Einsatzmöglichkeiten von Videokameras mit KI-getriebener Videoanalyse im Bereich der Sicherung

GRS - 748

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Einsatzmöglichkeiten von Videokameras mit KI-getriebener Videoanalyse im Bereich der Sicherung

Abschlussbericht

Alexander Rduch
Vitaliy Spektor
Sandra Zoller
Wenzel Brücher

Juli 2024

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4721R01620 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUV übereinstimmen.

GRS - 748
ISBN 978-3-910548-39-8

Deskriptoren
Künstliche Intelligenz, Sicherung, Videoanalyse

Kurzfassung

Im Rahmen des Vorhabens wurden die Einsatzmöglichkeiten von Videokamerasystemen mit KI-getriebener Videoanalyse zur Sicherung von Anlagen mit sehr hohem Schutzbedarf, insbesondere kerntechnischer Anlagen, untersucht. Ziel war es, technische und softwaretechnische Möglichkeiten dieser Systeme zu erfassen, ihre Zuverlässigkeit und Anwendbarkeit zu bewerten und mögliche Einschränkungen und Risiken zu identifizieren. Kerntechnische Anlagen erfordern hohen Schutz und nutzen bereits umfassend Videotechnik. Durch KI-getriebene Videoanalyse könnten bestehende Systeme verbessert und ergänzt werden. Die Eignung dieser Technologie für die spezifischen Anforderungen der Sicherung kerntechnischer Anlagen wurde untersucht.

Für das Vorhaben wurden die theoretischen Aspekte der KI-Technologie und der Sicherungstechnik untersucht, der aktuelle Stand der Technik ermittelte, eine Marktrecherche durchgeführt und darauf basierend die Anwendungs- und Einsatzmöglichkeiten der mit KI-getriebenen Videoanalyse ausgerüsteten Videokamerasysteme analysiert.

Technische Detektionssysteme sind in kerntechnischen Anlagen bereits etabliert. KI-getriebene Videoanalyse ist in diesen Anlagen allerdings noch nicht verbreitet. KI-gestützte Systeme haben insbesondere Potenzial in der Personenerkennung und der Verhaltensanalyse, können aber auch zur Überprüfung von Alarmmeldungen und zur allgemeinen Überwachung verwendet werden. Ausschlaggebend für den erfolgreichen Einsatz der Systeme sind eine niedrige Falschalarmrate bei hoher Detektionswahrscheinlichkeit. Die Untersuchung ergab, dass aktuelle Systeme ihre Zuverlässigkeit für den Einsatz in kerntechnischen Anlagen noch durch Praxistests unter Beweis stellen müssen. Die Ergebnisse des Vorhabens können zur Weiterentwicklung bestehender und neuer Sicherungskonzepte für kerntechnische Anlagen genutzt werden.

Inhaltsverzeichnis

1 Einleitung

Künstliche Intelligenz (KI) befasst sich als Teilgebiet der Informatik damit, wie ein Computer menschliche Intelligenz und Verhalten nachahmen kann. Dabei ist weder festgelegt was „intelligent“ bedeutet noch welche Technik zum Einsatz kommt. Die Definition von KI gestaltet sich daher als eine Herausforderung, die im Laufe der Zeit kontinuierlichen Veränderungen unterliegt. Jedoch scheint für KI ein grundlegendes Zusammentreffen von verschiedenen Elementen wichtig zu sein: Informatik und die Automatisierung von intelligentem Verhalten. Ein weiterer häufig erwähnter Aspekt sind Maschinen. Unter dem Begriff "Maschinen" fallen reale physische Apparate, Anlagen oder Roboter, aber auch virtuelle Softwareanwendungen. Letztere haben in den letzten Jahren an Bedeutung gewonnen.

Ein möglicher und vielversprechender Anwendungsbereich, der in den letzten Jahren große Fortschritte verzeichnen konnte, liegt in der KI-getriebenen Videoanalyse. Sie wird in vielen verschiedenen Fachkreisen als revolutionäre Zukunftstechnologie gehandelt und kann sich z. B. im Bereich der Videosicherheitstechnik zu einer elementaren Kernkomponente entwickeln. Sicherheitsdienstleister und Hersteller von Videokamerasystemen bieten inzwischen eine Vielzahl von Anwendungen und Lösungen an, die unter anderem auch auf die Sicherung von kritischen Infrastrukturen zugeschnitten sind. Die Möglichkeiten der intelligenten Videobildanalyse beinhalten beispielsweise die Detektion von Einbruch- oder Sabotageversuchen, die automatische Verfolgung von bewegten Objekten oder das Erkennen von unerwünschten Personen durch Messung der Verweildauer. Diese und weitere, durch die Hersteller beworbene Möglichkeiten, sorgen im Allgemeinen für eine hohe Erwartungshaltung, wobei die tatsächliche Anwendbarkeit, die Zuverlässigkeit und mögliche Risiken der KI-getriebenen Videoanalyse im Bereich der Sicherung von kerntechnischen Anlagen (KTA) bisher weitestgehend ungeklärt sind.

Kernkraftwerke gehörten zu den kritischen Infrastrukturen und auch heute weisen noch alle KTA einen hohen Schutzbedarf auf. Die bereits vorhandenen Sicherungskonzepte dieser Anlagen beinhalten üblicherweise bereits einen umfangreichen Einsatz von Videotechnik zur Identifizierung, Verifizierung und Überwachung. Durch Aufrüstung kann die KI-getriebene Videoanalyse auf vielfältige Weise implementiert werden und andere Sicherungskomponenten ergänzen oder gar ersetzen. Die Möglichkeit des Einbindens von intelligenter Videoanalyse in bereits bestehende oder neue Sicherungskonzepte macht es erforderlich, ihre grundsätzliche Eignung in Verbindung mit den Anforderungen an die Sicherung kerntechnischer Anlagen und Einrichtungen zu untersuchen. Das Ziel des

Vorhabens liegt somit in einer systematischen Erfassung der technischen und softwaretechnischen Möglichkeiten von verfügbaren und in der Entwicklung befindlichen Videosystemen mit KI-getriebener Videoanalyse, sowie in der anschließenden Auswertung dieser hinsichtlich ihrer Zuverlässigkeit und möglicher Einschränkungen in der Anwendbarkeit. Auf dieser Basis können das Potenzial und die möglichen Risiken dieser Technik im Zusammenhang mit ihrem Einsatz in KTA und Einrichtungen bewertet werden.

Im Rahmen des Eigenforschungsvorhabens wird eine umfangreiche Aufarbeitung des aktuellen Standes von Wissenschaft und Technik getätigt. Hierzu wird zunächst festgehalten, welche aktuellen und zukünftigen Lösungen auf dem Markt angeboten werden, wie diese Systeme funktionieren und wie sie in bereits bestehende Sicherheitskonzepte implementiert werden können. Anschließend können dann verschiedene Anwendungs- und Einsatzmöglichkeiten von KI-getriebener Videoanalyse für die Sicherung von kerntechnischen Anlagen und Einrichtungen identifiziert und bewertet werden.

Als technisch-wissenschaftliche Forschungs- und Sachverständigenorganisation ist die Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH gefordert, eine unabhängige Grundlage an fundierten Kenntnissen über aktuelle und zukünftige technologische Entwicklungen bereitzustellen, damit eine unabhängige und zuverlässige Bewertung gewährleistet werden kann. Das Eigenforschungsvorhaben zur KI-getriebenen Videoanalyse dient daher der Erarbeitung dieses Grundlagenwissens sowie einer ersten Analyse und Bewertung zukünftiger Einsatzmöglichkeiten.

2 Stand von Wissenschaft und Technik

2.1 Grundlagen der KI-Technologie

2.1.1 Ziele und Funktionsweise

Das übergeordnete Ziel der Entwicklung und des Ausbaus von KI ist stets die Schaffung von Systemen, die bestimmte Aufgaben ebenso gut oder sogar besser erledigen können als Menschen. Mit dem aktuellen Wissensstand ist es bislang nur gelungen, Maschinen jeweils eine separate Aufgabe zu lehren. Die Kombination mehrerer Aufgaben wird derzeitig erforscht. Gemäß /APT 19/ sind sowohl physische Maschinen als auch Softwareprogramme in der Lage folgende Aufgaben in Bezug auf die Einsatzmöglichkeiten von Videokameras zu erfüllen:

- Objekterkennung.
- Verhaltens und Emotionserkennung
- Sprach- und Geräuscherkennung
- Sprachübersetzung
- kreative Inhalts- und Bildgenerierung basierend aus vorhandenen Mustern, einschließlich menschlicher Gesichter
- Prognosen über zukünftige Ereignisse auf Grundlage historischer Daten

(Lern-) Algorithmus

In der Informatik ist ein Algorithmus eine genaue Berechnungsvorschrift zur Lösung einer Aufgabe. Ein Lernalgorithmus (oder selbstlernender Algorithmus) ist ein Algorithmus, der Beispieldaten (Lerndaten oder Trainingsdaten) erhält und ein Modell für die gesehenen Daten berechnet, das auf neue Beispieldaten angewendet werden kann /FRA 24/.

Machine Learning

Beim Machine Learning (z. Dt. Maschinelles Lernen) entwickeln Lernalgorithmen aus einer Vielzahl von Beispielen und vorhandenen Daten ein komplexes Modell, das „Wissen“ aus „Erfahrung“ generiert. Dieses Modell lässt sich dann auf neue, möglicherweise unbekannte Daten anwenden und ermöglicht es, Wissen automatisch zu generieren. Maschinelles Lernen eignet sich besonders für Prozesse, die zu komplex sind, um sie direkt zu beschreiben. Wenn jedoch ausreichend Beispieldaten wie Sensordaten, Bilder

oder Texte zum Anlernen verfügbar sind, lassen sich mit den gelernten Modellen neue Daten selbstständig einordnen, Vorhersagen treffen, Empfehlungen geben und Entscheidungen generieren, ohne dass zuvor Regeln oder Berechnungsvorschriften aufgestellt werden müssen /FRA 24/.

Deep Learning

Deep Learning, oder tiefes Lernen, vertieft das Prinzip des maschinellen Lernens, indem es künstliche neuronale Netze mit vielen Schichten nutzt. Diese Netze bestehen aus zahlreichen künstlichen Neuronen und können selbstständig die für das Lernen relevanten Merkmale generieren. Besonders bei der Verarbeitung von großen Datenmengen, sogenannter Big Data, zeigt Deep Learning seine Stärken. Deep Learning ist besonders verantwortlich für die Erfolge in der Sprach- und Text-, Bild- und Videoverarbeitung /FRA 24/.

2.1.2 Grenzen der KI-Technologie

Obwohl die Möglichkeiten der KI in vielen Anwendungsbereichen bereits beeindruckend sind, gibt es immer noch erhebliche Grenzen. Ein tiefgreifendes Verständnis dieser Grenzen ist entscheidend, um realistische Erwartungen an die Technologie zu setzen und ihre zukünftige Entwicklung effektiv zu nutzen. Eines der Hauptprobleme der heutigen KI-Systeme ist ihr begrenztes Kontextverständnis. Maschinen fehlt es an der menschlichen Fähigkeit, implizite Bedeutungen und Nuancen zu erfassen, die in der Kommunikation oder in komplexen Szenarien auftreten. Diese Einschränkung führt oft zu Fehlinterpretationen und Fehlentscheidungen, insbesondere in unstrukturierten Umgebungen /POO 17/. Dies ist insbesondere für die KI-basierte Videoanalyse von großer Wichtigkeit, da bisher immer von einem Menschen verifiziert wurde, was ein Videosystem erkannt hat, und Entscheidungen anhand dieser eigenen Verifizierung getroffen wurden. KI-Systeme sind in hohem Maße abhängig von der Qualität und Quantität der verfügbaren Daten. Unvollständige oder verzerrte Datensätze können zu verzerrten Ergebnissen führen, die nicht nur die Leistung der Systeme beeinträchtigen, sondern auch ethische Bedenken hervorrufen können /BAR 16/. Das Sammeln und Pflegen hochwertiger Datensätze ist daher eine wesentliche Herausforderung. Weiterhin sind viele KI-Modelle spezialisiert auf die Aufgaben, für die sie trainiert wurden, und es ergeben sich Probleme, das Gelernte auf neue, unähnliche Situationen zu übertragen. Diese mangelnde Generalisierungsfähigkeit begrenzt ihre Flexibilität und Anwendbarkeit in dynamischen und unbekannten Umgebungen /MAR 18/. Es ist eine enorme Rechenleistung

erforderlich, um fortgeschrittene KI-Algorithmen zu trainieren und zu betreiben. Dazu wird umfangreiche und teure Hardware benötigt, die viel Energie beansprucht. Dies stellt nicht nur finanzielle, sondern auch ökologische Herausforderungen dar, da der Energieverbrauch und die damit verbundenen CO2-Emissionen zunehmen /PAT 21/.

2.1.3 Ethik und Datenschutz

Mit dem Aufstieg der KI-Technologien rücken ethische Fragen und Datenschutzbedenken immer stärker in den Vordergrund. Die Fähigkeit von KI-Systemen, aus Daten zu lernen und Entscheidungen zu treffen, wirft wichtige Fragen über den Schutz der Privatsphäre und den verantwortungsvollen Umgang mit persönlichen Informationen auf. Zudem besteht die Gefahr, dass Voreingenommenheiten in den Trainingsdaten zu Diskriminierungen und falschen Darstellungen führen können, wenn Algorithmen diese unbewusst übernehmen und verstärken, da KI-Systeme ihre Entscheidungen basierend auf ihren Trainingsdaten treffen /DKE 20/. Entwickler müssen aktiv Strategien implementieren, um sicherstellen zu können, dass ihre KI-Modelle keine voreingenommenen bzw. diskriminierenden Vorurteile verstärken oder auf Grundlage von Voreingenommenheiten ihre Entscheidungen treffen. Dazu gehören die sorgfältige Auswahl und Überprüfung der verwendeten Trainingsdaten sowie die regelmäßige Überprüfung der Algorithmen auf Voreingenommenheit /LAN 24/. Transparenz ist ein zentraler Aspekt beim ethischen Einsatz von KI. Die Nutzer sollten verstehen können, wie und warum eine KI-Entscheidung getroffen wurde. Dies ist besonders wichtig in sensiblen Bereichen, wo Entscheidungen erhebliche Auswirkungen auf das Leben von Menschen haben können. Datenschutz spielt ebenfalls eine entscheidende Rolle. KI-Systeme benötigen oft große Mengen an Daten, um effektiv zu funktionieren. Der Schutz dieser Daten vor unbefugtem Zugriff und Missbrauch ist essenziell. Es müssen strenge Richtlinien eingehalten werden, die regeln, wie Daten gesammelt, gespeichert und verarbeitet werden, um die Privatsphäre von Individuen zu wahren. Außerdem muss die Verantwortlichkeit für Entscheidungen berücksichtigt werden /KIN 13/. Wenn eine KI-basierte Entscheidung negative Konsequenzen hat, muss klar sein, wer dafür verantwortlich ist - der Entwickler oder der Betreiber. Der verantwortungsvolle Umgang mit KI erfordert einen multidisziplinären Ansatz, der technische, rechtliche und ethische Expertise vereinigt.

2.1.4 EU-Regulierung zu Künstlicher Intelligenz

Das "AI Act" genannte KI-Gesetz verbietet den Einsatz von KI innerhalb der EU in bestimmten Fällen komplett. So ist eine Massenüberwachung und auch eine massenhafte Gesichtserkennung im öffentlichen Raum ausdrücklich verboten, sowohl dem Staat wie auch Unternehmen.

Dabei gibt es allerdings Ausnahmen: Polizei und andere Sicherheitsbehörden sollen eine solche Gesichtserkennung im öffentlichen Raum im Einzelfall nutzen dürfen, um ganz bestimmte Straftaten wie Menschenhandel oder Terrorismus zu verhindern oder zu verfolgen.

Diese Einschränkungen erfolgen gut begründet: In China kommt KI bereits zum Einsatz, um die Bevölkerung engmaschig zu überwachen. Gesichtserkennung identifiziert Personen, die sich in der Öffentlichkeit nicht regelkonform verhalten - und werden mit "Strafpunkten" im sogenannten "Social Scoring" bedacht. Eine solche Verwendung von KI soll durch das KI-Gesetz innerhalb der EU verhindert werden.

Aber auch KI-Systeme, die als besonders risikoreich gelten und in der kritischen Infrastruktur oder im Bildungs- und Gesundheitswesen zum Einsatz kommen, müssen künftig strenge Anforderungen erfüllen. KI-Systeme dürfen keine eigenständigen Entscheidungen fällen und müssen Transparenzpflichten erfüllen.

Die betroffenen Menschen müssen über den Einsatz "hochriskanter" KI-Systeme informiert werden. Außerdem muss gewährleistet bleiben, dass Menschen beim Einsatz KI-gestützter Verfahren die Kontrolle behalten.

KI-Systeme müssen außerdem so entwickelt sein, dass Risiken wie Fehler, Manipulationen oder Sicherheitslücken minimiert werden. Auch müssen durch KI erzeugte Inhalte gekennzeichnet werden. Dies bedeutet, dass beispielsweise mit KI generierte Texte, Bilder oder Videos gekennzeichnet werden müssen /WDR 24/.

Insbesondere verbieten die neuen Vorschriften bestimmte KI-Anwendungen, die die Rechte der Bürgerinnen und Bürger bedrohen. Dazu zählen unter anderem die biometrische Kategorisierung auf der Grundlage sensibler Merkmale und das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungskameras für Gesichtserkennungsdatenbanken. Ebenfalls verboten sind künftig Emotionserkennungs-

systeme am Arbeitsplatz und in Schulen sowie das Bewerten von sozialem Verhalten mit KI. Auch vorausschauende Polizeiarbeit, die einzig auf der Profilerstellung oder der Bewertung von Merkmalen einer Person beruht, und der Einsatz von KI, um das Verhalten von Menschen zu beeinflussen oder ihre Schwächen auszunutzen, ist nach den neuen Regeln nicht erlaubt.

Grundsätzlich ist die Nutzung von biometrischen Fernidentifizierungssystemen durch Strafverfolgungsbehörden verboten. Es gibt jedoch bestimmte ausführlich beschriebene und eng abgegrenzte Ausnahmefälle für Strafverfolgungsbehörden. Fernidentifizierung in Echtzeit ist nur dann erlaubt, wenn strenge Sicherheitsbestimmungen eingehalten werden – unter anderem gibt es zeitliche und räumliche Beschränkungen, und es muss vorab eine spezielle behördliche oder gerichtliche Genehmigung eingeholt werden. Entsprechende Systeme dürfen beispielsweise genutzt werden, um gezielt nach einer vermissten Person zu suchen oder einen Terroranschlag zu verhindern. Der Einsatz von KI-Systemen zur nachträglichen Fernidentifizierung gilt als hochriskant. Hierfür ist eine gerichtliche Genehmigung nötig, die mit einer Straftat in Verbindung stehen muss.

Auch für andere Hochrisiko-KI-Systeme sind bestimmte Verpflichtungen vorgesehen, denn sie können eine erhebliche Gefahr für Gesundheit, Sicherheit, Grundrechte, die Umwelt, Demokratie und den Rechtsstaat darstellen. Als hochriskant werden unter anderem KI-Systeme eingestuft, die in den Bereichen kritische Infrastruktur, allgemeine und berufliche Bildung oder Beschäftigung eingesetzt werden. Auch KI-Systeme, die für grundlegende private und öffentliche Dienstleistungen – etwa im Gesundheits- oder Bankwesen –, in bestimmten Bereichen der Strafverfolgung sowie im Zusammenhang mit Migration und Grenzmanagement, Justiz und demokratischen Prozessen (zum Beispiel zur Beeinflussung von Wahlen) genutzt werden, gelten als hochriskant. Solche Systeme müssen Risiken bewerten und verringern, Nutzungsprotokolle führen, transparent und genau sein und von Menschen beaufsichtigt werden. Die Bevölkerung hat künftig das Recht, Beschwerden über KI-Systeme einzureichen und Entscheidungen erklärt zu bekommen, die auf der Grundlage hochriskanter KI-Systeme getroffen wurden und ihre Rechte beeinträchtigen.

KI-Systeme mit allgemeinem Verwendungszweck und die Modelle, auf denen sie beruhen, müssen bestimmte Transparenzanforderungen erfüllen, darunter die Einhaltung des EU-Urheberrechts und die Veröffentlichung detaillierter Zusammenfassungen der für das Training verwendeten Inhalte. Für die leistungsfähigeren Modelle, die systemische Risiken bergen könnten, gelten künftig zusätzliche Anforderungen – etwa müssen

Modellbewertungen durchgeführt, systemische Risiken bewertet und gemindert und Vorfälle gemeldet werden.

Darüber hinaus müssen künstlich erzeugte oder bearbeitete Bilder bzw. Audio- und Videoinhalte (sogenannte Deepfakes) in Zukunft eindeutig als solche gekennzeichnet werden /EUP 24a/.

