31.10.2023

KIRaPol.5G

Künstliche **I**ntelligenz für **Ra**dar-systeme zur Unterstützung von **pol**izeilichen Überwachungen auf öffentlichen Plätzen und Bahnhöfen

Datenschutzkonzept

Verantwortlich:
Prof*in Monika Eigenstetter
Prof. Hans Günter Hirsch

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Ausgangslage

Die Beobachtung von sicherheitsrelevanten Bereichen ist eine Aufgabe, die von innovativer Sensor- und Kommunikationstechnik unterstützt wird. Videokameras spielen dabei eine wesentliche Rolle, da damit Situationen sehr genau erfasst und analysiert werden können. Im öffentlichen Raum sind dabei allerdings Persönlichkeitsrechte zu beachten, die den Einsatz von bildgebenden Sensoren einschränken. Kameras im öffentlichen Raum sind oft verpönt, denn Datenschutz und Persönlichkeitsrechte werden hier leicht verletzt, und eine kritische Öffentlichkeit fragt, was mit den Daten eigentlich geschieht. Das Dilemma Sicherheit versus Datenschutz ist nicht einfach zu lösen und sucht nach kreativen Lösungen. Radartechniken sind seit vielen Jahren im Einsatz und werden z.B. auch für die Entwicklungen des autonomen Fahrens genutzt. Für den Einsatz als Überwachungsmedium wird Künstliche Intelligenz (KI) eingesetzt. Die KI soll erkennen, ob ein gefährliches oder ungefährliches Verhalten bei Menschen vorliegt, zum Beispiel ob Personen in eine Schlägerei verwickelt sind. Ist das der Fall, schlägt das System Alarm. Um das zu bewerkstelligen, muss eine KI zuerst „trainiert“ werden. Dabei kommen unter anderem komplexe Verfahren zur Mustererkennung, insbesondere „Neuronale Netzwerke“, zum Einsatz. Mit den Radarsignalen werden bewegungscharakteristische Profile einzelner Objektklassen, wie sich bewegende Personen oder mitgeführte Gegenstände, erfasst.

Gegenüber der bisherigen eingesetzten Videobeobachtung für sicherheitsrelevante Bereiche bietet die Radartechnologie Vorteile: Während die Bildqualität der Videotechnologie wesentlich von Licht- und Wetterverhältnissen abhängig ist, beeinflussen Dunkelheit, Regen, Blendungen (z.B. durch helle Leuchtreklame oder Blaulicht) die Radartechnologie hingegen nicht. Auch aus datenschutzrechtlichen Aspekten überwiegt die Radartechnologie, da wir davon ausgehen können, keine bzw. nur sehr eingeschränkt personenbezogene Daten zu erheben.

Da die mit dem Radar erfassten Daten nicht einfach von einem Menschen bewertet werden können, ist für das Antrainieren der KI ein paralleler Einsatz von Radar- und Videotechnologie im Rahmen der geplanten Messkampagnen erforderlich. Dabei fließen die Videoaufnahmen nicht direkt in das Training der KI ein, sondern werden von Menschen bewertet und das Geschehen in der Szene wird kategorisiert. Diese Kategorisierung wird anschließend genutzt, um die Klassifizierung von Gefahrensituationen durch die KI zu verifizieren oder zu falsifizieren.

Ziel dieses Dokuments ist es, die geringe Beeinträchtigung von Persönlichkeits- und Datenschutzrechten durch den Einsatz der innovativen Radartechnologie darzustellen. Gleichzeitig wird dargelegt, dass die durch den Einsatz der Videobeobachtung ermittelten personenbezogenen Daten im Sinne der DSGVO rechtskonform verarbeitet werden.

2 Forschungsprojekt

Das Forschungsprojekt KIRaPol.5G (**K**ünstliche **I**ntelligenz für **Ra**darsysteme zur Unterstützung von **pol**izeilichen Überwachungen auf öffentlichen Plätzen und Bahnhöfen) ist ein für den Zeitraum vom 01.01.2022 bis 30.06.2024 vom Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen gefördertes Forschungsprojekt. Ziel von KIRaPol.5G ist die Entwicklung einer Radartechnologie zur Unterstützung der polizeilichen Videobeobachtung mithilfe einer Künstlichen Intelligenz, welche Szenarien für sicherheitstechnische Anwendungen klassifiziert.

3 Projektpartner

Das Projektkonsortium besteht aus mehreren unterschiedlichen Akteuren aus dem Wirtschafts-, Forschungs- und dem Polizeibereich. Verbundpartner sind IMST GmbH (IMST), Hochschule Niederrhein (HSNR), Telefonbau Arthur Schwabe GmbH & Co. KG (TAS), Polizei Mönchengladbach (Polizei MG) und m3connect GmbH (m3c). Dabei übernimmt die IMST GmbH die Konsortialführung.

3.1 IMST GmbH

Die IMST GmbH koordiniert als Konsortialführung das Projekt, d.h. organisiert die Arbeitsabläufe und die Schnittstellen zwischen den Partnern, organisiert die Meetings, überwacht die Meilensteine und die externe und interne Kommunikation. Neben der Projektkoordination entwickelt IMST die Radartechnologie in Hardware und Software. Die resultierenden Radarmodule werden dann zu Messungen in öffentlichen und nicht öffentlichen Bereichen eingesetzt und die aufgenommenen Daten ausgewertet und für die KI verwendet.

3.2 Hochschule Niederrhein (HSNR)

Die Hochschule Niederrhein (HSNR) ist verantwortlich für die Entwicklung der Klassifikationskonzepte – insbesondere für den Einsatz von Methoden der künstlichen Intelligenz zur Klassifikation mit Hilfe von Radarsignalen und der parallelen Aufzeichnung von Kameradaten zum Zweck der Annotation der aufgenommenen Szenen unter Verwendung von Verfahren zum Schutz der Privatsphären der beobachteten Personen. Weiterhin begleitet und unterstützt die HSNR die Generierung von Trainingsdaten durch simulative und messtechnische Untersuchungen. Die HSNR ist auch verantwortlich für die Durchführung der abschließenden Verifizierungs- und Validierungstests und die Optimierung des Gesamtsystems und unterstützt beim Aufbau des 5G-Campusnetzes. Zudem wird eine begleitende Bewertung von ethischen, rechtlichen und sozialen Aspekten durchgeführt.

3.3 Telefonbau Arthur Schwabe GmbH & Co. KG (TAS)

Die Telefonbau Arthur Schwabe GmbH & Co. KG (TAS) bringt ihr Know-how bei der Projektierung und Abstimmung der Sensorik-Standorte, der Auswahl der Sensorkonzepte und der Planung der Gesamtanwendung ein. Weiterhin unterstützt TAS bei der Generierung von Trainingsdaten, Klassifizierung der Gefährdungsszenarien und Bewertung der Datenschutzsituation, insbesondere aufgrund der Erfahrungen im Bereich der Videodaten. Für die Einrichtung der Datenanbindung stehen die Sicherheitsrouter zur Verfügung.

3.4 Polizei Mönchengladbach (Polizei MG)

Die Polizei Mönchengladbach (Polizei MG) überwacht auf Grundlage des Polizeigesetzes NRW mittels Videotechnik zur Abwehr von Gefahren räumlich und zeitlich eng begrenzt öffentliche Wege und Plätze im zentralen Stadtgebiet. Anlassbezogen dürfen die Aufnahmen

unter den gesetzlichen Voraussetzungen gespeichert und für die Strafverfolgung genutzt werden. Mit dem gespeicherten und anonymisierten Videomaterial, welches zu den für das Forschungsprojekt sicherheitsrelevanten Fallkonstellationen passt, erstellt die Polizei Schulungsmaterial für die Projektpartner, um Gefahrensituationen zu klassifizieren. Des Weiteren arbeitet die Polizei bei der Bearbeitung der Datenschutzaspekte mit.

3.5 m3connect GmbH (m3c)

Die m3connect GmbH (m3c) stellt auf Basis von 3GPP spezifizierten Mechanismen ein privates Hochsicherheitsnetzwerk bereit und sorgt für die Anbindung der Sensorik an die Verarbeitung. Hierfür werden sowohl 5G-Mobilfunk-Basistechnologien als auch spezifische Schnittstellen bereitgestellt. Fokus ist hierbei, ein robustes, sicheres 5G-Netzwerk zu gestalten und Abhängigkeiten von einzelnen Funkausrüstern und Endgeräteherstellern zu vermeiden. Darüber hinaus wird aus Betreibersicht evaluiert, ob und wie sich eine derartige Netzwerkstruktur in anderen Lokationen und Kontexten nutzen lässt.

3.6 Weitere assoziierte Partner

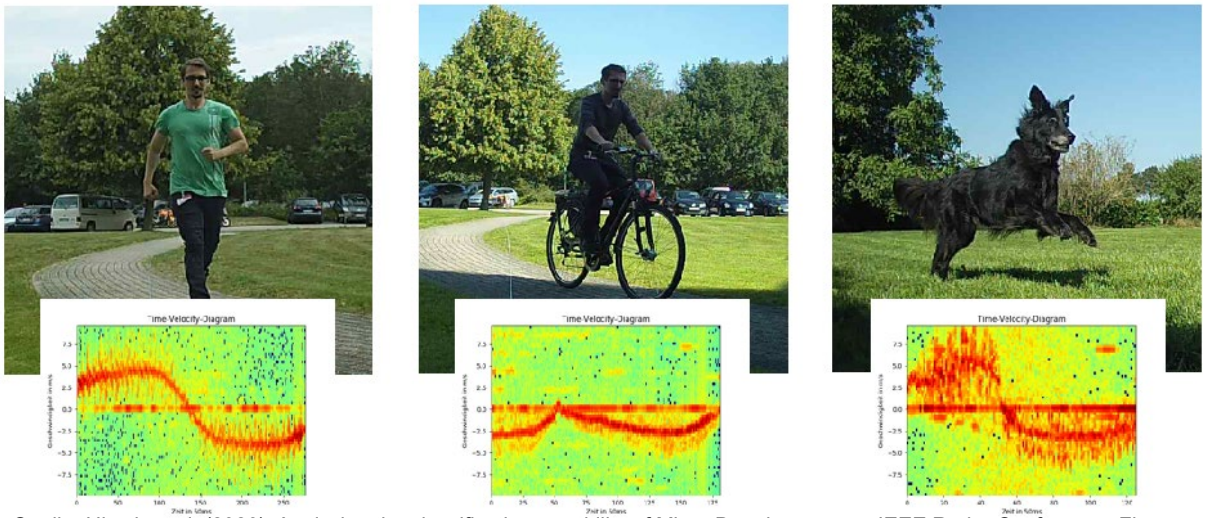
Als assoziierte Partner unterstützen sowohl die Bundespolizei, das Bayrische Landeskriminalamt, die Stadt Mönchengladbach als auch die Deutsche Bahn das Forschungsprojekt.

4 Radartechnologie und Künstliche Intelligenz

Die zum Einsatz kommende Radartechnologie stammt aus dem Verkehrsbereich. Die Anwendung ist unter dem Begriff „adaptiver Abstandsassistent“ bekannt. Radar wird ein wesentlicher Bestandteil für die Einführung des autonomen Fahrens in Europa werden, wobei nicht nur Fahrzeuge mit Modulen ausgerüstet werden, sondern auch die Straßeninfrastruktur. Diese Anwendungen für Sensoren (Short Range Devices) fallen unter den Begriff der Verkehrs-Telematik: „Transport and Traffic Telematics (TTT)“ und werden durch den europäischen Standard für festinstallierte Infrastruktur „ETSI EN 301 091-2, Part 2: Fixed Infrastructure“ festgelegt. Der Einsatz von Radarsensoren für Fahrzeuganwendungen erfolgt im Frequenzbereich von 76 bis 77 GHz gemäß dem Standard „ETSI EN 301 091-1, Part 1: Ground based vehicular radar“. Somit wird in KIRaPol.5G auf eine bereits weitverbreitete und standardisierte Radartechnologie zurückgegriffen.

