

# Neuartiges Konzept der Sicherheitsarchitektur eines Flughafens

## Ganzheitliche Interpretation der Sicherheitsinfrastruktur am Flughafen mithilfe von KI

Luftverkehr, Flughäfen, Security, Digitalisierung, Automatisierung, Künstliche Intelligenz

Sicherheit am Flughafen berührt einen wesentlichen Wert unserer Gesellschaft: sich angstfrei bewegen zu können. Um diesen Wert zu verteidigen, ist es unerlässlich, die Security am Flughafen weiterzuentwickeln. Digitalisierung und Automatisierung stellen eine Möglichkeit der Weiterentwicklung dar. Im vorliegenden Beitrag wird aufbauend auf dieser Entwicklung ein neuartiges Konzept der Sicherheitsarchitektur eines Flughafens vorgestellt. Das Konzept besteht aus einem zentralen KI-System, das alle verfügbaren Informationen, die durch alle Arten von Sensoren geliefert werden, interpretiert und adäquate Aktionen ausführt.

Olaf Milbredt, Andrei Popa, Friederike-Chantal Doenitz, Martin Hellman

**D**ie kommerzielle Luftfahrt ist seit Beginn Ziel krimineller und terroristischer Operationen. Betroffen sind dabei sowohl Flugzeuge, die als Waffe eingesetzt werden, als auch Flughäfen. Dabei wandelten sich die Herangehensweisen und technologischen Mittel der Angreifer ebenso wie die der Luftsicherheit als Reaktion auf Angriffe.

Zunehmend genutzte Methoden im Bereich Luftsicherheit sind Videoerkennung und -analyse sowie Profiling. Darüber hinaus ist gegenwärtig eine zunehmende Erweiterung dieser Methoden durch den Einsatz Künstlicher Intelligenz (KI) zu beobachten, die potentiell einen Mehrwert zur Steigerung der Sicherheit im Flughafen bietet.

Aktuell werden nicht alle Informationen der Luftsicherheit am Flughafen zentral gebündelt und interpretiert. Dies führt zu einer zeitverzögerten Reaktion im Falle eines sicherheitsrelevanten Vorfalls wie z. B. das Identifizieren eines nicht zuzuordnenden Gegenstands (NzG) und dessen Verursachers. Welche gravierenden Folgen ein NzG haben kann, zeigt das durch M. Mücke beschriebene Beispiel am Flughafen Düsseldorf. [1] Dieser war aufgrund eines NzG über mehrere Stunden gesperrt, 10.000 Personen mussten den Flughafen verlassen und insgesamt 140 Flüge fielen aus. Der entstandene Schaden wurde auf einen einstelligen Millionenbereich geschätzt. [1]

In diesem Beitrag wird ein Konzept beschrieben, das sicherheitsrelevante Informationen mithilfe einer KI zentral interpretiert und adäquat agiert. Eine solche KI wertet die von Sensoren im Flughafen gelieferten Informationen aus und führt Aktionen mittels Aktuatoren, wie automatische Türen, aus. Beteiligte Aktuatoren und Sensoren werden in einem Überblick über aktuelle Prozessarten beschrieben. Im Überblick erfolgen eine Einschätzung des Automatisierungsgrades sowie bereits verfügbare Anwendungen von KI. Die verfügbaren Anwendungen von KI sind Insellösungen, da ein Austausch der Informationen und den Ergebnissen nicht vorgesehen ist.

### Evolution der Security-Prozesse am Flughafen

Bis in die 1970er Jahre gab es keinen Grund, besondere Maßnahmen im Bereich der Sicherheit auf Flughäfen zu ergreifen. Seitdem haben zahlreiche Anschläge dazu geführt, dass heute an keinen Verkehrsträger höhere Sicherheitsanforderungen gestellt werden als an den Luftverkehr. Im Rahmen dessen wurden und werden die Empfehlungen und Verordnungen stetig weiterentwickelt. [2, 3] Im ICAO (International Civil Aviation Organization) Annex 17 werden Richtlinien vorgegeben, die für die Mitgliedsstaaten verbindliche, nationalstaatlich umzusetzende Regelungen enthalten. Für die Staaten der

Europäischen Gemeinschaft wurden insbesondere auf Basis dieser Dokumente sowie einer Reihe von sicherheitsrelevanten Ereignissen mit der EU-Verordnung 300/2008 der aktuell geltende, verbindliche und einheitliche Gesetzesrahmen verabschiedet. [4] In Deutschland mündet die Verordnung im Luftsicherheitsgesetz (LuftSiG). [5] *Bild 1* zeigt die Entwicklung dieser nationalen und internationalen Luftsicherheitsregelungen als Folge zahlreicher Anschläge und betont dadurch die Wichtigkeit der Sicherheitskontrollen. Die Einführung einer neuen, verschärfenden Regelung stellt stets die Konsequenz eines Angriffs dar, greift dessen Angriffsmuster auf und zielt darauf ab, genau dieses abzuwehren. In diesem Rahmen sind die im Folgenden beschriebenen Sicherheitsmaßnahmen entstanden.