KI-Systeme stellen ein unannehmbares Risiko dar, wenn sie als Bedrohung für Menschen gelten. Diese KI-Systeme werden verboten. Sie umfassen:

- kognitive Verhaltensmanipulation von Personen oder bestimmten gefährdeten Gruppen, zum Beispiel sprachgesteuertes Spielzeug, das gefährliches Verhalten bei Kindern fördert
- soziales Scoring: Klassifizierung von Menschen auf der Grundlage von Verhalten, sozioökonomischem Status und persönlichen Merkmalen
- biometrische Identifizierung und Kategorisierung natürlicher Personen
- biometrischen Echtzeit-Fernidentifizierungssystemen, zum Beispiel Gesichtserkennung

Einige Ausnahmen können für Strafverfolgungszwecke zugelassen werden. Biometrische Echtzeit-Fernidentifizierungssysteme werden in einer begrenzten Anzahl schwerwiegender Fälle zulässig sein. Systeme zur nachträglichen biometrischen Fernidentifizierung, bei denen die Identifizierung erst mit erheblicher Verzögerung erfolgt, können zur Verfolgung schwerer Straftaten und nur nach gerichtlicher Genehmigung zulässig sein. /EUP 24b/

Das KI-Gesetz wurde am 21.05.2024 beschlossen, ist aber noch nicht in Kraft. Nach der Bestätigung der EU-Länder werden die neuen KI-Regeln erst einmal im Amtsblatt veröffentlicht und treten 20 Tage später in Kraft. Die EU-Verordnung ist dann – bis auf einige Ausnahmen – erst zwei Jahre nach ihrem Inkrafttreten uneingeschränkt anwendbar. Die Ausnahmen sind Verbote sogenannter verbotener Praktiken, die bereits sechs Monate nach Inkrafttreten gelten, Verhaltenskodizes (sie gelten neun Monate nach Inkrafttreten), Regeln für KI mit allgemeinem Verwendungszweck, einschließlich Governance, (zwölf Monate nach Inkrafttreten) und Verpflichtungen für Hochrisikosysteme (36 Monate nach Inkrafttreten) /WDR 24/, /EUP 24a/.

Die EU-Verordnung zur KI wird mit dem Inkrafttreten sofort in allen EU-Staaten gelten; es ist nicht erforderlich, dass jedes einzelne Land sie bis dahin in ihrer Gesetzgebung umsetzen muss /WDR 24/. Verordnungen sind Rechtsakte, die bei Inkrafttreten automatisch und in einheitlicher Weise in allen EU-Ländern gelten, ohne dass sie in einzelstaatliches Recht umgesetzt werden müssen. Sie sind in allen ihren Teilen verbindlich und gelten unmittelbar in allen Mitgliedsländern /EUP 24c/.

2.2 Detektion und Erkennung in der Videoüberwachung

Die Videodetektion ist ein essenzieller Bestandteil moderner Überwachungssysteme und hat eine breite Anwendung in Sicherheits- und Überwachungsbereichen gefunden.

Für eine brauchbare Überwachung wird eine dafür ausgelegte Technik vorausgesetzt. Videoüberwachung hat sich in den 1970er Jahren durch die Speicherung mittels Videokassettenrecordern etabliert. Durch den technischen Fortschritt ist die Qualität gestiegen und der Aufwand gesunken /KRU 11/.

Durch die Verbesserung bestimmter Parameter lässt sich das wahrgenommene Bild optimieren und damit die Aufnahmedistanz und Erkennbarkeit verbessern. Dazu gehören sowohl Verbesserungen der Hardware als auch der Software. Zuerst war der Fortschritt der Hardware im Fokus, in den letzten Jahren wird immer mehr Fokus auf Voranbringen und Optimierung von Software gelegt. Somit wurden fortschrittliche Bildverarbeitungstechniken entwickelt, die nicht nur die visuelle Qualität der Aufnahmen verbessern, sondern auch wertvolle Informationen aus dem Bildmaterial extrahieren können. Es gibt zahlreiche Methoden der Bildanalyse, die oft KI und maschinelles Lernen nutzen, die für die Identifizierung und Lokalisierung von Objekten, Ereignissen oder Veränderungen in Videodaten ausgelegt sind. Diese Fähigkeiten sind besonders wertvoll in komplexen Überwachungssituationen, wo sie helfen, schnelle und fundierte Entscheidungen zu treffen. Besonders im Bereich der Sicherung von KTA ist die Zuverlässigkeit und Präzision dieser Detektionsmethoden von größter Bedeutung. Hier müssen Überwachungssysteme in der Lage sein, potenzielle Sicherheitsrisiken frühzeitig zu erkennen und zu bewerten, um die Sicherheit der Anlagen und des Personals zu gewährleisten.

2.2.1 Grundlagen der Videotechnik

Die Videotechnik bildet das Fundament für die Effektivität von Videodetektionssystemen. Der Aufbau und der Stand der Technik ist entscheidend, um die Qualität und Leistung von Überwachungssystemen zu optimieren. Die grundlegenden Konzepte und Begriffe der Videotechnik, die für eine solide Videoüberwachung von Nöten sind, werden im Folgenden angegangen.

Kameras

Kameras sind zentral für jedes Videosystem, da sie die primäre Funktion der visuellen Datenerfassung erfüllen. Sie erfassen Bilder aus der Umgebung und wandeln diese in elektronische Signale um, die für Speicherung und Analyse weiterverarbeitet werden können. Moderne Überwachungssysteme nutzen vorrangig digitale Kameras, da sie im Vergleich zu ihren analogen Vorgängern eine deutlich höhere Bildqualität und verbesserte Verarbeitungsmöglichkeiten bieten. Die Vielfalt an verfügbaren Kameratypen ermöglicht eine breite Anwendungspalette. Digitale Kameras unterscheiden sich vor allem in der Sensorgröße, der Bildauflösung und der Fähigkeit, unter verschiedenen Lichtbedingungen zu operieren. Zum Beispiel nutzen viele Sicherheitssysteme Kameras mit hoher Empfindlichkeit in schwach beleuchteten Bedingungen oder Kameras mit Infrarotfunktion für die Nachtüberwachung.

Zudem spielt die Auswahl der Kamera eine entscheidende Rolle hinsichtlich der spezifischen Anforderungen des Einsatzortes. In stark frequentierten öffentlichen Räumen wie Flughäfen oder Einkaufszentren sind beispielsweise Pan-Tilt-Zoom (PTZ) Kameras beliebt, da sie es ermöglichen, den Blickwinkel zu verändern und auf bestimmte Ereignisse zu zoomen. Dies macht das Überwachungssystem flexibler und effektiver /AND 23a/.

Neben der physikalischen Leistungsfähigkeit sind auch die Netzwerkfähigkeiten der Kameras von Bedeutung. Internet Protocol (IP)-Kameras, die über ein Netzwerk verbunden sind, ermöglichen eine Remote-Überwachung und -steuerung, was sie ideal für moderne Sicherheitssysteme macht, die oft zentral gesteuert und überwacht werden.

Auswahl und Konfiguration von Kameras müssen aufeinander abgestimmt sein, um die Kameras in einem Überwachungssystem effizient einsetzen zu können. Es sollte auch sichergestellt werden, dass das Überwachungssystem sowohl kosteneffektiv als auch technisch auf dem neuesten Stand ist.

Auflösung

Die Auflösung bestimmt die Bildschärfe und Detailgenauigkeit in einem Video. Sie wird in Pixeln gemessen und gibt die Anzahl der Bildpunkte auf der horizontalen und vertikalen Achse eines Bildes an. Höhere Auflösungen wie High Definition (HD), Full HD und Ultra HD erfassen mehr Details als Standard Definition (SD) und bieten eine klarere Bildqualität, was besonders wichtig ist, wenn feine Unterschiede in den Aufnahmen identifiziert werden müssen, wie etwa Gesichter oder Nummernschilder /SMI 12/. Die Wahl der richtigen Auflösung ist daher entscheidend und muss die Anforderungen der spezifischen Überwachungsaufgabe sowie die Kapazitäten der Speicher- und Übertragungssysteme berücksichtigen /APT 18/.

Bildfrequenz

Die Bildfrequenz, oft in Frames per Second (FPS) (z. Dt. Bilder pro Sekunde) ausgedrückt, ist entscheidend für die Flüssigkeit der Videobildwiedergabe. Eine höhere Bildfrequenz ermöglicht es, Bewegungen nahtlos und ohne Ruckeln zu erfassen, was besonders bei der Überwachung von sich schnell bewegenden Objekten wichtig ist /MOH 18/. Dies ist besonders wertvoll in sicherheitskritischen Situationen und Anwendungen wie der Verkehrsüberwachung oder der Verbrechensprävention. Bis zu 60 FPS oder mehr werden bei typischen Überwachungskameras verwendet, um auch schnellste Bewegungen präzise festzuhalten, wo viele kurze Abläufe entscheidend sein können /HAN 12/.

Objektive

Die Auswahl des Objektivs hat einen erheblichen Einfluss auf die Bildqualität und die Funktionalität des Überwachungssystems. Objektive bestimmen den Blickwinkel und die Schärfentiefe des aufgenommenen Bildes. Weitwinkelobjektive erfassen ein breites Feld und sind ideal für die Überwachung großer Bereiche, während Teleobjektive sich für die Beobachtung entfernter Objekte eignen. Zoomobjektive bieten die Flexibilität, den Fokus zwischen nahen und fernen Objekten zu verändern, was sie besonders vielseitig macht.

Die richtige Objektivauswahl ermöglicht eine optimale Abdeckung des Überwachungsbereichs und gewährleistet, dass kritische Bereiche effektiv überwacht werden /SUR 23/, /AND 23b/.

Beleuchtung

Gute Beleuchtung ist essenziell für die Qualität von Videoaufnahmen. Sie beeinflusst entscheidend die Helligkeit und den Kontrast eines Videos. Normale Kameras decken bei guter Beleuchtung das sichtbare Farbspektrum ab. Kameras, die farbige Bilder von Personen und Objekten liefern, indem sie Licht in den Wellenlängen Rot, Grün und Blau (RGB) aufnehmen, werden RGB-Kameras genannt. Spezialkameras, wie Infrarot- oder Wärmebildkameras, bieten Möglichkeiten zur Überwachung unter schlechten Lichtbedingungen oder sogar in völliger Dunkelheit, indem sie auf Wärme- oder Infrarotsignaturen reagieren. Solche Technologien sind unerlässlich für die Überwachung in allen Lichtverhältnissen und können kritische Informationen liefern, die mit herkömmlichen Kameras nicht erfasst werden können /MON 21/.

Bildkompression

Da Videodateien, besonders groß sein können, ist eine effektive Kompression entscheidend, um die Übertragung und Speicherung zu optimieren. Standards wie H.264 und H.265 (High Efficiency Video Coding (HEVC)) reduzieren die Dateigröße erheblich, während sie gleichzeitig eine hohe Bildqualität bewahren. Diese Technologien sind fundamental, um die Effizienz in Netzwerken mit begrenzter Bandbreite zu gewährleisten und die Kosten für Speichermedien zu minimieren /OBY 22/.

Übertragung

Die Übertragung und Speicherung von Videodaten müssen effizient und sicher gestaltet werden. Moderne Überwachungssysteme nutzen häufig drahtlose Übertragungstechnologien oder Netzwerkkabel, um Daten zu einem zentralen Speichersystem oder in die Cloud zu übermitteln. Die Wahl der Übertragungsmethode hängt von der erforderlichen Reaktionsgeschwindigkeit und der Infrastruktur ab. Cloud-basierte Lösungen bieten Flexibilität und Zugänglichkeit, während lokale Speicherlösungen oft höhere Sicherheit und Kontrolle ermöglichen /FRI 20/, /DIN 16c/.

Speicherung

Die Speicherung von Videomaterial und Bildern, die von Videoüberwachungsanlagen (VÜA) aufgezeichnet werden, ist ein wichtiger zentraler Aspekt jeder Sicherheitsinfrastruktur. Sinn und Zweck der Überwachung ist es auch zu einem anderen Zeitpunkt einsehen zu können, wann etwas passiert ist. Die Einrichtung eines ausreichend großen Speichersystems ist mit hohen Kosten für die Anschaffung und die Instandhaltung der Infrastruktur sowie den benötigten Strom verbunden. Aus Platz- und Kostengründen soll daher der verfügbare Speicher effizient genutzt werden. Die zuvor erwähnten Punkte der Auflösung, Bildfrequenz und Bildkompression spielen dabei eine erhebliche Rolle für die Dateigröße des Video- und Bildmaterials. Höhere Auflösungen, Bildraten und Frequenzen erfordern mehr Speicherplatz als niedrigere Qualitäten. Dazu kommt das längere Aufzeichnungszeiten mehr Speicherplatz benötigen. Daher ist es wichtig, genügend Speicherkapazität zur Verfügung zu haben und diesen zu optimieren. Die Sicherung der Daten vor Verlust durch Korruption oder physischen Schaden ist durch den Einsatz redundanter Mittel zu gewährleisten.

Für ein effizientes und sparsames Speichersystem könnte anstelle von Speicherung der originalen „rohen“ Aufnahmen, durch die Verwendung von Kompressionsalgorithmen der benötigte Speicherplatz erheblich reduziert und die Bildqualität weitgehend bewahrt werden, während die Dateigröße verkleinert wird. Durch Speichermanagement-Strategien lassen sich durch regelmäßige Überprüfung und Verwaltung von gespeicherten Daten, veraltete oder unwichtige Aufnahmen löschen, um Speicherplatz freizugeben. Anstatt kontinuierlich aufzuzeichnen, wird das System so konfiguriert, dass es nur bei Erkennung von Bewegungen oder anderen definierten Ereignissen aufzeichnet.

Die Sicherung der Daten vor Korruption oder Schaden ist ein kritischer Aspekt der Datenspeicherung. Eine gängige Methode zur Erhöhung der Datensicherheit ist die Verwendung von „Redundant Array of Independent Disks“ (RAID). RAID ist eine Technologie, die mehrere physische Festplatten zu einer logischen Einheit kombiniert, um entweder die Leistung zu steigern oder die Datensicherheit zu erhöhen. RAID bietet verschiedene Konfigurationsmöglichkeiten, die als RAID-Level bezeichnet werden und unterschiedliche Ansätze zur Datenverteilung und Redundanz bieten. RAID wird häufig in Servern und Speichersystemen verwendet, um die Zuverlässigkeit und Verfügbarkeit von Daten zu erhöhen. Zu den gängigen Nutzungszwecken gehören die Sicherstellung der Verfügbarkeit und Integrität von Datenbanken, der Schutz von Dateiservern vor Datenverlust bei Festplattenausfällen und die Sicherung von Backup-Systemen, um eine

hohe Verfügbarkeit und schnelle Wiederherstellung zu gewährleisten. Durch die Implementierung von RAID können Unternehmen die Datensicherheit erhöhen, die Systemleistung verbessern und gleichzeitig sicherstellen, dass ihre Daten im Falle eines Festplattenausfalls geschützt und zugänglich bleiben /WES 24/, /SYN 24/.

Ein verbreiteter RAID-Level ist RAID 0, bei dem die Daten auf mehrere Festplatten verteilt (gestriped) werden, ohne Redundanz. Dies erhöht die Leistung, da mehrere Festplatten gleichzeitig gelesen und beschrieben werden können. Allerdings bietet RAID 0 keine Datensicherheit, da der Ausfall einer einzelnen Festplatte zum Verlust aller Daten führt.

Ein weiterer wichtiger RAID-Level ist RAID 1, bei dem die Daten gespiegelt (mirrored) werden. Hierbei werden identische Kopien der Daten auf zwei oder mehr Festplatten gespeichert. Dies bietet hohe Datensicherheit, da bei Ausfall einer Festplatte die Daten weiterhin verfügbar sind. RAID 1 ist ideal für Anwendungen, bei denen Datensicherheit wichtiger ist als Leistung.

RAID 5 kombiniert Datenstriping mit Paritätsinformationen, die über alle Festplatten verteilt werden. Diese Paritätsinformationen ermöglichen die Wiederherstellung der Daten im Falle des Ausfalls einer Festplatte. RAID 5 bietet eine gute Balance zwischen Leistung und Sicherheit, da es sowohl die Lese- als auch die Schreibgeschwindigkeit erhöht und gleichzeitig eine gewisse Redundanz bietet.

RAID 6 ähnelt RAID 5, bietet jedoch zusätzliche Parität, die es dem System ermöglicht, den Ausfall von zwei Festplatten zu verkraften. Dies erhöht die Datensicherheit weiter, ist jedoch mit einer etwas geringeren Schreibgeschwindigkeit verbunden.

Eine Kombination aus RAID 1 und RAID 0 ist RAID 10 (auch RAID 1+0 genannt). Diese Konfiguration bietet sowohl hohe Leistung als auch Datensicherheit, indem die Daten zuerst gespiegelt und dann über mehrere Festplatten verteilt werden. RAID 10 ist ideal für Anwendungen, die sowohl schnelle Datenzugriffszeiten als auch hohe Zuverlässigkeit erfordern.

2.2.2 Videoüberwachung mittels Künstlicher Intelligenz

In der Videoüberwachung werden Videoanalysen immer wichtiger. Hier geht es darum, einen Videostream zu analysieren. Dies kann in Echtzeit oder auch im Nachhinein sein. Klassischerweise wird dies heute noch von einem Menschen vorgenommen, beispielsweise durch einen Mitarbeiter in einer Überwachungszentrale. Wenn ein Mensch ein Video analysiert, dann kann er das nur mit normaler menschlicher Geschwindigkeit machen. Auch mehrere Videos parallel zu analysieren, erscheint schwierig. Im Falle einer Analyse der Videoüberwachung mit dutzenden, hunderten oder tausenden Überwachungskameras, ist man auf die Hilfe von Videoanalyse-Software angewiesen. In der Videoanalyse gibt es heute Software, die auf Videos die unterschiedlichsten Ereignisse erkennen kann. Um diese Ereignisse erkennen zu können, wird meistens KI-Technologie eingesetzt. Wie bereits in Kapitel 2.1.1 erwähnt, lassen sich mit dadurch vielfältige Einsatzmöglichkeiten mit der Methode von Deep Learning erschließen /APT 19/.

Die wichtigsten Deep Learning Anwendungen in der Videoüberwachung sind /APT 19/:

- Gesichter erkennen
- Menschen erkennen
- Fahrzeuge erkennen
- Feuer erkennen
- Verhalten von Personen und Fahrzeugen erkennen:
  - Herumlungern (Loitering)
  - Panik in einer Menschenmenge
  - Entreissdiebstähle erkennen
  - gestürzte Personen erkennen und Alarm auslösen, wenn diese nicht wieder aufstehen
  - ein Fahrzeug erkennen, das auf einem Bahnübergang stehen bleibt
  - Geisterfahrer
- Autonummern erkennen
- zurückgelassene Objekte erkennen (Flughafen, wildes Müllabladen)
- gestohlene Objekte erkennen (Museen, Ausstellung)
- Fahrzeuge (oder andere Objekte) zählen
- Geschwindigkeit von Fahrzeugen ermitteln
- Skimming bei Bankautomaten erkennen
- leere Gestelle oder freie Parkplätze finden

- Personen oder Fahrzeuge über verschiedene Überwachungskameras hinweg verfolgen
- spezifische Anwendungen, wie z. B. Sprayer erkennen

Alle diese Anwendungsfälle lassen sich durch eine der folgend erklärten Methoden realisieren:

Objekterkennung

Objekterkennung ist einer der grundlegenden Aspekte der Videodetektion. Sie ermöglicht die Identifikation spezifischer Objekte oder Muster innerhalb eines Videostreams, beispielsweise Personen, Fahrzeuge, Tiere oder Gegenstände. Moderne Detektionssysteme nutzen KI und maschinelles Lernen, um aus einer Vielzahl von Bilddaten zu lernen und charakteristische Merkmale dieser Objekte präzise zu erkennen. Die Objekterkennung kann mit fortschrittlichen Deep Learning-Methoden wie Convolutional Neural Networks (CNN) (z. Dt. Faltendes neuronales Netzwerk) durchgeführt werden, um spezifische Objekte im Videostrom zu identifizieren. Ein CNN ist darauf spezialisiert, Muster und Strukturen in visuellen Daten zu erkennen, indem verschiedene Filter auf das Eingangsbild angewandt werden, um Merkmale wie Kanten, Texturen und Formen zu extrahieren. Einmal erkannt, ermöglicht die Objektverfolgung das kontinuierliche Monitoring dieser Objekte auch unter variierenden Bedingungen wie wechselnden Lichtverhältnissen oder unterschiedlichen Perspektiven über mehrere Frames hinweg. Dies ist in Szenarien wie der Personen- oder Fahrzeugverfolgung unabdingbar /GOO 16/.

Bewegungserkennung

Bewegungserkennung konzentriert sich darauf, Veränderungen im Bild zu erfassen, die durch bewegende Objekte verursacht werden. Dies ist insbesondere in Überwachungsszenarien nützlich, wo die frühzeitige Detektion von Bewegungen entscheidend für die Sicherheit sein kann. Die Bewegungserkennung identifiziert Veränderungen zwischen aufeinanderfolgenden Bildern, die durch bewegende Objekte verursacht werden. Methoden wie optischer Fluss, Hintergrundsubtraktion und Frame-Differenzierung ermöglichen es, Bewegungen zuverlässig zu erfassen und entsprechende Alarme oder Aktionen auszulösen. Dies hilft, die Überwachungseffizienz zu steigern und die Reaktionszeit auf mögliche Sicherheitsvorfälle zu minimieren /OLA 20/.