4.1 Mikro-Doppler-Spektrogramm

Mit einem Radarsensor können neben den Entfernungen und Richtungen (Winkeln), unter denen sich Zielobjekte bewegen, auch die Geschwindigkeitsanteile des jeweiligen Objekts bestimmt werden. Die zu einem Zeitpunkt erfassten Geschwindigkeitsanteile bezeichnet man als Mikro-Doppler-Spektrum. Die sich über die Zeit verändernden Geschwindigkeitsanteile eines sich bewegenden Objekts lassen sich in Form eines Mikro-Doppler-Spektrogramms visualisieren, das die zeitlich aufeinanderfolgenden Doppler-Spektren beinhaltet. Drei Spektrogramme sind beispielhaft in Abbildung 1dargestellt. Die Geschwindigkeitsanteile (in m/s) einer laufenden Person, eines Fahrradfahrers und eines Hundes werden dabei über einen Zeitraum von einigen Sekunden dargestellt. Die Intensität eines Geschwindigkeitsanteils wird farblich codiert. Gemäß dem Spektrum des Lichts werden mit „rot“ große Amplituden der Geschwindigkeit und über „gelb“ und „grün“ bis hin zu „blau“ immer kleiner werdende Amplituden dargestellt. Die durchgehend rote Konturlinie der laufenden Person resultiert aus dem Weglaufen der Person vom Radarsensor (positive Geschwindigkeit), einem Richtungswechsel und einer anschließenden Bewegung in Richtung des Sensors (negative Geschwindigkeit). Diese durchgehende Kontur entspricht der Geschwindigkeit des Torsos der Person. Die schwingenden Arme und Beine besitzen davon abweichende Geschwindigkeiten, die im Spektrogramm zu weiteren, um den Geschwindigkeitsanteil des Körpers herum auftretenden Anteilen mit geringerer oder größerer Geschwindigkeit führen. Bei Vergleich der Spektrogramme in Abbildung 1 kann man die Unterschiede zwischen einer laufenden Person, einem Radfahrer und einem Hund aufgrund der unterschiedlichen Bewegungsformen erkennen.



Quelle: Hirsch et al. (2020): Analyzing the classification capability of Micro-Doppler spectra, IEEE Radar Conference, Florence.

Abbildung 1: Mikro-Doppler-Spektrogramme einer laufenden Person, eines Radfahrers und eines Hundes

4.2 Einsatz Künstlicher Intelligenz

Die sich über die Zeit aufgrund der Bewegung verändernden Geschwindigkeitsanteile können verwendet werden, um ein Objekt als laufende Person, als Radfahrer oder als Hund zu klassifizieren, was die beispielhafte Darstellung in Abbildung 1betrifft. Die Aufgabe ist vergleichbar mit der Erkennung bestimmter Strukturen in Bildern.

Zur Klassifikation werden Verfahren der Künstlichen Intelligenz in Form von Neuronalen Netzen eingesetzt. Dabei werden die Amplituden der Geschwindigkeitsanteile, die in einem Doppler-Spektrogramm enthalten sind, als Eingangswerte des neuronalen Netzes verwendet. Am Ausgang können für die beispielhafte Anwendung drei Wahrscheinlichkeitswerte bestimmt werden, die die Wahrscheinlichkeit der Zuordnung des Objekts zur einer der drei Klassen beschreiben. Die Zuordnung zu einer Klasse kann anhand der höchsten Wahrscheinlichkeit vorgenommen werden. Zusätzlich kann dies mit dem Überschreiten einer minimal geforderten Wahrscheinlichkeit kombiniert werden.

Um das Training des neuronalen Netzes als Klassifikator vorzunehmen, wird eine möglichst große Anzahl von Spektrogrammen jeder Objektklasse benötigt. Um die für das Training benötigte Zuordnung von Spektrogrammen zu den Klassen vornehmen zu können, werden die Szenen in der Regel parallel mit einer Kamera erfasst. Durch eine Betrachtung der erfassten Bilder kann eine Person eine Zuordnung vornehmen. Alternativ kann die Zuordnung automatisch mit Verfahren der Objektdetektion und -klassifikation aus dem Bereich der Bildverarbeitung vorgenommen werden.

Mit der Erfassung der sich über die Zeit verändernden Geschwindigkeitsanteile eines Objekts, lässt sich ein Objekt grob bestimmten Klassen zuordnen. Die Zuordnung eines Spektrogramms zu einer speziellen Person wäre aufgrund bestimmter Merkmale wie Körpergröße, Bewegungsmuster oder spezifischer Gegenstände wie Rollstühle oder Rollatoren grundsätzlich möglich (s. dazu Abdulati, Sherif et.al. (2019): Person Identification and Body Mass Index: A Deep Learning-Based Study on Micro-Dopplers, Institute of Signal Processing and Systems Theory, University of Stuttgart, Fraunhofer Institute for Manufacturing Engineering and Automation IPA). Dies trifft jedoch nur zu, wenn die KI auch auf diese speziellen Merkmale hintrainiert würde. Eine solche Klassifizierung wird im Projekt nicht durchgeführt, so dass Personen mit auffälligen Bewegungsmerkmalen einer unbekannten Klasse zugeordnet werden und somit auch nicht weiter analysiert werden. Eine Anonymisierung eines Radar-Spektrogramms ist ebenfalls nicht erforderlich, da die genannten speziellen Bewegungsmerkmale ohne den Abgleich mit den Videoaufzeichnungen, die anonymisiert werden, mit dem bloßen Auge nicht identifizierbar sind.

4.3 Anonymisierung der Videodaten im Projekt

Im Folgenden ist das Vorgehen zur Anonymisierung der im Projekt aufgezeichneten Videos beschrieben. Dabei wird zunächst das Vorgehen bei der Anonymisierung behandelt. Anschließend wird beschrieben wo, wann und von wem die Anonymisierung durchgeführt wird.

4.3.1 Beschreibung des Vorgehens

Zu Beginn wird ein statisches Hintergrundbild für jede Kamera erstellt, indem keine Personen enthalten sind. Dieses dient als Hintergrund für die anonymisierten Aufnahmen. Anschließend werden auf den originalen Videoaufnahmen für jedes einzelne Bild eine Objektdetektion, eine Klassifizierung und eine Segmentierung durchgeführt. Dabei wird versucht, Objekte bekannter Klassen, wie etwa Personen, in den Aufnahmen zu erkennen und deren Position sowie deren Umrisse zu bestimmen. Diese Informationen werden in das anonymisierte Video übertragen. Dabei wird nicht die Abbildung der Person, sondern eine eingefärbte Fläche mit dem gleichen Umriss übertragen.

Dieses Vorgehen wird für einige ausgewählte Klassen von Objekten, unter anderem Personen, Hunde und Autos durchgeführt. Anschließend wird für Personen zusätzlich ein Skelett ermittelt und über die Objektmaske gezeichnet. Das Skelett wird durch einige markante Körperpunkte („keypoints“), mit denen die Positionen des Körpers, des Kopfs und der Gelenke einer Person festgelegt sind, und den Verbindungen zwischen den Punkten beschrieben. Gleichzeitig wird versucht, die erkannten Objekte über die Zeit zu verfolgen. Diese Information wird zusätzlich in Form einer Linie mit den Positionen des Objekts in vorhergehenden Bildern eingezeichnet. Dies ermöglicht es, die Herkunft eines Objektes auch in einem einzelnen Bild abzulesen.

Abbildung 2: Visualisierung einer detektierten Körperkontur und der zugehörigen Skelettpunkte

Beispiele für die Ergebnisse dieser Verarbeitung sind in Abbildung 2 zu sehen. Diese zeigt das statische Hintergrundbild einer Szene mit der eingezeichneten Körperkontur einer Person. Darüber sind zusätzlich die berechneten Skelette sowie das beschriebene Tracking als weiße Linie eingezeichnet.

Im Gegensatz zu einer Anonymisierung, bei der Personen bzw. Gesichter erkannt und unkenntlich gemacht werden, haben wir bei diesem Vorgehen den Vorteil, dass wir nur die erkannten Personen in anonymisierter Form aus dem Original in die anonymisierte Aufnahme übertragen. Dadurch ist z. B. ausgeschlossen, dass bei einem Fehler in der Personenerkennung ein nicht anonymisiertes Gesicht in den Aufnahmen verbleibt. Gleichzeitig gehen alle nicht aus der Kontur und dem Skelett der Person ableitbaren Merkmale verloren, was die Identität der Personen zusätzlich schützt.

4.3.2 Beschreibung der Durchführung

Die Anonymisierung wird in der Hochschule Niederrhein von einem Mitarbeiter des Projekts durchgeführt. Dies geschieht nach der Übertragung der verschlüsselten Videodaten vom Messstandort zur Hochschule Niederrhein. Dabei erfolgt die Anonymisierung vor der weiteren Verarbeitung und nur in diesem Verarbeitungsschritt wird mit den originalen Videodaten gearbeitet. Die originalen Videodaten werden nach der Anonymisierung gelöscht.

Eine frühere Anonymisierung z. B. am Messort während der Aufnahme ist nicht möglich, da dort die dazu benötigte Rechenleistung nicht zur Verfügung steht. Außerdem sind die an den Messorten genutzten Standorte für die Rechner nicht für den Einsatz solcher Hardware ausgelegt und verfügen unter anderem nicht über eine Kühlung. Aus diesen Gründen wäre eine frühere Anonymisierung nicht ohne erheblichen Aufwand möglich.

5 Klassifikation von sicherheitsrelevanten Szenarien

In diesem Projekt sollen die in dem Doppler-Spektrogramm enthaltenen Informationen dazu verwendet werden, um das Verhalten einer einzelnen Person oder einer Personengruppe als Gefahrensituation einzustufen. Die in diesem Projekt betrachteten Szenarien werden im nachfolgenden Unterkapitel 5.1 beschrieben. Wie bereits im vorhergehenden Abschnitt erläutert, wird zum Training des Klassifikators eine parallele Erfassung von entsprechenden Szenen mit einer Kamera benötigt, so dass die Einstufung als gefährlich oder nicht gefährlich vorgenommen werden kann.

5.1 Sicherheitsrelevante Szenarien

Im Zuge des Austausches zwischen den Projektpartnern wurden drei Gruppen von sicherheitsrelevanten Szenarien identifiziert, die im Rahmen des Projekts betrachtet werden:

- Gewalttätige Auseinandersetzungen einschließlich der Anbahnung zwischen zwei Personen,
- eine liegende Person (hilflose oder verletzte Person oder Obdachloser) und
- das Fluchtverhalten einer Gruppe oder Einzelner.

Innerhalb der drei Gruppen von Szenarien gibt es jeweils ein breites Spektrum an Variationen. Im Verlauf des Projektes wird eine Auswahl aus diesen getroffen. Fallvarianten aus allen drei Gruppen sind in dem in Betracht gezogenen Gebiet in der Vergangenheit aufgetreten.

5.2 Klassifikation

Als Ausgangswerte des Klassifikators werden Wahrscheinlichkeitswerte pro Klasse bestimmt. Die Entscheidung kann anhand der höheren Wahrscheinlichkeit in Kombination mit einer minimal geforderten Wahrscheinlichkeit getroffen werden.

Wird eine gefährliche Situation von dem Klassifikationssystem detektiert, so kann dies, in einem nach dem Projekt zu entwickelndem Produkt, z. B. zur Auslösung eines Alarms in einer Überwachungszentrale genutzt werden. In der Zentrale könnte in diesem Fall das Einschalten einer Kamera initiiert werden, mit der eine Person die Situation beobachten und beurteilen kann. Insgesamt kann bei korrekter oder falscher Klassifikation einer der in Tabelle 1 enthaltenen Zustände auftreten.

Tabelle 1: Mögliche Zustände bei korrekter oder fälschlicher Klassifikation

		Vorhergesagt	
		positiv	negativ
Tatsächlich	positiv	Gefahr vorhanden, KI erkennt Gefahr (richtig positiv)	Gefahr vorhanden, KI erkennt keine Gefahr (falsch negativ)
	negativ	Keine Gefahr, KI erkennt Gefahr (falsch positiv)	Keine Gefahr, KI erkennt keine Gefahr (richtig negativ)

Für diese Anwendung besteht die Zielsetzung darin, in möglichst wenigen Fällen eine tatsächlich vorhandene Gefahrensituation nicht zu erkennen und keinen Alarm (falsch negativ) auszulösen. Zwar sollte auch die Auslösung eines Alarms in Situationen ohne Gefahrenpotential (falsch positiv) vermieden werden. Aber an dieser Stelle ist ein höherer Prozentsatz tolerabel im Vergleich zur Nicht-Erkennung einer gefährlichen Situation.

6 Messkampagnen

Für das Anlernen der KI werden Radarsignale als Trainingsdaten benötigt, die in entsprechenden Szenen aufgezeichnet werden. Um die erfassten Radardaten bewerten und in Bezug auf eine vorhandene oder keine vorhandene Gefahr zuordnen zu können, werden parallel zur Erfassung der Radarsignale Videodaten mit einer Kamera aufgezeichnet. Die Videodaten werden von einer Person ausgewertet, um die Zuordnung der Radardaten zur entsprechenden Klasse vornehmen zu können.

Zudem können die Bilddaten dazu verwendet werden, für die sich in der Szene bewegenden Personen „Skelett“-Daten zu erzeugen, um diese für eine Simulation einer Radarbeobachtung mit einer künstlichen Bestimmung von Mikro-Doppler-Spektren zu benutzen. Die aus den „Skelett“-Daten ableitbare Modellierung eines Körpers ist beispielhaft in Abbildung 3 dargestellt.