### Sicherheitssysteme, ihre Sensoren und Aktuatoren

In diesem Abschnitt werden die üblichen Security-Stationen innerhalb des Flughafens betrachtet, mit denen der Passagier sowie das Gepäck in Berührung kommen (s. *Bild 2*). [7, 8] Dabei werden die Prozessarten, die Einschätzung des Automatisierungsgrades (s. *Bild 3*), die identifizierten Sensoren und Aktuatoren sowie bereits verfügbare Anwendungen von KI behandelt. Bei der Beschreibung aller Sicherheitsprozesse wurde berücksichtigt, dass falls eine Störung, Auf-

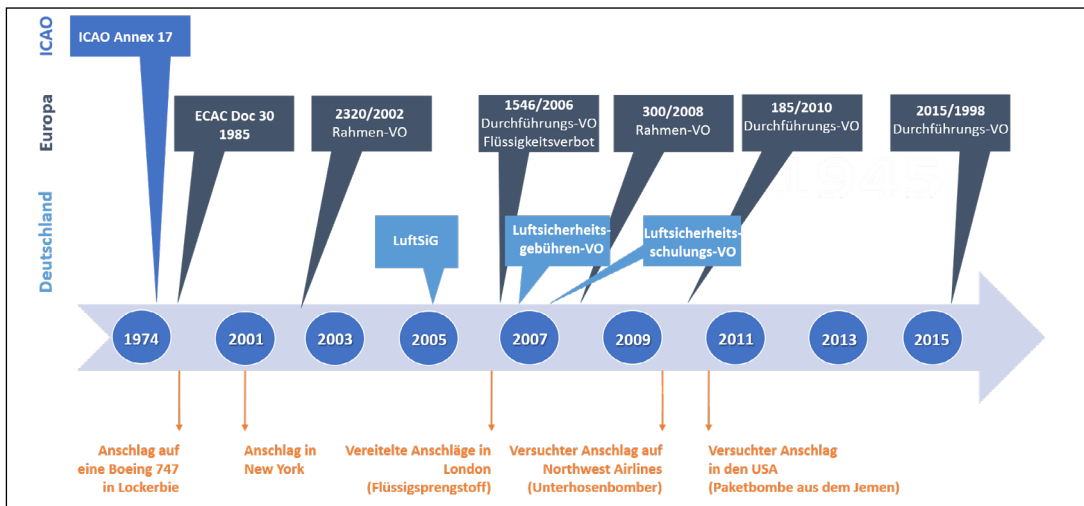


Bild 1: Evolution der Security-Prozesse am Flughafen [6]

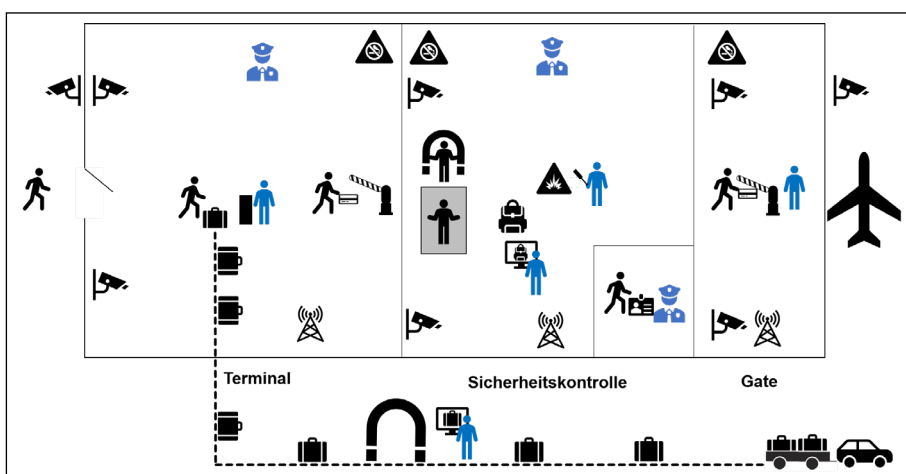


Bild 2: Abflugprozesse von Passagier und Gepäck in Flughäfen

Eigene Darstellung

fälligkeit oder Alarm auftreten, eine manuelle Kontrolle durchgeführt wird. Dies wurde bei der Einschätzung des Automatisierungsgrades berücksichtigt.