Mustererkennung

In der Mustererkennung kommen Algorithmen zum Einsatz, die spezielle Muster oder Merkmale in den Videodaten erkennen. Machine-Learning-Modelle wie Support Vector Machines (SVM) oder auch CNN werden genutzt, um komplexe Muster wie Gesichter, Nummernschilder oder charakteristische Verhaltensweisen zu identifizieren. Die Grundidee hinter SVM ist es, eine optimale Trennlinie für Datenpunkte zu finden, die die Datenpunkte in verschiedene Klassen trennt. SVM wählen die Linie so, dass der Abstand zu den nächsten Punkten auf beiden Seiten (sogenannte "Support-Vektoren") maximal ist. Dies macht die Trennung robust gegenüber neuen Datenpunkten. Wenn die Daten nicht einfach durch eine Linie getrennt werden können, verwenden SVM mathematische Tricks (sogenannte Kernelfunktionen), um die Daten in einen höherdimensionalen Raum zu transformieren, wo sie trennbar sind. Durch diesen Vorgang lassen sich Datenpunkte derart klassifizieren, dass wiederkehrende Muster ähnliche Daten aufweisen und somit von anderen unterschieden werden können /COR 95/.

Region of Interest (ROI)

Die Definition von Region of Interest (z. Dt. Region des Interesses) ist ein strategischer Ansatz in der Videodetektion, der es ermöglicht, die Aufmerksamkeit auf bestimmte Bereiche eines Videos zu konzentrieren. Indem man eine ROI festlegt, kann das System effizienter arbeiten, da es weniger Bildmaterial zu verarbeiten hat und sich stattdessen auf die Gebiete konzentriert, in denen die Wahrscheinlichkeit für relevante Ereignisse am höchsten ist. Dies verbessert nicht nur die Detektionsgenauigkeit, sondern reduziert auch die Belastung der Verarbeitungskapazitäten und optimiert so den gesamten Überwachungsprozess. Durch ROI können auch private Einrichtungen, die an öffentliche Orte oder Einrichtungen angrenzen, datenkonformer überwacht werden, indem die angrenzenden öffentlichen Bereiche als nicht speicherbar oder verschlüsselt eingestellt werden können. Dies könnte auch eine Echtzeitüberwachung von öffentlichen Plätzen ermöglichen, ohne die Rechte von Privatpersonen zu verletzen, und dafür sorgen, dass nur bei Detektion einer im Voraus eingestellten Situation die auschlaggebende Szene im Bild abgespeichert wird /LIH 21/, /ZHA 19/.

Detektionsgenauigkeit und Fehlalarmrate

Die Detektionsgenauigkeit beschreibt, wie zuverlässig ein Videosystem relevante Ereignisse und Objekte identifizieren kann, während die Fehlalarmrate angibt, wie oft irrtümlich ein Alarm ausgelöst wird. Eine hohe Detektionsgenauigkeit bei gleichzeitig niedriger Fehlalarmrate ist das Ziel, um die Effektivität von Sicherheitssystemen zu maximieren. Diese beiden Parameter sind voneinander abhängig und es gibt keine hundertprozentige Detektionsrate ohne Fehler. Die Einstellungen sind abhängig von der zu überwachenden Größe des Perimeters und sind für jeden Standort individuell. Die Herausforderung liegt darin, die Systeme so zu kalibrieren, dass sie auch in komplexen oder unklaren Situationen präzise arbeiten, ohne dabei durch zu viele harmlose Aktivitäten ausgelöst zu werden. Bei einer Videodetektion sollte gemäß /CPN 20/ eine Detektionsrate von mindestens 95% erreicht werden. Bei konventioneller Überwachung sollten Fehlalarme gemäß /CPN 20/ auf fünf bis zehn Alarme pro Tag pro Kilometer des Perimeters begrenzt werden. Obwohl eine höhere Zahl von Fehlalarmen tolerierbar erscheinen mag, werden die für die Alarmbearbeitung zuständigen Mitarbeiter in der Praxis nicht in der Lage sein, mit einer höheren Arbeitsbelastung umzugehen und könnten nach Möglichkeiten suchen, das Alarmsystem zu manipulieren. Dies geschieht entweder durch Ignorieren der Alarme, sofortiges Stummschalten der Alarme ohne weitere Untersuchung oder Unterdrückung der Alarme, entweder durch Softwareeinstellungen oder durch physische und möglicherweise destruktive Mittel. Standorte mit einem kleineren Perimeter könnten in diesem Bereich weniger strenge Anforderungen haben, da die Anzahl der Sicherheitskräfte pro Kilometer potenziell höher sein könnte /CPN 20/. Fortgeschrittene KI-Software könnte diese Fehlerquoten weiter minimieren und so die Mitarbeiter entlasten indem häufig auftretende Fehlalarme durch Tiere und Natur „raustrainiert“ werden und nur menschliches Wirken oder sonstige unnatürliche Phänomene, die auf menschliches Handeln deuten müssen, wie getarntes Anschleichen, registriert werden.

Die Auswahl der richtigen Auswertetechniken und -strategien hängt von den spezifischen Anforderungen der Anwendung ab. Moderne Videodetektionssysteme kombinieren oft mehrere dieser Techniken, um die Genauigkeit und Zuverlässigkeit zu maximieren. Durch kontinuierliches Training und Anpassung der Konfiguration können sie auch an sich ändernde Szenarien angepasst werden.

2.3 Sicherungstechnische Anforderungen für die Videodetektion

2.3.1 VDE-Anwendungsregeln zu autonomen, kognitiven Systemen

Die Normenfamilie der VDE-AR-E 2842-61 enthält normative Vorgaben für die Entwicklung und Vertrauenswürdigkeit von autonom/kognitiven Systemen (A/K-Systeme). KI-Systeme sind eine Teilmenge der A/K-Systeme. Umgekehrt können kognitive Systeme Verfahren der KI wie maschinelles Lernen, neuronale Netze und Deep Learning verwenden /FRA 24/, /VDE 21/.

So wird in VDE-AR-E 2842-61 gefordert, dass beim Einsatz von KI technische Regeln implementiert werden müssen, die festlegen, wie KI-Komponenten in Produkte integriert werden können und die den vorgelagerten Entwurfsprozess beschreiben.

Die Sicherheit von KI-Systemen und -Lösungen muss zu jeder Zeit gewährleistet sein, sobald diese im Markt zur Anwendung kommen. Die Besonderheit von KI-Systemen ist deren Komplexität: Funktionen können nicht einfach (durch den Menschen) geprüft werden. Das System muss die Sicherheit selbst gewährleisten und beispielsweise Anforderungen der funktionalen Sicherheit inhärent erfüllen.

Einen besonderen Schwerpunkt legen die VDE-Anwendungsregeln auf die Entwurfsphase (development): Die Abgrenzung im Vergleich zu den klassischen Grenzen einer Maschine wird weiter gefasst, da auch die Interaktion mit dem Menschen und die Interaktion mit der Umgebung spezifiziert werden müssen.

Insbesondere für KI-Systeme sind Vertrauenswürdigkeitsanforderungen (trustworthiness) zu Aspekten wie physische Sicherheit (safety), Informationssicherheit (IT-security), Gebrauchstauglichkeit (usability) oder ethische und regulatorische Fragestellungen, von elementarer Bedeutung.

Diese VDE-Anwendungsregeln definieren verschiedene Entwicklungsschritte anhand des Lebenszyklus für KI-Systeme. Hierzu gehören der Entwurf auf Systemebene (u. a. Vertrauenswürdigkeitsattribute), Komponentenebene (u. a. Hardware, Software und KI-Blaupausen zur Anwendung einer KI-Methodik), Integration, Verifikation und Validierung sowie Abnahme und Freigabe. Das Modell umfasst darüber hinaus auch Vorgaben zur Marktbeobachtung und korrigierende sowie schützende Maßnahmen (eng. Corrective And Preventive Action – CAPA) /VDE 21/.

Zu den VDE-Anwendungsregeln der VDE-AR-E 2842-61 „Entwicklung und Vertrauenswürdigkeit von autonom/kognitiven Systemen“ gehören sechs Normen:

- Teil 61-1: Terminologie und Grundkonzepte (2021-07)
- Teil 61-2: Management (2021-06)
- Teil 61-3: Entwicklung auf Ebene der Solution (Gesamte Anwendung) (2021-06)
- Teil 61-4: Entwicklung auf Ebene des Systems (2023-10)
- Teil 61-5: Entwicklung auf Technologie-Ebene (2022-12)
- Teil 61-6: Nach Freigabe der Solution (2021-06)

2.3.2 Anforderungen an Videoüberwachungsanlagen für Sicherungsanwendungen – DIN EN 62676

Die Normenreihe DIN EN 62676 „Videoüberwachungsanlagen für Sicherungsanwendungen“ umfasst eine Vielzahl von einzelnen Normen. Für die Darstellung der grundlegenden Anforderungen an VÜA werden hier nur ausgewählte Teile dieser Normenreihe vorgestellt.

2.3.2.1 Teil 1-1: Systemanforderungen – Allgemeines (2014-11)

Das Ziel dieser IEC-Norm /DIN 14b/ besteht darin, Sicherheitsunternehmen, Hersteller, Systemintegratoren, Installateure, Fachberater, Besitzer, Bediener, Versicherungen und die Polizei zu unterstützen, das Überwachungssystem vollständig und genau festzulegen. Diese internationale Norm legt nicht die Art der Technologie für eine bestimmte Beobachtungsaufgabe fest. Die Norm legt die Mindestanforderungen fest und gibt Empfehlungen für VÜA in Sicherheitsanwendungen. Sie legt die minimalen Leistungs- und Funktionsanforderungen für VÜA fest, die zwischen Auftragnehmer, Polizei (wenn zutreffend) und Auftraggeber in Form der Leistungsbeschreibung vereinbart werden, enthält aber keine Anforderungen an Entwurf, Planung, Installation, Prüfung, Betrieb oder Instandhaltung. Diese Norm schließt die Installation von fernüberwachten, detektoraktivierten VÜA-Systemen aus. Sie gilt auch für VÜA, die Komponenten für die Detektion, die Auslösung, die Verbindung, die Steuerung, die Kommunikation und die Stromversorgung mit anderen Anwendungen gemeinsam nutzen. Der Betrieb von VÜA-Systemen darf von anderen Anwendungen nicht negativ beeinflusst werden. In dieser Norm werden nur die Mindestanforderungen behandelt. Für bestimmte Anwendungen gelten zusätzlich Anforderungen.

Die funktionale Beschreibung einer VÜA wird in der Norm festgelegt. Eine VÜA kann mit folgenden funktionalen Blöcken dargestellt werden, die wiederum aus weiteren Komponenten und Funktionen des Systems bestehen.

1. Videoumgebung
   - Bilderfassung
   - Verbindungen
   - Bildhandhabung
2. Systemverwaltung
   - Aktivitäten- und Datenverwaltung
   - Schnittstellen zu anderen Systemen
3. Systemsicherheit
   - Systemintegrität
   - Datenintegrität

Sicherungsgrade

VÜA werden in einer vor vier Sicherungsgrade eingestuft:

- Grad 1: geringes Risiko –
  kein Schutzbedarf und keine Zugriffbeschränkung
- Grad 2: geringes bis mittleres Risiko –
  einfacher Schutzbedarf, geringe Zugriffbeschränkung
- Grad 3: mittleres bis hohes Risiko –
  hoher Schutzbedarf, hohe Zugriffsbeschränkung
- Grad 4: hohes Risiko –
  sehr hoher Schutzbedarf, sehr hohe Zugriffsbeschränkung

KTA werden in der Regel immer dem höchsten Sicherheitsgrad zugeordnet. Es werden daher im Weiteren nur die Anforderungen des Grades 4, im Fall der Unterteilung von Anforderung in Sicherungsgraden, betrachtet.

Videoumgebung

Bilderfassung

Zweck der Bilderfassung ist, ein Abbild der realen Welt zu erzeugen und in einem Format bereitzustellen, das von der gesamten VÜA für sofortige und spätere Verarbeitung verwendet werden kann. Die innerhalb des Sicherungsbereiches erfassten Bilder müssen eine ausreichende Genauigkeit und Detailtreue besitzen, um dem Benutzer die Extraktion der in den Anforderungen an die Bildqualität festgelegten Informationen zu ermöglichen. Bei einer Analyse müssen alle bildüberlagernden Informationen, die vom System erzeugt werden, als Metadaten verarbeitet werden und dürfen das Bild selbst nicht beeinflussen. Nur eine Privatzonenmaskierung aus Datenschutzgründen darf das Bildfeld beeinflussen. Es muss eine Angabe des Herstellers in der Systemdokumentation über Art und Anzahl der Videoeingangskanäle, die maximale FPS pro Kanal, die Auflösung und Größe der gespeicherten Bilder, die Speicherkapazität in Stunden sowie die Zeit bis zum Wiederanlauf der Aufzeichnung nach einem Neustart des Systems geben.

Verbindungen

Verbindungen und Kommunikation beschreiben jegliche Übertragung von Daten innerhalb der Videoumgebung. Die Kommunikation umfasst alle Videos und Steuerdatensignale. Die Verbindungen umfassen die Übertagungsmedien (z.B. Kabel, Leitungen, drahtlose Übertragungen), die für die Kommunikationssignale verwendet werden. Alle Verbindungen sind so auszulegen, dass die Wahrscheinlichkeit, dass Signale oder Nachrichten verzögert, geändert, ersetzt werden oder verloren gehen auf ein Mindestmaß reduziert werden.

Die Verbindungen müssen wie folgt überwacht werden

- Überprüfung aller Verbindungen mind. alle. 10 Sekunden,
- max. 2 Wiederholungen, bevor eine Meldung ausgegeben wird,
- max. 30 Sekunden Verbindungsunterbrechung, bevor eine Meldung ausgegeben wird.

Bildhandhabung

Die Funktionen der Bildhandhabung umfassen Analyse, Speicherung und Darstellung eines Bildes oder einer Bildfolge. Die Analyse kann unterschiedliche Zwecke erfüllen: zum einen kann der Nachweis der Integrität des Systems erbracht werden, beispielsweise durch Bewertung der korrekten Kameraposition, oder die erfasste Szene wird

ausgewertet, beispielsweise bei einer automatischen Nummernschilderkennung, oder es wird ein Ereignis erkannt, welches einen Alarm auslösen soll, beispielsweise die Bewegung einer Person im überwachten Bereich oder auch Raucherkennung. Die Speicherung von Videobilddaten findet auf einem Speichermedium statt. Die Darstellung des Bildes sollte innerhalb einer Alarmempfangsstelle erfolgen, an die als ständig besetzte Stelle die Informationen über den Status eines Alarmsystems gemeldet werden. Arbeitet die Kamera selbst als Alarmgeber beispielsweise als Videobewegungsmelder und generiert einen Alarm als Reaktion auf eine Änderung des Inhalts einer bestimmten Bildfolge, kann die Darstellung des Bildes zur Feststellung des Alarmgrunds genutzt werden.

Die Aktivitätenverwaltung umfasst alle Aktivitäten, die durch Ereignisse oder Benutzeraktionen angestoßen werden. Das Ereignis kann eine Alarmprozedur in der VÜA auslösen. Der Auslöser kann das Ergebnis einer Bildverarbeitung (beispielsweise einer Videoinhaltsanalyse oder eines Videobewegungsmelders), ein Signal eines Sensors, oder Empfang von Daten von einem anderen System sein.

Sind Schnittstellen zu anderen Systemen (Sicherungssysteme, beispielsweise Einbruchmeldeanlage oder Zutrittskontrollsystem, und Sicherheitsverwaltungssysteme wie zum Beispiel Alarmempfangsstellen) vorhanden, müssen Befehls- und Datenformate für alle miteinander verbundenen Systeme im Einzelnen festgelegt werden. Gemeinsame Einrichtungen müssen alle Standards für die Anwendungen, in denen sie verwendet werden (z.B. Einbruchmeldeanlage, Zutrittskontrollsystem), erfüllen.

Zur Systemsicherheit gehören die System- und die Datenintegrität. Die Systemintegrität umfasst den Schutz jeder einzelnen Systemkomponente oder jedes Gerätes sowie den Schutz des Gesamtsystems. Die Wahrung der Integrität besteht aus der Erkennung von Ausfällen, dem Schutz vor Sabotage und dem Schutz vor unberechtigtem Zugriff auf das System. Hierzu werden folgende Anforderungen definiert:

- Erkennung von Ausfällen oder Störungen des Videosignals
- Erkennung von Störung oder Ausfall der Speicherung
- Erkennung des Ausfalls einer Systemkomponente innerhalb von 100 Sekunden
- Erkennung von Störung der Energieversorgung
- Erkennung von Sabotagen durch Verdrehen der Kameras
- Erkennung von Sabotagen durch Abdeckung oder Blendung der Kameras
- Erkennung des Ersetzens von Videodaten
- Erkennung einer signifikanten Reduzierung des Bildkontrasts

- optische und akustische Anzeigen des Ausfalls der Speicherung
- optische Anzeigen, Meldung und Protokollierung jeglicher Störungen
- optische Anzeigen, Meldung und Protokollierung jeglicher Sabotage
- mindestens Schutzart IP 44 gemäß /DIN 14a/ gegen Fremdkörper und Wasser

Die Datenintegrität besteht aus Datenidentifikation, Datenauthentifizierung und dem Schutz der Daten vor Manipulation. Die Methode zum Schutz der Datenvertraulichkeit muss in der Systembeschreibung der VÜA angegeben werden.

2.3.2.2 Teil 1-2: Systemanforderungen - Allgemeine Anforderungen an die Videoübertragung (2014-11)

In der Norm /DIN 14c/ werden die Mindestanforderungen an die Leistung der Videoübertragung für Sicherheitsanwendungen in IP-Netzwerken und die strengen Zeit-, Qualitäts- und Verfügbarkeitsanforderungen für Überwachungsanwendungen festgelegt. Es wird ein Leitfaden für die Netzwerkarchitektur im Hinblick darauf bereitgestellt, wie diese Anforderungen erfüllt werden können. Ebenso werden in dieser Norm die Anforderungen an die grundlegende IP-Vernetzung von Videoübertragungsgeräten für Sicherheitsanwendungen festgelegt. Wenn ein Videoübertragungsgerät in einer Sicherheitsanwendung eingesetzt werden muss, gelten bestimmte grundlegende Anforderungen: Zunächst muss ein grundlegendes Verständnis der IP-Vernetzung bereitgestellt werden, welches erfordert, dass das Gerät mit den wesentlichen Netzwerkprotokollen konform ist. Dabei könnte es sich um Anforderungen handeln, die für alle sicherheitstechnischen IP-Geräte über IP-Videoübertragungsgeräte hinaus gelten können. Aus diesem Grund werden zusätzlich die Anforderungen für die Übereinstimmung mit grundlegenden Streaming-Protokollen eingeführt, die in dieser Norm auf das Video-Streaming und die Steuerung des Videodatenstroms angewendet werden. Da Sicherheitsanwendungen eine hohe Verfügbarkeit und Zuverlässigkeit erfordern, müssen allgemeine Möglichkeiten der Übertragung des Videostatus und der Übertragung von Ereignissen für die Überprüfung des Zustands behandelt werden. Diese sind in den allgemeinen Anforderungen an die Ereignisverarbeitung und an die Verwaltung der Netzwerkgeräte festgelegt. Bei Sicherheitsanwendungen ist eine ordnungsgemäße Wartung und Installation für die Funktionsfähigkeit des Videoübertragungsgeräts unerlässlich.

2.3.2.3 Teil 2-1: Videoübertragungsprotokolle - Allgemeine Anforderungen (2014-11)

Die Internationale Elektrotechnische Normungsorganisation für Alarmanlagen und elektronische Sicherheitssysteme hat zusammen mit vielen staatlichen Organisationen, Prüfstellen und Geräteherstellern zur Sicherstellung der Interoperabilität zwischen den einzelnen Produkten einen gemeinsamen Rahmen für die Übertragung von Videoüberwachungssignalen festgelegt. Der Zweck des Übertragungssystems in einer VÜA besteht in der zuverlässigen Übertragung von Videosignalen zwischen verschiedenen Arten von VÜA die bisher als Closed Circut Television (CCTV)-Einrichtungen für Sicherungs- und Überwachungsaufgaben bezeichnet wurden. Die Norm DIN EN 62676-2-1 /DIN 14d/ hat das Ziel, eine IP-Netzwerkschnittstelle für Geräte in Überwachungsanwendungen einzuführen. Im vorliegenden Teil dieser Norm ist ein Netzwerkprotokoll für die volle Interoperabilität von Videogeräten festgelegt. DIN EN 62676-1-1 und DIN EN 62676-1-2 legen die für die Netzwerkleistung geltenden Mindeststandards und die allgemeine Einhaltung von bestehenden, eingeführten internationalen Netzwerkstandards fest. Aufbauend auf diesen Grundlagen werden Protokolle festgelegt, mit deren Hilfe sich die volle Interoperabilität von Videogeräten erreichen lässt. Bei Überwachungsanwendungen müssen IP-Videogeräte genormte Protokolle verwenden, um folgende Funktionen erfüllen zu können: Videostreaming, Steuerung von Datenströmen, Ereignisbehandlung, Discovery, Fähigkeitsbeschreibung, Geräteverwaltung, PTZ-Steuerung, Zusatzeinrichtungen und weitere Funktionen.