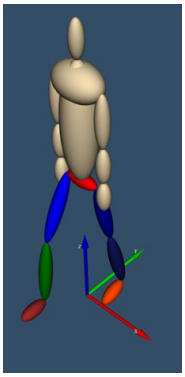


Abbildung 3: Modellierung eines menschlichen Körpers aus „Skelett“-Daten

Radar- und Videosignale sollen im Rahmen der folgenden drei Messkampagnen aufgezeichnet werden:

- **Hochschulcampus der Hochschule Niederrhein:**
  Auf einem abgegrenzten Areal werden Sensormasten, eine Basiseinheit und ein 5G-Campusnetz aufgebaut. Auf dem Areal können unter Ausschluss der Öffentlichkeit von Mitarbeitern der Hochschule bestimmte Szenen gestellt und aufgezeichnet werden.
- **Polizeitrainingszentrum in Linnich:**
  Während des Trainings polizeilicher Einsätze werden Radar- und Videodaten aufgezeichnet.
- **Platz-der-Republik in Mönchengladbach:**
  Jeweils ein Sensorknoten mit zwei Radarsensoren und zwei Videokameras sollen auf der Radstation und auf dem gegenüber liegenden Gladbach-Center installiert werden für Messungen in Richtung HBF und in Richtung Platzmitte (Skaterbahn). Installationen und Durchführung finden unter Einbeziehung und Genehmigung der Gebäudeeigentümer statt.

Im Rahmen einer Compliance-Prüfung wurden weitere tangierte Rechtsgebiete geprüft (s. Anlagen):

- Eigentumsrechte der Aufzeichnungsorte / Vor-Ort-Treffen mit Eigentümer
- Telekommunikationsrecht
- Strahlenschutzrecht
- Urheberrechte an den Bildern

Die Orte der drei Kampagnen werden im Folgenden einzeln vorgestellt.

6.1 Campus der Hochschule Niederrhein

Die Messungen an der HSNR dienen neben der Erfassung von Daten auch der Erprobung der für die Messungen eingesetzten Hard- und Software. Dazu wird ein Messaufbau entwickelt, der so weit wie möglich den in den anderen Messkampagnen eingesetzten Aufbauten entspricht. Auf einem abgegrenzten Areal werden Sensormasten, eine Basiseinheit und ein 5G-Campusnetz aufgebaut.

6.1.1 Platzierung der Sensoren

Bei dem Messaufbau an der HSNR handelt es sich um einen mobilen Aufbau. Dieser wird jeweils auf einem abgegrenzten Areal aufgebaut und nimmt dabei verschiedene Positionen ein, um Messungen unter unterschiedlichen Bedingungen durchzuführen. Der Aufbau ist in Abbildung 4 dargestellt.

6.1.2 Rechtliche Grundlage und Verantwortung

Die Aufzeichnungen an der HSNR erfolgen nach schriftlicher Einwilligungserklärung der Teilnehmenden. Hierbei erfolgt sowohl eine Einwilligungserklärung zur Radar- und Videoaufzeichnung durch die HSNR als auch eine Einwilligungserklärung für die Benutzung von Fotos zur späteren Presse- und Öffentlichkeitsarbeit. Die Verantwortung bezüglich der Verarbeitung der Radar- und Videoaufzeichnung sowie der Fotoaufnahmen liegt ausschließlich bei der Hochschule Niederrhein. Zur Sicherstellung einer freiwilligen, informierten Einwilligung der Teilnehmenden werden diesen die Ziele des Forschungsprojektes im Rahmen einer Kurzpräsentation und einer Live-Demonstration der Radartechnologie vermittelt. Außerdem wird die Einwilligungserklärung vorab zur Verfügung gestellt. Die Teilnehmer*innen wurden auf die Freiwilligkeit der Teilnahme hingewiesen. Durch eine Teilnahme an den Aufnahmen erhalten die Teilnehmer*innen keine Vorteile und eine Nichtteilnahme führt zu keinen Nachteilen. Alle an den Aufnahmen beteiligten Vorgesetzten und Professoren werden ausdrücklich über diesen Umstand informiert. Ebenso besteht die Möglichkeit des Widerrufrechts, sodass die Teilnehmenden ihr Einverständnis nachträglich zurückziehen können. Auch hierdurch entstehen keine Nachteile.

6.2 Polizeitrainingszentrum

Ebenfalls ist eine Messung bei den polizeilichen Einsatztrainings geplant. Im Rahmen des Einsatztrainings werden realitätsnahe, gewalttätige Auseinandersetzungen von der Polizei MG trainiert, welche durch eine geplante Radar- und Videoaufzeichnung ab Juni 2023 seitens der HSNR aufgenommen werden sollen. Hierbei werden keine konkreten Einsatztaktiken der Polizei erfasst, sondern lediglich die für das Forschungsprojekt relevanten Szenen auf Basis der drei Anwendungsfälle aufgenommen. Hierzu ist der Kontakt zu den geschulten Einsatztrainern der Polizei MG vermittelt worden. Darüber hinaus ist eine Ortsbesichtigung der Trainingsstätte durch die Hochschule Niederrhein genutzt worden, um sich einen Eindruck des Versuchsaufbaus zu verschaffen und die Ziele der Messkampagne den Teilnehmenden des polizeilichen Einsatztrainings zu vermitteln.

Abbildung 4: Messaufbau Campus der HSNR

6.2.1 Platzierung der Sensoren

Für die Begleitung des polizeilichen Einsatztrainings wird, wie beim Einsatz auf dem Campus der HSNR, ein mobiler Messaufbau verwendet. Dabei handelt es sich um eine vereinfachte Version des an der HSNR eingesetzten Aufbaus. Der Aufbau ist in Abbildung 4 und Abbildung 6 dargestellt. Auch hier wird die Positionierung der Sensoren variiert, um Aufnahmen in verschiedenen Konstellationen durchführen zu können.

6.2.2 Rechtliche Grundlage und Verantwortung

Die Aufzeichnungen der polizeilichen Einsatztrainings erfolgen nach schriftlicher Einwilligungserklärung der Teilnehmenden. Hierbei erfolgt sowohl eine Einwilligungserklärung zur Radar- und Videoaufzeichnung unter der Verantwortung der HSNR als auch eine Einwilligungserklärung für Fotoaufnahmen zur späteren Presse- und Öffentlichkeitsarbeit. Zur Sicherstellung einer freiwilligen, informierten Einwilligung der Polizeidienstvollzugsbeamten wurden den Beamten die Ziele des Forschungsprojektes im Rahmen einer Kurzpräsentation und einer Live-Demonstration der Radartechnologie vermittelt. Den Einsatztrainern wurde die Einwilligungserklärung vorab zur Verfügung gestellt. Die Beamten wurden auf die Freiwilligkeit der Teilnahme hingewiesen und sie wurden informiert, dass eine Enthaltung oder eine anschließende Widerrufung der Einwilligung zu keinen Nachteilen im Training oder bei den jeweiligen Vorgesetzten führt. Eine Enthaltung führt zu keinen Trainingsnachteilen, da im parallelen, nicht

aufgezeichneten Bereich das vollständige Training durchgeführt werden kann. Ebenso besteht die Möglichkeit des Widerrufrechts, sodass die Teilnehmenden des polizeilichen Einsatztrainings ihr Einverständnis – ohne Entstehung möglicher Nachteile – nachträglich zurückziehen können. Die Verantwortung bezüglich der Verarbeitung der Radar- und Videoaufzeichnung liegt ausschließlich bei der HSNR. Für die Fotoaufnahmen liegt die Verantwortung bei der Polizei MG.

Abbildung 5: Messaufbau im Polizeitrainingszentrum

6.3 Platz der Republik

Mit zwei Sensorknoten sollen auf dem Platz der Republik, der direkt an einem der Eingänge des Bahnhofs liegt, Radar- und Videosignale aufgezeichnet werden. Die Erfassungsbereiche der Sensoren liegen in Richtung des Bahnhofseingangs und in Richtung der Platzmitte (Skaterbahn).

6.3.1 Platzierung der Sensoren

Für die Messungen am Platz der Republik wird ein Sensorknoten auf dem Dach des Gladbach-Centers platziert, wie es mit den orangen Symbolen in Abbildung 9 veranschaulicht wird. Ein weiterer Sensorknoten soll entsprechend der roten Symbole in Abbildung 7 auf der Radstation installiert werden. Installationen und Durchführung finden unter Einbeziehung und Genehmigung der Gebäudeeigentümer statt. Ein abschließbarer Serverraum im Gladbach-Center wird für die Messung am Platz der Republik genutzt.

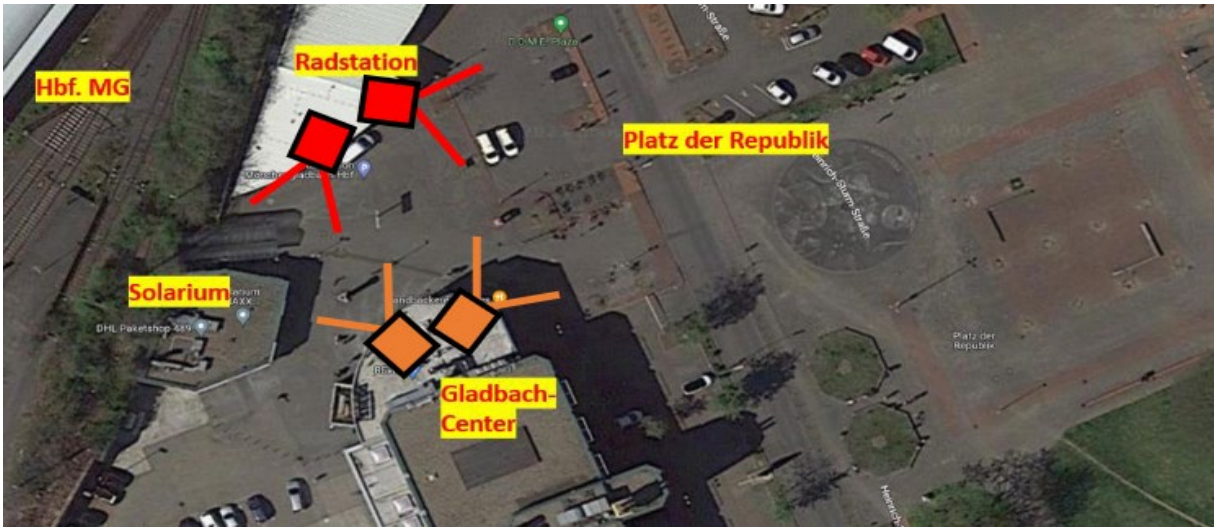


Abbildung 6: Platz der Republik vor dem Bahnhof in Mönchengladbach

6.3.2 Rechtliche Grundlage und Verantwortung

Es ist die HSNR, die über Zweck und Mittel der Datenverarbeitung entscheidet. Allein die Hochschule erhebt die Daten für das Forschungsvorhaben auf der Grundlage des §17 DSG NRW. Demnach ist die Verarbeitung personenbezogener Daten auch ohne Einwilligung für wissenschaftliche Forschungszwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und schutzwürdige Belange der betroffenen Person nicht überwiegen. Der wissenschaftliche Forschungszweck im Bereich der angewandten Forschung gem. Erwägungsgrund 159 (Verarbeitung zu wissenschaftlichen Forschungszwecken) ist mit dem Projekt KIRaPol.5G als Forschungsvorhaben gegeben, das durch ein Forschungsförderprogram des Ministeriums für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen unterstützt wird. Die Verarbeitung der Daten zu den vorab genannten Forschungszwecken ist auch erforderlich, da ohne die Daten ein Trainieren der KI nicht möglich ist. Nur mit diesen Daten kann die Künstliche Intelligenz auf das Erkennen der sicherheitsrelevanten Szenarien trainiert werden. „Ziel dieses überwachten Lernens ist es, ein KI-System mit Trainingsdaten so lange zu trainieren, bis das erwartete Ergebnis geliefert wird“ (vgl. Positionspapier

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 06.11.2019).