### Sicherheitsprozesse zur Passagierabfertigung

Der Prozess für Passagiere, vom Erwerb des Tickets bis zum Abflug, ist komplex und besteht aus vielen Stationen bezüglich Sicherheit im Sinne von Security. Nach Angaben der amerikanischen TSA (Transportation Security Administration) gibt es sichtbare und unsichtbare Verfahren. Dabei beginnen die Sicherheitsmaßnahmen bereits lange vor der Ankunft am Flughafen. [9]

Beim Kauf des Tickets findet die erste Sicherheitskontrolle statt, indem der Name des Passagiers mit verschiedenen Datenbanken verglichen wird. Die Übermittlung der dabei verwendeten Fluggastdaten erfolgt hochautomatisiert (s. Bild 3). [9]

Voraussetzung für einen Flug ist eine gültige Bordkarte, die der Passagier durch den Check-in erhält. Dieser Prozess kann online, am Automaten oder am Schalter

durchgeführt werden. Dabei wird der Ausweis des Fluggastes mit der Person verglichen, um dem Fluggast anschließend eine Bordkarte auszustellen. [9] Dafür werden Daten wie Name, Geburtsdatum und Ausweisnummer hinterlegt, welche mit Datenbanken unerwünschter Personen verglichen werden. [9, 10] Der Automatisierungsgrad beim Online-Check-in oder am Automaten ist hoch einzuschätzen, da i. d. R. kein Personal vonnöten ist. Beim Check-in am Schalter hingegen wird der Prozess mittels Personals ausgeführt. Die in Bild 3 dargestellte Einschätzung besteht aus dem Mittelwert der einzelnen Einschätzungen zum Automatisierungsgrad aller drei Ausführungsarten. Beim Online-Check-in werden eine Tastatur und eine Kamera als Sensoren eingesetzt und als Ergebnis ein elektronisches Dokument bereitgestellt. Beim Check-in per Automat werden ein Lesegerät und eine Tastatur als Sensoren verwendet und ebenso ein Dokument bereitgestellt.

Durch das Scannen der Bordkarte erlangt der Passagier Zutritt zu den Sicherheitskontrollen, die sich zwischen Land- und Luftsei-

te des Flughafens befinden. Seit 2017 haben jedoch einige US-Flughäfen von der TSA die Erlaubnis erhalten, ein Besucherprogramm anzubieten, das Besuchern auch ohne Ticket den Zugang zur Luftseite des Flughafens ermöglicht. [11] Der Sensor ist in diesem Prozess ein Lesegerät und der Aktuator eine automatische Tür. Folglich ist der Automatisierungsgrad beim Zutritt zu den Sicherheitskontrollen als sehr hoch einzuschätzen.

Innerhalb der Sicherheitskontrollen besteht der nächste Schritt aus der Durchleuchtung der Passagiere und deren Handgepäck. [12] Die Sicherheitskontrollen bestehen aus einer Personenkontrolle sowohl mittels Körperscanner oder Metalldetektor und Sprengstoffspürgeräten als auch der Handgepäckkontrolle mithilfe von X-Ray-Systemen oder CT-Scannern sowie Sprengstoffspürgeräten. Diese Geräte dienen als Sensoren und das Sicherheitspersonal als Aktuatoren.

Die Algorithmen der Körperscanner interpretieren mittels KI ein Abbild der Person und erkennen dabei nicht zugelassene Gegenstände sowie Plastik- und Flüssigsprengstoff. [13] Der Automatisierungsgrad der Sicherheitskontrollen mittels Metalldetektor ist geringer einzuschätzen als der mittels Körperscanner, da letzterer detaillierteren Aufschluss über verborgene Gegenstände gibt. [14, 15]

Für die Handgepäckkontrolle werden konventionelle X-Ray-Systeme oder CT-Scanner verwendet. Neuartige CT-Systeme ersparen dem Passagier das Entnehmen von Gegenständen aus dem Handgepäck. [15, 16, 17] Aufgrund dessen ist der Automatisierungsgrad der CT-Scanner als hoch einzuschätzen mit dem Potential des Einsatzes von KI. [18]

Zur Ausreise der Passagiere vom Abflughafen ist im Non-Schengen-Bereich (EU) und im Non-Pre-Clearance-Bereich (USA, Kanada, Irland) eine Pass- bzw. Grenzkon-

trolle notwendig. Diese kann sowohl durch Personal als auch durch Automaten durchgeführt werden. Der Automatisierungsgrad kann daher als niedrig eingeschätzt werden. [19] Es werden jedoch auch KI-Systeme, wie z. B. beim System EasyPASS, eingesetzt, die zur Identitätsprüfung Gesichter und Fingerabdrücke vergleichen. [20, 21, 22, 23] Dabei werden Kameras und Lesegeräte als Sensoren und automatische Türen als Aktuatoren eingesetzt.

