmodell TAM-VS bzw. seine Erweiterung TAM-VS2 konnten auch in Szenario NurseEye seine Einsatztauglichkeit nachweisen. Auch wenn nicht alle Qualitätskriterien erreicht werden konnten, weißt es für ein noch sehr junges Modell bereits sehr gute Ergebnisse auf. Das ist zweifellos der Nähe zu bereits erfolgreich genutzten Modellen wie TAM zu verdanken, womit viele der grundlegenden Arbeiten übernommen werden konnten.

Durch die Ergebnisse von TAM-VS konnten bisher lediglich vermutete Zusammenhänge zwischen der Akzeptanz von Videoüberwachungssystemen und ihrem technischen Aufbau nachgewiesen werden. Im nächsten Kapitel wird gezeigt werden, wie die konsequente Umsetzung dieser Erkenntnisse in NurseEye zu einem System mit hoher Akzeptanz geführt hat.

An dieser Stelle soll noch einmal der geringe Wert von R^2 bei der EMOTIONALEN EINSTELLUNG diskutiert werden. Die drei erfassten Faktoren EMPFUNDENES MISSBRAUCHSRISIKO, TRANSPARENZ der Datenverarbeitung und ANONYMISIERUNG zusammen, können lediglich 38% der beobachteten Varianz erklären. Dieser geringe Wert scheint einen deutlichen Mangel in TAM-VS darzustellen.

Betrachtet man jedoch das ursprüngliche Ziel von TAM-VS, wird der vermutliche Grund offensichtlich. Das Ziel von TAM-VS war es, Einflussfaktoren auf die Akzeptanz von Videoüberwachung zu finden, die durch die technische Ausgestaltung des Systems beeinflusst werden können. Gleichzeitig wissen wir aus der Sozialforschung, dass für die Akzeptanz der Videoüberwachung sozioökonomische Faktoren wie das Alter, Geschlecht oder Bildung einen sehr starken Einfluss haben. Ebenfalls einen starken Einfluss werden Faktoren, wie der gefühlten eigenen Sicherheitslage zugeordnet. Es ist zu vermuten, dass solche Faktoren zur besseren Erklärung der Varianz in der EMOTIONALEN EINSTELLUNG beitragen könnten. Da sie jedoch nicht durch die technische Ausgestaltung des Systems beeinflusst werden, sind sie für TAM-VS nicht relevant.

9.3 Evaluierung von NurseEye

Zuletzt sollen noch einige erweitere Fragen geklärt werden, um zu entscheiden, wie konkrete Designentscheidungen zukünftig die Akzeptanz von Systemen wie NurseEye beeinflussen können. Die dazu im Fragebogen in Anhang D erhobenen Fragen werden hier ausgewertet.
Dazu muss ergänzend ein Blick auf die verwendete Skala in der Befragung geworfen werden. Bis auf den sozioökonomischen Teil wurden alle Fragen mit einer 5-stufigen Ratingskala erfasst. Die Antwortmöglichkeiten waren: *Ich stimme zu (+2), (+1), Ich bin neutral (0), (-1), Ich stimme nicht zu (-2).* Diese sind rein äußerlich identisch zu den Likert-Skalen, die für TAM-VS verwendet wurden. Ob es sich bei einer solchen Skala um eine Intervall- oder Ordinalskala handelt, ist Mittelpunkt andauernder Fachdiskussionen. Jamieson Suson sei hier als ein Vertreter genannt, die Likert-Skalen als reine Ordinalskalen auffassen [Jam04], Lubke und Muthen widersprechen hier in so weit, dass es konkrete Situationen gibt, in denen eine Likert-Skala als Intervallskala aufgefasst werden kann [LM04].

Ein großer Teil des Problems liegt hier in der unsauberen Verwendung des Begriffs Likert-Skala. Eine Likert-Skala ist ein Fragenwerkzeug, das mit mehreren Fragen den Wert der abhängigen Variable bestimmt und bei dem unpassende

Fragen bereits eliminiert wurden. Beispielsweise werden in TAM-VS drei Fragen genutzt, um drei Items zu messen, die gemeinsam die abhängige Variable EMPFUNDENE NÜTZLICHKEIT erfassen. Korrekt darf nur das gesamte Fragenwerkzeug als Likert-Skala bezeichnet werden und nicht wie häufig gesehen, die einzelne Frage mit einer Ratingskala.

Somit lässt Section B des Fragebogens nur eine Verwendung von deskriptiver Statistik zu, die aber ausreicht, um die vermuteten Theorien zu testen. Dieses Vorgehen steht nicht im Widerspruch zum Einsatz von SmartPLS, welches die in Section A genutzten Likert-Skalen auswertet.

9.3.1 Einsatztauglichkeit von NurseEye

Zu Beginn wurde betrachtet, welche Einschätzung die Befragten zur Nützlichkeit des Systems haben. Abbildung 9.3 fasst die Antworten zusammen, die vollständige Auswertung der einzelnen Fragen ist im Anhang Tabelle F.1 bis Tabelle F.4 zu finden.

Der in der Literatur häufig zu findende Unterschied in der Akzeptanz zwischen Frauen und Männern soll ebenfalls betrachtet werden. Mit einem zweiseitigen Wilcoxon-Mann-Whitney-Test, auch U-Test genannt, wurde überprüft, ob sich die Antworten von Frauen und Männer signifikant unterscheiden. Als Signifikanzniveau α wurde der in der Statistik übliche Wert von 5% angenommen, um zu prüfen, ob die Hypothese „*Die Akzeptanz von Frauen und Männern unterscheidet sich*“ angenommen oder verworfen wird. Wie in Abbildung 9.3 zu erkennen ist, wurde sie nur für die Frage „*Klassische Videoüberwachung kann helfen, akute Sicherheitsprobleme zu lösen*“ verworfen, für alle anderen Fragen wurde sie akzeptiert.

Wie sich zeigt, genießt NurseEye ein deutlich höheres Vertrauen ein Sicherheitsproblem zu lösen, als die klassische Videoüberwachung. Weil nicht vorgegeben war, wie das klassische System arbeitet, kann vermutet werden, dass die Probanden insgesamt mehr Vertrauen in die intelligente Videoüberwachung setzten.

Überraschenderweise wird die allgemeine Frage „*NurseEye kann helfen, ein akutes Sicherheitsproblem zu lösen*“ weniger zustimmend beantwortet, wie die konkrete Frage, ob NurseEye dabei helfen kann, Menschenleben zu retten. Woher dieser Effekt kommt, kann leider nicht erklärt werden.

Erfreulich sind auch die Ergebnisse der letzten Fragen im Block zur Nützlichkeit. Über 50% der Teilnehmer lehnen die Aussage „*Systeme wie NurseEye werden nur eingesetzt, um Personal einzusparen*“ zumindest zum Teil ab. Eine hohe Skepsis gegenüber der Einführung des Systems, kann also nicht beobachtet werden.

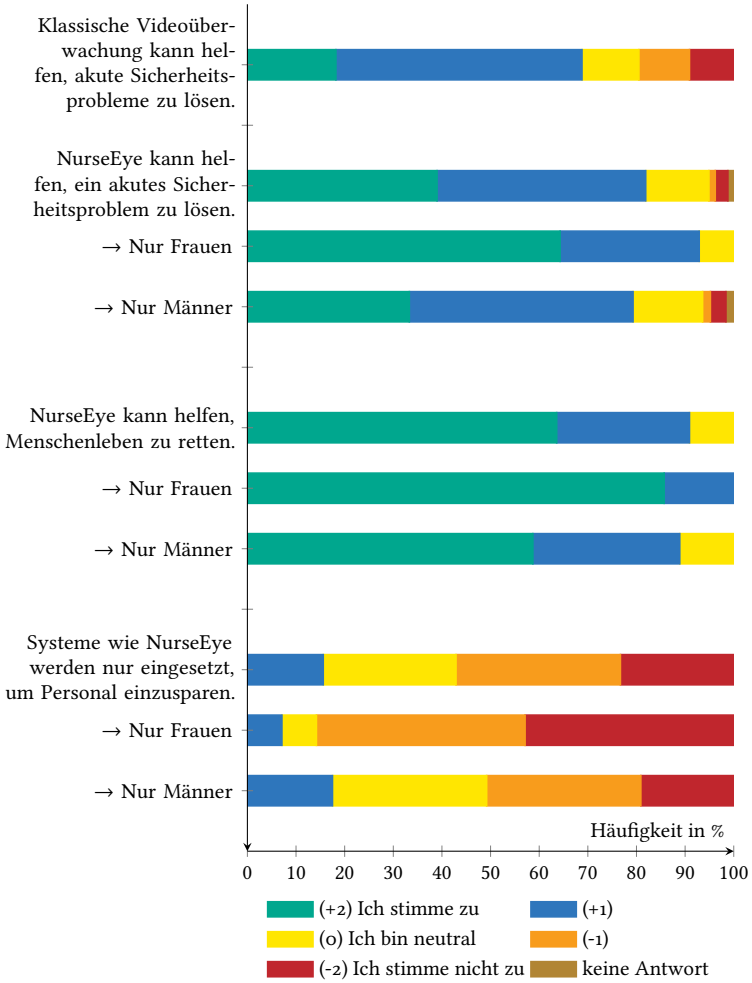


Abbildung 9.3: Einstellungen zur Nützlichkeit von NurseEye

9.3.2 Evaluation der Designentscheidungen

Mit der nächsten Gruppe an Fragen soll geklärt werden, wie die getroffenen Designentscheidungen bei der Entwicklung von NurseEye von den Betroffenen wahrgenommen werden. Interessant ist, dass in der gesamten folgenden Gruppe an Fragen, in der es um technische Elemente des Systems geht, kein signifikanter Unterschied zwischen Frauen und Männern festgestellt werden konnte.

Wie sich zeigt, sind die Befragten, was einen unbegründeten Zugriff auf das Videomaterial angeht, sehr kritisch. Die zusammengefassten Ergebnisse dazu sind in Abbildung 9.4 dargestellt und vollständig im Anhang in Tabelle F.5 bis Tabelle F.7 zu finden. Deutlich über 50% der Befragten sind nicht der Meinung, dass Krankenhauspersonal ohne einen akuten Alarm auf anonymisierte Livedaten der Kameras zugreifen können sollte. Wenn die Daten nicht anonymisiert werden, steigt die Ablehnung sogar bis auf über 80%. Gleichzeitig wird die Anonymisierung von Sturzvideos als wichtig wahrgenommen. Über 60% der Befragten stimmen der Aussage „*Ich finde es wichtig, Videos von möglichen Stürzen zu anonymisieren.*“ zumindest teilweise zu.

Es zeigt sich damit, dass die halbautomatische Sturzerkennung in NurseEye ein sehr guter Ansatz ist. Zwar ist es nicht möglich Zugriff auf Videomaterial jederzeit zu verhindern, aber ein anonymisierter Zugriff bei vorliegenden Alarmen scheint den Wünschen der Betroffenen zu entsprechen.

Die installierten Displays werden von den Befragten sehr gut aufgenommen. Die zusammengefassten Ergebnisse dazu sind in Abbildung 9.5 dargestellt und vollständig im Anhang in Tabelle F.8 und Tabelle F.9 zu finden. Über 70% der Befragten stimmen zumindest teilweise zu, dass sie die Displays für wichtig halten. Über 60% der Befragten halten die damit erreichte Transparenz in der Datenverarbeitung für ausreichend.

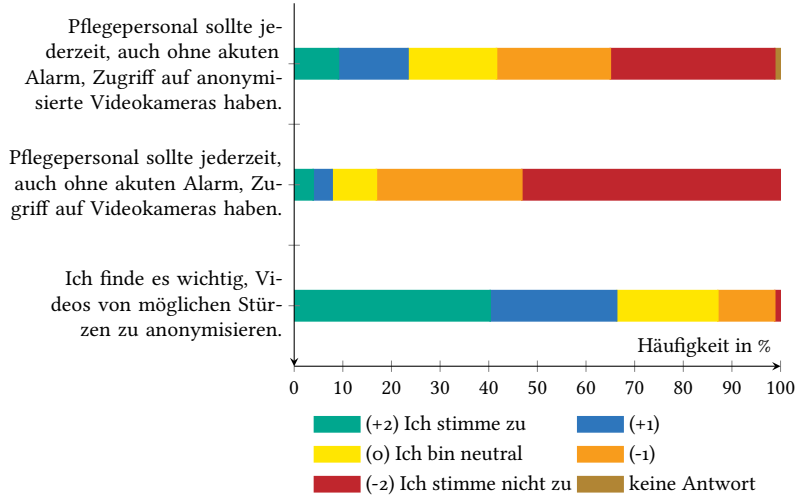


Abbildung 9.4: Einstellungen zum Zugriff auf Videomaterial

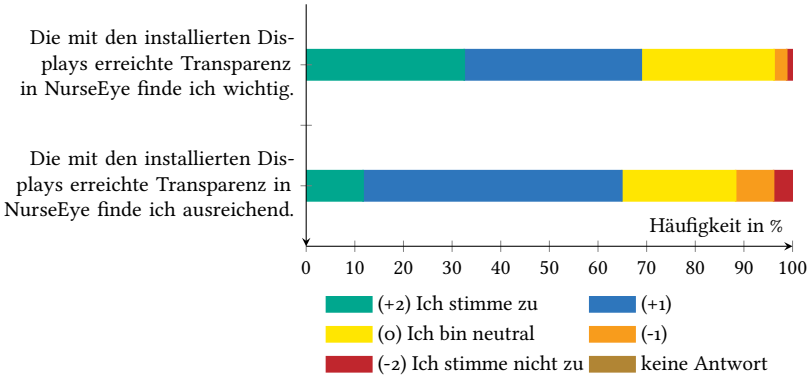


Abbildung 9.5: Einstellungen zur Transparenz von NurseEye

9.3.3 Gesamteindruck von NurseEye

Als letzter Block in der Befragung werden abschließende Fragen zum Gesamteindruck von NurseEye untersucht. Die zusammengefassten Ergebnisse dazu sind in Abbildung 9.6 dargestellt und vollständig im Anhang in Tabelle F.10 und Tabelle F.11 zu finden. Hier konnte wieder ein signifikanter Unterschied zwischen den Ergebnissen von Frauen und Männern festgestellt werden. Der Aussage „*NurseEye erfüllt meine Ansprüche an Sicherheit und Datenschutz*“ stimmen über 90% aller befragten Frauen zumindest teilweise zu. Bei den Männern sind es weniger als 60%, die der Aussage teilweise zustimmen. Noch deutlicher werden die Unterschiede bei der zweiten Frage aus dem Block. Der Aussage „*Ich halte die durch NurseEye gezeigte Entwicklung für einen wünschenswerten Fortschritt*“ stimmen alle befragten Frauen zumindest teilweise zu. Volle Zustimmung erhält es von mehr als 90%. Hier sind die Männer deutlich weniger von NurseEye überzeugt. Zwar stimmen der Aussage fast 90% aller befragten Männer teilweise zu, aber die volle Zustimmung ist gerade bei 50% der befragten Männer gegeben. Dies bestätigt einmal mehr, dass Frauen der Videoüberwachung eher positiv eingestellt sind als Männer.