Unter „schutzwürdige Belange“ i.S.d. §17 DSG-NRW versteht der Gesetzgeber die Interessen und Rechte der Personen, deren Daten verarbeitet werden. Die Berücksichtigung schutzwürdiger Belange der Betroffenen ist ein grundlegendes Prinzip des Datenschutzes und gewährleistet, dass die Datenverarbeitung im Einklang mit den Datenschutzrechten und -vorschriften erfolgt. Dies ist entscheidend, um die Privatsphäre und die Rechte der Betroffenen zu schützen. Dies kann sich auf verschiedene Aspekte beziehen, darunter:

1. Datenschutz: Personen haben ein berechtigtes Interesse daran, dass ihre persönlichen Informationen angemessen und sicher behandelt werden, um vor Missbrauch, Diebstahl oder unbefugtem Zugriff geschützt zu werden.
   ➔ Der Schutz der Daten bis zur relativen Anonymisierung wird durch adäquate technische und organisatorische Maßnahmen (TOM) gewährleistet.
2. Privatsphäre: Die Verarbeitung von personenbezogenen Daten darf nicht unverhältnismäßig in die Privatsphäre der Betroffenen eingreifen. Schutzwürdige Belange können beispielsweise die Offenlegung sensibler Informationen oder das Sammeln umfangreicher Datenmengen betreffen.
   ➔ Im Rahmen von KIRaPol.5G werden keine sensiblen Informationen offengelegt und keine umfangreichen personenbezogenen Datenmengen gesammelt.
3. Recht auf informationelle Selbstbestimmung: Betroffene haben das Recht, über die Verarbeitung ihrer Daten informiert zu werden. Schutzwürdige Belange könnten sich auf die Transparenz und die Art und Weise beziehen, wie Informationen über die Datenverarbeitung bereitgestellt werden.
   ➔ An den Messstellen werden Hinweisschilder mittels QR-Code auf eine spezielle Informationsseite verweisen. Dort wird über das Projekt, seine Ziele und die Beteiligten mit Hilfe umfangreicher FAQs informiert. Insbesondere die Art der Datenerhebung, das Anonymisierungsverfahren sowie die Verwendung der anonymisierten Daten wird erläutert. Weiterhin wird ein Ansprechpartner genannt, der auf spezielle Fragen und/oder Kritik reagieren kann.
4. Einwilligung: Schutzwürdige Belange können auch die Notwendigkeit einer wirksamen Einwilligung der Betroffenen in die Datenverarbeitung betreffen. Dies bedeutet, dass die Betroffenen über die Zwecke der Verarbeitung und andere relevante Informationen informiert werden sollten und die Möglichkeit haben sollten, ihre Zustimmung zu geben oder zu verweigern.
   ➔ Die direkt akquirierten Beteiligten der Messkampagnen haben ihre schriftliche Einwilligung nach einer umfangreichen Information über die Erhebung und Verarbeitung der Daten freiwillig erteilt. Im Rahmen der öffentlichen Messkampagne wird

rechtzeitig durch Hinweisschilder auf die Datenerhebung hingewiesen und welcher Bereich davon tangiert ist, so dass durch Umgehung des Bereichs einer Beteiligung am Verfahren widersprochen werden kann.

5. Diskriminierung: Betroffene sollten vor diskriminierender Verwendung ihrer Daten geschützt werden, wie beispielsweise bei der automatisierten Entscheidungsfindung.
   ➔ Dadurch, dass die Daten nur anonymisiert zur Validierung der Trainingsdaten verwendet werden, ist eine diskriminierende Verwendung der Daten nicht anzunehmen.

Die zum frühestmöglichen Zeitpunkt anonymisierten Daten, die im weiteren Projektverlauf von keinem Projektbeteiligten individualisiert werden können, sind zum Erreichen des Forschungszwecks erforderlich. Schutzwürdige Belange von betroffenen Personen überwiegen nicht, weil diese Aspekte bis zur Anonymisierung nur in geringem Maße tangiert werden. Das Gewährleistungsziel ist immer Datenminimierung. Bis zum Zeitpunkt der Anonymisierung werden technische und organisatorische Maßnahmen getroffen, d.h. die Daten sind sowohl physisch besonders gesichert, indem das Speichermedium im verschlossenen Serverraum in einem zusätzlich verschlossenen Schrank verwahrt und nur einem festen Personenkreis zugänglich gemacht wird (vgl. Gewährleistungsziel Vertraulichkeit, Positionspapier DSK; Seite 11; s. Kapitel 7.1: Rollenkonzept). Generell ist sichergestellt, dass das KI-System nur durch Befugte konzipiert, programmiert, trainiert, genutzt und überwacht wird (i.S.d. Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 06.11.2019; vgl. ebenda, Seite 7). Die HSNR entscheidet über Zweck und Mittel der Datenverarbeitung. Aufgrund der beschriebenen Datenerhebung und -verarbeitung sowie des alleinigen Zugriffs gehen wir von einer alleinigen Verantwortung der Hochschule Niederrhein aus. Einer entsprechenden Informationspflicht gem. § 12 DSG NRW kommen wir durch Kennzeichnung der betroffenen Flächen mit einem Hinweisschild nach. Genannt werden Präsident der HSNR als juristisch Verantwortlicher, Datenschutzbeauftragte sowie die Landesbeauftragte für Datenschutz und Informationsfreiheit in NRW. Zudem wird ein QR-Code sowie ein ausgeschriebener Link auf eine spezielle Informationsseite verweisen, auf der Projektziel sowie die eingesetzte Technik in verständlicher Sprache erläutert werden. Zusätzlich werden FAQs auf der Landingpage angeboten, um somit höchstmögliche Transparenz zu gewährleisten. Einem darüberhinausgehenden Informationsbedarf wird durch die Nennung eines speziellen Ansprechpartners für Fragen und Kritik der Betroffenen entsprochen.

7 Datenverarbeitung

Die Videodaten werden nur zur Annotation der aufgenommenen Szenen und zur Ableitung von Skelettinformationen für die Simulation von Radarsignalen aufgezeichnet. Die Videodaten

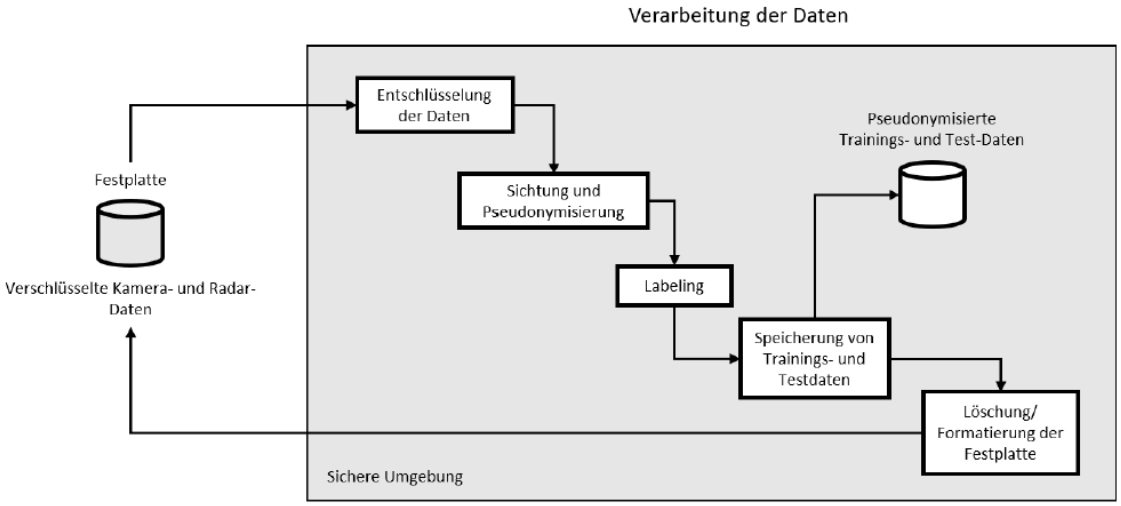
werden wie in Kapitel 4.3 beschrieben anonymisiert. Anschließend werden die originalen Aufnahmen gelöscht und alle weiteren Verarbeitungsschritte erfolgen auf Basis der anonymisierten Videodaten. Die Verantwortung bzgl. der Erhebung und Verarbeitung der personenbezogenen Daten ist jeweils in Tabelle 2 für die Messkampagnen aufgelistet. Eine Anonymisierung erfolgt in den jeweiligen Messkampagnen zum frühestmöglichen Zeitpunkt. Die Anonymisierung und wann diese durchgeführt wird, ist im Kapitel 4.3 beschrieben. Eine Anonymisierung der Daten vor Ort ist wie beschrieben auf Grund von unzureichender Rechenkapazität nicht bzw. nur mit einem erheblichen Mehraufwand möglich. Das Datennetzwerk wird so erstellt, dass kein Zugriff durch dienstleistende Partner auf die Daten vorhanden ist.

Tabelle 2: Datenverarbeitung nach Messkampagne

	Orte der Messkampagnen		
	HSNR	**Polizeiliche Einsatztrainings**	**Platz der Republik**
Verantwortung	HSNR	HSNR	HSNR
Beteiligung der Polizei	nein	Polizei MG	nein
Rechtliche Grundlage	§17 DSG NRW	§17 DSG NRW	§17 DSG NRW
Art der Datenerhebung	Video / Radar / Foto	Video / Radar/ Foto	Video / Radar / Foto
Einwilligung	Einwilligungserklärung		Keine vorherige Einwilligungserklärung, Aufklärung durch Hinweisschild inkl. QR-Code
Datenschutz	Entsprechend dieses Dokuments		
Speicherdauer	Radar bis Projektende, Roh-Video bis zur Anonymisierung, Anonymisiertes Video bis zum Projektende		

Eine Übersicht der Verarbeitung ist in Abbildung 8 dargestellt. In den folgenden Unterkapiteln sind die an der Verarbeitung beteiligten Rollen, die jeweils erhobenen Daten, die durchgeführten Verarbeitungsvorgänge sowie deren rechtliche Grundlage und Verantwortung beschrieben. Außerdem werden die Erstellung der Annotationen (= Labeling) aus den Videoaufzeichnungen sowie die Synthese von Trainingsdaten gesondert beschrieben.

Abbildung 7: Verarbeitung der Radar- und Kameradaten



7.1 An der Verarbeitung beteiligte Rollen

An der Durchführung des Projektes sind mehrere Personen beteiligt. Um den Schutz der im Projekt erhobenen personenbezogenen Daten zu gewährleisten, wurde ein Rollenkonzept erarbeitet, welches festlegt, wer auf welche Daten Zugriff hat. Die einzelnen Rollen sind in Tabelle 3 zusammen mit einer Kurzbeschreibung aufgelistet. Auf diese wird in Kapitel 7.3 bei der Beschreibung der einzelnen Verarbeitungsschritte referenziert.

Tabelle 3: Rollen in der Datenverarbeitung

Rolle	Beschreibung
Planung des Aufbaus	Konzeption des Hardware-Aufbaus sowie der Durchführung des Aufbaus
Aufbau Sensorknoten	Durchführung des Hardware-Aufbaus eines Sensorknotens am Einsatzort
Aufbau 5G-Netzwerk	Durchführung des Aufbaus des 5G-Netzwerks am Einsatzort
Aufbau Server-Rack	Durchführung des Hardware-Aufbaus des Server-Racks am Einsatzort
Verwaltung Sim-Karten	Freigabe und Verteilung von Sim-Karten für den Zugang zum 5G-Netzwerk

Übertragung (Festplatten-tausch) der Daten	Austausch der Festplatten am Messstandort und Transport dieser zur späteren Verarbeitung
Anonymisierung der Kamera-Daten	Anonymisierung der Kamera-Daten
Label-Erstellung	Erstellung von Labeln zu den anonymisierten Kamera-Daten
Auswertung Radar-Daten	Erstellung von Auswertungen zu den erhobenen Radar-Daten
Auswertung Label	Erstellung von Auswertungen zu den erstellten Labeln
Training KI(s)	Verwendung von Radar-Daten und Labeln zum Trainieren von KI-Modellen
Auswertung KI(s)	Erstellung von Auswertungen zu den trainierten KI-Modellen

7.2 Erhobene Daten

Die Verarbeitung der personenbezogenen Daten erfolgt von einem eingeschränkten Personenkreis entsprechend der in Tabelle 3 beschriebenen Rollen. Im Sinne der Datensparsamkeit erfolgt die frühestmögliche Anonymisierung der erhobenen personenbezogenen Daten unter den jeweiligen Rahmenbedingungen der Messkampagnen: Am Platz der Republik ist aufgrund fehlender Rechnerkapazitäten keine Anonymisierung vor Ort möglich. Die erhobenen Videosequenzen werden auf eine externe Festplatte gespeichert und anschließend im Labor der HSNR anonymisiert. Das Risiko möglicher Rückschlüsse der anonymisierten Daten auf natürliche Personen wird durch Einhaltung verschiedener Vorkehrungen als gering eingestuft. Der detaillierte Anonymisierungsprozess ist im Kapitel 4.3 beschrieben. Die Maßnahmen zur Sicherung der Daten sind in Kapitel 9 und 10 erörtert. Dies impliziert sowohl den unverhältnismäßig großen technischen Aufwand zur Rekonstruktion der anonymisierten Daten als auch den kleinen Personenkreis der wissenschaftlichen Mitarbeiter der HSNR, die einen Zugriff auf diese Daten haben. Die Angehörigen der HSNR haben sich im Dienstvertrag zur Vertraulichkeit verpflichtet. Auf die von der HSNR erhobenen Daten haben die anderen Projektbeteiligten keinen Zugriff.