2.3.2.4 Teil 2-31: Videoübertragungsprotokolle - IP-Interoperabilität auf Basis von Webservices - Echtzeit-Streaming und Konfiguration (2021-05)

Das Ziel dieser Norm /DIN 21/ besteht darin, Netzwerkvideo-Implementierungen zu realisieren, die vollständig interoperabel sind, auch wenn sie aus Produkten unterschiedlicher Netzwerkvideo-Lieferanten bestehen. Diese Norm beschreibt das Netzwerkvideomodell sowie Netzwerkvideo-Schnittstellen, -Datentypen und -Datenaustauschmuster. Die Norm greift auf bestehende Normen bzw. Standards zurück, soweit diese maßgeblich sind und zur Verfügung stehen, und führt neue Spezifikationen nur dann ein, wenn dies notwendig ist, um die speziellen Anforderungen der Netzwerkvideoüberwachung zu unterstützen. Diese Norm legt Verfahren für Kommunikation zwischen Netzwerkvideo-Clients und Videosendegeräten fest. Diese neue Reihe von Spezifikationen ermöglicht die Einrichtung von Netzwerkvideosystemen mit Geräten und Empfängern unterschiedlicher Hersteller unter Verwendung gemeinsamer und genau festgelegter Schnittstellen.

Diese Schnittstellen decken Funktionen wie z. B. Medien- und Bildgebungskonfiguration, Echtzeit-Streaming von Audio- und Videodaten, Steuerung von Schwenken, Neigen und Zoomen und auch Analyse ab. Die in dieser Norm festgelegten Verwaltungs- und Steuerungsschnittstellen werden als Webservices beschrieben.

2.3.2.5 Teil 2-33: Cloud-Uplink und Fernzugriff von Managementsystemen (2023-08)

Dieser Teil der Normenreihe IEC 62676 /DIN 23/ legt eine Schnittstelle für Managementsysteme sowie einen Mechanismus für den operativen Fernzugriff auf physische Sicherheitsgeräte, zum Beispiel Videoüberwachungsgeräte und -systeme, fest. Im Bereich der Videoüberwachung liegt der Schwerpunkt der Anwendungsfälle auf dem Zugriff auf Live-Videos und dem Abrufen von Aufzeichnungen. Der in dieser Spezifikation festgelegte Mechanismus ist nicht auf Überwachungsanwendungen beschränkt, sondern eignet sich auch für den Fernzugriff auf Sicherheitssysteme und elektronische Zutrittskontrollanlagen. Die Norm enthält eine Einführung in den Fernzugriff von Managementsystemen. und legt auch fest, wie eine Verbindung zu Geräten hergestellt werden kann, die nicht direkt erreichbar sind, weil sie sich beispielsweise hinter einer Firewall befinden.

2.3.2.6 Teil 3: Analoge und digitale Videoschnittstellen (2016-01)

Die DIN EN 62676-3 /DIN 16a/ legt zusammen mit den physikalischen und elektrischen Schnittstellen- und Software-Spezifikationen von analogen und digitalen Videoschnittstellen in VÜA, sogenannte Video-Überwachungs- und Aufzeichnungsanlagen, fest. Bei analogen Videoschnittstellen ist ein analoges Videosignal wie Signalgemisch (Bild-Austast-Synchron-(BAS)-Signal) nach wie vor die am häufigsten verwendete Schnittstelle in Einrichtungen von VÜA. Obwohl die Fernsehfunkindustrie Signalgemisch-Standards (zum Beispiel NTSC, PAL oder SECAM) übernommen hat, wurden diese nicht konsistent für VÜA angewendet, und es ist daher wichtig, die Schnittstellen zu normen, um eine Interoperabilität zwischen VÜA sicherzustellen. Die Berichtigung DIN EN 62676-3 aus dem Jahr 2018 /DIN 18/ ergänzt die Information, dass es sich bei der DIN EN 62676-3:2016-01 /DIN 16a/ um den Ersatz für DIN EN 50132-5-3:2013-02 handelt.

2.3.2.7 Teil 4: Anwendungsregeln (2016-07)

Der Teil 4 der Normenreihe IEC 62676 /DIN 16b/ richtet sich an jene, die für die Aufstellung von Betriebsanforderungen, das Verfassen von Spezifikationen, die Auswahl, die Errichtung, die Inbetriebnahme, den Gebrauch und die Instandhaltung von VÜA verantwortlich sind. In ihrer einfachsten Form sind VÜA ein Mittel zur Bereitstellung von Bildern von Überwachungskameras und Videoaufzeichnungseinrichtungen zum Anschauen auf Anzeigen über ein Übertragungssystem. Es gibt keine theoretischen Grenzen für die Anzahl von Kameras und Anzeigen, die in einer VÜA verwendet werden dürfen. In der Praxis ergibt sich jedoch eine Begrenzung durch die wirksame Kombination von Steuerungs- und Anzeigeeinrichtungen sowie der Fähigkeit des Bedienpersonals zur Handhabung des Systems. Der erfolgreiche Betrieb einer VÜA erfordert die aktive Mitwirkung des Anwenders bei der Durchführung der empfohlenen Verfahren. Aufgrund des großen Bereiches von VÜA-Anwendungen, wie zum Beispiel Überwachung, Sicherung, öffentliche Sicherheit, Transport usw., sind im Teil 4 der Normenreihe IEC 62676 nur die Mindestanforderungen dargestellt.

Basierend auf dem Einbau- bzw. Einsatzort einer VÜA sollte der Standort besichtigt und seine Umgebungsfaktoren ermittelt werden. Daraufhin sollte ein Lageplan erstellt werden, der die Standortfaktoren berücksichtigt und basierend darauf die Positionen und Anzahl der Hauptkomponenten (Kameras, Detektoren, Leitungen etc.) bezeichnet. Die Planung, Errichtung und Inbetriebnahme der Anlage sollten vollständig dokumentiert werden.

Es sollte eine Betriebsanforderung erstellt werden, die erklärt, was der spätere Betreiber von den Funktionen der Anlage erwartet. In dieser soll der Zweck des Systems und der erforderliche Sicherungsgrad formuliert werden. Der zu überwachende Standort und die Bereiche innerhalb dieses Standorts, die durch die VÜA abgedeckt werden, sowie die zu erfassenden Aktivitäten müssen festgelegt werden. Weiterhin müssen in der Betriebsanforderung die Leistungsparameter festgelegt werden, die die System- bzw. Bildqualität und die Bildanalysefunktionalitäten regeln. Die Betriebsdauer, die Umgebungsbedingungen und die Belastbarkeit/Robustheit des Systems müssen ebenfalls berücksichtigt werden. Die Speicherungsparameter bezüglich Aufzeichnungsdauer, Aufbewahrungszeit und Verfahren zur Handhabung der Bild- und Videodaten müssen ebenfalls definiert sein. Die Arbeitsbelastung der Bedienpersonen muss ebenfalls ermittelt werden, wobei die Festlegung der Anzahl an Bildschirmanzeigen, Alarmereignissen und

Live-Kameras sowie deren Verwaltung durch das Bedienpersonal zu berücksichtigen sind.

Die VÜA muss so entworfen werden, dass diese das Bedienpersonal durch die automatisierte Verarbeitung unterstützen und ihnen die Konzentration auf wesentliche Aufgaben ermöglicht wird. Die VÜA sollte es dem Bedienpersonal erlauben, in jeder Situation unabhängig vom Grad der Automatisierung die manuelle Steuerung des Systems zu übernehmen. Die Systemantwortzeit zwischen der Erzeugung einer Alarmbedingung und ihrer Anzeige auf den Anzeigeeinrichtungen muss auf einem annehmbaren Minimum gehalten werden. Optimalerweise sollte die Systemantwortzeit nicht mehr als 0,2 Sekunden betragen. Bei verzögerter Systemantwort wird es schwierig, Maßnahmen zu koordinieren und einzuleiten. Bei mehr als 2 Sekunden kann keine Verantwortung für manuelle Maßnahmen durch das Bedienpersonal übernommen werden. Das betrifft sowohl die Systemantwortzeit nach einem Ereignis, welches einen Alarm auslöst, als auch die Antwortzeit des Systems auf eine vom Bedienpersonal manuell veranlasste Maßnahme. Überwachungskameras sollen grundsätzlich eine feste Position beobachten. Schwenkbare Kameras, die sich auch für Verfolgung von Objekten eignen, sollten voreingestellte Positionen und Alarmpositionen besitzen. Bei Objektverfolgung müssen die Eigenschaften der Kameras dies hinreichend ermöglichen. Die Beleuchtung muss bezüglich der Stärke, Ausrichtung und des Farbspektrums bewertet und geplant werden. Eine homogene Beleuchtung sollte vorhanden sein, und Lichtquellen sollten so platziert werden, dass Blendung der Kameras verhindert und Sichtstörungen durch Insekten vermieden werden.

Zum Schutz vor Sabotage sollten alle Kameras eine feste Ausgangsposition besitzen, und das Sichtfeld darf von außen nur schwer bzw. gar nicht verändert werden können. Das Verdrehen, Blenden und der Signalverlust müssen zur Alarmmeldung führen, die manuell quittiert werden muss. Zum Schutz des Systems vor Sabotage muss die verbaute Zentralentechnik der Anlage in einem sicheren Einbauort mit kontrolliertem Zutritt errichtet werden.

Die Übertragung kann entweder analog oder digital erfolgen. Jeder Videotyp kann in einen anderen konvertiert werden, wobei die Konvertierung aus Qualitätsgründen auf ein Minimum zu beschränken sind. Für Zugriffsmöglichkeiten über Fernbedienung, hohe Bildauflösung, digitale Aufzeichnung und Wiedergabe, Integration und Skalierbarkeit wird die Verwendung von IP-Videoübertragung empfohlen. Dazu sollte das IP-Netzwerk in der Lage sein, die ankommenden Datenströme zu bewältigen. Wichtige Parameter,

die geplant werden müssen, sind der Datenstromdurchsatz, die Latenzzeit der Anfragen, Verzögerungsschwankungen und Paketverlust (Daten/Qualitätsverlust bei Übertragung). Für Hochsicherheitsanwendungen müssen auch Redundanz und Sicherheit des Netzwerks berücksichtigt werden.

Für den Durchsatz der Daten sind die Video-Leistungskenngrößen der Bildkompression, Auflösung und Bildfrequenz zu beachten. Diese drei Kenngrößen sollten in den Betriebsanforderungen festgelegt sein und nicht auf Speicherplatzkapazitäten basieren. Die Auflösung muss für jede Kamera zweckbestimmt sein. Eine Identifizierung, z. B. bei Zutrittskontrollen, benötigt eine hohe Auflösung, während eine reine Erkennung auch mit geringerer Auflösung funktionieren kann. Die FPS sollte für jede Kamera festgelegt sein, abhängig vom zu beobachtenden Bereich, Aktivität oder externer Auslösung durch einen Melder oder Ähnliches. Anhand dieser Faktoren lässt sich die Gesamtspeicheranforderung grob abschätzen. Die Auslegung des Speichers sollte eine ausreichende Aufbewahrungszeit und einen Puffer beinhalten. Faktoren, die Einfluss auf die Speicherkapazität haben, sind die Bildgröße, die FPS, Aufzeichnungsdauer, Aufbewahrungszeit, Anzahl der aktiven Kameras und gegebenenfalls die Dauer eines Überschreibschutzes mancher Dateien.

Für kabelgebundene Übertragungswege eignen sich Koaxialkabel, verdrillte Doppelkabel oder Lichtwellenleiter. Die wesentlichen drahtlosen Übertragungswege sind analoge Radiofrequenzen, Wireless Fidelity (WiFi), mobiles WiMax, 2G, 3G, 4G und 5G. Bei der Planung des Übertragungsnetzwerks soll die zweckmäßige Benutzung und Netzwerksicherheit berücksichtigt werden. Aus diesen Gründen wird für Hochsicherheitsanwendungen drahtlose Übertragung nicht empfohlen. Bei Verwendung ist eine sichere Verschlüsselung der Übertragungen notwendig.

Anders als bei der Funkübertragung darf bei der Speicherung keine Verschlüsselung von Bildern und Videomaterial erfolgen. Ein Export der Daten muss möglich sein und dabei dürfen keine Informationen der Datei negativ beeinflusst werden. Im Falle eines proprietären Exportformats sollte eine Software zur Verfügung stehen, um diese Daten anzusehen und die Videos abspielen zu können.

Bei Anforderungen an eine Echtzeit-Ansicht, Kamerasteuerung, Systemmanagement oder andere intensive externe Einwirkungen sollte eine Leitzentrale eingerichtet werden. DIN EN 62672-1-1 definiert eine Alarmempfangszentrale als ständig besetzte Zentrale, an die Informationen über den Status eines oder mehrerer Alarmsysteme gemeldet

werden. In diesem Sinne ist eine Leitzentrale für VÜA auch eine Alarmempfangsstelle. Basierend auf der erwarteten Anzahl von Alarmen, der erforderlichen Antwortzeit auf die eintretenden Ereignisse und der Anzahl der zu überwachenden Kameras ist die Anzahl der Arbeitsplätze innerhalb der Leitzentrale festzulegen. Es sollten ausreichende Kapazitäten des Bedienpersonals vorhanden sein, um sicherzustellen, dass alle Ereignisse zweckmäßig und vereinbarungsgemäß behandelt werden können. Die Arbeitsplätze sollten ergonomisch gestaltet werden. Die Einrichtungen zur Speicherung und Aufbewahrung der Speichermedien sollten in geschützten Bereichen installiert werden. Die VÜA und ihre Komponenten sollten an eine Notstromversorgung angeschlossen sein, um einem Stromausfall vorzubeugen.

2.3.2.8 Teil 5: Leistungsbeschreibung und Bildqualitätseigenschaften für Kameras (2019-05)

Teil 5 von IEC 62676-5 /DIN 19/ legt Empfehlungen und Anforderungen für Darstellungs- und Messverfahren von Leistungswerten für die Beschreibung in Handbüchern, Prospekten und Spezifikationen von Videoüberwachungskameras fest. Diese Norm besteht aus zwei Teilen. Der erste Teil enthält Anforderungen für die Beschreibung der Spezifikationsmerkmale von Videoüberwachungskameras. Der zweite Teil enthält Anforderungen für Messverfahren der Spezifikationsmerkmale von Videoüberwachungskameras.

2.3.3 Richtlinien für Videoüberwachungsanlagen

2.3.3.1 VdS 2364 –Systemanforderungen an Videoüberwachungsanlagen der Kat I

Die Richtlinien /VDS 06/ enthalten Mindestanforderungen an ein Videoüberwachungssystem (VÜS) der Kategorie I. Das VÜS besteht aus aufeinander abgestimmten Systemkomponenten. Diese werden in eigenständigen VÜA eingesetzt, die weder Einfluss auf eine Gefahrenmeldeanlage nehmen noch Teil davon sind. Die Kameras der VÜA sind daher entweder durchgehend aktiv oder werden erst nach Alarmauslösung zur Alarmverifikation aufgeschaltet. Sie selbst sind nicht tätig als Alarmauslöser.

Die Klassifikation eines VÜS erfolgt nach den drei Klassen A, B und C. Klasse A ist für kleine Risiken, Klasse B für mittlere Risiken und Klasse C für eine Überwachung mit hohen Risiken ausgelegt. Für den Einsatz in einer KTA ist nach dieser Richtlinie ein VÜS der Klasse C zu wählen, wobei diese Richtlinie nur Mindestanforderungen für den Einsatz von VÜS in KTA enthält. Nach dieser VdS-Richtlinie müssen die eingesetzten VÜS folgende Funktionen aufweisen bzw. Anforderungen erfüllen:

Funktionalität

- mindestens tägliche Überprüfung aller Systemkomponenten auf Störungen
- Erkennung und Meldung von Speicher-, Systemkomponenten-, Energieversorgungs- und Übertragungsstörungen
- optische und akustische Anzeigen bei Störungen, die erst nach deren Bearbeitung zurückgestellt werden können

Sabotage

- Erkennung von Sabotage durch Verdrehen, Abdeckung oder Blendung der Kameras
- optische Anzeigen, Meldung und Protokollierung von Sabotageereignissen

Zugriffsberechtigung

- für den Zugang zur Bildzentrale ist eine 2-Faktor-Authentisierung mit zwei technischen Maßnahmen notwendig (z.B. Passwort und Fingerabdruck)
- Bedienung der VÜA, Einsehen und Bearbeitung der Bilddaten erst nach Identifizierung möglich

Protokolldaten

- Erfassung und Speicherung von mindestens 10.000 Ereignissen
- optische und akustische Meldung vor Erreichen der Speichergrenze
- Protokollierung von Auslösungen, Benutzeraktionen, Konfigurationsänderungen und Benutzeridentifikationen

Energieversorgung

- Primärversorgung über das öffentliche Stromnetz
- Sekundärversorgung über eine redundante Notstromanlage, die in einem separaten Stromkreis ohne Fremdverbraucher betrieben wird
- datenverlustfreies Umschalten auf Notstrom bei Stromausfall und automatischer Selbstanlauf nach Wiederherstellung der Energieversorgung

Dokumentation

- Bereitstellung technischer Daten des Systems und seiner Komponenten.
- Liste der Systemkomponenten, Bedienungs-, Installations- und Montageanleitungen sowie Anschaltanleitungen.
- Lieferzusage herstellerfremder Systemkomponenten, falls vorhanden.

Diese Anforderungen gewährleisten, dass Videoüberwachungssysteme zuverlässig und sicher betrieben werden können, insbesondere in Bereichen mit hohen Sicherheitsanforderungen.

2.3.3.2 VdS 2365 – Anforderungen an Videoüberwachungssysteme der Kat II

Die Richtlinie VdS 2365 /VDS 08/ enthält Allgemeine Anforderungen (Teil 1), Systemanforderungen (Teil 2) und -prüfmethoden sowie Anforderungen und Prüfmethoden für Anlageteile für die Bilderzeugung (Teil 3), Bildaufzeichnung (Teil 4) und Bildübertragung (Teil 5) für Videoüberwachungssysteme der Kategorie II. Als System der Kategorie II werden Videoüberwachungssysteme bezeichnet, die ein Ereignis detektieren und aufgrund dessen eine Meldung in einer Gefahrenmeldeanlage erzeugen können. Damit übt die Videoüberwachungsanlage Funktionen einer Gefahrenmeldeanlage aus und unterliegt zusätzlich den Anforderungen für Gefahrmeldeanlagen (z.B. Einbruchmeldeanlagen).

Für eine Verwendung in KTA sind die Anforderungen der VdS-Richtlinie 2364 /VDS 06/ zu erfüllen, ergänzt um die hier wiedergegebene Richtlinie VdS 2365 /VDS 08/ für VÜS mit eigener Detektionsfähigkeit.

Die VdS 2365 definiert Mindestanforderungen für VÜS, die in sicherheitsrelevanten Anwendungen eingesetzt werden. Diese Systeme müssen robust gegen Umwelteinflüsse der Klasse IV sein, was den Einsatz im Freien und unter extremen Witterungsbedingungen ermöglicht. Dazu gehören Temperaturen von bis zu 70°C über 21 Tage, feuchte Hitze bis 40°C über denselben Zeitraum, sowie Kälte von -25°C für 16 Stunden. Zudem müssen sie korrosionsbeständig sein.

In Bezug auf die Funktionalität müssen VÜS der Klasse C folgende Anforderungen erfüllen: Sie müssen regelmäßig alle Systemkomponenten auf Störungen überprüfen und Ausfälle sofort anzeigen. Bei Speicherausfällen muss eine redundante Einheit innerhalb von 3 Minuten einsatzbereit sein, ohne Datenverlust. Bei automatischer Bildauswertung müssen Alarme wie Brand, Überfall oder Sabotage automatisch erkannt und angezeigt werden, wobei Störmeldungen erst nach Bearbeitung durch den Nutzer zurückgestellt werden können.

Zum Schutz vor Sabotage müssen alle Anlagenteile physisch geschützt sein, der Zugang zu sicherheitsrelevanten Bereichen darf nur autorisiertem Personal gestattet sein. Jegliche Manipulation an den Kameras wie Verdrehen oder Abdecken muss erkannt und protokolliert werden.

Der Zugriff auf die Bildzentrale erfordert eine 2-Faktor-Authentisierung, beispielsweise mit Passwort und Fingerabdruck. Anzeigen und Meldungen bei Störungen oder Sabotageversuchen müssen sofort erfolgen und bis zur manuellen Behebung bestehen bleiben.

Die Energieversorgung muss unterbrechungsfrei sichergestellt sein, mit sofortiger Meldung bei Störungen. Die Bildübertragungskomponenten und Kameras müssen ebenfalls auf Störungen überwacht werden, mit sofortiger Alarmierung bei Ausfällen oder längerer Unterbrechung der Übertragungswege.

Speichervorgaben umfassen die Aufzeichnung von mindestens 15 Sekunden vor und nach einem Alarmereignis, mit einer Speicherung von über 10.000 Ereignissen. Auch nach einem Stromausfall muss die Speicherung der Ereignisdaten für mindestens 8 Tage gewährleistet sein.