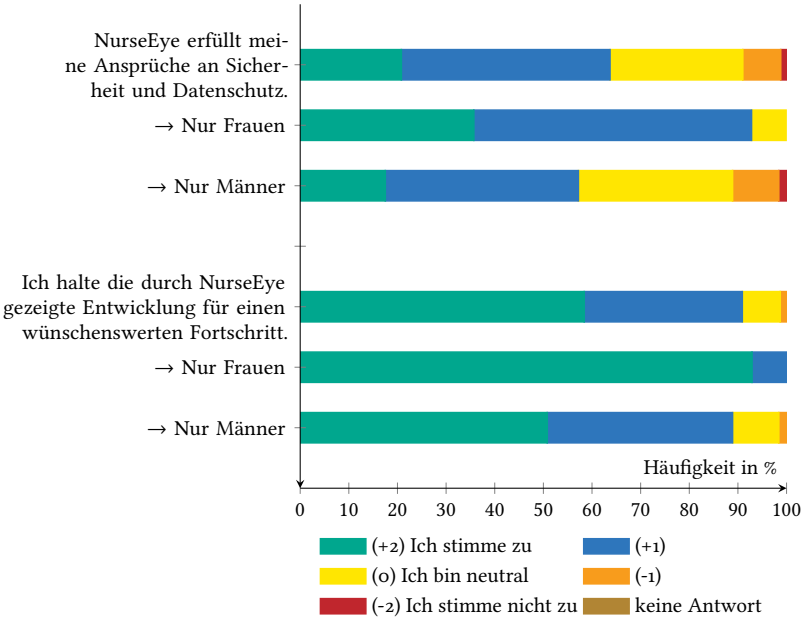


Abbildung 9.6: Gesamteindruck von NurseEye

10 Fazit und Ausblick

In der vorliegenden Arbeit wurde das Thema der Akzeptanz von Videoüberwachung breit untersucht. Dabei wurde mit einigen bisher typischen Ansätzen gebrochen. So konzentrieren sich die wenigen bisherigen Versuche, die Akzeptanz von Videoüberwachung zu steigern, fast ausschließlich auf die Anonymisierung der verarbeiteten Daten. Auch wenn dieses Vorgehen sehr vielversprechend ist, reicht er alleine nicht aus, um das komplexe Thema Akzeptanz abzudecken. Um neue Methoden und Ansätze zu entwickeln, wurden vielversprechende Methoden aus benachbarten Wissenschaftsdisziplinen auf die eigene Aufgabenstellung angewendet.

10.1 Fazit

Im ersten Schritt der Arbeit wurde untersucht, welche Faktoren die Akzeptanz der Videoüberwachung beeinflussen. Dazu wurden die, aus der Informations- und Kommunikationstechnologie (IKT) bekannten Technologieakzeptanzmodelle eingesetzt. Diese Modelle werden seit den frühen 80er Jahren genutzt, um die Verbreitung von neuer Technologie auf dem Markt zu prognostizieren. Auch wenn keines der vorhandenen Modelle für den Einsatz in der intelligenten Videoüberwachung geeignet war, bot sich mit dem Technology Acceptance Model (TAM) von Davis et al. ein vielversprechender Ausgangspunkt für die eigenen Arbeiten.

Mit Hilfe des eigens für diesen Zweck entwickelten Akzeptanzmodells Technology Acceptance Model-Video Surveillance (TAM-VS) konnten einige bisher nur vermutete Zusammenhänge der Akzeptanz von Videoüberwachung untersucht und bestätigt werden. Im Vergleich mit dem üblichen Einsatz von Akzeptanzmodellen, wurden dabei nur solche Akzeptanzfaktoren betrachtet, die sich direkt mit der technischen Ausgestaltung des Überwachungssystems

beeinflussen lassen. Dank den Sozialwissenschaften ist es zwar mittlerweile bekannt, dass Frauen tendenziell eine höhere Akzeptanz für die Videoüberwachung haben und auch dass ältere Menschen ihr eher zugeneigt sind. Dieses Wissen hilft Ingenieuren jedoch nicht dabei, Systeme zu bauen, die maximale Akzeptanz erfahren.

TAM-VS konnte einen fundierten Beitrag dazu leisten, die Faktoren zu verstehen, die die Akzeptanz beeinflussen und bisher lediglich vermutete Zusammenhänge statistisch nachweisen. Es konnte gezeigt werden, dass die *Steigerung der empfundenen Nützlichkeit*, *Senkung des empfunden Missbrauchsrisikos* und *Steigerung der Transparenz* geeignet sind, um die Akzeptanz von Videoüberwachung zu beeinflussen. Damit wurde die erste Hypothese „Technologieakzeptanzforschung kann einen wichtigen Beitrag leisten, um zu verstehen, welche Faktoren die Akzeptanz von intelligenter Videoüberwachung beeinflussen" bestätigt und die Grundlage für die weitere Arbeit geschaffen werden.

Im nächsten Schritt der Arbeit wurden die identifizierten Akzeptanztreiber jeweils einzeln betrachtet und untersucht, wie sie durch technische Komponenten und Prozesse verbessert werden können. Zur Steigerung der empfundenen Nützlichkeit wurden neue Konzepte untersucht, wie Betroffene mit dem System interagieren und somit von diesem Zusatzdienste nutzen können. Weiter wurde betrachtet, wie intelligente Videoüberwachungssysteme besser mit mobilen Einsatzkräften zusammenarbeiten und damit die Sicherheit gesteigert werden kann. Mit der interaktiven Überwachung wurde ein generisches Verfahren geschaffen, um die Mächtigkeit und damit auch die möglichen Eingriffe in die Privatsphäre von intelligenter Videoüberwachung zu regulieren. Der Operator bekommt damit immer genau die Funktionalität angeboten, die er zur Bearbeitung der aktuellen Sicherheitslage benötigt. Das vereinfacht die Nutzung und verhindert versehentliche oder absichtliche Verletzung der Privatsphäre Betroffener. Gelingt es, die so regulierte Mächtigkeit der Systeme für die Betroffenen transparent zu machen, kann eine erhöhte Akzeptanz erwartet werden.

Die Angst vor Missbrauch von Videoüberwachung ist tief in der Bevölkerung verankert. Gerade junge Menschen fürchten sich davor, Opfer von unbegründeten Eingriffen in ihre Privatsphäre zu werden. Um Betreibern und Operatoren

zu helfen, diese Angst zu reduzieren, wurden zwei Ansätze verfolgt. Privacy Score ist ein einfach zu nutzendes Werkzeug, mit dem Betreiber unterschiedliche Systeme auf ihre Datenschutzeigenschaften überprüfen können. Es wurde dafür entwickelt, Betreiber bei der Neuinstallation oder Veränderung bestehender Systeme eine Unterstützung zu bieten und auch den Datenschutz bei der Auswahl des eingesetzten Systems zu berücksichtigen.

Der aktuelle Entwurf der europäischen DSGVO lässt vermuten, dass zukünftig Datenschutz-Folgenabschätzung (DSFA) vorgeschrieben sein werden, um Datenschutzrisiken bei allen Systemen zu reduzieren, die persönliche Daten verarbeiten. Dabei beschreibt die DSFA selbst nur ein Vorgehen, dass sehr viel Fachwissen der Auditoren voraussetzt. Einfacher wird die Durchführung, wenn der Auditor auf ein Rahmenwerk zurückgreifen kann, das auf die zu auditierende Technologie abgestimmt ist. Da weder für die konventionelle noch die intelligente Videoüberwachung ein eigenes Rahmenwerk existiert, wurden bestehende Ansätze auf ihre Einsatztauglichkeit geprüft. Dabei wurde festgestellt, dass keines der aktuell verfügbaren Rahmenwerke ideal ist. Eine neue Kombination der existierenden Verfahren wurde entwickelt, um intelligente Videoüberwachung zu auditieren. Eine Angreiferanalyse für die intelligente Videoüberwachung ergänzt dieses, um die relevanten Bedrohungen.

Zur Steigerung der Transparenz in der Datenverarbeitung wurden mehrere Ansätze erfolgreich umgesetzt. Zum einen wurden mehrere Prototypen entwickelt, die interessierten Betroffenen erlauben mit ihrem mobilen Endgerät mit einem intelligenten Videoüberwachungssystem zu interagieren. Die Betroffenen können sich damit über das System, die Datenverarbeitung und auch verantwortliche Personen informieren. Zum anderen wurde untersucht, wie die bisher nur statischen Hinweisschilder auf Videoüberwachung überarbeitet werden können, um der technischen Weiterentwicklung gerecht zu werden. Dank Displays, die direkt an den Sensoren montiert sind, wird es möglich, viel genauer über die aktuelle Datenverarbeitung zu informieren. Kann das System beispielsweise mittels interaktiver Überwachung in verschiedenen Modi arbeiten, ist es der Transparenz und damit der Akzeptanz von Vorteil, dies direkt mit den Betroffenen zu kommunizieren. Bei konventioneller Videoüber-

wachung kann es leicht vorkommen, dass Personen eine Notlage beobachten, aber sich gänzlich auf die Videoüberwachung verlassen und nicht eingreifen. Dies ist gerade dann fatal, wenn das System nur aufzeichnet und keine Auswertung geschieht. Wird es für Betroffene transparent, wann und wie das System bestimmte Notlagen erkannt hat, kann somit auch der eigentliche Überwachungszweck unterstützt werden. Es ist offensichtlich, dass Transparenz und Nutzen der Videoüberwachung in bestimmten Szenarien im Konflikt stehen können. Dieser kann weder immer aufgelöst werden, noch konnte ein methodisches Vorgehen entwickelt werden, das garantiert, dass ein gewähltes Verfahren zur Transparenz nicht im Konflikt mit dem Überwachungszweck steht. Es bedarf weiterhin eines Datenschutzexperten, um geeignete Verfahren auszuwählen.

Hypothese 2: „Es können gezielt *technische* Komponenten entwickelt werden, die einen positiven Einfluss auf einen oder mehrere Akzeptanzfaktoren haben" konnte bestätigt werden.

Der letzte Schritt der Arbeit besteht darin, einen Prototyp zu entwerfen, der die intelligente Videoüberwachung mit möglichst vielen der entwickelten Konzepte zur Akzeptanzsteigerung vereint. Dieser NurseEye genannte Prototyp wurde für die Detektion und Alarmierung bei Stürzen in Krankenhäusern und Pflegeheimen entworfen. Nach den Vorgaben einer DSFA begann die Entwicklung mit der Analyse aller relevanten Stakeholder. Das besondere bei NurseEye war jedoch, dass nicht nur Betreiber und Betroffene analysiert, sondern auch die Pflegekräfte, rechtliche Experten und Privacy by Design (PbD) als eigene Stakeholder betrachtet wurden. Das nach diesen gesammelten Anforderungen entworfene und implementierte NurseEye unterscheidet sich deutlich vom Stand der Technik. Es vereint eine algorithmische Detektion von Stürzen mit der schnellen und unkomplizierten Alarmierung von nahen Pflegekräften über mobile Endgeräte. Den Betroffenen werden alle Verarbeitungsschritte transparent dargelegt, dazu sind die Kameras mit zusätzlichen Displays ausgestattet. Sie stellen einen bidirektionalen Kanal zwischen den Patienten und den Pflegern dar und gleichen das bei der Videoüberwachung typischer Informationsungleichgewicht zwischen Beobachtern und Beobachteten aus. Dank diesem *„Ich*

sehe, wer mich sieht"-Prinzip, können Betroffene sofort erkennen, wenn ein Pfleger Zugriff auf ihre Videodaten hat.

Um zu prüfen, ob mit diesem Design tatsächlich eine gesteigerte Akzeptanz erreicht wird, gab es eine abschließende Evaluation. Diese konnte, zumindest in der betrachteten Stichprobe, eine deutliche Steigerung erkennen. Damit kann auch die Hypothese 3: „Durch entsprechendes Design können Videoüberwachungssysteme mit höherer Akzeptanz, bei mindestens gleichbleibender Funktionalität, entwickelt werden" bestätigt werden. Somit sind am Ende der Arbeit alle drei untersuchten Hypothesen bestätigt und das Verständnis darüber, wie Videoüberwachung ausgestaltet sein muss, um die Akzeptanz zu steigern, wurde deutlich erweitert.

10.2 Ausblick

Die intelligente Videoüberwachung wird in den kommenden Jahren deutlich an Verbreitung gewinnen. Damit sind nicht nur die Systeme gemeint, die an Flughäfen, Bahnhöfen oder öffentlichen Plätzen für Sicherheit sorgen. Zunehmend werden Kamerasysteme auch an Orten Einzug halten, die bisher nicht videoüberwacht waren, wie beispielsweise in Krankenhäusern oder Pflegeheimen. Wurde Videoüberwachung, wenn auch teilweise nur zähneknirschend, für ihre Steigerung der Sicherheit an öffentlichen Orten geduldet, wird dies zukünftig nicht mehr ausreichen. Anbieter und Entwickler werden sich mehr Gedanken darüber machen müssen, wie sie Systeme entwickeln, die für die Bevölkerung akzeptabel sind.