Bei der Hochschule Niederrhein erfolgt eine Anonymisierung der Videosequenzen wie in Kapitel 4.3 beschrieben. Nach der Anonymisierung werden die originalen Videoaufzeichnungen

umgehend gelöscht. Nach der Anonymisierung handelt es sich im weiteren Verlauf nicht mehr um personenbezogene Daten.

Die KI wird nur mit den Radaraufnahmen sowie mit der aus den anonymisierten Videoaufnahmen abgeleiteten Annotation trainiert. Die Videoaufnahmen fließen nur in Form der daraus abgeleiteten Annotation in das Training ein. Die Annotation, also das Erstellen von „Labeln“, wird in Kapitel7.5beschrieben.

Im Folgenden sind die Informationen zu den erhobenen Daten zusammengefasst:

- Welche Daten werden erhoben?
  - Videoaufnahmen
  - Radar: Mikro-Doppler-Spektren, Ziel-Positionen
- Wo werden die Daten gespeichert?
  - Radar und verschlüsseltes Video: Auf der zentralen Recheneinheit des jeweiligen Standorts (siehe Standortbeschreibung für weitere Details)
  - Alles weitere: HSNR
- Wie lange werden die Daten gespeichert?
  - Video-Aufnahmen:
    - Nicht Anonymisierte Video-Aufnahmen: bis zur Anonymisierung
    - Anonymisierte Video-Aufnahmen: bis zum Projektende
  - Label: bis zu drei Jahre nach Projektende
  - Radar-Aufnahmen: bis zu drei Jahre nach Projektende
- Zu welchem Zeitpunkt werden die Daten anonymisiert?
  - nach Überführung zur HSNR, vor weiterer Verarbeitung

7.3 Verarbeitungsvorgänge

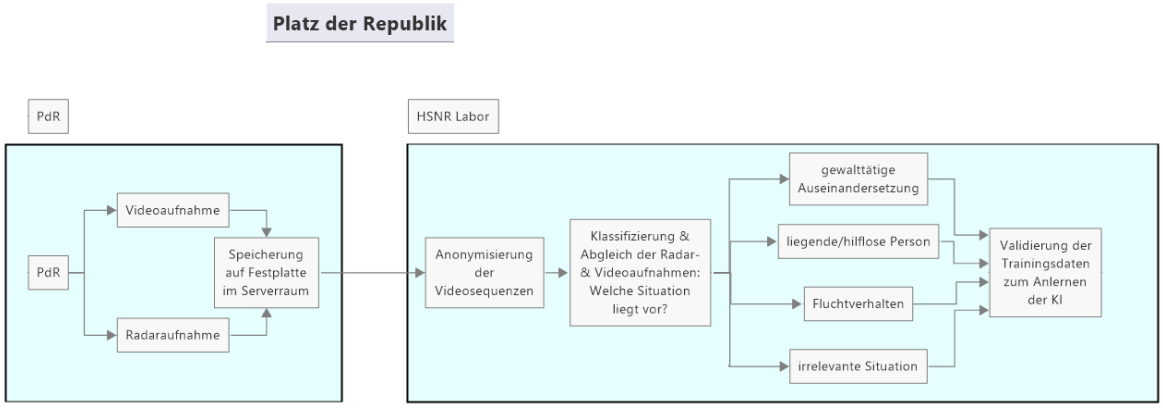
Hier werden die einzelnen Schritte der Verarbeitung aufgeführt. In dem in Abbildung 11 dargestellten Flussdiagramm der Verarbeitung findet sich außerdem eine Übersicht dieser Schritte.

Nr.	Vorhergehende Vorgänge	Beschreibung	Zweck
1	-	Erfassung per Kamera	Erfassung als Referenz für die Ableitung der Label
2	1	Übertragung (Kabel) der Bilder zum Sicherheitsrouter	Die Daten müssen zum Verarbeitungs-Server zur Speicherung
3	-	Erfassung per Radar	Erfassung als Eingabe für das Training der KI
4	3	Übertragung (Kabel) der Daten zum Sicherheitsrouter durch den Switch	Die Daten müssen zum Verarbeitungs-Server zur Speicherung
5	2, 4	Datenübertragung via 5G von Sicherheitsrouter zur 5G Basisstation	Die Daten müssen zum Verarbeitungs-Server zur Speicherung
6	5	Übertragung (Kabel) vom 5G Basisstation zum 5G Core-Server	Die Daten müssen zum Verarbeitungs-Server zur Speicherung
7	6	Übertragung (Kabel) vom 5G Core-Server zum Verarbeitungs-Server	Die Daten müssen zum Verarbeitungs-Server zur Speicherung
8	7	Verschlüsselung der Kamera-Daten	Schutz vor unbefugtem Zugriff
9	8	Abspeichern Kamera-Daten	Die Kamera-Daten werden später zur Bestimmung der Label benötigt

10	8	Abspeichern Radar-Daten	Die Radar-Daten werden später zum Training der KI(s) benötigt
11	9	Übertragung (Festplattentausch) der gespeicherten Kamera-Daten	Übertragung großer Datenmengen zur weiteren Verarbeitung
12	10	Übertragung (Festplattentausch) der gespeicherten Radar-Daten	Übertragung großer Datenmengen zur weiteren Verarbeitung
13	11	Anonymisierung der Kamera-Daten	Schutz der Persönlichkeitsrechte(?)
14	13	Erstellung der Label aus den Kamera-Daten	Training der KI(s) benötigt Referenz
15	14	Löschen der Kamera-Daten	Nach der Erstellung der Label werden die Kamera-Daten nicht mehr benötigt
16	12	Auswertung der Radar-Daten	Auswertung von Einflüssen auf die Radar-Daten und Auswertung der Qualität dieser
17	14	Auswertung der Label	Auswertung der Label
18	12, 14	Training der KI(s)	Erstellung eines Klassifikators für Gefahrensituationen; Projektziel
19	18	Bewertung der KI(s)	Die Qualität der KI(s) muss ausgewertet werden

Tabelle 4: Verarbeitungsschritte

Abbildung 8: Flussdiagramm der Verarbeitung



7.4 Rechtliche Grundlage und Verantwortung

Nach § 40 DSG NRW ist eine Verarbeitung von personenbezogenen Daten in archivarischer, wissenschaftlicher oder statistischer Form zulässig, sofern dies im Rahmen wissenschaftlicher Forschung erfolgt.

> „Personenbezogene Daten dürfen im Rahmen der in § 35 genannten Zwecke in archivarischer, wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.“

Nach § 36 Nr.6 DSG NRW ist das Anonymisieren das „Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten, Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“. Die Unkenntlichkeit der Personen steht nicht konträr zur weiteren Datenverarbeitung, da die HSNR ebenfalls mit den anonymisierten Daten weiterarbeiten kann, d.h. eine Anonymisierung dem Forschungszweck nicht entgegensteht. Nach § 40 DSG NRW dürfen personenbezogene Daten in wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen sind. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten bestehen. KIRaPol.5G zielt darauf ab, Gefahrensituationen zu erkennen und dient damit der Verbesserung, der Verhütung, der Verfolgung und der Ahndung von Straftaten und verfolgt somit ein öffentliches Interesse. Werden die personenbezogenen

Daten so früh wie möglich anonymisiert, d.h. an der Hochschule Niederrhein, so ist ihre Erhebung nach § 17 DSG NRW und Verarbeitung nach § 40 DSG NRW zulässig. Die Verantwortung für die Datenverarbeitung in den einzelnen Messkampagnen ist in Tabelle 2, die die Datenverarbeitung nach der jeweiligen Messkampagne beinhaltet, aufgeführt.

7.5 Erstellung der Label

Aus den anonymisierten Videodaten wird durch einen Menschen eine Bewertung der aufgenommenen Szene abgeleitet. Dabei handelt es sich um eine abstrakte Beschreibung der relevanten Aspekte der Szene, die keine personenbezogenen Daten mehr enthält. Im einfachsten Fall gibt es hier pro Zeitschritt nur die Information, ob eine Gefahrensituation vorliegt oder nicht. Voraussichtlich werden die Label jedoch zusätzlich die Art der Gefahrensituation sowie deren Position im Bild enthalten. Die genaue Form der Label wird im Verlauf des Projektes festgelegt.

Dabei wird der Mensch gegebenenfalls durch eine Software unterstützt, die einen Vorschlag für die Erstellung der Label bereitstellt. Diese Software basiert auf zuvor gesammelten Daten und steht erst später im Projekt zur Verfügung.

Für die Bewertung der Szenen durch einen Menschen sind die anonymisierten Videoaufnahmen ausreichend. Die originalen Videoaufzeichnungen werden dafür nicht mehr benötigt und stehen nach der Anonymisierung auch nicht mehr zur Verfügung.

7.6 Synthese und Modellierung von Trainingsdaten

Eine weitere Möglichkeit, Radardaten in Form von Mikro-Doppler Spektren für das Training der KI zu erhalten, besteht in der Modellierung der Radarübertragung bestimmter Szenen und der synthetischen Generierung von Doppler-Spektren. Dadurch ist es möglich, künstliche Radardaten für Szenen zu generieren, die sich nur schlecht nachstellen lassen. Vor allem kann die Anzahl von Trainingsdaten damit erheblich vergrößert werden.

Das Geschehen in einer Szene, also insbesondere die Bewegungen der beteiligten Personen, können von einer Person festgelegt und modelliert werden. Eine alternative Möglichkeit besteht in der Extraktion der Bewegungsinformationen aus aufgenommenen Videosequenzen der Messkampagnen, wobei dies auch für die anonymisierten Videosignale möglich ist. Mit Verfahren der Bildverarbeitung können Daten bestimmt werden, die die Skelette der in der Szene auftretenden Personen und ihrer Bewegungen beinhalten und mit denen eine Modellierung der Radarsignale möglich wird. Die Skelettdaten beschreiben eine Person in anonymisierter Form, da eine Rekonstruktion des Gesichts unmöglich ist und der Körper nur durch wenige Punkte beschrieben wird. Die Daten der extrahierten Körperskelette werden von der Hochschule Niederrhein an den Projektpartner IMST übermittelt, der damit die Radarsignale

in Form von Doppler-Spektren künstlich generieren kann. Das Ergebnis ist eine Synthese von Radar Trainingsdaten für die KI, die auf der Auswertung realer Szenen beruht. Ein Ziel des Projekts besteht in der Untersuchung, ob die mit Hilfe der Simulation generierten Radardaten für das Training der KI verwendbar sind und möglicherweise die aufwendige Aufnahme von Daten ersetzen kann.

8 Hardware-Aufbau

Für die in Kapitel 7 beschriebene Datenverarbeitung und vor allem für die Datenerhebung ist der Einsatz von spezieller Hardware erforderlich. In diesem Kapitel findet sich neben einer Übersicht der Gesamt-Architektur auch jeweils eine ausführliche Beschreibung der Komponenten, deren Zusammenspiel sowie Abweichungen der Hardware für spezielle Messkampagnen.

8.1 Übersicht des Hardwareaufbaus

Das Messsystem für eine Messkampagne besteht aus einer zentralen Rechnereinheit für die Datensammlung und deren Vorverarbeitung und mehreren (meist zwei) voneinander unabhängigen Sensorknoten, welche die Daten erheben und direkt an den zentralen Rechner weiterleiten. Der Aufbau ist in Abbildung 10 dargestellt.

Ein Sensorknoten (SK) besteht dabei jeweils aus einem Sicherheitsrouter für die verschlüsselte Datenübertragung zur zentralen Recheneinheit, einem oder mehreren Sensorpaaren, die sich wiederum jeweils aus einer Kamera und einem Radar zusammensetzen, einem Switch sowie einem Kleinrechner des Typs Raspberry Pi, welcher mit einem GPS Modul ausgestattet ist. Im Sensorknoten erfolgt keine Abspeicherung der gesammelten Daten. Die Daten werden direkt durch einen verschlüsselten Tunnel an die zentrale Recheneinheit übertragen.