2.3.3.3 VdS 2366 – Anforderungen an Videoüberwachungsanlagen, Planung und Eigenbau

Die VdS-Richtlinie VdS 2366 /VDS 17/ enthält Mindestanforderungen an Planung, Einbau, Betrieb und Instandhaltung von VÜA. Bei VÜA mit direktem Anschluss an die Polizei gelten zusätzlich die entsprechenden Bestimmungen der bundeseinheitlichen Richtlinie für Überfall-/Einbruchmeldeanlagen bzw. Anlagen für Notfälle/Gefahren mit Anschluss an die Polizei (ÜEA-Richtlinie) /POL 21/.

Die Schutzziele für die VÜA sind individuell festzulegen. Für KTA sind dies insbesondere die Erkennung bzw. das Erschweren von Einbruch, Diebstahl und Sabotage. Aber ein Überfall auf die Sicherungszentrale oder ein Brandanschlag auf Sicherheits- oder Sicherungseinrichtungen muss berücksichtigt werden. Basierend auf diesen Schutzzielen sind Aufgaben für die VÜA zu definieren.

Für die Sicherung in KTA können einer VÜA zumindest folgende Aufgaben zugeordnet werden:

- Alarmverifikation für Einbruch, Diebstahl, Überfall, Sabotage, Brand
- Freigeländeüberwachung
- Täterlokalisierung
- Zutrittskontrolle

Zur Erfüllung der Schutzziele ist die richtige Auflösung und die damit hervorgehende Erkennbarkeit relevant. Die Auflösung bei der Darstellung des Zielobjektes ist hierbei in Abbildungsklassen unterteilt.

Tab. 2.1 Übersicht der Abbildungsgrößen nach VdS und DIN Einteilung. /VDS 17/

VdS-Klasse	Bezeichnung nach DIN EN 62676-4	1 Pixel entspricht in natura	Pixel pro Meter
-	Überwachung	80 mm	12,5 Pixel
Klasse 1	Detektieren (Erkennen)	40 mm	25 Pixel
-	Beobachten	16 mm	62,5 Pixel
Klasse 2	Erkennen	8 mm	125
-	Identifizieren	4 mm	250
Klasse 3	Überprüfen	1 mm	1000

Nach /VDS 17/ werden die Abbildungsklassen der VÜA in drei Abbildungsgrößen unterteilt:

- Klasse 1 – Detektieren (Erfassen)
- Klasse 2 – Erkennen
- Klasse 3 – Überprüfen

Weiterhin sind die Leistungsmerkmale der VÜA in Klassen A, B und C unterteilt welche die Funktions-, Bedienungs-, und Sabotagesicherheit kennzeichnet. Diese wurden bereits in Kapitel. 2.3.3.1 dargestellt. Diese VdS-Klassen sind bei Planung und Einbau zu beachten.

Für die Anwendung in der Sicherung ist mindestens Klasse C1 zu erfüllen. Diese kann zur Überwachung der äußeren Peripherie genutzt werden, um unautorisierte Personen zu detektieren (z.B. an Grundstücksgrenze bzw. Anlagenumzäunung). Klasse C2 kann zur Geländeüberwachung genutzt werden. Klasse C3 kann zur Zutrittskontrolle verwendet werden.

Zum Überwachen und Abwickeln der Alarme sollte eine Bildempfangszentrale (BEZ) ein Bestandteil der VÜA sein. Eine BEZ ist eine ständig besetzte Stelle, die mit eingewiesenem Personal besetzt ist, Meldungen annimmt und notwendige Maßnahmen veranlasst. In KTA der wird eine solche ständig besetzte Stelle häufig auch Sicherungszentrale genannt.

Es ist nicht zwingend notwendig eine BEZ zu haben, da der Bildempfang da auch durch eine nicht vor Ort befindliche, beauftragte Stelle erfolgen kann. In KTA sind BEZ grundsätzlich Teil der VÜA, die Bearbeitung der Meldungen und der empfangenen Bilder erfolgt in einer dafür eingerichteten ständig besetzten Stelle. Wird eine externe Stelle als BEZ eingesetzt, sollte diese über eine Alarmempfangsstelle aufgeschaltet werden. Bildzentralen (BZ) und Bildübertragungseinrichtungen (BÜE) müssen in geschlossenen Sicherungsbereichen eingerichtet sein, dürfen nur für Berechtigte zugänglich und für Dritte nicht sichtbar sein.

Gemäß /VdS 17/ gelten für eine BEZ, die mehr als fünf Kameras bedient folgende Anforderungen:

- die Anzahl der aktiv angezeigten Kamerabilder sollte eine sinnvolle Bearbeitung ermöglichen
- erkennbare Anzeige, welcher Melder einer GMA ausgelöst hat
- nachvollziehbare Reihenfolge bei Auslösung mehrerer Melder
- Bildspeicherung nach Auslösung, mit Vor- und Nachlauf sowie Recherchemöglichkeit

Nach Einbau und Übergabe der VÜA sollte die Anlage über einen definierten Zeitraum im Probebetrieb laufen, um eventuelle Probleme diagnostizieren zu können. Folgend sollten regelmäßige Inspektionen, für KTA mindestens einmal jährlich, durchgeführt werden, um die Anlage auf bestimmungsgemäße Funktion zu überprüfen. Dabei sollte insbesondere die Verfügbarkeit der Anlage und die Bilder der Kameras, die Bildqualität, Referenzbilder und die Energieversorgung überprüft werden. Wartungen sollten im Zusammenhang mit den Inspektionen durchgeführt werden. Dabei erfolgt eine Prüfung auf Verschmutzung und der Ersatz von Anlagenteilen mit begrenzter Lebensdauer wie Batterien oder Lampen.

In regelmäßigen Abständen, jedoch höchstens alle 10 Jahre, muss die VÜA auf die Einhaltung der jeweils gültigen Richtlinien überprüft werden und bei Bedarf auf den Stand der Technik aufgerüstet werden. Alle Instandhaltungsarbeiten, Änderungen, Erweiterungen, Störungen und Betriebsereignisse sind in einem Betriebsbuch zu führen und mindestens fünf Jahre nach der letzten Eintragung aufzubewahren. Alle für die Instandhaltung nötigen Unterlagen sind unter Verschluss zu halten.

2.3.4 Generisches Anforderungsprofil für die Anwendung in kerntechnischen Anlagen und Einrichtungen

Um ein Verwenden in KTA und Einrichtungen zu ermöglichen, müssen die VÜS sowie die verwendete Software bestimmten Sicherheitsanforderungen gerecht werden, die für den kerntechnischen Bereich maßgebend sind. Dazu gehören technische Normen, Leitfäden und Richtlinien. Einige dieser Anforderungen sind als „Verschlusssache - Nur für den Dienstgebraucht (VS-NfD)“ eingestuft und der Öffentlichkeit nicht zugänglich. Die relevanten Inhalte dieser verschlossenen Dokumente werden hier deshalb nur oberflächlich und verallgemeinert zusammengefast wiedergegeben. In diesen Richtlinien und Leitfäden werden Anforderungen genannt, die unabdingbar umgesetzt werden müssen. Die Art der Umsetzung ist den Betreibern selbst überlassen, aber es ist von Vorteil, wenn viele dieser Anforderungen durch wenige Maßnahmen abgedeckt werden. Eine Maßnahme ist die Videoüberwachung durch Kamerasysteme, welche bisher nur auf konventionelle Art ohne Hilfe von KI oder KI-gestützten Analysemethoden eingesetzt wird. Es könnte jedoch in Zukunft von Vorteil sein, wenn durch eine KI-basierte Videoüberwachung und Analyse, noch mehr Anforderungen abgedeckt werden würden, da sich dadurch ein effizienterer Workflow einstellen ließe und gleichzeitig das zuständige Personal entlastet werden könnte.

VÜA sind ein wesentlicher Bestandteil des Sicherungskonzepts für KTA, welches die Maßnahmen beschreibt, die den erforderlichen Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD), im Wesentlichen den Schutz genehmigungspflichtiger Tätigkeiten gegen Terrorismus, gewährleisten. Dieser Schutz ist eine Genehmigungsvoraussetzung für alle nach dem Atomgesetz (AtG) zu genehmigenden kerntechnischen Einrichtungen und Tätigkeiten, wie beispielsweise Kernkraftwerke, Kernkraftwerke im Rückbau, Forschungsreaktoren, Zwischenlager, Einrichtungen des Kernbrennstoffkreislaufs, wie Anreichungsanlagen, aber auch für Kernbrennstofftransporte /BMU 24/.

Die für den Schutz gegen SEWD erforderlichen Maßnahmen sind in SEWD-Richtlinien niedergelegt. Zu den im Geheimhaltungsgrad VS-NfD eingestuften Anforderungen gehören die folgenden SEWD-Richtlinien:

- Richtlinie für den Schutz von Kernkraftwerken mit Leichtwasserreaktoren gegen Störmaßnahmen oder sonstige Einwirkungen Dritter /BMU 95/
- Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und der Beförderung von sonstigen radioaktiven Stoffen (SEWD-Richtlinie sonstige radioaktive Stoffe – SisoraSt) /BMU 22a/
- Sicherungsmaßnahmen für den Schutz von kerntechnischen Anlagen mit Kernmaterial der Kategorie III /BMU 93/
- Richtlinie zur Sicherung von Zwischenlagern gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) - SEWD-Richtlinie Zwischenlager /BMU 12/
- Richtlinie zur Sicherung sonstiger radioaktiver Stoffe in kerntechnischen Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie sonstige radioaktive Stoffe in Kerntechnischen Anlagen – SisoraK) /BMU 22b/
- Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) /BMU 13/
- Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III) /BMU 20/

Die folgenden SEWD-Richtlinien sind nicht als VS-NfD eingestuft. Die Inhalte können offen diskutiert werden und werden hier auch für die Zusammenstellung eines generisches Anforderungsprofil herangezogen:

- Richtlinie über Maßnahmen für den Schutz von Anlagen des Kernbrennstoffkreislaufs und sonstigen kerntechnischen Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen zugangsberechtigter Einzelpersonen /BMU 91/
- Merkpostenliste für die Sicherung sonstiger radioaktiver Stoffe und kleiner Mengen Kernbrennstoff gegen Entwendung aus Anlagen und Einrichtungen /BMU 03/
- Leitfaden Deterministische Sicherungsanalyse (DSA) /BMU 97/

Die deterministische Sicherungsanalyse ist Teil der periodischen Sicherheitsüberprüfung. Es ist ihr Ziel, ausgehend von einer aktuellen Gesamtdarstellung und vollständigen Behandlung der Anlagensicherung (Sicherungsstatus) zu prüfen, ob die vom Betreiber der Anlagen vorgesehenen Sicherungsmaßnahmen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter geeignet sind, die Erfüllung der Schutzziele der Anlagensicherung zu ermöglichen. Der Nachweis orientiert sich an 19 definierten Sicherungsfunktionen. Diese dienen als Grundlage für die Definition von Anforderungen an VÜA.

Grundsätzlich wird von den Systemen der Anlagensicherung erwartet, dass die normale Funktionsfähigkeit gewährleistet ist und jede Störung vom System erkannt und gemeldet werden kann. Bei Ausfall der normalen Stromversorgung muss es möglich sein die Anlage ohne Unterbrechung weiter betreiben zu können. Eine Detektion, das Erkennen und eine Alarmverifikation sollen auch bei ungünstigen Sichtbedingungen möglich sein. Eine Kontrolle der Personen und des Fahrzeugverkehrs soll gewährleistet sein. Vor Zutritt zu den Sicherungsbereichen einer KTA muss Identitätskontrolle stattfinden. Dabei muss eine Dokumentation der Ereignisse stattfinden.

Die daraus abzuleitenden generischen Anforderungen an eine VÜA mit KI-gestützter Videoanalyse für den Einsatz zur Sicherung von KTA sind in der folgenden Tabelle zusammengestellt.

Tab. 2.2 Anforderungen an Videoüberwachungssysteme von KTA

Nr.	Anforderung an VÜA	Teilanforderung für KI-Videoanalyse	Randbedingungen
1	Beobachtung des Vorfeldes auf Vorbereitungshandlungen.	Erkennen und Verfolgen von Personen, Fahrzeugen, Handlungen, Bewegungen etc. im Vorfeld.	unbeleuchtet freie Sicht Witterung ≥ 10 m Tiefe
2	Erkennen, lokalisieren und verifizieren von Eindringversuchen an der Äußeren Umschließung.	Annähern (Personen, Fahrzeuge etc.) erkennen und Eindringen verfolgen.	beleuchtet freie Sicht Witterung Entfernung > 10 m
3	Erkennen von Nötigungslagen an der Äußeren Umschließung.	Handlungen erkennen.	beleuchtet ggf. eingeschränkte Sicht geringe Entfernungen (wenige Meter)
4	Gesamtüberblick über den Sicherungszustand der Anlage und Unterstützung des Einsatzes der Polizei.	Personen und Fahrzeuge etc. lokalisieren und verfolgen.	überwiegend beleuchtet teilweise eingeschränkte Sicht durch Gebäude, Objekte etc. Witterung große Entfernungen
5	Maßnahmen gegen Einwirkung oder Unterstützung einer zugangsberechtigten Einzelperson.	Handlungen wie Manipulations- und Sabotageversuche erkennen.	beleuchtet unübersichtlich unterschiedlich große Entfernungen
6	Integritätsüberwachung von Barrieren.	Handlungen und Veränderungen erkennen und lokalisieren.	unterschiedlich beleuchtet überwiegend freie Sicht Witterung große Flächen / Entfernungen
7	Verifizieren von zugangsberechtigten Personen an der Zutrittskontrolle.	Verifikation und Zugangserteilung für zugangsberechtigtes Personal.	hohe Anforderung an Manipulations- und Sabotageschutz
8	Kontrolle und Dokumentation der Zufahrt von Fahrzeugen an den Verkehrsdurchgängen	Identifikation der Fahrzeuge, Dokumentation der Zufahrten	beleuchtet freie Sicht Witterung geringe Entfernung

3 Marktrecherche

3.1 Überblick

Die Ziele der durchgeführten Marktrecherche waren einen Überblick über die Angebote und Dienstleistungen der zahlreichen Hersteller von KI-Videoanalyse zu gewinnen und zu ermitteln, wie diese in verschiedenen Szenarien und Bedingungen gegeneinander abschneiden. Die möglichen Anwendungen der KI-basierten Videoanalyse müssen basierend auf ihrem Einsatzzweck verschiedene Anforderungen erfüllen. Im Falle eines Einsatzes zur Überwachung einer KTA und deren Gebäude wurden die Hauptanforderungen eines Überwachungssystems den gezielten Aufgaben bzw. Teilanforderungen der KI-Videoanalyse unter bestimmten Bedingungen gegenübergestellt und sind in Tab. 2.2 zu finden.

3.2 GIT System Test Videoanalytik - Videoanalyse-Vergleich namhafter Hersteller im Jahr 2022

In der Zeitschrift GITSicherheit vom Jahr 2022 /GIT 22/ wurde ein Systemtest von auf dem Markt erhältlichen Videoanalysesystem-Lösungen mehrerer Hersteller durchgeführt und die Ergebnisse veröffentlicht. Dazu gehörten einzelne Videosysteme mit einem Gerät und Kombi-Geräte mit mehreren Kameras bzw. Sensoren. Dieser Test ist der erste bekannte veröffentlichte Test dieser Art und präsentiert die aktuellen Testergebnisse zu Videoanalysesystemen. Der Testbericht wird hier zusammengefasst wiedergegeben.

Es wurden die verschiedenen Videoanalysen mehrere Hersteller im freien Gelände in 85 verschiedenen Szenarien getestet. Hierbei hatten die Tester die Freiheit, die Art der Videoanalyse nach ihren Bedürfnissen auszuwählen. Die gesamte technische Ausstattung wurde in einem Container untergebracht, wo die Resultate dokumentiert und protokolliert wurden. Die Durchführung der Tests erfolgte systematisch und orientierte sich nach bekannten Prüfanforderungen und Richtlinien, wurden jedoch zu einem gewissen Teil abgeändert und modifiziert, wenn die Prüfer sich einigen waren, dass manche Prüfpunkte und Durchführung veraltet und nicht mehr zeitgemäß sind.

Die Szenarien wurden gleichmäßig auf verschiedene Entfernungsbereiche aufgeteilt, und jedes Szenario wurde dreimal durchgeführt. Das Testgelände erstreckte sich über einen Bereich ab 20 Metern bis 120 Metern, der in drei Entfernungsbereiche unterteilt

wurde: Alpha (30-50 Meter), Bravo (51-80 Meter) und Charlie (81-120 Meter). Als erfolgreich galt ein Durchgang, wenn bei mindestens zwei von drei Durchgängen eine Alarmmeldung generiert wurde. Da die Tests im Freien durchgeführt wurden, hatten die unterschiedlichen Witterungsbedingungen und Temperaturen während der Testperiode zwar einen Einfluss auf die Ergebnisse der Tests, jedoch war dieser Einfluss für alle Systeme gleich.

Die Testblöcke umfassten die Untersuchung von Fehlalarmen, die Performance bei Tag und Nacht, verschiedene Bewegungsarten, Bekleidungsarten sowie die Reaktion auf Sabotage oder Manipulation. Die Performance der Alarmqualität wurde über die Fehlalarmrate (NAR/FAR) geprüft. Dabei ist zu unterscheiden zwischen Nuisance Alarm Rate (NAR, z. Dt. lästige Alarmrate) und False Alarm Rate (FAR, z. Dt. Falschalarmrate). Mit NAR sind gültige Alarme gemeint, die keine echte Bedrohungen bzw. Gefahren melden, ausgelöst durch z.B. Natureinflüsse. FAR bezeichnet Alarme, welche durch das System selbst verursacht werden, also durch Fehler ohne Mitwirken der Kamerasensorik. Für die Prüfung der Fehlalarme wurden eingehende Alarme außerhalb des Testzeitraums über mehrere Wochen beobachtet und die Zahl der Alarme in der ruhenden Phase ausgewertet. Es wurden auch Täuschungsversuche der Videosysteme mit spezieller Pyrotechnik durchgeführt, es wurden jedoch keine physischen Angriffe oder Hacking Angriffe durchgeführt. Die Konzeption der Testszenarien wurde anhand verschiedener Täterklassen entwickelt, von Spontantätern und Kleinkriminellen bis hin zu organisiertem Verbrechen sowie terroristischen Gruppierungen. Dieser umfassende Testansatz ermöglichte eine umfassende Beurteilung der KI-basierten Videoanalysen in realen Umgebungen und unter verschiedenen Bedingungen.

Die getesteten Kamerasysteme für Tag und Nacht sind in Tab. 3.1, die thermaltechnikbasierten Kameras sind in Tab. 3.2 aufgelistet. In Tab. 3.3 sind die verschiedenen Versionen der Videoanalysesoftware der Hersteller gelistet. Insgesamt wurden bei dem Systemtest 11 Systeme getestet.

Tab. 3.1 Vergleich der Thermalkameras nach /GIT 22/

	Kamera-hersteller	Kameratyp/ Modellname	Auflösung	Objektivdaten (Brennweite [mm] /Blende [f])	Überdeckungs-Bereich ÜB am Testfeld 1
Avigilon	Avigilon	640S-H4A-THC-BO24	640 x 512	18 mm	23 m
Axis	Axis	Q1952-E 35mm	640 x 480	hfov: 35 mm / 17° F1.14	21m – 120m
Bosch RGB	-	-	-	-	-
Bosch Thermal	Bosch	NHT-8001-F35VF	VGA	35 mm, Viewing angle: 17,6° x 13,2° (H x V);	18 m
Dahua	Dahua	Thermalkamera/ TPC-BF5601	640 x 512	25 mm	18 m
Dallmeier	Dallmeier Electronic	Panomera S8 190 / 30 DN / C Ultraline	190 Mpe; >160 Px/m	kein Wechselobjektiv	FOV (h) 30° FOV (v) 52°
Hikvision RGB	-	-	-	-	-
Hikvision Thermal	Hikvision	DS-2TD2138-25/QY	384 x 288	25 mm / F1.1	-
Honeywell	Dahua	DH-TPC-BF5421	400 x 300	13 mm	-
Milestone/ Saimos/ Vivotek	Vivotek	TB9330-E	384 x 256	19 mm	20 m
Mobotix	Mobotix	M73TB-640R150/8DN150	4K	18 mm f/1.8	5,53 m

Tab. 3.2 Vergleich der Tag/Nacht Kameras nach /GIT 22/

	Kameraherstel-ler	Kameratyp/ Modellname	Auflösung [MP]	Objektiv-hersteller	Objektivdaten (Brennweite [mm] /Blende [f])	Überdeckungs-bereich ÜB am Testfeld 1
Avigilon	Avigilon	5.0C-H5A-BO2-IR	5 MP	-	9 – 22 mm; F/1.6	21 m
Axis	Axis	Q1656-BLE	4 MP	Axis / Computar	iCS – 9 – 50 mm / F1.5	20 – 120 m
Bosch RGB	Bosch	NDE-8513-RXT	4 MP	Bosch	Optical (12 - 40 mm), F-stop 2.3 – 2.3	15 m
Bosch Thermal	-	-	-	-	-	-
Dahua	Dahua	Speed-dome/DHSD6AL445XA-HNR	4 MP	-	3,95 ~ 177,7 mm	27 m
Dallmeier	-	-	-	-	-	-
Hikvision RGB	Hikvision	iDS-2CD7A86G0-IZHS(Y)	8 MP	-	8-32 mm / F1.7 - F1.73	20 m
Hikvision Ther-mal	-	-	-	-	-	-
Honeywell	Honeywell	HC60WB5R2	5 MP	-	2.7 – 13.5 mm	20 m
Milestone/ Saimos/ Vivotek	Vivotek	Vivotek PTZ SD9368-EHL Box IP9165-HT-V2	2 MP / 2 MP	-	4,25-170 mm / kameraintegrier-tes Objektiv	5 m
Mobotix	-	-	-	-	-	-

Tab. 3.3 Vergleich der Videoanalyse nach /GIT 22/

	Hersteller der Videoanalyse	Versionsname	Versionsnummer	Detektionsart [Objekt/Pixelorientiert]	Analyse erfolgt (Server/Edge*)
Avigilon	Avigilon	Avigilon VAL5 (Integriert in Kamera)	VAL5	Objektorientiert für Personen und Fahrzeuge-	Edge
Axis	Axis	Perimeter Defender auf der Q1952	3.1.0	Personen- und Objektorientiert	Edge
Bosch RGB	Bosch	Intelligent Video Analytics on the edge	8.10	Objektorientiert	Edge
Bosch Thermal	Bosch	Intelligent Video Analytics on the edge	8.10	Objektorientiert	Edge
Dahua	Dahua	Embedded Firmware	2.6.01.05.53098	Objektorientiert	Edge
Dallmeier	Dallmeier Electronic	IPS 10.000 MKII	10.7.2. SpB	Personen- und Objektorientiert	Edge und Server
Hikvision RGB	Hikvision	VCA Analyse integriert in Firmware	-	-	Edge
Hikvision Thermal	Hiksion	VCA Analyse integriert in Firmware	-	-	Edge
Honeywell	Honeywell	Intrusion Trace	X0.5	Personenorientiert	Server
Milestone/ Saimos/Vivotek	Saimos	Saimos Video Analytics Standard	2022 R1 /1.4.1	Deep Learning Objektklassifizierung, Bewegungs-/Pixelanalyse	Server
Mobotix	Mobotix AG	Activity Sensor	2.1	Personenorientiert	Edge

*Edge: Echtzeitauswertungen von Daten unmittelbar an der Datenquelle.