Mit dem erstellten Modell TAM-VS konnte ein grundlegendes Verständnis über die Akzeptanztreiber der Videoüberwachung erzeugt werden. Trotzdem wurde erkannt, dass der Einfluss der bisher identifizierten Akzeptanzfaktoren begrenzt ist. Gerade der sehr starke Faktor EMOTIONALE EINSTELLUNG wird durch die erfassten Faktoren nur zu knapp 40% in seiner Varianz erklärt. Auch wenn davon auszugehen ist, dass ein Großteil der verbleibenden 60% Varianz durch nicht technische Faktoren, wie das Alter der Befragten bestimmt ist, sind hier weitere Arbeiten zu leisten. Ein sehr spannendes Ergebnis kann

erwartet werden, wenn man TAM-VS mit den Überlegungen von Dominic Kudlacek kombiniert [Kud15]. Beide Ansätze versuchen, die wahrnehmbare Varianz in der Akzeptanz auf unterschiedliche Art zu verstehen. Während TAM-VS die technische Seite betrachtet, untersucht Kudlacek, wie Faktoren wie die individuelle Kriminalitätsfurcht, die Akzeptanz beeinflussen. Gelingt es, beide zu kombinieren, könnte die Varianz der Akzeptanz viel umfassender verstanden werden, um möglicherweise noch mehr Faktoren zu identifizieren, die sich durch das Design verbessern lassen.

TAM-VS kann jedoch nicht nur für das Verständnis der Akzeptanz von Videoüberwachung einen Beitrag leisten. So gelten viele der Rahmenbedingungen der Videoüberwachung, beispielsweise dass Betroffene die Systeme nicht selbst beschaffen oder nutzen, hohes Informationsungleichgewicht und Missbrauchsangst, auch für andere Sicherheitssysteme. Erste Versuche könnten klären, ob TAM-VS auch eingesetzt werden kann, um beispielsweise die Akzeptanz von Sicherheitskontrollen am Flughafen zu verstehen und im einem zweiten Schritt zu verbessern. Realistisch muss jedoch gesagt werden, dass dies in der nahen Zukunft nicht zu erwarten ist. Betrachtet man die öffentliche Diskussion rund um Sicherheit, Privatsphäre und Akzeptanz, kann beobachtet werden, dass der Sicherheit immer ein höherer Stellenwert eingeräumt wird, als dem Schutz der Privatsphäre. Dies ist einerseits verständlich, immerhin würden die meisten Menschen zustimmen, dass geringe Eingriffe in die Privatsphäre erlaubt sein sollten, um Menschenleben zu schützen. Anderseits sollte es nicht davon abhalten, Systeme in ihren Eingriffen zu reduzieren, wenn dadurch die Nützlichkeit nicht nachteilig beeinträchtigt wird. Mit dem aktuellen Entwurf der europäischen DSGVO ist bereits ein Gesetz zu erkennen, das genau dies fordert. Leider kann 15 Jahren nach den Terroranschlägen vom 11. September immer noch beobachtet werden, dass Verantwortliche von einer Unvereinbarkeit von Sicherheit und Privatsphäre ausgehen und die Bevölkerung dementsprechend ihre Privatsphäre für ihre Sicherheit aufgeben soll. So lange diese Grundhaltung nicht korrigiert wurde, ist nicht davon auszugehen, dass Themen wie Akzeptanz von Sicherheitstechnologie breit untersucht werden.

Wo sehr wohl zu erwarten ist, dass die Akzeptanzforschung in den kommenden Jahren Einfluss haben wird, sind Bereiche, die klassisch noch nicht videoüberwacht sind. Dazu zählen die bereits beschriebenen Einsätze in Krankenhäusern und der Pflege. Hier wird die Akzeptanz der Betroffenen eine viel höhere Rolle spielen, als in klassischen Sicherheitsanwendungen.

Mit der Weitereinwicklung der algorithmischen Bildauswertung wird die Kamera jedoch noch näher an das tägliche Leben der Menschen rücken. Mit der „Nest Cam“ von Google und der Netatmo „Smart Home Camera“ sind bereits zwei Produkte auf dem Markt, die eine begrenzt intelligente Videoüberwachung in die Privatwohnung bringen. Es kann nur vermutet werden, dass technische Entwicklungen zum Smart Home, Internet of Things oder Ambient Assisted Living noch mehr dazu beitragen werden, dass mehr Bereiche mit einer Kamera beobachtet werden. Für diese Technologien wird es entscheidend sein, ob sie bei ihren Betroffenen, die gleichzeitig auch Käufer sind, ein hohes Maß an Akzeptanz erreichen können. Dies wird neben der reinen Funktionalität auch über die Transparenz und einer geringen Angst vor Missbrauch erreicht werden. TAM-VS oder daraus abgeleitete Modelle können hier einen wichtigen Beitrag leisten.

Seit der erste Röhrenbildschirm das Bild einer analogen Kamera wiedergegeben hat, konnte eine enorme Entwicklung bei der Videoüberwachung beobachtet werden. Moderne Systeme sind bereits heute so komplex, dass selbst Experten die Datenverarbeitung nicht immer nachvollziehen können. Wie bei sehr vielen komplexen Technologien, bei denen die Betroffenen nicht mehr selbst überprüfen können, ob sie wie versprochen arbeiten, wird auch für die intelligente Videoüberwachung eine unabhängige Prüfung und Zertifizierung an Bedeutung gewinnen. Durch Datenschutzzertifikate können Betreiber nachweisen, dass sie den Schutz der Betroffenen ernst nehmen und in technische Systeme investiert haben, die Eingriffe in die Privatsphäre aktiv verhindern. Wie weit dies einen gesellschaftlichen Druck zu Systemen mit hohem Datenschutz zur Folge haben wird, ist abzuwarten.

Mit NurseEye wurde ein erster Prototyp für eine datenschutzfreundliche Sturzerkennung und Alarmierung für Krankenhäuser geschaffen. Dieser wurde

mit dem Ziel ein Höchstmaß an Akzeptanz zu erreichen entworfen, was er in einer ersten Befragung auch erreicht hat. Aktuell werden Anschlussprojekte verhandelt, die NurseEye vom Prototyp in den echten Einsatz bringen sollen. Wie viele der Konzepte und Designentscheidungen sich vom Prototyp in den Markt übertragen lassen, wird sich in den kommenden Jahren zeigen. Gerade die Frage, ob eine reine algorithmische Erkennung von Stürzen in Nicht-Laborumgebungen ausreichende Qualität erreicht ist spannend. Damit wird sich auch entscheiden, ob NurseEye mit seinem Ansatz der interaktiven Überwachung tatsächlich die Sicherheit von Patienten steigern kann oder ob das Konzept aufgrund bisher unbekannter Probleme oder Anforderungen nicht umsetzbar ist.

A Fragebogen zu TAM-VS Version 1

Der Fragebogen, wie er für die erste Datenerhebung für das Akzeptanzmodell TAM-VS in den Szenarien „konventionelle Videoüberwachung“ und „intelligente Videoüberwachung“ am Flughafen genutzt wurde.

Vielen Dank, dass Sie sich zur Teilnahme an dieser Befragung bereiterklärt haben. Sie ist in 3 Böcke gegliedert und wird zusammen mit den dazugehörigen Demonstrationen ungefähr eine Stunde dauern.

Section A: Klassisches Überwachungssystem

Wir haben Ihnen nun an Hand unseres Demonstrators ein Szenario mit einem klassischen Videoüberwachungssystem präsentieren. Bitte beachten Sie, dass sich alle nun folgenden Fragen auf dieses System beziehen!

A1. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Das vorgestellte System erleichtert die Arbeit des Sicherheitspersonals.	☐	☐	☐	☐	☐
Das vorgestellte System steigert die Sicherheit im überwachten Bereich.	☐	☐	☐	☐	☐
Das vorgestellte System erleichtert das Erkennen von Straftaten.	☐	☐	☐	☐	☐
Das vorgestellte System ermöglicht, dass das Sicherheitspersonal große Bereiche sichern kann.	☐	☐	☐	☐	☐
Insgesamt finde ich das vorgestellte System zur Steigerung der Sicherheit nützlich.	☐	☐	☐	☐	☐
Solche Systeme können Verbrechen nur erkennen, aber nicht verhindern.	☐	☐	☐	☐	☐

A2. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich weiß aus welchen Gründen das System installiert ist.	☐	☐	☐	☐	☐
Ich fühle mich gut darüber informiert, welche Informationen vom System erfasst werden.	☐	☐	☐	☐	☐
Ich fühle mich gut darüber informiert, wie die gesammelten Daten vom System verarbeitet werden.	☐	☐	☐	☐	☐
Ich weiß, wer der verantwortliche Betreiber der Anlage ist.	☐	☐	☐	☐	☐

A3. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Die Verarbeitung von Daten durch das System ist für mich nachteilig.	☐	☐	☐	☐	☐
Die erfassten Daten könnten unerlaubt verwendet werden.	☐	☐	☐	☐	☐
Durch Fehler in der Erfassung oder Verarbeitung können mir Nachteile entstehen.	☐	☐	☐	☐	☐

A4. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich glaube, dass der Einsatz solcher Systeme sinnvoll ist.	☐	☐	☐	☐	☐
Der Betreiber eines solchen Systems kümmert sich darum, dass das System korrekt und verlässlich arbeitet.	☐	☐	☐	☐	☐
Wenn die Vorteile nicht überwiegen, würde ein solches System nicht eingesetzt werden.	☐	☐	☐	☐	☐
Ich muss mir wegen des Einsatzes eines solchen Systems keine Sorgen machen.	☐	☐	☐	☐	☐
Durch ein solches System fühle ich mich im überwachten Bereich sicherer.	☐	☐	☐	☐	☐

A5. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich finde solche Systeme gut.	☐	☐	☐	☐	☐
Solche Systeme sollten gesetzlich verboten werden.	☐	☐	☐	☐	☐
Die erreichte Sicherheit steht in keinem Verhältnis zu der verlorenen Freiheit.	☐	☐	☐	☐	☐
Es sollten mehr Systeme dieser Art installiert werden.	☐	☐	☐	☐	☐
Durch solche Systeme wird Sicherheitspersonal ersetzt, das die notwendigen Aufgaben besser erledigen könnte.	☐	☐	☐	☐	☐

Section B: Intelligentes Überwachungssystem

Wir haben Ihnen nun an Hand unseres Demonstrators ein Szenario mit einem klassischen Videoüberwachungssystem präsentieren. Bitte beachten Sie, dass sich alle nun folgenden Fragen auf dieses System beziehen!

B1. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Das vorgestellte System erleichtert die Arbeit des Sicherheitspersonals.	☐	☐	☐	☐	☐
Das vorgestellte System steigert die Sicherheit im überwachten Bereich.	☐	☐	☐	☐	☐
Das vorgestellte System erleichtert das Erkennen von Straftaten.	☐	☐	☐	☐	☐
Das vorgestellte System ermöglicht, dass das Sicherheitspersonal große Bereiche sichern kann.	☐	☐	☐	☐	☐
Insgesamt finde ich das vorgestellte System zur Steigerung der Sicherheit nützlich.	☐	☐	☐	☐	☐
Solche Systeme können Verbrechen nur erkennen, aber nicht verhindern.	☐	☐	☐	☐	☐

B2. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich weiß zu welchem Zweck das System installiert ist.	☐	☐	☐	☐	☐
Ich fühle mich gut darüber informiert, welche Informationen vom System erfasst werden.	☐	☐	☐	☐	☐
Ich fühle mich gut darüber informiert, wie die Daten vom System verarbeitet werden.	☐	☐	☐	☐	☐
Ich weiß, wer der verantwortliche Betreiber der Anlage ist.	☐	☐	☐	☐	☐

B3. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Die Verarbeitung von Daten durch das System ist für mich nachteilig.	☐	☐	☐	☐	☐
Die erfassten Daten könnten unerlaubt verwendet werden.	☐	☐	☐	☐	☐
Durch Fehler in der Erfassung oder Verarbeitung können mir Nachteile entstehen.	☐	☐	☐	☐	☐

B4. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich glaube, dass der Einsatz solcher Systeme sinnvoll ist.	☐	☐	☐	☐	☐
Der Betreiber eines solchen Systems kümmert sich darum, dass das System korrekt und verlässlich arbeitet.	☐	☐	☐	☐	☐
Wenn die Vorteile nicht überwiegen, würde ein solches System nicht eingesetzt werden.	☐	☐	☐	☐	☐
Ich muss mir wegen des Einsatzes eines solchen Systems keine Sorgen machen.	☐	☐	☐	☐	☐
Durch ein solches System fühle ich mich im überwachten Bereich sicherer.	☐	☐	☐	☐	☐

B5. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich finde solche Systeme gut.	☐	☐	☐	☐	☐
Solche Systeme sollten gesetzlich verboten werden.	☐	☐	☐	☐	☐
Die erreichte Sicherheit steht in keinem Verhältnis zu der verlorenen Freiheit.	☐	☐	☐	☐	☐
Es sollten mehr Systeme dieser Art installiert werden.	☐	☐	☐	☐	☐
Durch solche Systeme wird Sicherheitspersonal ersetzt, das die notwendigen Aufgaben besser erledigen könnte.	☐	☐	☐	☐	☐

Section C: Techniken

Wir werden Ihnen nun mehrere Techniken präsentieren die in einem intelligenten Überwachungssystem zum Einsatz kommen können. Dabei werden wir immer eine Technik demonstrieren und Ihnen danach Zeit geben den dazugehörigen Fragen zu beantworten. Bitte warten Sie mit dem Ausfüllen der Fragen immer bis zum Ende der Demonstration.