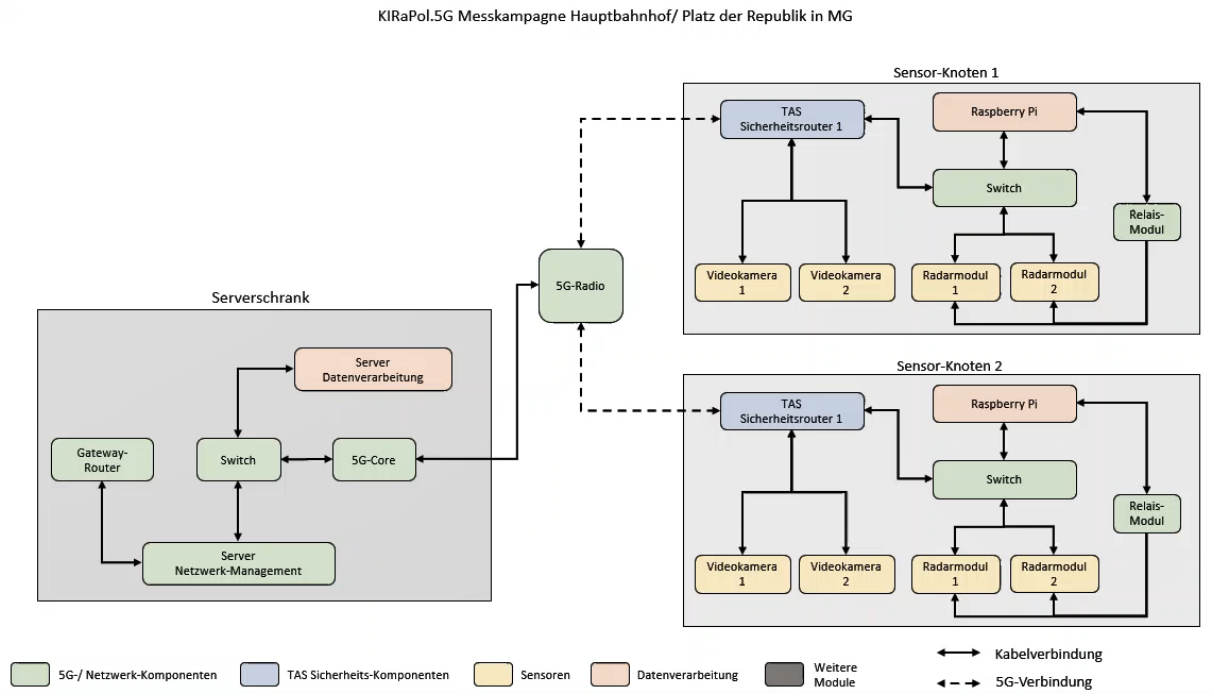


Abbildung 9: Übersicht des Hardware-Aufbau

Auf der zentralen Recheneinheit (ZR) werden die Daten der einzelnen Sensorpaare entgegengenommen und weiterverarbeitet. Die Kamera- und Radardaten werden unabhängig voneinander übertragen und verarbeitet. Es gibt jedoch einen synchronisierten Zeitstempel, über den eine zeitliche Zuordnung einzelner Radar- und Videoaufnahmen möglich ist. Dieser wird genutzt um eine Zuordnung zwischen den aus den Videos abgeleiteten Labeln und den Radaraufnahmen zu ermöglichen. Die Verarbeitung beschränkt sich hier aufgrund von Beschränkungen der Rechenkapazität auf das Verschlüsseln und Abspeichern der gesammelten Daten.

8.2 Zentrale Recheneinheit

Die Aufzeichnung und Speicherung der Messdaten, wird mit Hilfe einer zentralen Einheit durchgeführt. Diese Zentrale Recheneinheit (ZR) ist hierfür mit einem Rechner ausgestattet, welcher über mehrere auswechselbaren Festplatten verfügt, auf denen die von den Sensorknoten übermittelten Daten abgespeichert werden. Diese Festplatten können für die weitere Verarbeitung der Daten von außen entnommen und ausgelesen werden.

Die Zentrale Recheneinheit ist jeweils in der Form zugriffsgeschützt, wie es für die einzelnen Messkampagnen in Kapitel 6 beschrieben wurde. Bei den Messkampagnen, bei denen 5G zur Übertragung eingesetzt wird, befindet sich die Zentrale Recheneinheit zusammen mit der für 5G notwendigen Hardware in einem zugriffsgeschützten Server-Rack (SR).

8.3 Sensorknoten

Ein Sensorknoten besteht jeweils aus einem Sicherheitsrouter der Firma TAS, einem Switch, einem Raspberry Pi sowie (zwei) Sensorpaaren. Ein Sensorpaar besteht jeweils aus einer Videokamera sowie einem Radarmodul. Die Hardware-Komponenten sind in Tabelle 5 aufgeführt. Die Verbindung der Komponenten ist in Abbildung 10 dargestellt.

Der Raspberry Pi ist mit einem GPS-Modul, einer Realtime-Clock (RTC) sowie einem Relay-Modul ausgestattet. Über das Relay-Modul ist es möglich, die Radarmodule von der Stromversorgung zu trennen, da diese nicht selbst die Möglichkeit haben, abgeschaltet zu werden. Die Kombination aus GPS-Modul und Realtime-Clock ermöglicht es dem Raspberry Pi als Zeitserver zu agieren. Diese Zeitquelle wird dazu genutzt, die Video- und Radar-Aufnahmen untereinander zu synchronisieren. Außerdem dient der Raspberry Pi als Auslöser für die Radarmodule. Da es sich bei Radar um eine aktive Sensortechnologie handelt, ist es notwendig, dass Radarmodule mit sich überschneidenden Sendebereichen nicht zur gleichen Zeit aktiv sind. Auch hierfür ist die zeitliche Synchronisierung notwendig, da eine Abstimmung zwischen Sensorknoten notwendig ist.

Komponente	**Hersteller**	**Typ/Modell**
Sicherheitsrouter	TAS	TAS Link IV IP/ 5G
Videokamera	Axis	Axis p1468 LE
Radarmodul	IMST	sR77-3403e
Switch	D-Link	DGS-105GL/E
Raspberry Pi	Raspberry Pi Trading	Raspberry Pi 3 Model B+

Tabelle 5: Übersicht Hardwarekomponenten im Sensorknoten

8.4 Verbindungen zwischen den Komponenten im Sensorknoten

Die Komponenten innerhalb eines Sensorknotens und ihre Verbindungen sind in Abbildung 11 dargestellt. Die Verbindung der Komponenten im Server-Schrank ist in Abbildung 10 dargestellt. Tabelle 4 gibt eine Übersicht über alle Verbindungen in einem Messaufbau.

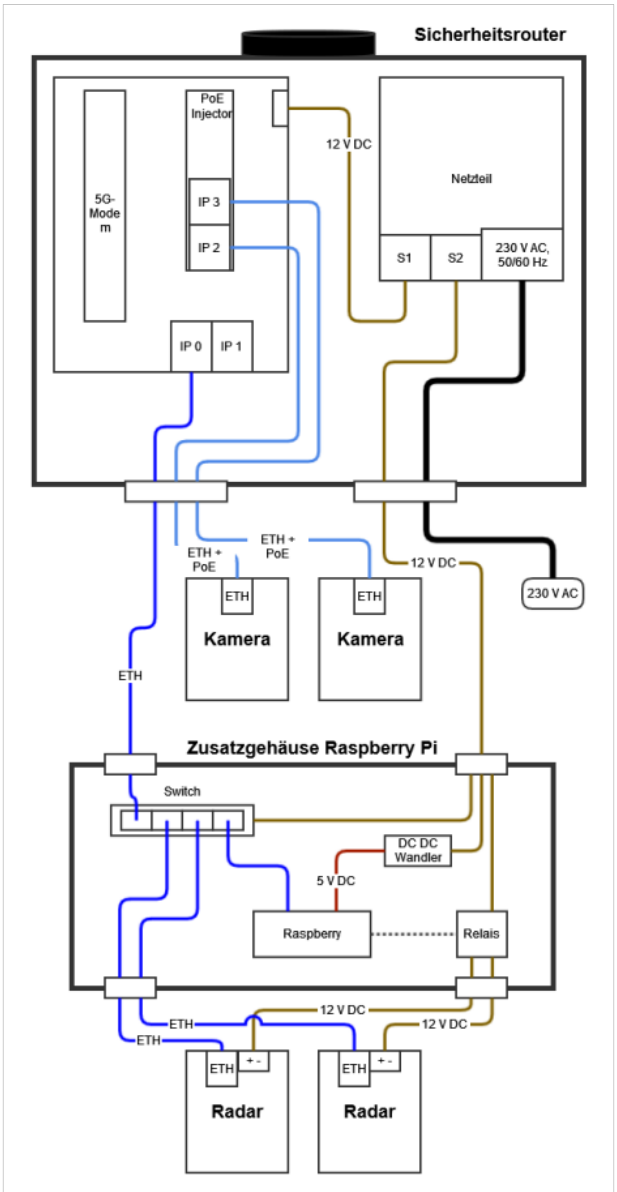


Abbildung 10: Übersicht Sensorknoten

Ort	Verbindung	Transportmedium	Sicherheitsmaß-nahmen
SR	Switch, Server Datenverarbeitung	Ethernet	VLAN Trennung
SR	Switch, 5G-Core	Ethernet	VLAN Trennung IPsec-Tunnel
SR	Switch, Server Netz.-Management	Ethernet	VLAN Trennung IPsec-Tunnel
SR	Switch, Gateway-Router	Ethernet	VLAN Trennung
SR	5G-Core, 5G-Radio	Lichtwellenleiter (LWL)	5G-Encryption IPsec-Tunnel
SR	Gateway-Router, TAS Secure Cloud	DSL oder öffentliches Mobilfunknetz	IPsec-Tunnel
	5G-Radio, TAS-Sicherheitsrouter	Mobilfunk	SIM-Karten, 5G-Encryption, IPsec-Tunnel
SK	TAS-Sicherheitsrouter, Videokamera	Ethernet	-
SK	TAS-Sicherheitsrouter, Switch	Ethernet	-
SK	Switch, Radarmodul	Ethernet	-
SK	Switch, Raspberry Pi	Ethernet	-

Tabelle 4: Verbindungen im Messaufbau

8.5 Abweichungen des Hardware-Aufbaus für einzelne Messstandorte

Der hier allgemein beschriebene Aufbau wird für einige der geplanten Messkampagnen abgeändert, um sich an die speziellen Gegebenheiten der Örtlichkeiten anzupassen. Die Messkampagnen mit den speziellen Gegebenheiten wurden in Kapitel 6 beschrieben. Dabei handelt es

sich jeweils um Vereinfachungen mit dem Ziel, den Aufbau und den Transport der Hardware zu erleichtern. Die sich daraus ergebenden Änderungen sind in den folgenden beiden Kapiteln beschrieben.

8.5.1 Messstandort: Hochschule Niederrhein

Für die Messkampagne an der Hochschule Niederrhein ist ein mobiles Messsystem geplant, welches bei der Durchführung von Messungen aufgebaut und nach der Messung wieder abgebaut werden kann. Dieses mobile Messsystem hat den wesentlichen Vorteil, dass Messungen an verschiedenen Standorten durchgeführt werden können. Dazu ist der Sensorknoten an einem mobilen, ausfahrbaren Mast befestigt.

Dieser Messaufbau dient auch als Prototyp für alle anderen Aufbauten. Aus diesem Grund wird der Aufbau nach und nach erweitert. Aktuell gibt es nur einen Sensorknoten und auch dieser ist noch nicht voll ausgestattet. Die Nutzung von 5G wird erst zu einem späteren Zeitpunkt eingeführt, da eine Erprobung in einem kabelgebundenen Aufbau einfacher ist.

8.5.2 Messstandort: Begleitung des Polizeitrainings

Auch bei dem Messaufbau für die Begleitung des Polizeitrainings handelt es sich um eine vereinfachte Version des Messaufbaus. Da diese Messungen jeweils nur für einige Stunden während eines Moduls des Polizeitrainings im Polizeitrainingszentrum Linnich stattfinden, ist hier ein einfacher Transport sowie ein schneller Aufbau und Abbau nötig. Eine Beschreibung der Messkampagne ist in Kapitel 6 zu finden.

Dazu wird bei dieser Messkampagne nur ein Sensorpaar eingesetzt und ein Laptop als Zentrale Recheneinheit genutzt. Die Sensoren sind dabei direkt über einen Switch mit dem Laptop verbunden. Die Nutzung von 5G sowie die Synchronisierung der Radarauslösungen wird nicht benötigt.

8.6 5G-Campusnetz

Durch die räumliche Verteilung der Sensorknoten an Orten, zwischen denen eine Verkabelung nicht ohne erheblichen Aufwand möglich ist und auch der Zugang zu den Sensorknoten einen hohen Aufwand erfordert, ist der Einsatz einer Funktechnologie notwendig, um die Zentrale Recheneinheit mit den Sensorknoten zu verbinden. Dazu kommt in diesem Projekt ein System des Mobilfunks der fünften Generation (5G) zum Einsatz.

5G ist die fünfte Generation des Mobilfunkstandards und wird in Deutschland seit 2020 zunehmend für die Endnutzer bereitgestellt. Er verspricht im Vergleich zu seinen Vorläufern höhere Bandbreiten, niedrigere Latenzen, mehr Teilnehmerkapazität und erhöhte Sicherheit.

Im Rahmen der Messkampagnen wird die m3connect ein privates Mobilfunknetz im Umfeld des Mönchengladbacher Hauptbahnhofes aufbauen und betreiben. Das Mobilfunknetz wird am Platz der Republik installiert.