Testergebnisse

Eine detaillierte Beurteilung der NAR/FAR-Bewertung im Sinne einer Beurteilung von NAR/FAR pro 100 m Zaun und Tag ist nicht erfolgt, stattdessen eine qualitative Einschätzung durch die Sachverständigen, basierend auf den Aufzeichnungen in der Ruhephase.

Die Beurteilung der Bedienung der Systeme und ihre Nutzerfreundlichkeit basierten jeweils auf einer Rückmeldung durch Errichter und Sachverständigen zur Installation und Parametrierung der jeweiligen Systeme. Die erfahrenen Techniker gaben Rückmeldungen zur Installation, Montage, Konfiguration und Parametrierung der Systeme. Die für die jeweiligen Systeme zuständigen Mitarbeiter im Leitstand wurden bezüglich Bedienbarkeit, Einarbeitung, Übersichtlichkeit und Auswertbarkeit der Alarme befragt.

Insgesamt wurden an drei Testtagen bei Tag und Nacht 85 Szenarien durchgeführt. Die meisten davon liefen mit drei Durchgängen ab. In der Auswertung sind die Szenarien in verschiedenen Blöcken zusammengefasst:

- Tag/Nacht-Bewertung:
  Perfomance der Systeme in Abhängigkeit der Lichteinflüsse
- Bewertung der Entfernungsbereiche:
  Einfluss der unterschiedlichen Entfernungen auf die Detektionsrate der Szenarien
- Bekleidung:
  Einfluss der Bekleidungsformen auf die Erkennung der Bewegungsarten.
  Einfluss der Tarnmitteln auf die Detektionsrate
- Sabotage:
  Manipulationserkennung des Systems bei bekannten Stör- und Sabotageversuchen.
  Prüfung der ordnungsgemäßen Detektion auf Eindringversuche trotz angewandter Maßnahmen
- Gesamtbewertung:
  Keine Gesamtbewertung der Systeme, sondern Gesamtdetektionsrate in Prozent für alle Szenarien

In den Tab. 3.4 und Tab. 3.5 sind die Ergebnisse der jeweiligen Systeme dargestellt. Die Prozentangabe ist der Anteil der positiv bewerteten Testszenarien. Werte über 90 % sind

als „hervorragend“ und Werte zwischen 80-89 % als „sehr empfehlenswert“ durch die Prüfer des Systemtests definiert /GIT 22/. Niedrigere Werte fallen in die Kategorien „empfehlenswert“, „bedingt empfehlenswert“ und „nicht empfehlenswert“.

Die Kombination von Thermal- und RGB-Kameras hat sich als effektiv erwiesen und lieferte die besten Ergebnisse. Generell lässt sich erkennen, dass der Einsatz verschiedener Detektionstechnologien die Detektionsrate erheblich erhöhen kann, insbesondere wenn eine Technologie die Schwächen einer anderen ausgleicht. Dies kann durch verschiedene Videosensoren, wie in dem vorgestellten Test, oder durch die Ergänzung anderer erweiterter Technik wie Radar, Light Detection and Radar (LiDAR), Sensorkabel oder andere erfolgen.

Die Kombinationssysteme von Dahua und Honeywell haben daher am besten abgeschnitten. Einige Ergebnisse zeigten jedoch auch, dass ebenso Systeme mit nur einem Videosensor hervorragende Ergebnisse erzielen konnten.

Das Thermal-System von Bosch und das RGB-System von Bosch sowie das Thermal System von Dallmeier folgten als nächstbeste Kontrahenten und lieferten bessere Ergebnisse und haben eine größere Anzahl an Szenarien bestanden als die Kombi-Systeme von Avigilon und Axis sowie das Kombi-System von Milestone, Saimos und Vivotek. Es ist daher nicht pauschal davon auszugehen, dass Kombi-Systeme automatisch besser sind. Es kommt darauf an, wie gut das System abgestimmt und wie optimiert die Videoanalyse-Software ist.

Während das Thermalsystem von Hikvision noch gute Ergebnisse lieferte, zeigten sich beim Tag/Nacht-System von Hikvision deutliche Schwächen. Zusammen mit dem Tag/Nacht-System von Mobotix performten diese beiden Systeme mit Abstand am schlechtesten im Vergleich zu allen anderen Systemen und belegten die letzten Plätze.

Sofern es der finanzielle Rahmen des Anwenders erlaubt, ist die Kombination von Thermal- und RGB-Kameras besonders für den effektiven Perimeterschutz eine sichere und empfehlenswerte Wahl. Thermalkameras bieten bei Nacht eine bessere Detektion als RGB-Kameras, selbst mit IR-Beleuchtung, arbeiten jedoch an warmen Tagen weniger effizient als bei kühlerem Wetter.

Für Entscheidungsträger in sicherheitsrelevanten Bereichen, Planer, Errichter, Systemintegratoren, Versicherer und Betreiber ist es unerlässlich, den eigenen Bedarf

genau zu analysieren. Eine gut vorbereitete Analyse erleichtert es, das am besten passende System für die spezifischen Anforderungen und Gegebenheiten zu finden. Hierbei kann die Unterstützung durch unabhängige Experten mit Erfahrung von großem Vorteil sein. Anschließend ist es gut über einen Probezeitraum unter realen Bedingungen zu testen, da dies andere Herausforderungen mit sich bringt als Laborbedingungen. Kleine Details können über Erfolg und Misserfolg entscheiden, und die Natur kann unvorhersehbare Schwierigkeiten verursachen. Jedes System ist nur so gut wie seine Einrichtung und Installation vor Ort, und absolute Sicherheit kann niemals garantiert werden /GIT 22/.

Tab. 3.4 Ergebnisbewertung der Tag/Nacht Kamerasysteme nach /GIT 22/

	Avigilon	**Axis**	**Bosch RGB**	**Bosch Thermal**	**Dahua**
NAR/FAR-Bewertung	Hervorragend	Hervorragend	Sehr empfehlenswert	Empfehlenswert	Sehr empfehlens-wert
Bedienung	Hervorragend	Hervorragend	Hervorragend	Hervorragend	Sehr empfehlens-wert
Performance bei Tag	81%	87%	92%	96%	100%
Performance bei Nacht	87%	90%	87%	86%	91%
Nahbereich (Alpha)	91%	91%	94%	91%	91%
Mittlerer Bereich (Bravo)	77%	90%	90%	97%	100%
Entfernter Bereich (Char-lie)	77%	86%	97%	95%	95%
Bekleidung 1	89%	96%	96%	100%	100%
Bekleidung 2	77%	97%	97%	95%	95%
Sabotage/Manipula-tion/Störung	82%	59%	82%	76%	82%
Bewegungsart 1 (auf-recht gehend)	95%	87%	95%	95%	96%
Bewegungsart 2 (kniend, liegend oder rollend)	52%	61%	91%	96%	91%
Anzahl aller bestandenen Szenarien	82%	86%	89%	94%	95%

Tab. 3.5 Ergebnisbewertung der Thermalkamerasysteme nach /GIT 22/

	Dallmeier	**Hikvision RGB**	**Hikvision Thermal**	**Honeywell**	**Milestone/ Saimos/Vivo-tek**	**Mobotix**
NAR/FAR-Bewertung	Hervorragend	Sehr empfehlens-wert	Empfehlens-wert	Empfehlens-wert	Sehr empfehlens-wert	Hervorra-gend
Bedienung	Sehr empfehlens-wert	Sehr empfehlens-wert	Sehr empfehlens-wert	Sehr empfehlens-wert	Hervorragend	Hervorra-gend
Performance bei Tag	91%	57%	91%	94%	89%	34%
Performance bei Nacht	82%	30%	70%	100%	83%	57%
Nahbereich (Alpha)	91%	56%	75%	100%	81%	44%
Mittlerer Bereich (Bravo)	93%	53%	90%	97%	90%	40%
Entfernter Bereich (Charlie)	90%	23%	86%	90%	86%	41%
Bekleidung 1	96%	54%	96%	96%	89%	21%
Bekleidung 2	85%	54%	77%	95%	87%	38%
Sabotage/Manipulation/Störung	100%	18%	76%	100%	76%	82%
Bewegungsart 1 (aufrecht gehend)	91%	58%	93%	95%	95%	58%
Bewegungsart 2 (kniend, liegend oder rollend)	91%	17%	61%	100%	65%	0%
Anzahl aller bestandenen Szenarien	91%	46%	83%	96%	86%	42%

3.3 KI-basiertes Zutrittskontrollsystem und Videoüberwachung von IDEMIA GmbH

IDEMIA SAS ist ein französisches Unternehmen im Bereich der digitalen Identitätslösungen und bietet eine breite Palette an Technologien und Dienstleistungen, die in verschiedenen Sektoren Anwendung finden. Das Unternehmen ist weltweit tätig und hat mit IDEMIA Germany GmbH einen Zweig in Deutschland. IDEMIA spezialisiert sich auf die Entwicklung von biometrischen und kryptographischen Technologien. Beispiele sind Fingerabdruck- und Gesichtserkennungssysteme, die in verschiedenen Bereichen wie Grenzkontrollen und Strafverfolgung eingesetzt werden. Interessant sind hierbei die Zugangskontrolllösungen. Diese umfassen physische und digitale Zutrittssysteme, die in Unternehmensumgebungen, öffentlichen Einrichtungen und zur Kontrolle öffentlicher Bereiche eingesetzt werden. Diese Systeme verwenden oft biometrische Technologien, um sicherzustellen, dass nur autorisierte Personen Zugang erhalten. Interessant ist hierbei der Einsatz von KI in den Erkennungssystemen. Die KI wird zur Verbesserung von biometrischen Erkennungssysteme wie Gesichtserkennung, Fingerabdruck- und Iris-Scan-Technologien eingesetzt.

Die von IDEMIA entwickelte KI-basierte Videoanalyse Plattform, „Augmented Vision“ genannt, ermöglicht es Personen, Gesichter, Silhouetten, Geschlecht, Alter und Farbe der Kleidung zu erkennen, zu identifizieren und zu verfolgen. Die Gesichtserkennung namens „IsiPass Fr“ kann allein oder kombiniert mit anderen biometrischen Methoden, wie Finger- oder Augenscan, als Zutrittskontrollsystem fungieren /PRN 23/. Für die Gesichtserfassung muss zuerst ein Bild aufgenommen oder hochgeladen werden. Aus diesem Bild werden Vorlagen anhand von Gesichtsmerkmalen generiert, das Bild selbst wird gelöscht. Diese Vorlage wird anschließend binär codiert, verschlüsselt und gespeichert. Aus der Vorlage ist es nicht möglich, reversibel Bilder der Person zu generieren. Die Vorlage kann lokal auf dem Gerät, auf einer Radio Frequency Identification (RFID) Karte oder auf einem ausgelagerten Speichersystem in einer Datenbank gespeichert werden. Dieses Vorgehen ist gemäß Angaben des Herstellers konform mit der europäischen Datenschutz-Grundverordnung (DSGVO). Die Vorlage dient als Merkmalprofil, stellt die Zugangsberechtigung der jeweiligen Person dar und wird bei jedem Eintritt abgeglichen /IDE 23b/. Die dafür entwickelten Gesichtserkennungsalgorithmen wurden in verschiedenen Tests des National Institute of Standards and Technology (NIST) als hervorragend eingestuft und fielen unter die Top 3 im Jahr 2023 und Platz 1 im Jahr 2021 in der Kategorie „Face Recognition Vendor Tests (FRVT) 1:N Identification“. Die Testergebnisse berichteten über die Leistungsfähigkeit der Gesichtserkennungstechnologie in

Eins-zu-Viele-Szenarien (1:N), bei denen ein Gesichtsbild mit einer großen Datenbank von Gesichtern verglichen wird, um ein oder mehrere übereinstimmende Bilder zurückzugeben. IDEMIAs Gesichtserkennungsalgorithmus erzielte die beste Genauigkeit mit einer Trefferquote von 99,88% korrekten Übereinstimmungen bei 12 Millionen Gesichtern. /IDE 23a/

Eine von IDEMIA angebotene Produktlösung, welche primär für die Gesichtserkennung vermarktet wird, nennt sich „VisionPass“. Durch gleichzeitige Verwendung von 2D-, 3D- und Infrarot-Sensorik ist es möglich, dass Gesichter bei allen Lichtverhältnissen identifiziert werden können. Die Gesichter können mit einer Identifikationsdauer von ca. 1 Sekunde gelesen werden. Auch mit Masken, Bartwuchs, Make-Up, offenem Motorradhelm und anderen Gesichtsbedeckungen lässt sich eine Gesichtserkennung, bei mindestens 30% sichtbarer Fläche des Gesichts, erfolgreich durchführen /IDE 23b/. Das Gerät kann mit seiner IP65 (Staubdicht u. Wasserschutz) und Schutzklasse IK08 (Stoßfestigkeit) im Innen- und Außenbereich verbaut werden. Es ist möglich eine Person in der Laufbewegung zu identifizieren. Der Erkennungswinkel ist so eingestellt, dass Personen mit einer Körpergröße von 120 cm bis 200 cm identifiziert werden können.

Die „Augmented Vision“ Plattform kann auch in ein bestehendes IP Kameranetzwerk inkludiert werden und somit ein bestehendes Überwachungssystem mit einer Videoanalyse nachrüsten. Die Videoanalyse kann sowohl Einzelpersonen als auch große Menschenmengen erkennen. Es eignet sich daher für viele Einsatzzwecke von Bürokomplexen, wo sich ein kleinerer Verkehrsfluss von Menschen bewegt, bis hin zu Stadien und Flughäfen, wo es einen großen Personenverkehr gibt. Der Scanbereich bzw. die ROI kann in den gefilmten Bereichen eingestellt werden, sodass nur die Personen gescannt werden, die sich mit Absicht einem Zugang oder gekennzeichneten Bereich nähern. Das System ist gegen Tailgaiting (z. Dt. Durchschlüpfen) gesichert, was bedeutet, dass eine autorisierte Person keinen Zugang erhält, solange das System im Scanbereich eine nicht autorisierte Person erkennt. Dies soll ein geplantes oder ungeplantes Miteinschleusen einer weiteren Person verhindern. Falls während des Öffnungszeitraums des Zugangs dennoch eine nicht-autorisierte Person hineinläuft, kann ein Alarm ausgelöst werden. Das System kann aber auch so eingestellt werden, dass ein Mitarbeiter mit einer höheren Zutrittsberechtigung durch Bestätigung einer doppelbiometrischen Identifikation gezielt externe Personen ohne Zugangsberechtigung mitnehmen kann. Die von IDEMIA entwickelte KI Plattform kann so gleichzeitig für die Zugangserkennung und für die Überwachung genutzt werden.

Zur Erklärung der Funktionsweise im Detail, den Trainingsdaten oder der Art verwendeten KI in der Videoanalyse von IDEMIA, gibt es keine öffentlich zugänglichen Daten. Weitergehende Aussagen zur verbauten KI lassen sich daher nicht treffen.

3.4 Unterstützte Überwachung durch KI-Robotik

Im VdS Fachmagazin s+s report 3/2023 /TOK 23/ wird in einem Artikel die Idee von Schadenverhütung durch moderne Robotertechnik vorgestellt. Die Nutzung smarter KI-Robotik kann demnach Vorteile bei der Schadensverhütung und dem Diebstahlschutz in sicherheitskritischen Bereichen bieten. Dabei wird auf den Aspekt der Schadenverhütung durch Überwachung und Abschreckung gesetzt.

KI-gestützte Roboter können autonom patrouillieren und dabei verdächtige Aktivitäten erkennen. Sie sind in der Lage, sofort Alarm auszulösen, wenn sie Anomalien feststellen. Diese Echtzeit-Überwachung ermöglicht es, potenzielle Bedrohungen frühzeitig zu identifizieren und zu neutralisieren. Sie können eventuell schneller und präziser auf Sicherheitsvorfälle reagieren als menschliches Sicherheitspersonal. Durch die kontinuierliche Überwachung und Analyse von Daten können diese Systeme effizient Maßnahmen ergreifen, um Einbrüche und Diebstähle zu verhindern. Ein weiterer Vorteil von KI-Robotern ist, dass der Einsatz langfristig Kosten sparen kann, da sie rund um die Uhr arbeiten können und weniger Personal für die Überwachung benötigt wird. Zudem könnten sie die Notwendigkeit für teure physische Sicherheitsbarrieren und Wartungsarbeiten an herkömmlichen Sicherheitssystemen reduzieren. Die Einsatzbereiche von smarten Robotern können sehr vielfältig ausfallen. Sie können in verschiedenen sicherheitskritischen Bereichen eingesetzt werden, einschließlich Industrieanlagen, Lagerhäusern und sensiblen Forschungszentren. Sie überwachen nicht nur den Zugang, sondern auch sensible Bereiche innerhalb der Anlagen. Das Verwenden solche Roboter in KTA innerhalb des Betriebsgelände oder sensibler Bereiche würde in dessen Einsatzbereich fallen.

Die in /TOK 23/ vorgestellten Roboterlösungen wurden speziell für Sicherheitsanwendungen entwickelt. Diese Roboter sind mit einer aktuellen Technologie ausgestattet und bieten verschiedene Funktionen zur Überwachung und Sicherung von Anlagen. Die Hauptlösungen von Security Robotics und ihre Kenndaten werden hier folgend vorgestellt:

Tab. 3.6 Merkmale des Radroboters /SMP 24/

Name	ARGUS Radroboter
Hersteller:	SMP Robotics
Einsatzzweck:	Patrouillendienst, mobile intelligente Videoüberwachung
Höchstgeschwindigkeit:	6 km/h
Wenderadius:	5 m
Einsatzdauer:	ca. 10 -12 h
Akkuladezeit:	ca. 8 Stunden
Kameratechnik:	Sechs Panoramakameras 1280x720p bei 0,005 lx PTZ Kamera 752x582p bei 0,01 lx; 36facher Zoom Thermalkamera 640x480p; 19 mm Brennweite

Der ARGUS Radroboter ist ein mobiler Sicherheitsroboter, der speziell für die Überwachung großer Flächen entwickelt wurde. Er wiegt 189 kg und fährt mit einer Geschwindigkeit von 4 - 6 km/h, dies ist mit Schritttempo vergleichbar. Der Roboter ist mit sechs HD Panoramakameras, einer 360° Full HD PTZ Kamera und einer Thermalkamera ausgestattet, die eine präzise Überwachung bei Tag und Nacht ermöglicht. Zwei verbaute Computer sind für die Videoanalyse des Roboters verantwortlich. Eine automatischen Personenerkennung ist ab 130 m Entfernung möglich, Gesichtserkennung ist bei guten Tageslichtverhältnissen bis zu 60 m Entfernung möglich. Eine Bewegungserkennung ist bei guten Tageslichtverhältnissen in einem Bereich von bis zu 30 m möglich. Die große Akkukapazität von 5040 Wh ermöglicht eine durchgehende Einsatzdauer von ca. 10 - 12 Stunden, muss jedoch nach vollständiger Entladung bis zu 8 Stunden lang wiederaufladen. Das System ist IP65 (/DIN 14a/) zertifiziert (Staubdicht und Druckwasserschutz) und kann bei Umgebungstemperaturen von -25° – +55°C eingesetzt werden. Durch die verbaute Sprechanlage ist eine bidirektionale Kommunikation mit Personen in der Nähe möglich /SEC 23a/, /SMP 24/.