C1. Wir haben Ihnen einige Möglichkeiten gezeigt, um mittels eines Smartphones zusätzliche Informationen über ein Überwachungssystem zu bekommen. Bitte bewerten Sie, ob Sie folgenden Aussagen zur präsentierten Technik zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich finde die Angabe von Basisinformationen des Systems gut.	☐	☐	☐	☐	☐
Ich finde die Angabe über die Speicherung der Videodaten gut.	☐	☐	☐	☐	☐
Ich finde die Angabe des Datenschutzbeauftragten gut.	☐	☐	☐	☐	☐
Ich finde die Angabe über den Zweck einer Überwachungsanlage gut.	☐	☐	☐	☐	☐
Die angebotene Transparenz steigert mein Vertrauen in den Datenschutz des Systems.	☐	☐	☐	☐	☐
Die angebotene Transparenz steigert mein Vertrauen in die Sicherheit des Systems.	☐	☐	☐	☐	☐

C2. Wir haben Ihnen einige Möglichkeiten gezeigt, um mittels eines Smartphones zusätzliche Informationen über die Kameras eines Überwachungssystems zu bekommen. Bitte bewerten Sie, ob Sie folgenden Aussagen zur präsentierten Technik zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Die Komfortfunktion, um mittels Kamera zu schauen ob z.B. noch Taxis da sind, finde ich gut.	☐	☐	☐	☐	☐
Ich würde die Komfortfunktion selbst nutzten, um mich zu informieren ob z.B. noch Taxis da sind.	☐	☐	☐	☐	☐
Ich finde die Angaben zu den einzelnen Kameras gut.	☐	☐	☐	☐	☐
Die Idee, nach einer Anmeldung kurze Zeit Zugriff auf die Bilder einer Kamera zu haben, gefällt mir.	☐	☐	☐	☐	☐
Ich hätte Angst, dass der Zugriff auf die Bilder einer Kamera trotz der gezeigten Sicherheitsvorkehrung missbraucht wird.	☐	☐	☐	☐	☐
Jeder sollte auch ohne eine Anmeldung immer Zugriff auf die aufgenommenen Bilder aller Kameras haben.	☐	☐	☐	☐	☐

C3. Wir haben Ihnen eine Möglichkeit gezeigt, um mittels eines Smartphones das Überwachungssystem als Navigationshilfe einzusetzen. Bitte bewerten Sie, ob Sie folgenden Aussagen zur präsentierten Technik zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Den Service, das System als Navigationshilfe zu verwenden, finde ich gut.	☐	☐	☐	☐	☐
Ich würde die Navigationshilfe selbst nutzten.	☐	☐	☐	☐	☐
Ich hätte Angst, dass die für die Navigation erfassten Daten noch für andere Zwecke genutzt werden.	☐	☐	☐	☐	☐
Die Navigationshilfe steigert meine Akzeptanz des Systems.	☐	☐	☐	☐	☐

C4. Wir haben Ihnen eine Möglichkeit gezeigt, um mittels eines Smartphones das Überwachungssystems zu nutzen, um sich mit Ihren Freunden zu treffen. Bitte bewerten Sie, ob Sie folgenden Aussagen zur eben präsentierten Technik zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Die Idee, das System zu nutzen um mich mit meinen Freunden zu treffen, finde ich gut.	☐	☐	☐	☐	☐
Ich würde den Buddy Finder selbst nutzen.	☐	☐	☐	☐	☐
Ich würde den Buddy Finder immer nur kurzzeitig nutzen und danach wieder ausschalten.	☐	☐	☐	☐	☐
Ich würde den Buddy Finder immer aktivieren, damit ich besser von Freunden gefunden werden kann.	☐	☐	☐	☐	☐
Es reicht mir, wenn ich für Freunde den Zugriff auf meine Position erlauben oder sperren kann.	☐	☐	☐	☐	☐
Ich würde die Möglichkeit nutzen, meine Position weiter zu anonymisieren.	☐	☐	☐	☐	☐
Ich würde für alle Freunde die gleichen Datenschutzeinstellungen aktivieren.	☐	☐	☐	☐	☐
Ich würde je nach Freund unterschiedliche Datenschutzeinstellungen nutzen.	☐	☐	☐	☐	☐
Ich hätte Angst, dass die für den Buddy Finder erfassten Daten noch für andere Zwecke genutzt werden.	☐	☐	☐	☐	☐
Der Buddy Finder steigert meine Akzeptanz des Systems.	☐	☐	☐	☐	☐

C5. Wir haben Ihnen eine Möglichkeit gezeigt, um einen Operator bei der Auswertung der Kamerabilder zu unterstützen. Bitte bewerten Sie, ob Sie folgenden Aussagen zur präsentierten Technik zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich finde es gut, wenn ich mittels einer Geste einen Alarm auslösen kann.	☐	☐	☐	☐	☐
Ich würde im Bedarfsfall selbst eine Geste nutzen um einen Alarm auszulösen.	☐	☐	☐	☐	☐
Wenn Systeme Gesten einsetzen um Alarme auszulösen, soll der Operator nur Bilder von Kameras sehen, wenn eine solche Geste erkannt wurde.	☐	☐	☐	☐	☐
Die Möglichkeit, Alarme per Geste auszulösen sollte bestehende Systeme erweitern, ohne dabei den Zugriff des Operators auf Videobilder zu beschränken.	☐	☐	☐	☐	☐
Ich hätte Angst, dass das Auslösen eines Alarms mittels Geste im Notfall nicht richtig funktioniert.	☐	☐	☐	☐	☐
Ich hätte Angst, dass der Gestenalarm, beispielsweise von Jugendlichen, zum Spaß ausgelöst wird und dadurch die Sicherheitsleute abgelenkt werden.	☐	☐	☐	☐	☐
Ich hätte Angst, dass der Gestenalarm absichtlich falsch ausgelöst wird, um die Aufmerksamkeit der Sicherheitsleute von echten Straftaten abzulenken.	☐	☐	☐	☐	☐
Der Gestenalarm steigert meine Akzeptanz des Überwachungssystems.	☐	☐	☐	☐	☐

C6. Wir haben Ihnen einige Möglichkeiten gezeigt, um mittels einer Smartphone App mobiles Sicherheitspersonal durch das Überwachungssystem zu unterstützen. Bitte bewerten Sie, ob Sie folgenden Aussagen zur präsentierten Technik zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich finde es gut, wenn die Zentrale die Position der mobilen Kollegen einsehen kann.	☐	☐	☐	☐	☐
Wenn die Zentrale die Position aller mobilen Kollegen kennt, steigt die Sicherheit.	☐	☐	☐	☐	☐
Ich finde es gut, wenn mobiles Sicherheitspersonal jederzeit Zugriff auf die Bilder aller Kameras hat.	☐	☐	☐	☐	☐
Mobiles Sicherheitspersonal sollte nur Zugriff auf die Bilder der Kameras in seiner Umgebung haben.	☐	☐	☐	☐	☐
Mobiles Sicherheitspersonal sollte keinen Zugriff auf die Bilder der Kameras haben.	☐	☐	☐	☐	☐
Wenn mobiles Sicherheitspersonal Zugriff auf die Bilder der Kameras hat, steigert dies die Sicherheit.	☐	☐	☐	☐	☐
Ich finde es gut, wenn mobiles Sicherheitspersonal die Position von Alarmen einsehen kann.	☐	☐	☐	☐	☐
Wenn mobiles Sicherheitspersonal die Position von Alarmen einsehen kann, steigert dies die Sicherheit.	☐	☐	☐	☐	☐

Section D: Abschließende Fragen zur Videoüberwachung

In diesem Abschnitt möchten wir noch einige allgemeine Fragen zum Thema Videoüberwachung stellen.

D1. Bitte bewerten Sie, für die unten angegebenen Szenarien welches Videosystem Sie bevorzugen würden.

	unbedingt intelligentes System	eher intelligentes System	unentschieden	eher konventionelles System	unbedingt konventionelles System
Flughafen	☐	☐	☐	☐	☐
Öffentlicher Nahverkehr (U-Bahn, Tram, ...)	☐	☐	☐	☐	☐
Fernverkehrszüge	☐	☐	☐	☐	☐
Öffentliche Plätze	☐	☐	☐	☐	☐
Sportstätten	☐	☐	☐	☐	☐
Banken	☐	☐	☐	☐	☐
Parkhäusern	☐	☐	☐	☐	☐
An Arbeitsplätzen mit gefährlichen Stoffen	☐	☐	☐	☐	☐

D2. Bitte bewerten Sie, ob Sie folgenden abschließenden Aussagen zur Videoüberwachung zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Generell fühle ich mich durch Videoüberwachung belästigt.	☐	☐	☐	☐	☐
An Orten mit Videoüberwachung fühle ich mich unwohl.	☐	☐	☐	☐	☐
Videoüberwachungssysteme werden nur an sehr gefährlichen Orten installiert.	☐	☐	☐	☐	☐
In einer überwachten Umgebung fühle ich mich in meinem Verhalten eingeschränkt.	☐	☐	☐	☐	☐
In einer überwachten Umgebung fühle ich mich beobachtet.	☐	☐	☐	☐	☐
Ich halte die gezeigte Entwicklung für einen wünschenswerten Fortschritt.	☐	☐	☐	☐	☐
Der technische Fortschritt von intelligenten Systemen sollte gesetzlich reguliert werden.	☐	☐	☐	☐	☐

Section E: Sozioökonomischer Teil

Bitte beantworten Sie uns noch einige letzte Fragen für die Statistik.

E1. Welches Geschlecht haben Sie?

- ☐ weiblich
- ☐ männlich
- ☐ Keine Angabe

E2. Wie alt sind Sie?

- ☐ 14-19 Jahre
- ☐ 20-29 Jahre
- ☐ 30-39 Jahre
- ☐ 40-49 Jahre
- ☐ 50-59 Jahre
- ☐ 60-69 Jahre
- ☐ 70 und älter
- ☐ Keine Angabe

E3. Welchen höchsten Schulabschluss haben Sie?

Sollten Sie einen ausländischen Schulabschluss haben, so versuchen Sie bitte diesen einem der deutschen Bildungsabschlüsse zuzuordnen.

- ☐ Sonderschulabschluss, Abschluss der Förderschule
- ☐ Volks- oder Hauptschulabschluss / Polytechnische Oberschule 8. Klasse
- ☐ Mittlere Reife (Realschulabschluss, Polytechnische Oberschule 10. Klasse)
- ☐ Fachhochschulreife, Abitur, Erweiterte Oberschule
- ☐ Abgeschlossenes Studium
- ☐ Weiß nicht
- ☐ Keine Angabe

E4. Was machen Sie derzeit hauptsächlich?

- ☐ Erwerbstätig (auch selbstständig)
- ☐ In Ausbildung, Schule, Umschulung, Studium, Wehr-/Zivildienst
- ☐ Rentner, Pensionär, Vorruhestand
- ☐ Hausmann/-frau, Elternzeit, Mutterschutz
- ☐ Zurzeit arbeitslos
- ☐ Keine Angabe

E5. Haben Sie mindestens einen eigenen PC oder Laptop?

- ☐ Ja
- ☐ Nein
- ☐ Keine Angabe

E6. Was ist das modernste Mobiltelefon das sie besitzen?

- ☐ Ein herkömmliches Mobiltelefon
- ☐ Ein Smartphone (iPhone, Android, Blackberry, Windows Phone 7)
- ☐ Besitze gar kein Mobiltelefon
- ☐ Keine Angabe

E7. Wenn sie technische Probleme mit beispielsweise Ihrem PC oder Handy haben, können Sie diese:

- ☐ fast immer selbst lösen
- ☐ manchmal selbst lösen
- ☐ fast niemals selbst lösen
- ☐ Weiß nicht
- ☐ Keine Angabe

E8. Wie würden Sie Ihre Wohngegend einordnen? Ist Ihre Gegend …

- ☐ Großstädtisch und Einzugsbereich
- ☐ Städtisch
- ☐ Kleinstädtisch
- ☐ Ländlich geprägt
- ☐ Weiß nicht
- ☐ Keine Angabe

E9. Wie sind Sie auf diese Befragung aufmerksam geworden?

- ☐ Mailingliste WIR
- ☐ Mailingliste FU-Informatik
- ☐ UdK-Mailingliste(n)
- ☐ NTF-Mailingliste
- ☐ XING
- ☐ Facebook
- ☐ Google+
- ☐ Twitter
- ☐ Persönliche Empfehlung
- ☐ Keine Angabe
- ☐ Andere Quelle:

Andere Quelle:

Vielen Dank, dass Sie sich die Zeit genommen haben, den Fragebogen auszufüllen. Wenn Sie noch Fragen zur Demonstration haben, sprechen Sie uns an oder schreiben Sie eine E-Mail an: erik.krempel@iosb.fraunhofer.de

B Verwendete Skalen für die Evaluierung von TAM-VS

Item	Fragentext	Loadings konv. Szenario	Loadings int. Szenario
PU1	Das vorgestellte System erleichtert die Arbeit des Sicherheitspersonals.	0,81	0,74
PU2	Das vorgestellte System steigert die Sicherheit im überwachten Bereich.	0,85	0,84
PU3	Das vorgestellte System erleichtert das Erkennen von Straftaten.	0,64	0,80
PU5	Das vorgestellte System ermöglicht, dass das Sicherheitspersonal große Bereiche sichern kann.	0,89	0,90
	Average Variance Extracted (AVE)	0,64	0,68
	Composite Reliability	0,88	0,89
	Cronbach α	0,82	0,84

Tabelle B.1: Skaleninstrument für die empfundene Nützlichkeit

Item	Fragentext	Loadings konv. Szenario	Loadings int. Szenario
RI1	Die Verarbeitung von Daten durch das System ist für mich nachteilig.	0,78	0,90
RI3	Durch Fehler in der Erfassung oder Verarbeitung können mir Nachteile entstehen.	0,81	0,85
	Average Variance Extracted (AVE)	0,63	0,77
	Composite Reliability	0,77	0,87
	Cronbach α	0,42	0,70

Tabelle B.2: Skaleninstrument für das empfundene Missbrauchsrisiko

Item	Fragentext	Loadings konv. Szenario	Loadings int. Szenario
TR2	Ich fühle mich gut darüber informiert, wie die Daten vom System verarbeitet werden.	0,91	0,81
TR3	Ich weiß zu welchem Zweck das System installiert ist.	0,92	0,86
TR4	Ich weiß, wer der verantwortliche Betreiber der Anlage ist.	0,60	0,78
	Average Variance Extracted (AVE)	0,68	0,67
	Composite Reliability	0,86	0,86
	Cronbach α	0,76	0,75

Tabelle B.3: Skaleninstrument für die Transparenz der Datenverarbeitung

Item	Fragentext	Loadings konv. Szenario	Loadings int. Szenario
EA1	Ich glaube, dass der Einsatz solcher Systeme sinnvoll ist.	0,83	0,85
EA4	Ich muss mir wegen des Einsatzes eines solchen Systems keine Sorgen machen.	0,79	0,77
EA5	Durch ein solches System fühle ich mich im überwachten Bereich sicherer.	0,83	0,81
	Average Variance Extracted (AVE)	0,67	0,66
	Composite Reliability	0,86	0,85
	Cronbach α	0,75	0,74

Tabelle B.4: Skaleninstrument für die emotionale Einstellung

Item	Fragentext	Loadings konv. Szenario	Loadings int. Szenario
AC1	Ich finde solche Systeme gut.	0,92	0,93
AC2	Solche Systeme sollten gesetzlich verboten werden.	0,76	0,78
AC4	Es sollten mehr Systeme dieser Art installiert werden.	0,83	0,87
	Average Variance Extracted (AVE)	0,71	0,75
	Composite Reliability	0,88	0,90
	Cronbach α	0,79	0,83

Tabelle B.5: Skaleninstrument für die Akzeptanz

C Vorprüfung der Datenschutz-Folgenabschätzung

Mit diesem Fragebogen wird untersucht, ob für eine vorliegende Technologie eine DSFA gemacht werden muss. Die Durchführung wird empfohlen, wenn mindestens eine der Fragen mit „Ja“ beantwortet wird.