Private Mobilfunknetze sind anders als die Netze der großen Mobilfunknetzbetreiber in Deutschland auf kleine geographische Areale beschränkt. Diese Netze werden in der Regel für die Kommunikation zwischen Maschinen und IT-Systemen verwendet. Nur selten sind diese Netze auch für Telefonie ausgelegt. Für diese lokalen und privaten Mobilfunknetze ist der Frequenzbereich von 3,7 GHz bis 3,8 GHz vorgesehen. Sie werden in erster Linie im Industrieumfeld eingesetzt, um die drahtlose Kommunikation in der Produktion und Logistik bereitzustellen.

Im Gegensatz zu WiFi ist es erheblich schwieriger, ein solches Funknetz zu stören, weil nur wenige Geräte auf solchen Frequenzen senden können. Zudem sind das Einwählen und Authentifizieren in ein solches Funknetz nur mit einer speziell konfigurierten SIM-Karte möglich. Eine solche SIM-Karte wird nur vom Betreiber des Netzes ausgegeben und kann nicht im Handel gekauft werden. Deswegen eignen sich private Mobilfunknetze besonders für Hochsicherheitsnetze, die kritische und sensible Informationen übertragen. Im Rahmen des Forschungsprojektes KIRaPol.5G kann so sichergestellt werden, dass keine unautorisierte Person Zugriff auf die drahtlos übertragenen Daten erhalten kann. Darüber hinaus werden innerhalb des 5G Campusnetz die Videodaten durch einen IPsec-Tunnel verschlüsselt.

9 Maßnahmen zur Minimierung der Risiken

Um die Sicherheit der im Projekt erhobenen personenbezogenen Daten zu erhöhen, werden eine Vielzahl von Maßnahmen ergriffen. Darunter bilden folgende generelle Maßnahmen den Kern des Sicherheitskonzeptes:

- Installation der Hardware-Komponenten nur durch geschultes Personal
- Zugangsbeschränkung entsprechend dem Rollenkonzept (siehe Kapitel 7.1)
- Auf allen Systemen werden aktuelle Softwareversionen eingesetzt
- Regelmäßige Sichtkontrollen, ob Komponenten Schäden oder Manipulationen aufweisen
- Alle Systeme sind durch individuelle Passwörter bzw. Schlüssel gesichert

Weitere hardware- und verarbeitungsspezifische Maßnahmen sind jeweils direkt bei den in Kapitel 10 aufgeführten und beschriebenen Risiken angegeben.

10 Abschätzung der vorhandenen Risiken

Im Folgenden werden Risiken beschrieben, die die Durchführung des Projektes oder die Sicherheit der erhobenen personenbezogenen Daten gefährden. Dazu werden zunächst in Kapitel 10.1 die Risikoquellen und in Kapitel 10.2 das Vorgehen zur Bewertung der Risiken beschrieben. Anschließend werden in Kapitel 10.3 die einzelnen Risiken aufgeführt. Dabei werden jeweils auch direkt die Maßnahmen aufgeführt, die ergriffen werden, um das Risiko so weit wie möglich zu senken. Neben diesen risikospezifischen Maßnahmen werden noch die Maßnahmen zur Minimierung der Risiken ergriffen, die in Kapitel 9 beschrieben wurden.

Die beschriebenen Risiken beziehen sich jeweils auf die in Kapitel 7 beschriebene Datenverarbeitung unter Verwendung der in Kapitel 8 beschriebenen Hardware. Da sich die Hardware zwischen den Messkampagnen leicht unterscheidet, sind nicht alle Risiken auf alle Messkampagnen anwendbar. Hier werden die Risiken für alle Messkampagnen gemeinsam aufgeführt und bewertet.

Die Risiken lassen sich grob in zwei Risikogruppen aufteilen. Das sind zum einen Risiken, die die Projektdurchführung gefährden und zum anderen Risiken beim Verarbeiten der personenbezogenen Daten. Besonders relevant sind hier die Risiken der zweiten Gruppe, da diese potenziell in die Persönlichkeitsrechte von vielen Menschen eingreifen.

10.1 Risikoquellen

In Tabelle 5 sind die für das Projekt relevanten Risikoquellen aufgeführt. Dabei werden die Risikoquellen während der Projektdurchführung und zum Schutz der personenbezogenen Daten hier gemeinsam aufgeführt.

Die Risikoquellen 2 und 4 stellen dabei die größte Gefahr für die erhobenen persönlichen Daten dar, da hier ein Vorsatz vorliegt und entsprechend mit einem höheren Aufwand versucht wird, die ergriffenen Schutzmaßnahmen zu umgehen. Unbeabsichtigte Risikoquellen lassen sich leichter durch die technisch-organisatorischen Maßnahmen verhindern, da hier kein Vorsatz vorliegt und entsprechend kein höherer Aufwand zu deren Umgehung aufgebracht wird.

Die nichtmenschlichen Risikoquellen stellen hauptsächlich eine Gefahr für die Projektdurchführung dar und betreffen den Schutz der personenbezogenen Daten nur in wenigen Fällen.

Tabelle 5: Risikoquellen

Nr.	Typ	Intern/ex-tern	Art	Beispiele für relevante Risiko-quellen
1	Menschlich	Intern	Unbeabsichtigt	Mitarbeiter, Vorgesetzte
2	Menschlich	Intern	Vorsätzlich	Mitarbeiter, Vorgesetzte
3	Menschlich	Extern	Unbeabsichtigt	Wartungspersonal
4	Menschlich	Extern	Vorsätzlich	Wartungspersonal, Mitbewerber, Hacker
5	Nichtmenschlich	Intern	-	Wasserschaden, Feuer, Defekte Komponenten
6	Nichtmenschlich	Extern	-	Stromausfall, extreme Wetterbedingungen, Katastrophen

10.2 Beschreibung der Risikobewertung

Die für das Projekt relevanten Risiken werden mit einer Risikokennzahl (RKZ) aus dem Bereich von 1 bis einschließlich 25 bewertet. Eine RKZ kleiner vier wird dabei als „geringes“ Risiko eingestuft. Der Bereich von vier bis einschließlich 12 wird als „mittleres“ Risiko eingestuft. Der Bereich ab 13 wird als „hohes“ Risiko eingestuft. Die Risikolevel zusammen mit den dazu passenden Bewertungen sind in Tabelle 7 dargestellt.

Die RKZ setzt sich dabei aus einer Bewertung der Schwere (S) aus dem Bereich von 1 bis einschließlich 5 und einer Bewertung der Häufigkeit aus dem Bereich von 1 bis einschließlich 5 zusammen. Dabei steht eine größere Zahl jeweils für ein höhere Schwere bzw. eine höhere Häufigkeit. Die RKZ ergibt sich durch Multiplikation der beiden Einzelbewertungen für Schwere und Häufigkeit. Die so erreichbaren RKZs sind in Tabelle 6 dargestellt.

Tabelle 6: Skala zur Risikobewertung

S / H	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Tabelle 7: Risikobewertung: Risikolevel

Risikolevel	Werte
gering	1; 2; 3;
mittel	4; 5; 6; 8; 9; 10; 12
hoch	15; 16; 20; 25

10.3 Risiken

In den Tabellen 8, 9, und 10 sind die Risiken getrennt für den Sensorknoten, den Serverschrank und die Verarbeitung in der Hochschule aufgeführt. Außerdem werden die Risiken gruppiert für verschiedene Risikoformen aufgelistet.

In der Spalte RQ findet sich jeweils eine Zuordnung zu den in Kapitel 10.1 definierten Risikoquellen. Die Bewertung in den Spalten S, H sowie die RKZ entsprechen der in Kapitel 10.2 beschriebenen Bewertung. Die Benennung der Hardware folgt der Beschreibung aus Kapitel 8.

10.3.1 Risiken: Sensor-Knoten

Tabelle 8: Risiken im Sensor-Knoten

RQ	Beschreibung	Folge	S	H	RKZ	Sicherheitsmaßnahmen
Physischer Zugriff						
2, 4	Zugriff auf die Kamera	• Fehlende oder manipulierte Aufnahmen • Angreifer kann Kamera-Daten auf das eigene System speichern	4	2	8	• Installation an schwer zugänglichem Ort • keine Speicherung von Daten in der Kamera • Passwortschutz der Einstellungen
2, 4	Zugriff auf das Radar-Modul	• Fehlende oder manipulierte Aufnahmen • Angreifer kann Radar-Daten auf das eigene System speichern	2	2	4	• Installation an schwer zugänglichem Ort • keine Speicherung von Daten im Radar
2, 4	Zugriff auf den Switch	• Fehlende oder manipulierte Radar Aufnahmen	2	2	4	• Installation an schwer zugänglichem Ort
2, 4	Zugriff auf den Raspberry Pi	• Fehlende oder manipulierte Radar Aufnahmen	2	2	4	• Installation an schwer zugänglichem Ort • Passwortschutz der Einstellungen
2, 4	Zugriff auf Sicherheits-router	• Fehlende oder manipulierte Radar Aufnahmen • Keine Verbindung zur Sensorik und Serverschrank möglich	2	2	4	• Installation an schwer zugänglichem Ort • Passwortschutz der Einstellungen • Deaktivierung der SIM-Karte
Manipulation						
2, 4	Kamera wird manipu-liert, sodass Daten auf eine SD-Karte gespei-chert werden	• Zusätzliche Speicherung der Daten auf eine SD-Karte ggf. durch unbefugte	5	1	5	• Nicht für Speicherung auf SD-Karte konfiguriert • Montage nach 4-Augen-Prinzip • Passwortschutz

2, 4	Radar-Modul wird manipuliert	• Fehlende oder manipulierte Radar Aufnahmen	2	2	4	• Installation an schwer zugänglichem Ort
2, 4	Switch wird manipuliert	• Fehlende oder manipulierte Radar Aufnahmen	2	2	4	• Installation an schwer zugänglichem Ort
2, 4	Raspberry Pi wird manipuliert	• Fehlende oder manipulierte Radar Aufnahmen	2	2	4	• Installation an schwer zugänglichem Ort • Passwortschutz der Einstellungen
2, 4	Sicherheitsrouter wird manipuliert	• Fehlende oder manipulierte Aufnahmen • Keine Verbindung zwischen Sensorik und Serverschrank möglich	2	2	4	• Installation an schwer zugänglichem Ort • Passwortschutz der Einstellungen
Diebstahl						
2, 4	Sensorknoten wird gestohlen	• Generierung von Daten nicht möglich	1	2	2	• Installation an schwer zugänglichem Ort • Regelmäßige Sichtprüfung • Keine Speicherung von Daten im Senor-Knoten
2, 4	Kamera wird gestohlen	• Lücke in der Aufzeichnung	1	2	2	• Installation an schwer zugänglichem Ort • Regelmäßige Sichtprüfung • Keine Speicherung von Daten im Sensorknoten
2, 4	Radar wird gestohlen	• Lücke in der Aufzeichnung	1	2	2	• Installation an schwer zugänglichem Ort • Regelmäßige Sichtprüfung
2, 4	Switch wird gestohlen	• Lücke in der Aufzeichnung	1	2	2	• Installation an schwer zugänglichem Ort • Regelmäßige Sichtprüfung
2, 4	Raspberry Pi wird gestohlen	• Lücke in der Aufzeichnung	1	2	2	• Installation an schwer zugänglichem Ort • Regelmäßige Sichtprüfung
2, 4	Sicherheitsrouter wird gestohlen	• Fehlende Aufnahmen • SIM-Karte entwendet	1	2	2	• Installation an schwer zugänglichem Ort • Regelmäßige Sichtprüfung • Deaktivierung der SIM-Karte
2, 4	SIM-Karte wird gestohlen	• Einwahl in das 5G-Netz möglich	2	2	4	• Deaktivierung der SIM-Karte • Authentifizierungs-Mechanismen (PPP

						oder PIN)
Abhören von Datenleitungen						
2, 4	Verbindung Sicherheitsrouter & Videokamera wird angezapft	• Kamera-Daten werden abgegriffen	5	1	5	• Kurzes und schwer zugängliches Kabel • Verschlüsselte Übertragung
2, 4	Verbindung Sicherheitsrouter & Switch wird angezapft	• Radar-Daten werden abgegriffen	2	1	2	• Kurzes und schwer zugängliches Kabel
2, 4	Verbindung Switch & Radar wird angezapft	• Radar-Daten werden abgegriffen	2	1	2	• Kurzes und schwer zugängliches Kabel
2, 4	Verbindung Switch & Raspberry Pi wird angezapft	• Auslöse Signale werden abgegriffen	2	1	2	• Kurzes und schwer zugängliches Kabel • Keine Übertragung von Persönlichen Daten
2, 4	Verbindung Sicherheitsrouter & 5G-Radio wird abgehört	• Übertragene Daten werden abgegriffen	4	1	4	• Verwendung von Protokollen für die sichere Übertragung von Daten (Verschlüsselung) • 3GPP Sicherheitsmechanismen
Verbindungsabbruch						
1-6	Verbindung Sicherheitsrouter & Videokamera wird unterbrochen	• Lücke in der Aufzeichnung • Keine Verbindung zur Kamera möglich	1	1	1	• Regelmäßige Kontrollen
1-6	Verbindung Sicherheitsrouter & Switch wird unterbrochen	• Lücke in der Aufzeichnung • Keine Verbindung zum Radar-Modul und Raspberry Pi möglich	1	1	1	• Regelmäßige Kontrollen
1-6	Verbindung Switch & Radar-Modul wird unterbrochen	• Lücke in der Aufzeichnung • Keine Verbindung zum Radar-Modul möglich	1	1	1	• Regelmäßige Kontrollen
1-6	Verbindung Switch &	• Lücke in der Aufzeichnung	1	1	1	• Regelmäßige Kontrollen