Tab. 3.7 Merkmale des Laufroboters /SEC 23b/, /BOS 24/

Name	SPOT Laufroboter
Hersteller:	Boston Dynamics
Einsatzzweck:	Kontrollgänge, Messen, Prüfen
Höchstgeschwindigkeit:	5,7 km/h
Neigungswinkel:	Max. 30°
Schritthöhe	Max. 300 mm
Einsatzdauer:	90 min
Akkuladezeit:	60 min
Kameratechnik:	Basis: Stereokameras 360° Zusatzmodul: LIDAR Sensor, PTZ Kamera, Thermalbildkamera,

Der SPOT Laufroboter ist ein vielseitiger und hochmobiler Roboter, der sich durch seine fortschrittliche Lauftechnik auszeichnet. Das Basismodul wiegt 32,7 kg und bewegt sich mit einer Höchstgeschwindigkeit von 5,4 km/h. Mit seiner hohen Schritthöhe und seinem hohen Neigungswinkel ist es ihm möglich, auch bei unebenem Gelände zu agieren. Der Laufroboter ist mit einer Vielzahl von Sensoren ausgestattet, bei der eine gute Navigation mit 360° Sichtfeld und 4 m Umgebungserkennung ermöglicht wird. Dadurch ist der Roboter in der Lage, Gelände autonom zu patrouillieren, potenzielle Eindringlinge zu erkennen und Sicherheitslücken zu identifizieren, da er auch zur Identifikation und Verfolgung von Personen mithilfe von Gesichtserkennungstechnologien eingesetzt werden kann. Zudem ist er IP54 (/DIN 14a) zertifiziert (grober Staub- und Spritzwasserschutz) und er kann bei Umgebungstemperaturen von -20 – 55°C eingesetzt werden. Er kann modular modifiziert und angepasst werden, um ihn für individuelle Aufgaben mit bis zu 14 kg zusätzlichen Gepäck bzw. Technik aufzurüsten, um ihn mit thermaler, visueller oder akustischer Sensorik für zusätzliche Aufgaben zu konfigurieren. Durch seine robuste Bauweise und einem Akku mit 564 Wh Kapazität, lässt sich eine Laufzeit von bis zu 90 Minuten erreichen. Es ist möglich, ihn autonom operieren und auf Veränderungen in seiner Umgebung reagieren zu lassen oder ihn manuell zu steuern. Die verschiedenen Konfigurationsmöglichkeiten, die Agilität und das durch KI unterstütze System, machen den Roboter zu einer fähigen Lösung für moderne mittelfristige Sicherheitsanwendungen /SEC 23b/, /BOS 24/.

Tab. 3.8 Merkmale des Drohnensystems /SUN 23/

Name	BEEHIVE Drohnensystem
Hersteller:	Sunflower Labs
Einsatzzweck:	Flugpatrouille, Alarmverifizierung, Videodokumentation
Höchstgeschwindigkeit:	14,5 km/h
Reichweite:	Bis zu 600 m von der Dockingstation
Windgeschwindig-keit/Böen-widerstand	20 km/h / 30 km/h
Einsatzdauer:	20 min
Akkuladezeit:	25 min
Kameratechnik:	Sony IMX385 Sensor; 1920x1080p bei 25 FPS

Das BEEHIVE Drohnensystem ist eine fortschrittliche Drohnenlösung für die Luftüberwachung, Sicherheitsüberwachung und Alarmverifizierung aus der Vogelperspektive. Im Alarmfall, ausgelöst durch beispielsweise einen Zaunsensor, kann die Drohne automatisch an den Alarmort geschickt werden. Durch Live-Videoübertragung bietet sie eine schnelle und klare Sicht auf die Situation, was zu einer effizienten Klärung von Sicherheitsereignissen beiträgt. Mit einer Flugdistanz von bis zu 600 m (von der Dockingstation), einem Gewicht von 1,56 kg und einer Geschwindigkeit von 14,5 km/h kann die Drohne zügig große Gebiete überwachen. Mit einer Akkukapazität von 4000 mAh kann eine Flugzeit von bis zu 20 Minuten (15 min Flugzeit + 5 min Puffer für Rückweg) erreicht werden und mit der relativ kurzen Akkuladezeit von 25 Minuten lässt sich eine zügige Wiederaufnahme eines Einsatzes starten. Die Drohne ist mit hochauflösenden Kameras und fortschrittlichen Sensoren ausgestattet, die eine detaillierte Überwachung, Erkennung und Analyse in Full HD bei 25 FPS und einem erweiterten Blickfeld, auch bei schwachem Licht, ermöglichen. Die Auswertung der Daten erfolgt in der Dockingstation. Eine Ausstattung mit Thermal-Kameras ist bei Bedarf ebenfalls möglich, um anhand von Wärmesignaturen und Temperaturunterschieden Auffälligkeiten sofort zu bemerken. Das System verwendet keine Gesichtserkennung, sondern nur eine Identifizierungsmethode zur Unterscheidung von Menschen, Tieren und Fahrzeug /SUN 24/. Die Drohne kann bei Betriebstemperaturen von -10 – 40°C eingesetzt werden, jedoch ist keine IP Zertifizierung oder sonstiger Schutz gegen Wasser angegeben /SEC 23c/, /SUN 23/.

Anhand der hier vorgestellten Optionen zu KI-Robotik im Einsatz von sicherheitskritischen Bereichen gibt es ein großes Potenzial zur Verbesserung der Sicherheitsinfrastruktur. Durch die Kombination von Echtzeit-Überwachung, automatisierter Reaktion und fortschrittlicher Datenanalyse können diese Systeme einen wesentlichen Beitrag in

der Unterstützung von Schadensverhütung, Diebstahlschutz und Ereigniskontrollen leisten. Zur Erklärung der Funktionsweise im Detail, den Trainingsdaten oder der Art verwendeten KI in der Videoanalyse der vorgestellten Robotersystem, gibt es keine öffentlich zugänglichen Daten. Tiefere Aussagen zur verbauten KI lassen sich daher nicht treffen.

4 Analyse und Bewertung von Anwendungsmöglichkeiten

4.1 Berücksichtigung generischer Anforderungen, Normen und Regelwerke

Gemäß der EU-Verordnung zur Künstlichen Intelligenz dürfen KI-System keine eigenständigen Entscheidungen treffen. Wie ist diese Anforderung für einen KI-basierten Videomelder zu verstehen, der eine Videosequenz zu bewerten hat und je nach Ergebnis der Bewertung einen Alarm ausgibt oder keinen Alarm ausgibt? Wäre dies schon eine Entscheidung? Eine KI-getriebene Videoanalyse muss in der Lage sein, auf Grundlage der Parametrierung über die Frage Alarm oder kein Alarm zu entscheiden. Die VÜA muss dann keine weiteren Maßnahmen selbständig einleiten. Es reicht, wenn der Alarm ausgegeben wird. Welche Maßnahmen auf Grundlage der Alarmmeldung einzuleiten sind, sollte weiterhin das Bedienpersonal in der Sicherungszentrale der KTA entscheiden, beispielsweise ob der Alarm vor Ort nochmals personell überprüft werden sollte oder ob direkt der Anruf bei der Polizei erfolgen soll.

Gemäß /CPN 20/ sollten bei einer Videodetektion eine Detektionsrate von mindestens 95 % erreicht werden. Diese Anforderung wäre also noch erfüllt, wenn in 5 % der Fälle eine Alarmierung, obwohl es einen Alarmgrund gibt, unterbleibt. Für eine KTA wäre eine solche Detektionsrate nicht akzeptabel.

Wenn es möglich ist, die Detektionsrate zu erhöhen, notfalls auch auf Kosten einer erhöhten FAR, sollte dies unbedingt so konfiguriert werden. Statt einer Quote von Falschalarmen pro Kilometer des Perimeters sollte vorzugsweise eine Falschalarmrate pro Mitarbeiter pro Stunde definiert werden. Eine etwas höhere FAR ist besser als einer zu niedrige Detektionsrate. Tatsächlich darf die FAR jedoch auch nicht zu niedrig sein, damit die Mitarbeiter nicht den Eindruck bekommen, dass das System abgestürzt wäre.

Es muss beachtet werden, dass nicht jede Videoanlage gleich ist. Das eine System ist beispielsweise auf die Detektion von Eindringversuchen am Perimeter optimiert, das nächste System ist wiederum auf die Erkennung von Täterverhalten im Kassenbereich von Supermärkten oder Tankstellen oder die Erkennung von Kfz-Kennzeichen optimiert. Letzteres System könnte eventuell gut im Bereich der Wache am Zugang zum Sicherungsbereich einer KTA eingesetzt werden, um beispielsweise Situationen im Wachlokal beobachten und beurteilen zu können, die Kfz-Zufahrt zu überwachen und die Zufahrt

von Fahrzeugen zu dokumentieren oder auch um allgemein Situationen an kontrollierten Zugängen zu beobachten und bei verdächtigem Verhalten zu alarmieren.

Bei einer KTA soll jeder Eindringversuch immer sicher detektiert werden, daher müsste die Detektionsrate nahezu bei 100% liegen. Da dies nicht realistisch zu gewährleisten ist, sollte die Detektionsrate im Idealfall größer als 99% betragen. Die Detektionsrate lässt sich durch die Gestaltung der Randbedingung des Prüfszenarios steigern, sodass realistische Eindringszenarien speziell auf KTA ausgelegt und geprüft werden und nicht generische Einbruchszenarien, die auf Diebstahl von Wertsachen abzielen, herangezogen werden müssen. Es kommt auf also besonders auf die Situation an, welche Vorgänge mit einer KI gestützten Videokamera beobachtet werden sollen. Durch die Vorgabe bzw. Gestaltung der Randbedingungen, also Beobachten eines langsamen Übersteigens einer Zaunanlage oder Durchdringen einer stabilen Barrierewand, werden die relevanten Szenarien, bei denen die Kamera garantiert detektieren muss, derart beschränkt, dass damit die Detektionsrate gesteigert werden kann.

4.2 GIT System Test der Videoanalytik

Die Ergebnisse des GIT System Tests aus Kap. 3.2 zeigen, dass die getesteten Systeme in der Lage sind, die in Tab. 2.2 aufgeführten Anforderungen zu gewissen Teilen zu erfüllen. Es wurden keine Fahrzeuge in die Tests mit einbezogen und daher ist die Erkennung von Fahrzeugen nicht bewertbar. Auch wenn davon ausgegangen werden darf, dass die Systeme die Anforderung aus Tab. 2.2 erfüllen könnten, da Videoanalyse, die auf Basis von Lernalgorithmen ohne fortschrittliche KI-Technik arbeitet, bereits den Anforderungen entspricht, lässt sich dennoch nicht pauschal beurteilen, ob dies auch wirklich der Fall ist, ohne eigene Tests durchgeführt zu haben. Mit den Tests wurden die Leistungen bei Tag und bei Nacht bewertet. Es ist aber weder die Uhrzeit noch die Jahreszeit bekannt oder ob andere Lichtquellen den Testperimeter aus der Entfernung möglichweise beleuchtet haben. Die Beleuchtungsanforderungen für KTA lassen sich mit den gegebenen Informationen für die Testszenarien nicht vergleichen. Dies ist relevant für die Interpretation der Ergebnisse, da beispielsweise eine Sommernacht heller ist als eine Winternacht, und auch Vollmond oder Neumondnächte sowie andere Witterungsbedingungen mit schlechten Sichtverhältnissen (Nebel, Regen, Schnee etc.) berücksichtig werden müssen. Die Tests beinhalteten auch Sabotageversuche, allerdings ohne

einen physischen Angriff auf die Systeme. Auch auf einen Hackerangriff wurde verzichtet. Die Szenarien beschränkten sich darauf, die Systeme zu stören, zu manipulieren oder zu irritieren, um den Perimeter ohne Alarmauslösung zu überwinden /GIT 22/. Um die Eignung für den Einsatz in KTA bewerten zu können, sind daher über die durchgeführten Tests hinaus auch Versuche mit IT-Angriffen und physischen Angriffen auf KI-gestützte Videokamerasysteme erforderlich.

Die Autoren dieses Forschungsberichts sind der Meinung, dass alle Systeme mit einer Erfolgsquote unter 90% fraglich sind und mit einer Erfolgsquote unter 80% schon sehr fraglich und nicht empfehlenswert sind. Eine Detektionsquote, bei der in einem von zehn Fällen ein Eindringversuch unerkannt bleibt, liegt für KTA nicht mehr im akzeptablen Bereich. Für KTA gilt die Vorgabe, dass jedes sicherungsrelevante Szenario lückenlos und im Ereignisfall garantiert detektiert werden muss. Demnach wäre eine theoretische Detektionsrate von 100% erforderlich. Das dies praktisch unmöglich zu gewährleisten ist, sind für Szenarien, die nicht mit einer einzigen Sicherungsmaßnahme (hier KI gestützte Videodetektion) beherrscht werden können, kompensierenden Maßnahmen zu treffen. Die Detektionsrate sollte so groß wie möglich sein, im Idealfall mehr als 99%, sodass nur in sehr seltenen Fällen kompensierende Maßnahmen notwendig werden. Für die Berechnung der Detektionsrate dürfen auch Zeiten, bei denen die Detektionseinrichtung aus bekannten Gründen nicht verfügbar ist, beispielsweise bei ungünstiger Sonneneinstrahlung, Starkregen oder Nebel, aus der Betrachtung herausgenommen werden, wenn für diese Zeiten andere aber gleichwertige Detektionsmaßnahmen getroffen werden können.

Die betrachteten Tests bieten eine gute Basis, um die verschiedenen Modelle unter gleichen Rahmenbedingungen miteinander vergleichen zu können. Anhand der Ergebnisse lässt sich erkennen, dass kombinierte Systeme mit Thermal und Tag/Nacht-Funktion tendenziell am besten abgeschnitten haben. Danach folgten einige Systeme mit reiner Tag/Nacht-Funktion. Die Bewertung der Videoanalyse ist zugleich von der Qualität der verbauten bzw. verwendeten Kamerakomponenten abhängig, so dass eine separate Bewertung der verwendeten Videoanalyse nicht konkret abgeleitet werden konnte.

4.3 Zutrittskontrolle und Videoüberwachung durch „Augmented Vision“

Die beworbenen Funktionen der Videoanalyse Plattform „Augmented Vision“ von IDEMIA wurden Rahmen in einer Präsentation anhand ausgewählter Szenarien vorgestellt und erklärt. Die angebotenen Lösungen eignen sich in der Theorie für die Zutrittskontrolle und Überwachung und Verfolgung von Personen. In der Praxis werden sie auch bereits an acht deutschen Flughäfen von der Bundespolizei verwendet /BUN 24/, /MON 19/. Die lässt darauf schließen, dass bestimmte Anforderungen an Orten mit höherem Sicherheitsniveau eingehalten werden. Allerdings ist die Performance der Videoanalyse bei einem Einsatz im Freien unter verschiedenen Wetterbedingungen nicht bekannt. Die vorgestellten Szenarien wurden bei mildem Wetter durchgeführt. Das Erkennen von Handlungen und damit auch die Sabotageerkennung, wurde nicht vorgestellt. Zwar ist die Überwachung von VÜA mit Videoanalyse auf Sabotage auch mit konventionellen Sabotageschutzeinrichtungen möglich, ob aber die KI-Software selbst einen Beitrag zur automatischen Sabotageerkennung liefert, ist aus den Informationen nicht abzuleiten. Die angebotenen Produktlösungen haben jedoch eine ausgezeichnete Personenerkennungsrate und eine gute Personenverfolgung mit automatischer Aufschaltung der nächsten erfassenden Kamera. Die Erkennung ist abhängig von der Qualität und Detailtreue des verwendeten Kamerasystem, daher wird ein gewisser Standard benötigt, um Personenerkennung bis zu einer bestimmten Distanz zu gewährleisten. Die genauen Details wurden nicht vorgestellt. Die Videoanalyse wurde auch während der Nacht vorgestellt und hat auch im Dunkeln (basierend auf der Fähigkeit des verwendeten Kamerasystems) keine Schwierigkeiten, Personen zu erkennen. Laut Angaben der Hersteller ist es möglich teilverdeckte Gesichter zu identifizieren, solange mindestens 30% des Gesichts sichtbar sind. Mithilfe der genannten Personenerkennung lässt sich eine effektive Zutrittskontrolle realisieren. IDEMIA bietet eigene Standalone-Lösungen mit integrierter Videoanalyse an und ermöglicht auch die Integration der Videoanalyse in bestehende IP-Kameranetzwerke. Dies erweist sich als flexible Option und könnte sich durchaus für KTA lohnen, wo ein erhöhter Personenverkehr auf engerem Raum stattfindet. Dadurch könnte das eigene Personal unterstützt und entlastet werden, sodass sie andere Aufgaben nachgehen und insbesondere auf Alarmauslösungen reagieren können.

4.4 KI Robotik

Die vorgestellte KI-Robotik der Firma Security Robotics zeigt gutes Potenzial. Die verschiedenen Roboter sind auf verschiedene Szenarien ausgelegt und es gibt jeweils Indoor und Outdoor-Lösungen. Durch den mobilen Einsatz der Roboter können große oder kleine Fläche individuell patrouilliert werden. Die Roboter sind laut Herstellerangaben gegen eine Vielzahl von Wetterbedingungen geschützt. Manche Anforderungen werden aber dennoch nicht konkret angesprochen und können daher nicht bewertet werden. Eine Objekterkennung ist erwähnt, ob dadurch aber auch explizit eine Fahrzeugerkennung konfiguriert werden kann, ist nicht beschrieben. Es ist fraglich wie effizient die Roboter bei der Überwachung auf Vorbereitungshandlungen vor dem Perimeter sein könnten. Das Filmen von Privatpersonen außerhalb des privaten Grundstücks ist datenschutzrechtlich verboten und zusätzlich ist der Aufenthalt außerhalb des Grundstücks nicht gesetzeswidrig. Es ist daher eher vorstellbar, die Roboter als Interventionsmittel nach Alarmauslösung loszuschicken. Die Roboter sollten den Einsatz von Personal in den Punkten Kosten, Koordination und Ausdauervermögen übertreffen können, haben jedoch den Nachteil, dass diese nicht aktiv in das Geschehen eingreifen können und dabei, bis auf den Flugroboter, auch zu langsam sind, um einen laufenden Eindringling zu verfolgen. Sie eignen sich daher besser für alltägliche und repetitive Handlungen wie Streifengänge und Patrouillen. Eine echte Zutrittskontrolle können die Roboter nicht ersetzen, aber die Prüfung einer Aufenthaltsbefugnis ist durch die Personenerkennung möglich, da befugte von unbefugten Personen auf dem Gelände während der Kontrollgänge unterschieden werden und bei Bedarf ein Alarm ausgelöst werden kann. Als alleinstehende Lösung können daher bestimmte Anforderungen oder Teile davon nicht erfüllt werden, die Roboter könnten aber als zusätzliche Maßnahmen eine ergänzende Rolle spielen.

Eine eigene KI-Software für die Videoanalyse wird für den Laufroboter nicht vorgestellt. Es wird die individuelle Anpassung, Programmierung und Einbindung bzw. Nachrüstung der Roboter durch die Hersteller beworben, daher ist davon auszugehen, dass keine proprietäre KI-Software verwendet werden muss und der Kunde sich frei entscheiden, kann welche KI-Software er für die Videoanalyse nutzen möchte. Durch das Einbinden einer KI-Videoanalyse, die die Anforderungen an das System erfüllen kann, sollte es möglich sein, eine passende Lösung zu konfigurieren. Der Flugroboter ist herstellerseitig mit einer eigenen KI-Software ausgestattet, welche in der Dockingstation verbaut ist und die übermittelten Kameradaten des Flugroboters auswertet. Der Radroboter besitzt einen verbauten Computer, der den Roboter lenkt und die Kameradaten mithilfe von KI-Software auswertet.

4.5 Ausblick

In den allermeisten Fällen gibt es zu den verwendeten KI-Systemen keine öffentlichen Daten, die Leistungsfähigkeit und die Lernfähigkeit der KI-Systeme lässt sich damit nicht objektiv bewerten und vergleichen. Es ist nachvollziehbar, dass solche internen Informationen vertraulich gehandhabt werden. Ob die Systeme mit Deep Learning KI oder mit effizienten Lernalgorithmen betrieben werden, bleibt offen. Praxis-Tests wie der von GIT Sicherheit eignen sich daher als guter Marktvergleich für die verfügbaren Optionen und den Direktvergleich bestimmter Leistungsparameter.

Die Lösungen der Firmen IDEMIA und Security Robotics sind systemunabhängig und lassen sich in andere bereits bestehende normgerechte VÜA integrieren und wären damit auch normkonform, solange sie die Systeme nicht negativ beeinflussen. Die getesteten Kamerasysteme lassen sich größtenteils ebenso in ein bereits bestehendes VÜA einpflegen, da bei den meisten verwendeten Videokameras die Videoanalyse lokal auf dem Gerät erfolgt. Es müssten allerdings bisher genutzte Kameras durch neue ersetzt werden. Auch Server-basierte Datenverarbeitung wäre für KTA vorstellbar, solange die Server im Verantwortungsbereich der KTA verbleiben. Eine Übertragung der Videobildsignale an Dritte und die Verarbeitung der sensiblen Videobilddaten durch Dritte wäre ein zusätzliches Sicherheitsrisiko. Die einfachere Lösung wäre eine lokale Auswertung auf dem Anlagengelände.