	WERDEN INNERHALB DES PROJEKTES…	JA	NEIN
1.	Öffentliche Register erstellt oder verändert?	☐	☐
2.	Personenbezogene Daten verarbeitet?	☐	☐
3.	Bereits gespeicherte personenbezogene Daten für einen neuen Zweck verarbeitet?	☐	☐
4.	Personenbezogene Daten der Öffentlichkeit oder dritten Stellen offengelegt?	☐	☐
5.	Die Zugriffsmöglichkeiten von Individuen auf die über sie gespeicherten Daten eingeschränkt?	☐	☐
6.	Geheimhaltungspflichten oder Vertraulichkeitsvereinbarungen erstellt oder geändert, die sich auf personenbezogenen Daten beziehen?	☐	☐
7.	Der Missbrauch personenbezogener Daten durch neue oder bekannte Angriffsszenarien begünstigt?	☐	☐
8.	Anforderungen gestellt oder geändert um personenbezogene Daten zu speichern, aufzubewahren oder zu sichern?	☐	☐
9.	Neue Anforderungen an die Erfassung, Erhebung oder Verarbeitung bestehender IDs gestellt?	☐	☐
10.	Systeme entwickelt, die zur Identifizierung von Personen dienen? (z.B. durch den Einsatz von Biometrie)	☐	☐
11.	Personenbezogene Daten durch oder innerhalb von Behörden verknüpft oder zusammengeführt? (Data Matching)	☐	☐
12.	Personenbezogene Daten an Stellen außerhalb von Deutschland übermittelt oder mit diesen ausgetauscht?	☐	☐
13.	Personenbezogene Informationen für wissenschaftliche oder statistische Zwecke verwendet?	☐	☐
14.	Befugnisse zur Durchsuchung, Festnahme oder Berührung von Personen gegeben, die zu körperlichen Kontakten führen? (z.B. Blutabnahme)	☐	☐
15.	Bewegungen, das Verhalten oder die Kommunikation von Individuen überwacht, aufgezeichnet oder ausgewertet?	☐	☐
16.	Änderungen an Gebäuden oder Räumlichkeiten vorgenommen, die private Bereiche betreffen?	☐	☐
17.	Andere Auswirkungen auf die Privatsphäre erwartet?	☐	☐

D Fragebogen zu TAM-VS Version 2

Der Fragebogen, wie er für die zweite Datenerhebung für das Akzeptanzmodell TAM-VS2 im Szenario „NurseEye im Krankenhaus“ genutzt wurde.

Vielen Dank, dass Sie sich zur Teilnahme an dieser Befragung bereiterklärt haben. Die Bearbeitung des gesamten Fragenbogens sollte nach der Demonstration ca. 15 Minuten dauern.

Section A: NurseEye-Demonstrator

Wir haben Ihnen an Hand unseres Demonstrators NurseEye ein Szenario für eine automatische Sturzdetektion und Alarmierung gezeigt. Bitte beachten Sie, dass sich alle nun folgenden Fragen auf dieses System beziehen!

A1. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Das vorgestellte System erleichtert die Arbeit des Pflegepersonals.	☐	☐	☐	☐	☐
Das vorgestellte System steigert die Sicherheit im überwachten Bereich.	☐	☐	☐	☐	☐
Das vorgestellte System erleichtert das Erkennen von Unfällen.	☐	☐	☐	☐	☐
Das vorgestellte System ermöglicht, dass das Pflegepersonal große Bereiche sichern kann.	☐	☐	☐	☐	☐
Insgesamt finde ich das vorgestellte System zur Steigerung der Sicherheit nützlich.	☐	☐	☐	☐	☐

A2. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich weiß, zu welchem Zweck das System installiert ist.	☐	☐	☐	☐	☐
Ich fühle mich gut darüber informiert, welche Informationen vom System erfasst werden.	☐	☐	☐	☐	☐
Ich fühle mich gut darüber informiert, wie die Daten vom System verarbeitet werden.	☐	☐	☐	☐	☐

A3. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Die Verarbeitung von Daten durch das System ist für mich nachteilig.	☐	☐	☐	☐	☐
Die erfassten Daten könnten unerlaubt verwendet werden.	☐	☐	☐	☐	☐
Durch Fehler in der Erfassung oder Verarbeitung können mir Nachteile entstehen.	☐	☐	☐	☐	☐

A4. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich glaube, dass die Vertraulichkeit meiner Daten gewährleistet ist.	☐	☐	☐	☐	☐
Meine Privatsphäre wird durch das System geschützt.	☐	☐	☐	☐	☐
Die Anonymität von Betroffenen ist sichergestellt.	☐	☐	☐	☐	☐
Die automatische Verarbeitung meiner Daten beunruhigt mich.	☐	☐	☐	☐	☐
Ich hätte Angst, dass Aufnahmen von peinlichen Situationen an Dritte weitergegeben werden.	☐	☐	☐	☐	☐

A5. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich glaube, dass der Einsatz solcher Systeme sinnvoll ist.	☐	☐	☐	☐	☐
Der Betreiber eines solchen Systems kümmert sich darum, dass das System korrekt und verlässlich arbeitet.	☐	☐	☐	☐	☐
Ich muss mir wegen des Einsatzes eines solchen Systems keine Sorgen machen.	☐	☐	☐	☐	☐
Durch ein solches System fühle ich mich im überwachten Bereich sicherer.	☐	☐	☐	☐	☐

A6. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich finde solche Systeme gut.	☐	☐	☐	☐	☐
Solche Systeme sollten gesetzlich verboten werden.	☐	☐	☐	☐	☐
Die erreichte Sicherheit steht in keinem Verhältnis zu der verlorenen Freiheit.	☐	☐	☐	☐	☐
Es sollten mehr Systeme dieser Art installiert werden.	☐	☐	☐	☐	☐
Durch solche Systeme wird nur Pflegepersonal ersetzt, das die notwendigen Aufgaben besser erledigen könnte.	☐	☐	☐	☐	☐

Section B: Vergleichende Fragen NurseEye und klassische Videoüberwachung

In diesem Abschnitt möchten wir noch einige vergleichende Fragen stellen. Wir unterscheiden zwischen dem Ihnen vorgestellten NurseEye-Demonstrator und klassischer Videoüberwachung. Dabei verstehen wir unter klassischer Videoüberwachung ein System, bei dem mehrere Videokameras im überwachten Bereich installiert sind, deren Bilder durchgängig von Wachpersonal gesichtet werden.

B1. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Generell fühle ich mich durch klassische Videoüberwachung belästigt.	☐	☐	☐	☐	☐
An Orten mit klassischer Videoüberwachung fühle ich mich unwohl.	☐	☐	☐	☐	☐
Videoüberwachung unterhöhlt unsere Bürgerrechte.	☐	☐	☐	☐	☐
Klassische Videoüberwachungssysteme werden nur an sehr gefährlichen Orten installiert.	☐	☐	☐	☐	☐
In einer mit einem klassischen Videoüberwachungssystem überwachten Umgebung fühle ich mich in meinem Verhalten eingeschränkt.	☐	☐	☐	☐	☐
In einer mit einem klassischen Videoüberwachungssystem überwachten Umgebung fühle ich mich beobachtet.	☐	☐	☐	☐	☐

B2. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Klassische Videoüberwachung kann helfen, akute Sicherheitsprobleme zu lösen.	☐	☐	☐	☐	☐
NurseEye kann helfen, ein akutes Sicherheitsproblem zu lösen.	☐	☐	☐	☐	☐
NurseEye kann helfen, Menschenleben zu retten.	☐	☐	☐	☐	☐
Systeme wie NurseEye werden nur eingesetzt, um Personal einzusparen.	☐	☐	☐	☐	☐
Pflegepersonal sollte jederzeit, auch ohne akuten Alarm, Zugriff auf anonymisierte Videokameras haben.	☐	☐	☐	☐	☐
Pflegepersonal sollte jederzeit, auch ohne akuten Alarm, Zugriff auf Videokameras haben.	☐	☐	☐	☐	☐

B3. Bitte bewerten Sie, ob Sie folgenden Aussagen zustimmen:

	Ich stimme zu (+2)	(+1)	Ich bin neutral (0)	(-1)	Ich stimme nicht zu (-2)
Ich hätte Freude daran, ein System wie NurseEye zu verwenden.	☐	☐	☐	☐	☐
Die mit den installierten Display erreichte Transparenz in NurseEye finde ich wichtig.	☐	☐	☐	☐	☐
Die mit den installierten Display erreichte Transparenz in NurseEye finde ich ausreichend.	☐	☐	☐	☐	☐
Ich finde es wichtig, Videos von möglichen Stürzen zu anonymisieren.	☐	☐	☐	☐	☐
NurseEye erfüllt meine Ansprüche an Sicherheit und Datenschutz.	☐	☐	☐	☐	☐
Ich halte die durch NurseEye gezeigte Entwicklung für einen wünschenswerten Fortschritt.	☐	☐	☐	☐	☐

Section C: Sozioökonomischer Teil

Bitte beantworten Sie uns noch einige letzte Fragen für die Statistik.

C1. Welches Geschlecht haben Sie?

- ☐ Weiblich
- ☐ Männlich
- ☐ Keine Angabe

C2. Wie alt sind Sie?

- ☐ 14-19 Jahre
- ☐ 20-29 Jahre
- ☐ 30-39 Jahre
- ☐ 40-49 Jahre
- ☐ 50-59 Jahre
- ☐ 60-69 Jahre
- ☐ 70 und älter
- ☐ Keine Angabe

C3. Welchen höchsten Schulabschluss haben Sie?

Sollten Sie einen ausländischen Schulabschluss haben, so versuchen Sie bitte diesen einem der deutschen Bildungsabschlüsse zuzuordnen.

- ☐ Sonderschulabschluss, Abschluss der Förderschule
- ☐ Volks- oder Hauptschulabschluss / Polytechnische Oberschule 8. Klasse
- ☐ Mittlere Reife (Realschulabschluss, Polytechnische Oberschule 10. Klasse)
- ☐ Fachhochschulreife, Abitur, Erweiterte Oberschule
- ☐ Abgeschlossenes Studium
- ☐ Weiß nicht
- ☐ Keine Angabe

C4. Was machen Sie derzeit hauptsächlich?

- ☐ Erwerbstätig (auch selbstständig)
- ☐ In Ausbildung, Schule, Umschulung, Studium, Wehr-/Zivildienst
- ☐ Rentner, Pensionär, Vorruhestand
- ☐ Hausmann/-frau, Elternzeit, Mutterschutz
- ☐ Zurzeit arbeitslos
- ☐ Keine Angabe

C5. Was ist das modernste Mobiltelefon, das Sie besitzen?

- ☐ Ein herkömmliches Mobiltelefon
- ☐ Ein Smartphone (iPhone, Android, Blackberry, Windows Phone)
- ☐ Besitze gar kein Mobiltelefon
- ☐ Keine Angabe

C6. Wenn sie technische Probleme mit beispielsweise Ihrem PC oder Handy haben, können Sie diese:

- ☐ Fast immer selbst lösen
- ☐ Manchmal selbst lösen
- ☐ Fast niemals selbst lösen
- ☐ Weiß nicht
- ☐ Keine Angabe

C7. Wie würden Sie Ihre Wohngegend einordnen? Ist sie…

- ☐ Großstädtisch und Einzugsbereich
- ☐ Städtisch
- ☐ Kleinstädtisch
- ☐ Ländlich geprägt
- ☐ Weiß nicht
- ☐ Keine Angabe

Vielen Dank, dass Sie sich die Zeit genommen haben, den Fragebogen auszufüllen.

Wenn Sie noch Fragen zu NurseEye oder unserer Forschung haben, sprechen Sie uns an oder schreiben Sie eine E-Mail an:

erik.krempel@iosb.fraunhofer.de

E Verwendete Skalen für die Evaluierung von TAM-VS2

Item	Fragentext	Loadings
PU1	Das vorgestellte System erleichtert die Arbeit des Pflegepersonals.	0,68
PU6	Insgesamt finde ich das vorgestellte System zur Steigerung der Sicherheit nützlich.	0,89
PU7	NurseEye kann helfen, ein akutes Sicherheitsproblem zu lösen.	0,83
	Average Variance Extracted (AVE)	0,65
	Composite Reliability	0,84
	Cronbach α	0,73

Tabelle E.1: Skaleninstrument für die empfundene Nützlichkeit

Item	Fragentext	Loadings
RI2	Die erfassten Daten könnten unerlaubt verwendet werden.	0,73
RI4	Durch Fehler in der Erfassung oder Verarbeitung können mir Nachteile entstehen.	0,82
RI5	Ich hätte Angst, dass Aufnahmen von peinlichen Situationen an Dritte weitergegeben werden.	0,80
	Average Variance Extracted (AVE)	0,62
	Composite Reliability	0,83
	Cronbach α	0,69

Tabelle E.2: Skaleninstrument für das empfundene Missbrauchsrisiko

Item	Fragentext	Loadings
TR1	Ich fühle mich gut darüber informiert, welche Informationen vom System erfasst werden.	0,96
TR2	Ich fühle mich gut darüber informiert, wie die Daten vom System verarbeitet werden.	0,87
	Average Variance Extracted (AVE)	0,83
	Composite Reliability	0,91
	Cronbach α	0,81

Tabelle E.3: Skaleninstrument für die Transparenz der Datenverarbeitung

Item	Fragentext	Loadings
AN1	Ich glaube, dass die Vertraulichkeit meiner Daten gewährleistet ist.	0,83
AN2	Meine Privatsphäre wird durch das System geschützt.	0,77
AN3	Die Anonymität von Betroffenen ist sichergestellt.	0,78
	Average Variance Extracted (AVE)	0,64
	Composite Reliability	0,84
	Cronbach α	0,73

Tabelle E.4: Skaleninstrument für die Anonymisierung

Item	Fragentext	Loadings
EA1	Ich glaube, dass der Einsatz solcher Systeme sinnvoll ist.	0,80
EA2	Der Betreiber eines solchen Systems kümmert sich darum, dass das System korrekt und verlässlich arbeitet.	0,86
EA4	Ich muss mir wegen des Einsatzes eines solchen Systems keine Sorgen machen.	0,79
	Average Variance Extracted (AVE)	0,67
	Composite Reliability	0,86
	Cronbach α	0,75

Tabelle E.5: Skaleninstrument für die emotionale Einstellung

Item	Fragentext	Loadings
AC1	Solche Systeme sollten gesetzlich verboten werden.	0,89
AC4	Es sollten mehr Systeme dieser Art installiert werden.	0,82
AC8	Ich halte die durch NurseEye gezeigte Entwicklung für einen wünschenswerten Fortschritt.	0,82
	Average Variance Extracted (AVE)	0,71
	Composite Reliability	0,88
	Cronbach α	0,80

Tabelle E.6: Skaleninstrument für die Akzeptanz

F Datentabellen zur statistischen Analyse

	Stichprobe	
Antwort	#	%
Ich stimme zu (+2)	14	18,2
(+1)	39	50,6
Ich bin neutral (0)	9	11,7
(-1)	8	10,4
Ich stimme nicht zu (-2)	7	9,1
Keine Antwort	0	0,0
Gesamt	**77**	**100,0**

Tabelle F.1: Auswertung der Frage: Klassische Videoüberwachung kann helfen, akutes Sicherheitsprobleme zu lösen.