	Raspberry Pi wird unterbrochen	• Keine Verbindung zum Raspberry Pi möglich				
1-6	Verbindung Sicherheitsrouter & 5G-Radio wird unterbrochen/ gestört	• Speicherung der Daten nicht möglich • Keine Verbindungen zu der Sensorik möglich	1	2	2	• Regelmäßige Kontrollen
Zugriff aus dem Serverraum auf den Sensorknoten						
1-4	Zugriff auf Kamera	• Änderung der Konfiguration • Fehlende oder manipulierte Aufnahmen • Zugriff auf Videoaufnahme	5	1	5	• Zugangsbeschränkung • Passwortgeschützt
1-4	Zugriff auf Radar	• Änderung der Konfiguration • Fehlende oder manipulierte Aufnahmen	2	1	2	• Zugangsbeschränkung • Passwortgeschützt
1-4	Zugriff auf Sicherheitsrouter	• Änderung der Konfiguration • Fehlende oder manipulierte Aufnahmen	4	1	4	• Zugangsbeschränkung • Passwortgeschützt
1-4	Zugriff auf Switch	• Änderung der Konfiguration • Fehlende oder manipulierte Aufnahmen	4	1	4	• Zugangsbeschränkung • Passwortgeschützt
1-4	Zugriff auf Raspberry Pi	• Änderung der Konfiguration • Fehlende oder manipulierte Aufnahmen	4	1	4	• Zugangsbeschränkung • Passwortgeschützt
Weitere Quellen						
5, 6	Gefahren durch extreme Wetterbedingungen	• Beschädigung der Komponenten • Fehlende Aufnahmen	1	3	3	• Verwendung von Komponenten mit hohe Schutzklassen • Geeignet für den Einsatz im Außenbereich
5, 6	Brand durch defekte Komponenten	• Personenschaden • Schäden an dem Gebäude/ weiteren Komponenten	1	1	1	• Verwendung von geprüften/ zugelassenen Komponenten

10.3.2 Risiken: Serverschrank

Tabelle 9: Risiken im Serverschrank

RQ	Beschreibung	Folge	S	H	RKZ	Sicherheitsmaßnahmen
Physischer Zugriff und Manipulation						
2, 4	Zugriff auf den Serverschrank	• Beschädigungen/ Manipulation von Komponenten • Komponenten können gestohlen werden	5	1	5	• Installation in einem abschließbaren Serverschrank • Installation in einem abschließbaren Serverraum • Zugangsbeschränkung • Passwortgeschützt
2, 4	Zugriff auf den Switch	• Zugriff auf alle Komponenten im Netzwerk • Keine Kommunikation durch Trennen der Verbindungsleitungen	5	1	5	• VPN • Zugangsbeschränkung • Passwortgeschützt
2, 4	Zugriff auf den Server für die Datenverarbeitung	• Festplatte mit den Daten kann entnommen werden • Ausschalten des Servers	5	1	5	• Personenbezogene Daten sind verschlüsselt • Zugangsbeschränkung • Passwortgeschützt
2, 4	Zugriff auf den Server für das Netzwerk-Management-System	• Verbindungsabbrüche • Keine/ Lücken in der Aufnahme	3	1	3	• Zugangsbeschränkung • Passwortgeschützt
2, 4	Serverschrank wird manipuliert	• Beschädigungen/ Manipulation von Komponenten • Schließmechanismus wird zerstört & Zugang zu den Komponenten ohne Schlüssel möglich	3	1	3	• Zugangsbeschränkung
2, 4	Switch wird manipuliert	• Keine Verbindung zu den Komponenten möglich	5	1	5	• Zugangsbeschränkung

2, 4	Server für die Datenverarbeitung wird manipuliert	• Fehlende oder manipulierte Daten	3	1	3	• Daten auf der Festplatte sind verschlüsselt • Zugangsbeschränkung • Passwortgeschützt
2, 4	Server für das Netzwerk-Management-System wird manipuliert	• Keine 5G-Verbindung möglich	3	1	3	• Zugangsbeschränkung • Passwortgeschützt
Diebstahl						
2, 4	Server Datenverarbeitung wird gestohlen	• Keine weiteren Aufzeichnungen möglich • Gespeicherte Daten gestohlen	3	1	3	• Personenbezogene Daten sind verschlüsselt • Zugangsbeschränkung • Passwortgeschützt
2, 4	Festplatte auf dem Server wird gestohlen	• Gespeicherte Daten (Kamera, Radar) werden gestohlen	3	1	3	• Personenbezogene Daten sind verschlüsselt in Diebstahl gesichertem Server • Zugangsbeschränkung • Passwortgeschützt
2, 4	Server Netzwerk-Management wird gestohlen	• Keine 5G-Kommunikation möglich	3	1	3	• Zugangsbeschränkung
2, 4	Schlüssel für Übertragung wird gestohlen	• Entschlüsselung der übertragenen Daten möglich	5	1	5	• Zugangsbeschränkt
2, 4	Schlüssel für Kamera-Daten wird gestohlen	• Entschlüsselung der Kamera-Daten möglich	5	1	5	• Zugangsbeschränkt
Abhören von Datenleitungen						
2, 4	Verbindung 5G-Core & 5G-Radio wird angezapft	• Übertragung der Sensor-Daten werden abgegriffen	2	1	2	• Verschlüsselte Übertragung der Daten • Campusnetz Frequenzen • SIM-Karten Authentifizierung
2, 4	Verbindung Switch & Server Datenverarbei-	• Unverschlüsselte Daten gelangen in Hände Fremder	5	1	5	• Zugangsbeschränkung

	tung wird angezapft					
2, 4	Verbindung Switch & 5G-Core wird angezapft	• Fehlende Daten in der Aufzeichnung	3	1	3	• Zugangsbeschränkung
2, 4	Verbindung Switch & Server Netzwerk-Management wird angezapft	• Tunnel-Kommunikation möglich/ gestört • Monitoring Daten fehlerhaft	5	1	5	• Zugangsbeschränkung
Verbindungsabbruch						
1-6	Verbindung 5G-Core & 5G-Radio wird unterbrochen	• Keine Datenübertragung möglich	2	2	4	• Regelmäßige Kontrolle
1-6	Verbindung Switch & Server Datenverarbeitung wird unterbrochen	• Keine Datenübertragung möglich	2	2	4	• Regelmäßige Kontrolle
1-6	Verbindung Switch & 5G-Core wird unterbrochen	• Keine Datenübertragung möglich	2	2	4	• Regelmäßige Kontrolle
1-6	Verbindung Switch & Server Netzwerk-Management wird unterbrochen	• Keine Datenübertragung möglich	2	2	4	• Regelmäßige Kontrolle
Weitere Risiken						
5, 6	Brand durch defekte Komponenten	• Personenschaden • Schäden an dem Gebäude/ weiteren Komponenten	5	1	5	• Nutzung von Räumlichkeiten mit Brandmeldesysteme • Brandmeldesystem prüfen
5, 6	Brand durch Vandalismus	• Personenschaden	5	1	5	• Nutzung von Räumlichkeiten mit Brandmeldesysteme

		• Schäden an dem Gebäude/ weiteren Komponenten				

10.3.3 Risiken: Verarbeitung der Daten an der Hochschule

Tabelle 10: Risiken bei der Verarbeitung der Daten an der Hochschule

RQ	Beschreibung	Folge	S	H	RKZ	Sicherheitsmaßnahmen
Physischer Zugriff und Manipulation						
2, 4	Zugriff auf die Recheneinheit durch unbefugte	• Trainings- und Testdaten gelangen in Hände fremder • Zugang zur KI/ zu den Verarbeitungsprogrammen • Komponenten (Grafikkarte, CPU etc.) können manipuliert/ zerstört werden	5	2	10	• Recheneinheit nicht mit dem Internet verbunden während die Daten entschlüsselt sind • Zugangsbeschränkung • Passwortschutz • Festplattenverschlüsselung
2, 4	Radar-Daten werden manipuliert	• Training/ Evaluation der KI nicht möglich • Manipulierte Daten beeinflussen die Genauigkeit der KI	2	2	4	• Zugangsbeschränkung • Passwortschutz • Bei Radar-Daten keine Rückschlüsse zu Objekten/ Personen möglich
2, 4	Verschlüsselte Kamera-Daten werden manipuliert	• Training/ Evaluation der KI ohne Referenzsystem nicht möglich • Manipulierte Daten beeinflussen die Genauigkeit der KI	4	2	8	• Zugangsbeschränkung • Passwortschutz • Manipulation von verschlüsselten Daten bei der Entschlüsselung erkennbar
2, 4	Gespeicherte Labels werden manipuliert	• Training/ Evaluation der KI ohne Referenzsystem nicht möglich • Manipulierte Daten beeinflussen die Genauigkeit der KI	3	2	6	• Zugangsbeschränkung • Passwortschutz
2, 4	Die KI wird manipuliert	• KI liefert falsche Ergebnisse • Gefahrensituationen	4	2	8	• Zugangsbeschränkung • Passwortschutz

		werden nicht erkannt				
2, 4	Programm für die Anonymisierung wird manipuliert	• Daten werden nicht/ falsch anonymisiert • Nicht anonymisierte Daten sind auf der Festplatte und können auf ein externes Speichermedium gespeichert werden	5	2	10	• Zugangsbeschränkung • Passwortschutz • Stichproben Kontrolle der Anonymisierung
2, 4	Falsches Labeling von Daten	• Manipulierte Daten beeinflussen die Genauigkeit der KI	3	2	6	• Zugangsbeschränkung • Passwortschutz
Diebstahl						
2, 4	Recheneinheit für die Vorverarbeitung wird gestohlen	• Programme für die Vorverarbeitung der Daten und die KI gelangen in Hände unbefugter Personen • Test- und Trainingsdaten sind gestohlen • Kein Training/ Test der KI möglich	5	2	10	• Zugangsbeschränkung • Passwortschutz
2, 4	Hardware-Komponenten (z.B. Grafikkarte) aus der Recheneinheit werden gestohlen	• Nutzung der Recheneinheit beschränkt/ nicht möglich	5	2	10	• Zugangsbeschränkung
2, 4	Verschlüsselte Kamera-Daten werden gestohlen	• Training/ Evaluation der KI ohne Referenzsystem nicht möglich • Angreifer kann versuchen die Daten zu entschlüsseln	5	2	10	• Zugangsbeschränkung • Passwortschutz • Verschlüsselung
2, 4	Radar-Daten werden gestohlen	• Training/ Evaluation der KI ohne Messsystem nicht	4	2	8	• Zugangsbeschränkung • Passwortschutz

		möglich				
2, 4	Festplatte wird gestohlen	• Training/ Evaluation der KI nicht möglich • Vorverarbeitung der Daten nicht möglich	5	2	10	• Zugangsbeschränkung • Passwortschutz
2, 4	Labels werden gestohlen	• Training/ Evaluation der KI nicht möglich	4	2	8	• Zugangsbeschränkung • Passwortschutz
2, 4	Trainingsdaten werden gestohlen	• Training der KI nicht möglich	3	2	6	• Zugangsbeschränkung • Passwortschutz • Anonymisierte Trainingsdaten
2, 4	Testdaten werden gestohlen	• Evaluation der KI nicht möglich	3	2	6	• Zugangsbeschränkung • Passwortschutz • Anonymisierte Restdaten
2, 4	Trainierte KI wird gestohlen	• Erkennung von Gefahrensituationen nicht möglich	4	2	8	• Zugangsbeschränkung • Passwortschutz

11 Anhang

1. Einverständniserklärung Aufzeichnung ETM
2. Einverständniserklärung Bildrechte ETM
3. Hinweisschild
4. Versuchsfunklizenz Radar 77 GHz. Einsatzgebiet: IMST GmbH und bundesweit.
5. Funklizenzen für 5G befinden sich gerade in Antragsphase und werden nachgereicht, sobald diese von der Bundesnetzagentur genehmigt sind

Zur Dokumentation der Vereinbarungen über die Messkampagnen

6. Protokoll über Ortstreffen mit Vertretern der Stadt MG an der Radstation
7. Protokoll über Ortstreffen mit Verwaltung Gladbach-Center