Bereits bestehende Detektionssysteme könnten mit KI-gestützter Videodetektion ergänzt werden. Bestehende VÜA ließen sich erweitern, um die Beobachtung und Verifikation von Alarmen zu optimieren oder auch um die Falschalarmrate zu verbessern, ohne dass dazu die eingesetzten Kamerasysteme eine 100%-ige Detektionsrate erreichen müssten. Darüber hinaus kann zum aktuellen vorliegenden Informationsstand kein vollständiger Ersatz etablierter Detektionsverfahren uneingeschränkt empfohlen werden. Die Bewertung der Tester zur Bedienung und Fehlalarmrate (/GIT 22/) ist in jedem Fall subjektiv und sollten daher nur relativ als Vergleichsgrundlage mit den jeweils anderen Systemen gesehen werden.

Zur Entlastung des Personals bei der Zutrittskontrolle und bei der Geländeüberwachung könnte sich die Verwendung von KI-gestützten Videokameras als hilfreich erweisen, sofern die speziellen Anforderungen für den Einsatz im Bereich der KTA erfüllt werden können. Inwiefern diese neuen Technologien einer KTA einen Mehrwert bringen könnten, da bereits alle nötigen Anforderungen durch bereits bestehende Maßnahmen abgedeckt sind, bleibt vorerst offen. Um diese Neuerungen auch speziell für die Anforderungen von KTA prüfen zu können, müsste anhand eines Testaufbaus die Einrichtung, Bedienung und Funktionen an einem Standort einer KTA zeitweise erprobt werden

Die möglichen Auswirkungen des EU-Gesetztes auf den Einsatz von KI-getriebenen Videokameras konnten im Rahmen dieses Vorhabens nicht bewertet werden.

Literaturverzeichnis

/AND 23a/ Anderson, N. für SecurityCamsBlog: "Optimizing PTZ Camera Performance: A Complete Guide." Stand 26.04.2023, zuletzt besucht am 13.05.2023, erreichbar unter: https://securitycamsblog.com/optimize-ptz-camera/

/AND 23b/ Anderson, N. für SecurityCamsBlog: "Choosing the Right Lens for Your Surveillance Camera: A Comprehensive Guide." Stand 26.04.2023, zuletzt besucht am 13.05.2023, erreichbar unter: https://securitycamsblog.com/surveillance-camera-lens/

/APT 18/ Aptex Security AG: "Was muss man zu Videoauflösung und Videokompression wissen?“, Stand vom 6.11.2018, zuletzt besucht am 14.05.2024, erreichbar unter: https://www.aptex.ch/videoueberwachungssysteme/was-muss-man-zu-videoaufloesung-und-videokompression-wissen/

/APT 19/ Aptex Security AG: “Künstliche Intelligenz: Deep Learning mit Videoüberwachung“, Stand vom 16.08.2019, zuletzt besucht am 13.05.2024, erreichbar unter: https://www.aptex.ch/videoueberwachungssysteme/kuenstliche-intelligenz-deep-learning-in-der-videoueberwachung/

/BAR 16/ Barocas, S., Selbst, A.: “Big Data’s Disparate Impact”, California Law Review, Band 104, S.671 – 732, 11.08.2014

/BMU 03/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Merkpostenliste für die Sicherung sonstiger radioaktiver Stoffe und kleiner Mengen Kernbrennstoff gegen Entwendung aus Anlagen und Einrichtungen, Stand 03.04.2003

/BMU 12/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Richtlinie zur Sicherung von Zwischenlagern gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) - SEWD-Richtlinie Zwischenlager, Stand 10.05.2012, VS-NfD

/BMU 13/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT), Stand 13.06.2013, VS-NfD

/BMU 20/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit: Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III), Stand 25.08.2020, VS-NfD

/BMU 22a/ Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz: Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und der Beförderung von sonstigen radioaktiven Stoffen (SEWD-Richtlinie sonstige radioaktive Stoffe – SisoraSt), Revision 2.0, Stand 01.07.2022, VS-NfD

/BMU 22b/ Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz: Richtlinie zur Sicherung sonstiger radioaktiver Stoffe in kerntechnischen Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie sonstige radioaktive Stoffe in Kerntechnischen Anlagen – SisoraK), Stand 01.07.2022, VS-NfD

/BMU 24/ Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz: BMUV Nukleare Sicherung, Stand 17.06.2024, erreichbar unter: https://www.bmuv.de/themen/nukleare-sicherheit/nukleare-sicherung

/BMU 91/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Richtlinie über Maßnahmen für den Schutz von Anlagen des Kernbrennstoffkreislaufs und sonstigen kerntechnischen Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen zugangsberechtigter Einzelpersonen, Stand: 12.12.1990, Bekanntmachung vom 29.01.1991

/BMU 93/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Sicherungsmaßnahmen für den Schutz von kerntechnischen Anlagen mit Kernmaterial der Kategorie III, Stand: 10.02.1993, VS-NfD

/BMU 95/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Richtlinie für den Schutz von Kernkraftwerken mit Leichtwasserreaktoren gegen Störmaßnahmen oder sonstige Einwirkungen Dritter, Stand 05.12.1995, VS-NfD

/BMU 97/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: „Periodische Sicherheitsüberprüfung für Kernkraftwerke - Leitfaden Deterministische Sicherungsanalyse“, Stand 22.05.1997

/BUN 24/ Bundespolizei: “Wo gibt es EasyPass?“ Stand 2024, zuletzt besucht am 21.06.2024, erreichbar unter: https://www.easypass.de/EasyPass/DE/Wo_gibt_es_EasyPass/wo_gibt_es_easypass_node.html

/BOS 24/ Boston Dynamics: “Spot Specificantions” Stand 2024, zuletzt besucht am 10.06.2024, erreichbar unter: https://bostondynamics.com/products/spot/

/COR 95/ Cortes, C., Vapnik, V.: “Support-vector networks”. Machine Learning, Band 20, S. 273–297, 1995, https://doi.org/10.1007/BF00994018

/CPN 20/ Centre for the Protection of National Infrastructure: “Testing installed Video Analytic System”. 06.2020, erreichbar unter: https://www.npsa.gov.uk/resources/testing-installed-video-analytic-systems-2020

/DIN 14a/ DIN EN 60529:2014-09 „Schutzarten durch Gehäuse (IP-Code)“, 09.2014

/DIN 14b/ DIN EN 62676-1-1:2014-11: „Videoüberwachungsanlagen für Sicherheitsanwendungen - Teil 1-1: Systemanforderungen – Allgemeines“, 11.2014

/DIN 14c/ DIN EN 62676-1-2:2014-11: „Videoüberwachungsanlagen für Sicherheitsanwendungen - Teil 1-2: Systemanforderungen – Allgemeine Anforderungen an die Videoübertragung“, 11.2014

/DIN 14d/ DIN EN 62676-2-1:2014-11: „Videoüberwachungsanlagen für Sicherheitsanwendungen - Teil 2-1: Videoübertragungsprotokolle – Allgemeine Anforderungen“, 11.2014

/DIN 16a/ DIN EN 62676-3:2016-01: „Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 3: Analoge und digitale Videoschnittstellen“, 01.2016

/DIN 16b/ DIN EN 62676-4:2016-07: „Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 4: Anwendungsregeln“, 07.2016

/DIN 16c/ DIN EN ISO 22311:2016-12: „Sicherheit und Schutz des Gemeinwesens – Videoüberwachung – Datenschnittstellen (ISO 22311:2012), Deutsche Fassung EN ISO 22311:2014“, 12.2016

/DIN 18/ DIN EN 62676-3 Berichtigung 1:2018-12: „Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 3: Analoge und digitale Videoschnittstellen“, 12.2018

/DIN 19/ DIN EN IEC 62676-5:2019-05: „Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 5: Leistungsbeschreibung und Bildqualitätseigenschaften für Kameras“, 05.2019

/DIN 21/ DIN EN IEC 62676-2-31:2021-05: „Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 2-31: Videoübertragungsprotokolle – IP-Interoperabilität auf Basis von Webservices – Echtzeit-Streaming und Konfiguration“, 05.2021

/DIN 23/ DIN EN IEC 62676-2-33:2023-08: „Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 2-33: Cloud-Uplink und Fernzugriff von Managementsystemen“, 08.2023

/DKE 20/ Wahlster, W.; Winterhalter C.: „Deutsche Normungsroadmap – Künstlicher Intelligenz“
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Ausgabe 1, 2020

/EUP 24a/ Europäisches Parlament: „Gesetz über künstliche Intelligenz: Parlament verabschiedet wegweisende Regeln“, Stand 13.03.2024, zuletzt besucht am 17.06.2024, erreichbar unter:
https://www.europarl.europa.eu/news/de/press-room/20240308IPR19015/gesetz-uber-kunstliche-intelligenz-parlament-verabschiedet-wegweisende-regeln

/EUP 24b/ Europäisches Parlament: „KI-Gesetz: erste Regulierung der künstlichen Intelligenz“, Stand 13.03.2024, zuletzt besucht am 17.06.2024, erreichbar unter:
https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz

/EUP 24c/ Europäisches Parlament: „Arten von EU-Rechtsvorschriften“, Stand 2024, zuletzt besucht am 21.06.2024 erreichbar unter:
https://commission.europa.eu/law/law-making-process/types-eu-law_de#:~:text=an%20ein%20Referendum.-,Verordnungen,gelten%20unmittelbar%20in%20allen%20Mitgliedsl%C3%A4ndern.

/FRA 24/ Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS: Stand 2024, zuletzt besucht am 13.05.2024, erreichbar unter:
https://www.iais.fraunhofer.de/de/forschung/kuenstliche-intelligenz.html#faq_faqitem-answer

/FRI 20/ Friend, D. für Security Magazine: "Disruptively Affordable Cloud Storage Saves Lives and Enhances Video Surveillance Security”, Stand 30.04.2020, zuletzt besucht am 13.04.2024, erreichbar unter:
https://www.securitymagazine.com/articles/92278-disruptively-affordable-cloud-storage-saves-lives-and-enhances-video-surveillance-security

/GIT 22/ GIT Sicherheit: „GIT Sicherheit - Magazin für Safety und Security“. Band 31, Ausgabe 9, Wiley, 09.2022

/GOO 16/ Goodfellow, I., Bengio, Y., Courville, A.: “Deep Learning”, MIT Press Book, ISBN 978-0262035613, 18.11.2016

/HAN 12/ Handa, A., Newcombe, R.A., Angeli, A., Davison, A.J.: “Real-Time Camera Tracking: When is High Frame-Rate Best?”.
In: Fitzgibbon, A., Lazebnik, S., Perona, P., Sato, Y., Schmid, C. (eds) “Computer Vision – ECCV 2012. ECCV 2012. Lecture Notes in Computer Science”, Band 7578. Springer, Berlin, Heidelberg, “https://doi.org/10.1007/978-3-642-33786-4_17"

/IDE 23a/ IDEMIA Group
“IDEMIA’s facial recognition ranked #1 in NIST’s latest ranking”, Stand 24.02.2023, zuletzt besucht am 7.06.2024
"https://www.idemia.com/press-release/idemias-facial-recognition-ranked-1-nists-latest-ranking-2023-02-24"/IDE 23a/IDEMIA Group:
“IDEMIA’s facial recognition ranked #1 in NIST’s latest ranking”, Stand 24.02.2023, zuletzt besucht am 7.06.2024, erreichbar unter:
https://www.idemia.com/press-release/idemias-facial-recognition-ranked-1-nists-latest-ranking-2023-02-24

/IDE 23b/ Wendland, S., Wendt, N.: „IDEMIA Webinar: Augmented Vision“, Präsentation im Rahmen des Webinars am 11.10.2023

/KIN 13/ Kindt, E.: “Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis”. Springer, Band 12, 2013

/KRU 11/ Kruegle, H.: “CCTV Surveillance: Video Practices and Technology”. ISBN 9780080468181, Elsevier, 15.03.2011

/LAN 24/ Lanum, N. für FOXBusiness: “Google Gemini is 'the tip of the iceberg': AI bias can have 'devastating impact' on humanity, say experts”, Stand 6.03.2024, zuletzt besucht am 13.05.2024, erreichbar unter:
https://www.foxbusiness.com/media/google-gemini-tip-iceberg-ai-bias-devastating-impact-humanity-experts

/LIH 21/ Li, H.; Xiezhang, T.; Yang, C.; Deng, L.; Yi, P.: “Secure Video Surveillance Framework in Smart City”. Sensors, Band 21, 28.06.2021 https://doi.org/10.3390/s21134419

/MAR 18/ Marcus, G.: “Deep Learning: A Critical Appraisal”. Auf arXiv.org: https://doi.org/10.48550/arXiv.1801.00631, Stand 02.01.2018

/MOH 18/ Mohan, A., Kaseb, A., Gauen, K., Lu, Y., Reibman, A., Hacker, T.: “Determining the Necessary Frame Rate of Video Data for Object Tracking under Accuracy Constraints”. EEE Conference on Multimedia Information Processing and Retrieval, 2018 https://doi.org/10.1109/MIPR.2018.00081

/MON 19/ Monroy, M.: “Deutsche Großflughäfen: Gesichtserkennung jetzt auch für Kinder“
Stand. 13.07.2019, zuletzt besucht am 21.06.2024, erreichbar unter: https://netzpolitik.org/2019/deutsche-grossflughaefen-gesichtserkennung-jetzt-auch-fuer-kinder/

/MON 21/ Moncino, K. für Security Magazine:.
“Determining the right combination of visible and thermal imaging for perimeter security”, Stand 25.05.2021, zuletzt besucht am 13.05.2024, erreichbar unter:
https://www.securitymagazine.com/articles/95285-determining-the-right-combination-of-visible-and-thermal-imaging-for-perimeter-security

/OBY 22/ O’Byrne, M., Vibhoothi, Sugrue, M., Kokaram, A.: “Impact of Video Compression on the Performance of Object Detection Systems for Surveillance Applications”. Auf arXiv.org
https://doi.org/10.48550/arXiv.2211.05805, Stand 10.11.2022

/OLA 20/ Olaniyi, O., Bala, J., Ganiyu, S., Wisdom, P.: “A Systematic Review of Background Subtraction Algorithms for Smart Surveillance System” International Journal of Information Processing and Communication, Band 8, S. 35-54, 05.2020

/PAT 21/ Patterson, D., Gonzalez, J., Le, Q., Liang, C., Munguía, L., Rothchild, D., So, D., Texiert, M., Dean, J.: “Carbon Emissions and Large Neural Network Training”. Auf arXiv.org: https://doi.org/10.48550/arXiv.2104.10350, Stand 23.04.2021

/POL 21/ Polizeiliche Informations- und Kommunikationsstrategie und Technik: „Bundeseinheitliche Richtlinien für Überfall-/Einbruchmeldeanlagen bzw. Anlagen für Notfälle/Gefahren mit Anschluss an die Polizei (ÜEA) - (ÜEA Richtlinie)“, Stand 10.2021

/POO 17/ Poole, D., Mackworth, A.: “Artificial Intelligence: Foundations of Computational Agents”. Cambrige Univerty Press, 2. Auflage, S.491 - 542, 2017

/PRN 23/ PR Newswire: „IDEMIA cements biometric technologies leadership in new NIST rankings“ Stand 08.2023, zuletzt besucht am 21.06.2024, erreichbar unter: https://ai-techpark.com/idemia-cements-biometric-technologies-leadership-in-new-nist-rankings/

/SEC 23a/ SecurityRobotics: “Patrouillenroboter mit Wärmeblick: Radgetriebene Roboter sind perfekt für ausgedehnte Outdoor-Überwachung und Inspektionen“ Stand 2023, zuletzt besucht am 10.06-2024, erreichbar unter: https://security-robotics.de/radgetriebene-roboter

/SEC 23b/ SecurityRobotics: “SPOT - der Allrounder: Flexibler Indoor / Outdoot Experte für kleine bis mittelgroße Areale“ Stand. 2023, zuletzt besucht am 10.06.2024, erreichbar unter: https://security-robotics.de/allrounder-spot

/SEC 23c/ SecurityRobotics: “Die Vogelperspektive für beste Übersicht: Flugroboter agieren geländeunabhängig, perfekt für mittelgroße bis große Areale“ Stand. 2023, zuletzt besucht am 10.06.2024, erreichbar unter: https://security-robotics.de/flugroboter

/SMI 12/ Smith, S.: “The Scientist and Engineer's Guide to Digital Signal Processing." California Technical Publishing, 2012

/SMP 24/ SMP Robotics: “S5.2 IR Argus: Thermal imaging dual-spectrum security robot”, Stand 2024, zuletzt besucht am: 10.06.2024, erreichbar unter https://smprobotics.com/security_robot/thermal-security-robot/

/SUN 23/ Sunflower Labs: “Technical Spec”, Stand 08.03.2023, zuletzt besucht am 10.06.2024, erreichbar unter: https://sunflower-labs.com/specs

/SUN 24/ Sunflower Labs: “Frequently Asked Questions”, Stand 2024, zuletzt besucht 10.06.2024, erreichbar unter: https://sunflower-labs.com/specs

/SUR 23/ Surveillance-Video: “How To Choose The Right Lens For Your Surveillance Camera”. Stand 10.05.2023, zuletzt besucht am 13.04.2024, erreichbar unter: https://www.surveillance-video.com/blog/how-to-choose-best-surveillance-camera-lens.html/

/SYN 24/ Synology: “Choose a RAID Type”, Stand 2024, zuletzt besucht am 27.05.2024, erreichbar unter: https://kb.synology.com/en-id/DSM/help/DSM/StorageManager/storage_pool_what_is_raid?version=7

/TOK 23/ Aleksej Tokarev, „Schaden verhüten mithilfe smarter KI-Robotik“, in s+s report 3/2023, VdS Köln, September 2023

/VDE 21/ VDE-AR-E 2842-61-1 Anwendungsregel:2021-07: Entwicklung und Vertrauenswürdigkeit von autonom/kognitiven Systemen, erreichbar unter: https://www.vde-verlag.de/normen/0800738/vde-ar-e-2842-61-1-anwendungsregel-2021-07.html

/VDS 06/ VdS-Richtlinien für Videoüberwachungsanlagen: Systemanforderungen Kategorie I, VdS 2364 : 2006-08 (ENTWURF)

/VDS 08/ VdS-Richtlinien für Videoüberwachungsanlagen: Anforderungen an Videoüberwachungssystem der Kategorie II, VdS 2365 : 2008-10

/VDS 17/ VdS-Richtlinien für Videoüberwachungsanlagen: Planung und Einbau, VdS 2366 : 2017-11

/WDR 24/ Westdeutscher Rundfunk: „KI-Gesetz: Wie die EU die Bürger vor zu gefährlicher KI schützen will“
Stand 21.05.2024, zuletzt besucht am 17.06.2024, erreichbar unter: https://www1.wdr.de/nachrichten/ki-gesetz-100.html

/WES 24/ Western Digital: “What is RAID Storage?”, Stand 2024, zuletzt besucht am 27.05.2024, erreichbar unter: https://www.westerndigital.com/solutions/raid

/ZHA 19/ Zhang, Z.; Jing, T.; Ding, B.; Gao, M.; Li, X.: “A Model-Based Approach of Foreground Region of Interest Detection for Video Codecs”. Applied Sciences, Band 9, 30.06.2019
https://doi.org/10.3390/app9132670

Tabellenverzeichnis

Abkürzungsverzeichnis

A/K	autonom/kognitiv
AtG	Atomgesetz
BAS	Bild-Austast-Synchron
BEZ	Bildempfangszentrale
BÜE	Bildübertragungseinrichtungen
BZ	Bildzentrale
CAPA	Corrective and Preventive Action
CCTV	Closed Circut Television
CNN	Convolutional Neural Network
DSA	Deterministische Sicherungsanalyse
DSGVO	Datenschutz-Grundverordnung
FAR	Falschalarmrate
FRVT	Face Recognition Vendor Tests
FPS	frames per second (Bilder pro Sekunde)
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
HD	High Definition
HEVC	High Efficiency Video Coding
IP	Internet Protocol
KI	Künstliche Intelligenz
KTA	Kerntechnische Anlagen
LiDAR	Light Detection and Radar
NAR	Alarmrate
NIST	National Institute of Standards and Technology
NTSC	National Television systems Committee - Fernsehnorm
PAL	Phase Alternating Line - Fernsehnorm

PTZ	Pan Tilt Zoom (Schenken-Neigen-Zoomen)
RAID	Redundant Array of Independent Disks
RFID	Radio Frequency Identification
RGB	Rot, Grün, Blau
ROI	Region of Interest
SD	Standard Definition
SECAM	Séquentiel couleur à mémoire – Fernsehnorm
SEWD	Störrmaßnahmen oder sonstige Einwirkungen Dritter
SVM	Support Vector Machine
ÜEA	Überfall-/Einbruchmeldeanlgen mit Anschluss an die Polizei
VÜA	Videoüberwachungsanlage
VÜS	Videoüberwachungssystem
WiFi	Wireless Fidelity

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-910548-39-8