	Stichprobe		Frauen		Männer	
Antwort	#	%	#	%	#	%
Ich stimme zu (+2)	30	39,0	9	64,3	21	33,3
(+1)	33	42,9	4	28,6	29	46,0
Ich bin neutral (0)	10	13,0	1	7,1	9	14,3
(-1)	1	1,3	0	0,0	1	1,6
Ich stimme nicht zu (-2)	2	2,6	0	0,0	2	3,2
Keine Antwort	1	1,3	0	0,0	1	1,6
Gesamt	77	100,0	14	100,0	63	100,0

Tabelle F.2: Auswertung der Frage: NurseEye kann helfen, ein akute Sicherheitsprobleme zu lösen.

	Stichprobe		Frauen		Männer	
Antwort	#	%	#	%	#	%
Ich stimme zu (+2)	49	63,6	12	85,7	37	58,7
(+1)	21	27,3	2	14,3	19	30,2
Ich bin neutral (0)	7	9,1	0	0,0	7	11,1
(-1)	0	0,0	0	0,0	0	0,0
Ich stimme nicht zu (-2)	0	0,0	0	0,0	0	0,0
Keine Antwort	0	0,0	0	0,0	0	0,0
Gesamt	77	100,0	14	100,0	63	100,0

Tabelle F.3: Auswertung der Frage: NurseEye kann helfen, Menschenleben zu retten.

	Stichprobe		Frauen		Männer	
Antwort	#	%	#	%	#	%
Ich stimme zu (+2)	0	0,0	0	0,0	0	0,0
(+1)	12	15,6	1	7,1	11	17,5
Ich bin neutral (0)	21	27,3	1	7,1	20	31,7
(-1)	26	33,8	6	42,9	20	31,7
Ich stimme nicht zu (-2)	18	23,4	6	42,9	12	19,0
Keine Antwort	0	0,0	0	0,0	0	0,0
Gesamt	77	100,0	14	100,0	63	100,0

Tabelle F.4: Auswertung der Frage: Systeme wie NurseEye werden nur eingesetzt, um Personal zu sparen.

	Stichprobe	
Antwort	#	%
Ich stimme zu (+2)	7	9,1
(+1)	11	14,3
Ich bin neutral (0)	14	18,2
(-1)	18	23,4
Ich stimme nicht zu (-2)	26	33,8
Keine Antwort	1	1,3
Gesamt	77	100,0

Tabelle F.5: Auswertung der Frage: Pflegepersonal sollte jederzeit, auch ohne akuten Alarm, Zugriff auf anonymisierte Videokameras haben.

	Stichprobe	
Antwort	#	%
Ich stimme zu (+2)	3	3,9
(+1)	3	3,9
Ich bin neutral (0)	7	9,1
(-1)	23	29,9
Ich stimme nicht zu (-2)	41	53,2
Keine Antwort	0	0,0
Gesamt	77	100,0

Tabelle F.6: Auswertung der Frage: Pflegepersonal sollte jederzeit, auch ohne akuten Alarm, Zugriff auf Videokameras haben.

	Stichprobe	
Antwort	#	%
Ich stimme zu (+2)	31	40,3
(+1)	20	26,0
Ich bin neutral (0)	16	20,8
(-1)	9	11,7
Ich stimme nicht zu (-2)	1	1,3
Keine Antwort	0	0,0

Tabelle F.7: Auswertung der Frage: Ich finde es wichtig, Videos von möglichen Stürzen zu anonymisieren.

	Stichprobe	
Antwort	#	%
Ich stimme zu (+2)	25	32,5
(+1)	28	36,4
Ich bin neutral (0)	21	27,3
(-1)	2	2,6
Ich stimme nicht zu (-2)	1	1,3
Keine Antwort	0	0,0
Gesamt	77	100,0

Tabelle F.8: Auswertung der Frage: Die mit den installierten Displays erreichte Transparenz in NurseEye finde ich wichtig.

	Stichprobe	
Antwort	#	%
Ich stimme zu (+2)	9	11,7
(+1)	41	53,2
Ich bin neutral (0)	18	23,4
(-1)	6	7,8
Ich stimme nicht zu (-2)	3	3,9
Keine Antwort	0	0,0
Gesamt	77	100,0

Tabelle F.9: Auswertung der Frage: Die mit den installierten Displays erreichte Transparenz in NurseEye finde ich ausreichend.

	Stichprobe		Frauen		Männer	
Antwort	#	%	#	%	#	%
Ich stimme zu (+2)	16	20,8	5	35,7	11	17,5
(+1)	33	42,9	8	57,1	25	39,7
Ich bin neutral (0)	21	27,3	1	7,1	20	31,7
(-1)	6	7,8	0	0,0	6	9,5
Ich stimme nicht zu (-2)	1	1,3	0	0,0	1	1,6
Keine Antwort	0	0	0	0,0	0	0,0
Gesamt	77	100	14	100,0	63	100,0

Tabelle F.10: Auswertung der Frage: NurseEye erfüllt meine Ansprüche an Sicherheit und Datenschutz.

	Stichprobe		Frauen		Männer	
Antwort	#	%	#	%	#	%
Ich stimme zu (+2)	45	58,4	13	92,9	32	50,8
(+1)	25	32,5	1	7,1	24	38,1
Ich bin neutral (0)	6	7,8	0	0,0	6	9,5
(-1)	1	1,3	0	0,0	1	1,6
Ich stimme nicht zu (-2)	0	0,0	0	0,0	0	0,0
Keine Antwort	0	0,0	0	0,0	0	0,0
Gesamt	77	100,0	14	100,0	63	100,0

Tabelle F.11: Auswertung der Frage: Ich halte die durch NurseEye gezeigte Entwicklung für einen wünschenswerten Fortschritt.

Eigene Veröffentlichungen

[Bie+12a] Christoph Bier, Pascal Birnstill, Erik Krempel, Hauke Vagts und Jürgen Beyerer. „Enhancing Privacy by Design From a Developer's Perspective". In: *Privacy technologies and policy: 1st Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012*. 2012, S. 73–85.

[Bie+12b] Christoph Bier, Pascal Birnstill, Erik Krempel, Hauke Vagts und Jürgen Beyerer. „How is Positive-Sum Privacy Feasible". In: *7th Future Security, Security Research Conference, Berlin, September 2012*. Bonn, Germany, Sep. 2012, S. 265–268.

[Bir+13] Pascal Birnstill, Sebastian Bretthauer, Simon Greiner und Erik Krempel. „Privacy Preserving Surveillance: An Interdisciplinary Approach". In: *SMART Workshop 2013 - Brussels*. Berlin, Germany, Sep. 2013.

[BK12] Christoph Bier und Erik Krempel. „Common Privacy Patterns in Video Surveillance and Smart Energy". In: *7th ICCCT: 2012 International Conference on Computing and Convergence Technology*. 2012, S. 610–615.

[BK14] Sebastian Bretthauer und Erik Krempel. „Videomonitoring zur Sturzdetektion und Alarmierung - Eine technische und rechtliche Analyse". In: *17. Internationales Rechtsinformatik Symposion (IRIS) 2014 - Transparenz*. zugleich online in: Jusletter IT 20. Februar 2014, http://jusletter-it.weblaw.ch/]. 2014, S. 525–534.

[BKB15] Sebastian Bretthauer, Erik Krempel und Pascal Birnstill. „Intelligente Videoüberwachung in Kranken- und Pflegeeinrichtungen von morgen: eine Analyse der Bedingungen nach den Entwürfen

der EU-Kommission und des EU-Parlaments für eine DS-GVO". In: *Computer und Recht : CR ; Zeitschrift für die Praxis des Rechts der Informationstechnologien* 31.31 (2015), S. 239–245.

[Fis+14] Yvonne Fischer, Erik Krempel, Pascal Birnstill, Gabriel Unmüßig, Eduardo Monari, Jürgen Moßgraber, Manfred Schenk und Jürgen Beyerer. „Privacy-Aware Smart Video Surveillance Revisited". In: *9th Future Security, Security Research Conference, Berlin, September 16-18.* 2014, S. 91–99.

[Gra+14] Gunther Grasemann, Mario Kaufmann, Erik Krempel, C. Hurrey und T. Ahonen. „Multi-Criteria Evaluation for Automated Border Control". In: *9th Future Security, Security Research Conference, Berlin, September 16-18.* 2014, S. 624–627.

[Gre+13] Simon Greiner, Pascal Birnstill, Erik Krempel, Bernhard Beckert und Jürgen Beyerer. „Privacy Preserving Surveillance and the Tracking-Paradox". In: *8th Future Security: Security Research Conference, Berlin 17.-19. September 2013.* Berlin, Germany, Sep. 2013, S. 296–302.

[KB14] Erik Krempel und Jürgen Beyerer. „TAM-VS: A Technology Acceptance Model for Video Surveillance". In: *Privacy technologies and policy: 2nd Annual Privacy Forum, APF 2014, Athens, Greece, May 20 - 21, 2014.* Hrsg. von Bart Preneel und Demosthenes Ikonomou. Bd. 8450. Lecture Notes in Computer Science. Springer International Publishing, 2014, S. 86–100. URL: http://dx.doi.org/10.1007/978-3-319-06749-0_6.

[KB15] Erik Krempel und Jürgen Beyerer. „Privacy Score: Making privacy aspects of surveillance systems comparable". In: *10th Future Security Conference 2015 (Future Security 2015).* Berlin, Germany, Sep. 2015, S. 65–72.

[KBB16a] Erik Krempel, Pascal Birnstill und Jürgen Beyerer. „A Privacy-aware Fall Detection System for Hospitals and Nursing Facilities“. In: *CPDP Computers, Privacy & Data Protection*. 2016.

[KBB16b] Erik Krempel, Pascal Birnstill und Jürgen Beyerer. „Working and Living in Interactive Environments: Requirements fpr Security and Privacy“. In: *11th Future Security Conference 2016 (Future Security 2016)*. Berlin, Germany, Sep. 2016, S. 65–72.

[KG13] Erik Krempel und Coen van Gulijk. *SURVEILLE Deliverable 3.3b Report on system effectiveness, efficiency and satisfaction assessment; Data Protection*. Sep. 2013. URL: `https://surveille.eui.eu/wp-content/uploads/2015/04/D3.3b-System-Effectiveness-and-Efficiency-Data-Protection.pdf`.

[Oos+14] Anne-Marie Oostveen, Mario Kaufmann, Erik Krempel und Gunther Grasemann. „Automated Border Control: A Comparative Usability Study at Two European Airports“. In: *8th International Conference on Interfaces and Human Computer Interaction (IHCI 2014), Lisbon, Portugal*. 2014.

[VKB10] Hauke Vagts, Erik Krempel und Jürgen Beyerer. „Privacy Enforcement by Identity Management in Smart Surveillance Systems“. In: *Proceedings of the International Conference on Distributed Multimedia Systems*. 16. Knowledge Systems Institute Graduate School. Okt. 2010, S. 64–69.

[VKB12] Hauke Vagts, Erik Krempel und Jürgen Beyerer. „User-centric Protection and Privacy in Smart Surveillance Systems“. In: *7th Future Security, Security Research Conference, Berlin, September 2012*. Bonn, Germany, Sep. 2012, S. 237–248.

[VKF11] Hauke Vagts, Erik Krempel und Yvonne Fischer. „Access Controls for Privacy Protection in Pervasive Environments“. In: *4th ACM International Conference on PErvasive Technologies Related to Assistive Environments PETRA*. 2011.

Betreute Abschlussarbeiten

[Kau13] Mario Kaufmann. „Visualisierung und Manipulation von XACML-Policies für intelligente Überwachungssysteme“. Masterarbeit. Hochschule Karlsruhe, 2013.

[Koc13] Anja Koch. „Privacy Risk Assessments & Privacy Impact Assessments: Eine methodische Analyse von Risiken für die Privatsphäre und ihrer Behandlung in der IT“. Diplomarbeit. Karlsruhe Institut für Technology (KIT), 2013.

[Lau14] Kevin Laubis. „Vorausgreifende Methoden der Transparenz in intelligenten Videoüberwachungsanlagen“. Masterarbeit. Karlsruhe Institut für Technology (KIT), 2014.

[Näg13] Markus Nägelin. „Konzeption und Realisierung einer mobilen Applikation zur Visualisierung von Videoüberwachungssystemen“. Magisterarb. Hochschule Karlsruhe, 2013.

[Rik15] Oleksandr Rikhter. „Entwurf, Implementierung und Integration einer Authentifizierungsmethode für ein Versionsverwaltungssystem mit Hilfe von mobilen Endgeräten“. Bachelorarbeit. Hochschule Karlsruhe, 2015.

[War14] Robert Warzecha. „Komparative Analyse der Privatheits-, Datenschutz- und IT-Sicherheitsansätze der intelligenten Überwachungssysteme NEST und PAWS“. Diplomarbeit. Karlsruhe Institut für Technology (KIT), 2014.

Literatur

Gedruckte Veröffentlichungen

[Ang+05] D. Angiati, G. Gera, S. Piva und C.S. Regazzoni. „A novel method for graffiti detection using change detection algorithm". In: *Advanced Video and Signal Based Surveillance, 2005. AVSS 2005. IEEE Conference on.* Sep. 2005, S. 242–246.

[Ask72] Frank Askin. „Surveillance: The social science perspective". In: *Colum. Hum. Rts. L. Rev.* 4 (1972), S. 59.

[Baa+07] Nadia Baaziz, Nathalie Lolo, Oscar Padilla und Felix Petngang. „Security and privacy protection for automated video surveillance". In: *Signal Processing and Information Technology, 2007 IEEE International Symposium on.* IEEE. 2007, S. 17–22.

[Bay05] F. Bayreuther. „Videoüberwachung am Arbeitsplatz". In: *Neue Zeitschrift für Arbeitsrecht* 18 (2005), S. 1038–1044.

[BD12] Christoph Bier und Indra Spiecker Döhmann. „Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz?" In: *Computer Und Recht: Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation.* Bd. 28. 9. Otto Schmidt. 2012, S. 610–618.

[Bel10] Ahmed Nabil Belbachir. *Smart cameras.* Bd. 20. 10. Springer, 2010.

[Ber00] Andres M. Berger. *Privacy mode for acquisition cameras and camcorders.* US Patent 6,067,399. Mai 2000.

[BG15] Jürgen Beyerer und Jürgen Geisler. „A quantitative risk model for a uniform description of safety and security". In: *10th Future Security Conference 2015 (Future Security 2015)*. Berlin, Germany, Sep. 2015.

[Bie10] Christoph Bier. „Die Anonymisierung von Videoüberwachungsdaten in intelligenten Überwachungssystemen und ihre datenschutzrechtliche Bewertung". Diplomarbeit. Lehrstuhl für Interaktive Echtzeitsysteme, Karlsruher Institut für Technologie, 2010.

[Bir+15] Pascal Birnstill, Sebastian Bretthauer, Simon Greiner und Erik Krempel. „Privacy-preserving surveillance: an interdisciplinary approach". In: Oxford University Press, 2015.

[Bir13] Pascal Birnstill. „Usage Controlled Video Surveillance - Revealing its Potentials for Privacy". In: *8th Future Security. Security Research Conference. Proceedings*. Hrsg. von M. (Ed.) Lauster. Berlin: Fraunhofer Verlag, Sep. 2013.

[Birn16ch] Pascal Birnstill. *Privacy-Respecting Smart Video Surveillance Based on Usage Control Enforcement*. KIT Scientific Publishing, 2016 (voraussichtlich).

[Bou05] Terrance Edward Boult. „PICO: Privacy through invertible cryptographic obscuration". In: *Computer Vision for Interactive and Intelligent Environment, 2005*. IEEE. 2005, S. 27–38.

[BP13] Pascal Birnstill und Alexander Pretschner. „Enforcing privacy through usage-controlled video surveillance". In: *Advanced Video and Signal Based Surveillance (AVSS), 2013 10th IEEE International Conference on*. Aug. 2013, S. 318–323.

[BRB15] Pascal Birnstill, Daoyuan Ren und Jürgen Beyerer. „A user study on anonymization techniques for smart video surveillance". In: *Advanced Video and Signal Based Surveillance (AVSS), 2015 12th IEEE International Conference on*. IEEE. 2015, S. 1–6.

[Buno6] Bundesamt für Sicherheit in der Informationstechnik. *Leitfaden IT-Sicherheit IT-Grundschutz kompakt*. De. Bonn: Bundesamt für Sicherheit in der Informationstechnik, Referat 114 IT-Sicherheitsmanagement und IT-Grundschutz, 2006. URL: http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf (besucht am 16. 10. 2006).

[Bun11] Bundesamt für Sicherheit in der Informationstechnik. *Privacy Impact Assessment Guideline*. Nov. 2011.

[CF11] Andrew Clement und Joseph Ferenbok. „Mitigating Asymmetric Visibilities: Towards a Signage Code for Surveillance Camera Networks". In: *Eyes Everywhere: The Global Growth of Camera Surveillance. London: Routledge* (2011).

[Chi98] Wynne W. Chin. „The partial least squares approach to structural equation modeling". In: *Modern methods for business research* 295.2 (1998), S. 295–336.

[CP84] Gilbert A. Churchill Jr. und J. Paul Peter. „Research design effects on the reliability of rating scales: a meta-analysis". In: *Journal of marketing research* (1984), S. 360–375.

[CPN08] Sen-ching S. Cheung, Jithendra K. Paruchuri und Thinh P. Nguyen. „Managing privacy data in pervasive camera networks". In: *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*. IEEE. 2008, S. 1676–1679.

[CZV06] Sen-ching S. Cheung, Junhua Zhao und M. Vijay Venkatesh. „Efficient object-based video inpainting". In: *Image Processing, 2006 IEEE International Conference on*. IEEE. 2006, S. 705–708.

[Dav89] Fred D. Davis. „Perceived usefulness, perceived ease of use, and user acceptance of information technology". In: *MIS quarterly* 13 (1989), S. 319–340.

[DE06] F. Dufaux und T. Ebrahimi. „Scrambling for Video Surveillance with Privacy“. In: *Computer Vision and Pattern Recognition Workshop (CVPRW'06)*. IEEE. 2006, S. 160.

[DE10] F. Dufaux und T. Ebrahimi. „A framework for the validation of privacy protection solutions in video surveillance“. In: *Multimedia and Expo (ICME), 2010 IEEE International Conference on*. IEEE. 2010, S. 66–71.

[Deg14] Sara Degli Esposti. „A Roadmap for developing acceptable surveillance-based security measures“. In: *9th Future Security, Security Research Conference, Berlin, September 16-18, 2014*. 2014, S. 71–80.

[DSC07] D. Duque, H. Santos und P. Cortez. „Prediction of Abnormal Behaviors for Intelligent Video Surveillance Systems“. In: *Computational Intelligence and Data Mining, 2007. CIDM 2007. IEEE Symposium on*. März 2007, S. 362–367.

[End02] Günter Endruweit. „Akzeptanz und Sozialverträglichkeit“. In: *Wörterbuch der Soziologie* 2 (2002), S. 6–7.

[ETB89] Günter Endruweit, Gisela Trommsdorff und Gerhard Berger. *Wörterbuch der Soziologie*. Bd. 1. Enke Stuttgart, 1989.

[Eur10] European Forum for Urban Security. *Charta für die demokratische Nutzung von Videoüberwachung*. Paris: EFUS, R. Calfa und S. Sperber, 2010. URL: http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_DE.pdf.

[Fis79] Martin Fishbein. „A theory of reasoned action: some applications and implications.“ In: *Nebraska Symposium on Motivation* 27 (Dez. 1979), S. 65–116.

[FL81] C. Fornell und D. F. Larcker. „Evaluating structural equation models with unobservable variables and measurement error“. In: *Journal of marketing research* (1981), S. 39–50.

[FS08] S. Fleck und W. Straßer. „Smart Camera Based Monitoring System and Its Application to Assisted Living". In: *Proceedings of the IEEE* 96 (2008), S. 1698–1714.

[GBA07] Martin Gill, Jane Bryan und Jenna Allen. „Public Perceptions of CCTV in Residential Areas ‚It Is Not As Good As We Thought It Would Be.'" In: *International Criminal Justice Review* 17.4 (2007), S. 304–324.

[Geo03] Darren George. *SPSS for windows step by step: A simple study guide and reference, 17.0 update, 10/e*. Pearson Education India, 2003.

[GKS08] Srivatsava R. Ganta, Shiva P. Kasiviswanathan und Adam Smith. „Composition attacks and auxiliary information in data privacy". In: *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 2008, S. 265–273.

[GM10] Darren George und Paul Mallery. *SPSS for Windows Step by Step: A Simple Guide and Reference 18.0 Update*. 11th. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010.

[Gra86] Jennifer M. Granholm. „Video surveillance on public streets: The constitutionality of invisible citizen searches". In: *U. Det. L. Rev.* 64 (1986), S. 687.

[HD11] Gerrit Hornung und Monika Desoi. „‚Smart Cameras' und automatische Verhaltensanalyse". In: *Verfassungs-und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung Kommunikation & Recht* 3 (2011), S. 153–158.

[Hil09] Thomas Hilpert. „Zulässigkeit der Videoüberwachung nach 9 6b BDSG am Beispiel des ÖPNV". In: *RDV* (2009).

[HRS11] J. F. Hair, C. M. Ringle und M. Sarstedt. „PLS-SEM: Indeed a silver bullet". In: *The Journal of Marketing Theory and Practice* 19.2 (2011), S. 139–152.

[Hu+04] Weiming Hu, Tieniu Tan, Liang Wang und Steve Maybank. „A survey on visual surveillance of object motion and behaviors". In: *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 34.3 (2004), S. 334–352.

[Hul99] John Hulland. „Use of partial least squares (PLS) in strategic management research: A review of four recent studies". In: *Strategic management journal* 20.2 (1999), S. 195–204.

[HVL08] Niels Haering, Péter L. Venetianer und Alan Lipton. „The evolution of video surveillance: an overview". In: *Machine Vision and Applications* 19.5-6 (2008), S. 279–290.

[Jam04] Susan Jamieson. „Likert scales: how to (ab) use them". In: *Medical education* 38.12 (2004), S. 1217–1218.

[Kla06] Francisco Reto Klauser. *Die Videoüberwachung öffentlicher Räume: zur Ambivalenz eines Instruments sozialer Kontrolle*. Bd. 902. Campus Verlag, 2006.

[Kud15] Dominic Kudlacek. *Akzeptanz von Videoüberwachung – Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen*. Springer, 2015.

[LA04] Che-Bin Liu und Narendra Ahuja. „Vision based fire detection". In: *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*. Bd. 4. IEEE. 2004, S. 134–137.

[LKL03b] Younghwa Lee, Kenneth A Kozar und Kai RT Larsen. „The technology acceptance model: Past, present, and future". In: *Communications of the Association for information systems* 12.1 (2003), S. 50.

[LM04] Gitta H. Lubke und Bengt O. Muthén. „Applying multigroup confirmatory factor models for continuous outcomes to Likert scale data complicates meaningful group comparisons". In: *Structural Equation Modeling* 11.4 (2004), S. 514–534.

[MC05] M. Moniri und Claude C. Chibelushi. „Classification of smart video surveillance systems for commercial applications". In: *Advanced Video and Signal Based Surveillance, 2005. AVSS 2005. IEEE Conference on*. IEEE. 2005, S. 638–643.

[MRV10] Jurgen Mossgraber, Frank Reinert und Hauke Vagts. „An architecture for a task-oriented surveillance system: A service-and event-based approach". In: *Systems (ICONS), 2010 Fifth International Conference on*. IEEE. 2010, S. 146–151.

[NAT98] Jeho Nam, Masoud Alghoniemy und Ahmed H. Tewfik. „Audio-visual content-based violent scene characterization". In: *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*. Bd. 1. IEEE. 1998, S. 353–357.

[Nor97] C. A. Norris. *Surveillance Order and Social Control*. Economic und Social Research Council, 1997.

[Nou+07] N. Noury, A. Fleury, P. Rumeau, A. K. Bourke, G. O. Laighin, V. Rialle und J. E. Lundy. „Fall detection - Principles and Methods". In: *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*. Aug. 2007, S. 1663–1666.

[Off05] Office of the Victorian Privacy Commissioner. *Privacy Impact Assessments - A guide for the victorian public sector*. 2005.

[PL12] David Xiaosong Peng und Fujun Lai. „Using partial least squares in operations management research: A practical guideline and summary of past research". In: *Journal of Operations Management* 30.6 (2012), S. 467–480.

[Qui06] Oliver Quiring. „Methodische Aspekte der Akzeptanzforschung bei interaktiven Medientechnologien". In: *Münchner Beiträge zur Kommunikationswissenschaft* 6 (2006), S. 1–29.

[Raj+12] Jyri Rajamäki, Jutta Tervahartiala, Sofia Tervola, Sari Johansson, Leila Ovaska und Paresh Rathod. „How Transparency Improves the Control of Law Enforcement Authorities' Activities?" In: *Intelligence and Security Informatics Conference (EISIC), 2012 European*. IEEE. 2012, S. 14–21.

[RB11] M. Rost und K. Bock. „Privacy by Design und die neuen Schutzziele". In: *Datenschutz und Datensicherheit* 35 (2011), S. 30–35.

[RDH11] A. Roßnagel, M. Desoi und G. Hornung. „Gestufte Kontrolle bei Videoüberwachungsanlagen". In: *Datenschutz und Datensicherheit (DuD)* 35.10 (2011), S. 694–701.

[Rob79] Gary C. Robb. „Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations". In: *U. Mich. JL Reform* 13 (1979), S. 571.

[Ros02] John R. Rossiter. „The C-OAR-SE procedure for scale development in marketing". In: *International journal of research in marketing* 19.4 (2002), S. 305–335.

[Ryb07] Jesper Ryberg. „Privacy rights, crime prevention, CCTV, and the life of Mrs Aremac". In: *Res Publica* 13.2 (2007), S. 127–143.

[Sau+05] Alexandra Sauer, Frieder Luz, Michael Suda und Ulrike Weiland. „Steigerung der Akzeptanz von FFH-Gebieten". In: *BfN Skripten, Bd* 144 (2005).

[Sch+09] Jeremy Schiff, Marci Meingast, Deirdre K Mulligan, Shankar Sastry und Ken Goldberg. „Respectful cameras: Detecting visual markers in real-time to address privacy concerns". In: *Protecting Privacy in Video Surveillance*. Springer, 2009, S. 65–89.

[Sch06] Bruce Schneier. *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media, 2006.

[Sch13] Burkhard Schafer. „Crowdsourcing and cloudsourcing CCTV surveillance". English. In: *Datenschutz und Datensicherheit - DuD* 37.7 (2013), S. 434–439. URL: http://dx.doi.org/10.1007/s11623-013-0173-3.

[Sen+05] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Ying-Li Tian, A. Ekin, J. Connell, Chiao Fe Shu und M. Lu. „Enabling video privacy through computer vision". In: *Security & Privacy, IEEE* 3 (Juni 2005), S. 50–57.

[Ser+15] Marcello Serra, Anja Geisler, Herbert Prirsch, Aigul Talzhanova und Olga Trofimova. „Acceptance of Video Surveillance Among Younger and Elder Generations in Graz". 2015.

[SK94] N. Sellin und J. P. Keeves. „Path analysis with latent variables". In: *International encyclopedia of education* (1994), S. 4352–4359.

[SM11] M. Schwaiger und A. Meyer. *Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende.* Vahlen, 2011.

[SR00] Claudio Sacchi und Carlo S Regazzoni. „A distributed surveillance system for detection of abandoned objects in unmanned railway environments". In: *Vehicular Technology, IEEE Transactions on* 49.5 (2000), S. 2013–2026.

[Sta+08] Amory Starr, Luis A Fernandez, Randall Amster, Lesley J Wood und Manuel J Caro. „The impacts of state surveillance on political assembly and association: A socio-legal analysis". In: *Qualitative Sociology* 31.3 (2008), S. 251–270.

[Tao+05] Ji Tao, M. Turjo, Mun-Fei Wong, Mengdi Wang und Yap-Peng Tan. „Fall Incidents Detection for Intelligent Video Surveillance". In: *Information, Communications and Signal Processing, 2005 Fifth International Conference on.* 2005, S. 1590–1594.

[TL97] Avis Thomas-Lester und Toni Locy. „Chief's friend accused of extortion". In: *The Washington Post A* 1 (1997).

[Vag13] Hauke-Hendrik Vagts. *Privatheit und Datenschutz in der intelligenten Überwachung: Ein datenschutzgewährendes System, entworfen nach dem "Privacy by Design"Prinzip.* KIT Scientific Publishing, 2013.

[VD00] Viswanath Venkatesh und Fred D. Davis. „A theoretical extension of the technology acceptance model: Four longitudinal field studies". In: *Management science* 46.2 (2000), S. 186–204.

[Ven+03] Viswanath Venkatesh, Michael G Morris, Gordon B Davis und Fred D Davis. „User acceptance of information technology: Toward a unified view". In: *MIS quarterly* 27 (2003), S. 425–478.

[Wan13] Xiaogang Wang. „Intelligent multi-camera video surveillance: A review". In: *Pattern recognition letters* 34.1 (2013), S. 3–19.

[Win11] Thomas Winkler. „Vertrauenswürdige Videoüberwachung". In: *Datenschutz und Datensicherheit-DuD* 35.11 (2011), S. 797–801.

[WR10] Thomas Winkler und Bernhard Rinner. „A systematic approach towards user-centric privacy and security for smart camera networks". In: *Proceedings of the Fourth ACM/IEEE International Conference on Distributed Smart Cameras.* ACM. 2010, S. 133–141.

[WR12] Thomas Winkler und Bernhard Rinner. „User-centric privacy awareness in video surveillance". In: *Multimedia systems* 18.2 (2012), S. 99–121.

[WR14] Thomas Winkler und Bernhard Rinner. „Security and Privacy Protection in Visual Sensor Networks: A Survey". In: *ACM Computing Surveys (CSUR)* 47.1 (2014), S. 2.

[Zha+11] Guotao Zhao, Huadong Ma, Yan Sun, Hong Luo und Xufei Mao. „Enhanced surveillance platform with low-power wireless audio sensor networks". In: *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a.* IEEE. 2011, S. 1–9.

Online Veröffentlichungen

[95/46/EC] European Commision. *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (besucht am 20. 03. 2016).

[Ame] American Civil Liberties Union (ACLU). *WHAT'S WRONG WITH PUBLIC VIDEO SURVEILLANCE?* URL: https://www.aclu.org/whats-wrong-public-video-surveillance (besucht am 20. 03. 2016).

[BDSG] Bundesrepublik Deutschland. *Bundesdatenschutzgesetz (BDSG).* Bundesministerium der Justiz und für Verbraucherschutz. URL: http://www.gesetze-im-internet.de/bdsg_1990/ (besucht am 20. 03. 2016).

[Cav09a] Ann Cavoukian. *Privacy by Design.* 2009. URL: http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (besucht am 20. 03. 2016).

[Cav09b] Ann Cavoukian. *Privacy by Design - Die 7 Grundprinzipen.* Aug. 2009. URL: https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf (besucht am 20. 03. 2016).

[Die16] Die Welt. *Deutsche Frauen wollen mehr Videoüberwachung.* Jan. 2016. URL: http://www.welt.de/politik/deutschland/article150749181/Deutsche-Frauen-wollen-mehr-Videoueberwachung.html.

[DSGVO] Europäisches Parlament. *Entwurf der Europäischen Datenschutzgrundverordnung (DSGVO).* URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE&language=DE (besucht am 20. 03. 2016).

[Hei07] Heise Verlag. *Studie: Videoüberwachung in Berliner U-Bahn brachte keinen Sicherheitsgewinn.* Okt. 2007. URL: http://www.heise.de/newsticker/meldung/Studie-Videoueberwachung-in-Berliner-U-Bahn-brachte-keinen-Sicherheitsgewinn-183294.html.

[HT04] Leon Hempel und Eric Töpfer. *On the threshold to Urban Panopticon: Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts; Working Paper No. 15.* Centre for Technology und Society Technical, University Berlin. Aug. 2004. URL: http://www.urbaneye.net/results/ue_wp15.pdf (besucht am 20. 03. 2016).

[KAS13] KASTEL. *Begriffsdefinitionen in KASTEL.* deutsch. Sep. 2013. URL: http://www.kastel.kit.edu/downloads/Begriffsdefinitionen_in_KASTEL.pdf (besucht am 20. 03. 2016).

[Org13] Organisation for Economic Cooperation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* 2013. URL: http://www.oecd.org/sti/ieconomy/privacy.htm (besucht am 20. 03. 2016).

[Stu12] Stuttgarter Zeitung. *Forschungsprojekt Indect: Kommunikationspannen befeuern Kritik.* Juli 2012. URL: http://www.stuttgarter-zeitung.de/inhalt.forschungsprojekt-indect-das-neue-acta-page1.7531b116-0e15-40ba-b792-356714d461fe.html.

[SUR] SURVEILLE Consortium funded under the EU grant agreement no. 284725. URL: https://surveille.eui.eu/ (besucht am 20. 03. 2016).

[WDR16] WDR. *Mehr Videoüberwachung soll Köln sicherer machen.* Feb. 2016. URL: http://www1.wdr.de/koeln-uebergriffe-hauptbahnhof-krisentreffen-100.html.

[Zei13] Zeit Online. *Mehr Kameras, gleich viel Unsicherheit.* Apr. 2013. URL: http://www.zeit.de/digital/datenschutz/2013-04/videoueberwachung-panopticon.

Webseiten

[AIS] *AIS Ship Locations worldwide.* URL: http://www.marinetraffic.com/ (besucht am 09. 02. 2016).

[CC] *Common Criteria Editorial Board.* URL: https://www.commoncriteriaportal.org/cc/ (besucht am 20. 03. 2016).

[EuroPrise] *European Privacy Seal.* URL: https://www.european-privacy-seal.eu/EPS-en/Certification (besucht am 20. 03. 2016).

[Kiw] KiwiVision. *KiwiVision Privacy Protector.* URL: http://www.kiwisecurity.com/privacy-protector/?lang=de (besucht am 20. 03. 2016).

[KK15] Mario Kaufmann und Erik Krempel. *CCTV Map.* Fraunhofer Gesellschaft. 2015. URL: https://cctv-map.de/ (besucht am 20. 03. 2016).

[Ope] OpenStreetMap Foundation. *Open Street Map.* URL: http://www.openstreetmap.org/ (besucht am 20. 03. 2016).

[RWW05] Christian Marc Ringle, Sven Wende und Alexander Will. *SmartPLS 2.0 (M3) Beta.* 2005. URL: http://www.smartpls.de (besucht am 20. 03. 2016).

[SCOPUS] Elsevier Verlag. *Scopus Online.* URL: http://www.scopus.com/ (besucht am 20. 03. 2016).

[UrbanEye] *Urban Eye Project.* URL: http://www.urbaneye.net/index.html (besucht am 20. 03. 2016).

Tabellenverzeichnis

Abbildungsverzeichnis

Karlsruher Schriftenreihe zur Anthropomatik (ISSN 1863-6489)

Herausgeber: Prof. Dr.-Ing. Jürgen Beyerer

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

Band 1 Jürgen Geisler
Leistung des Menschen am Bildschirmarbeitsplatz. 2006
ISBN 3-86644-070-7

Band 2 Elisabeth Peinsipp-Byma
Leistungserhöhung durch Assistenz in interaktiven Systemen zur Szenenanalyse. 2007
ISBN 978-3-86644-149-1

Band 3 Jürgen Geisler, Jürgen Beyerer (Hrsg.)
Mensch-Maschine-Systeme. 2010
ISBN 978-3-86644-457-7

Band 4 Jürgen Beyerer, Marco Huber (Hrsg.)
Proceedings of the 2009 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2010
ISBN 978-3-86644-469-0

Band 5 Thomas Usländer
Service-oriented design of environmental information systems. 2010
ISBN 978-3-86644-499-7

Band 6 Giulio Milighetti
Multisensorielle diskret-kontinuierliche Überwachung und Regelung humanoider Roboter. 2010
ISBN 978-3-86644-568-0

Band 7 Jürgen Beyerer, Marco Huber (Hrsg.)
Proceedings of the 2010 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2011
ISBN 978-3-86644-609-0

Band 8 Eduardo Monari
Dynamische Sensorselektion zur auftragsorientierten Objektverfolgung in Kameranetzwerken. 2011
ISBN 978-3-86644-729-5

Band 9 Thomas Bader
Multimodale Interaktion in Multi-Display-Umgebungen. 2011
ISBN 3-86644-760-8

Band 10 Christian Frese
Planung kooperativer Fahrmanöver für kognitive Automobile. 2012
ISBN 978-3-86644-798-1

Band 11 Jürgen Beyerer, Alexey Pak (Hrsg.)
Proceedings of the 2011 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2012
ISBN 978-3-86644-855-1

Band 12 Miriam Schleipen
Adaptivität und Interoperabilität von Manufacturing Execution Systemen (MES). 2013
ISBN 978-3-86644-955-8

Band 13 Jürgen Beyerer, Alexey Pak (Hrsg.)
Proceedings of the 2012 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2013
ISBN 978-3-86644-988-6

Band 14 Hauke-Hendrik Vagts
Privatheit und Datenschutz in der intelligenten Überwachung: Ein datenschutzgewährendes System, entworfen nach dem „Privacy by Design" Prinzip. 2013
ISBN 978-3-7315-0041-4

Band 15 Christian Kühnert
Data-driven Methods for Fault Localization in Process Technology. 2013
ISBN 978-3-7315-0098-8

Band 16 Alexander Bauer
Probabilistische Szenenmodelle für die Luftbildauswertung. 2014
ISBN 978-3-7315-0167-1

Band 17 Jürgen Beyerer, Alexey Pak (Hrsg.)
Proceedings of the 2013 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2014
ISBN 978-3-7315-0212-8

Band 18 Michael Teutsch
Moving Object Detection and Segmentation for Remote Aerial Video Surveillance. 2015
ISBN 978-3-7315-0320-0

Band 19 Marco Huber
Nonlinear Gaussian Filtering:
Theory, Algorithms, and Applications. 2015
ISBN 978-3-7315-0338-5

Band 20 Jürgen Beyerer, Alexey Pak (Hrsg.)
Proceedings of the 2014 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2014
ISBN 978-3-7315-0401-6

Band 21 Todor Dimitrov
Permanente Optimierung dynamischer Probleme der Fertigungssteuerung unter Einbeziehung von Benutzerinteraktionen. 2015
ISBN 978-3-7315-0426-9

Band 22 Benjamin Kühn
Interessengetriebene audiovisuelle Szenenexploration. 2016
ISBN 978-3-7315-0457-3

Band 23 Yvonne Fischer
Wissensbasierte probabilistische Modellierung für die Situationsanalyse am Beispiel der maritimen Überwachung. 2016
ISBN 978-3-7315-0460-3

Band 24 Jürgen Beyerer, Alexey Pak (Hrsg.)
Proceedings of the 2015 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory. 2016
ISBN 978-3-7315-0519-8

Band 25 Pascal Birnstill
Privacy-Respecting Smart Video Surveillance Based on Usage Control Enforcement. 2016
ISBN 978-3-7315-0538-9

Band 26 Philipp Woock
Umgebungskartenschätzung aus Sidescan-Sonardaten für ein autonomes Unterwasserfahrzeug. 2016
ISBN 978-3-7315-0541-9

Band 27 Janko Petereit
Adaptive State × Time Lattices: A Contribution to Mobile Robot Motion Planning in Unstructured Dynamic Environments. 2017
ISBN 978-3-7315-0580-8

Band 28 Erik Ludwig Krempel
Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen. 2017
ISBN 978-3-7315-0598-3

Lehrstuhl für Interaktive Echtzeitsysteme
Karlsruher Institut für Technologie

Fraunhofer-Institut für Optronik, Systemtechnik und
Bildauswertung IOSB Karlsruhe

Der Einsatz intelligenter Videoüberwachung stellt für eine Vielzahl von Überwachungsaufgaben ein probates Mittel dar. Neben der (teil-) automatischen Detektion von Gefährdungen, wie beispielsweise Überfüllung in bestimmten Bereichen oder Stürze von Patienten in Krankenhäusern oder Pflegeheimen, können intelligente Videoüberwachungssysteme wertvolle Zusatzdienste zur Lösung kritischer Situationen beitragen.
Während die Leistungsfähigkeit intelligenter Videoüberwachung stetig vorangetrieben wird, steht das Verständnis über die technischen Faktoren der Akzeptanz noch ganz am Anfang. Diese bisher vernachlässigte Forschungsfrage wird in dieser Arbeit aufgegriffen. Ausgehend von der Akzeptanzforschung der Informations- und Kommunikationstechnologie wird ein Akzeptanzmodell für die intelligente Videoüberwachung erstellt. Getrieben durch ein ausgewähltes Szenario, der datenschutzfreundlichen Sturzerkennung, werden akzeptanzsteigernde Technologien entwickelt, in einen Prototyp integriert und evaluiert. Die Arbeit vereint somit theoretische Überlegungen zur Akzeptanz von Videoüberwachung mit deren gezielten Entwicklung.

ISSN 1863-6489
ISBN 978-3-7315-0598-3