Die letzte Kontrolle vor dem Boarding stellt die Bordkartenüberprüfung am Gate dar. Diese kann sowohl durch Personal als auch durch einen Automaten stattfinden. Der Automatisierungsgrad bei Automaten ist als hoch einzuschätzen, da dabei Lesensensoren zum Einsatz kommen, die zusätzlich biometrische Daten überprüfen können. [24] Der Aktuator besteht aus einer automatisch steuerbaren Schranke.

### Sicherheitsprozesse für Reisegepäckabfertigung

Nach dem Einchecken durch den Passagier bringt ein Mitarbeiter des Flughafens oder der Passagier selbst ein Label an den Koffer an, das sogenannte Baggage Source Message, das Flugnummer, Flugdatum, Flugziel sowie den Passagiernamen und eine sogenannte Licence Plate Number enthält. Anschließend wird das Gepäck vollautomatisch auf einem Fördersystem transportiert. [25]

Ähnlich wie beim Durchleuchten des Handgepäcks, wird das Reisegepäck ebenfalls mit CT-Scannern überprüft. [19, 26] Folglich ist der Automatisierungsgrad, analog zur Handgepäckkontrolle, als hoch einzuschätzen. Weiterhin werden Sprengstoffspürhunde eingesetzt, um das Reisegepäck auf gefährliche Substanzen zu überprüfen. Diese sind jedoch nur begrenzt einsetzbar, da sie nach jedem Einsatz eine Pause benötigen. [27]

### Sicherheitsprozess der Raumüberwachung

Dieser Prozess behandelt die Überwachung des Terminals zum Aufspüren verdächtigen Verhaltens oder von Gegenständen (NzG). Weiterhin werden dadurch Personendichten bestimmt und Personenprozesse optimiert. [28] Dieser Prozess wird durch Polizisten auf Streife, Kameras und Ortung von Passagieren durchgeführt. [9, 29]

Polizisten fungieren sowohl als Sensoren als auch als Aktuatoren, indem diese durch das Beobachten einen Alarm auslösen können. Die Polizeistreife weist nur geringe Möglichkeiten zur Automatisierung auf. [30]

Kameras dienen als Sensoren der Raumüberwachung in Form von Bild und Temperatur von Passagieren. Letzteres dient dem

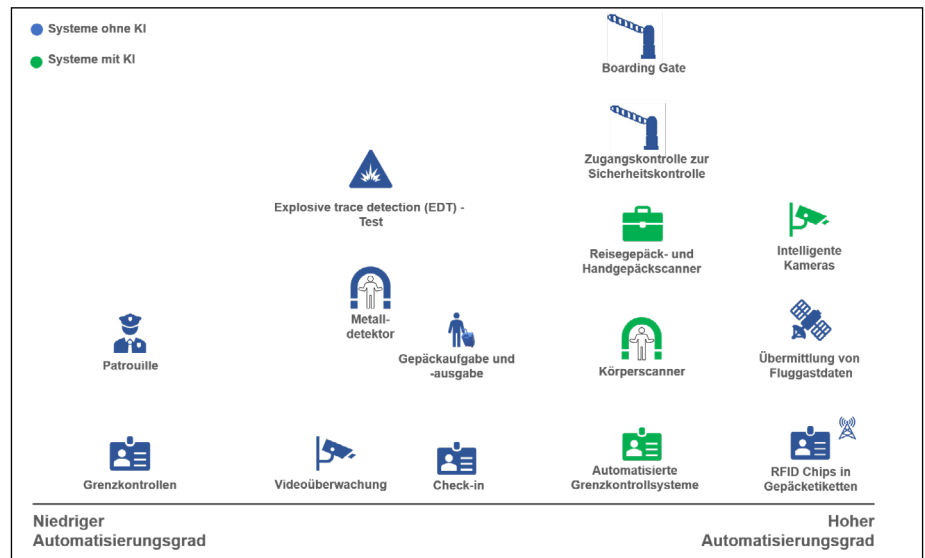


Bild 3: Einschätzung des Automatisierungsgrades der Sicherheitsprozesse an Flughäfen basierend auf dem aktuellen Marktangebot und nicht nach dem Einsatz der Systeme.

Eigene Darstellung

Infektionsschutz. [31] Weiterhin kann im Rahmen dessen verdächtiges Verhalten von Personen detektiert sowie mit dem Brandmeldesystem mit intelligenten Algorithmen verbunden werden, um Rauch und Feuer zu erkennen. [31] Aktuatoren im Brandalarmfall sind, neben Fachpersonal, automatisch gesteuerte Brandtüren und Löschsysteme. Der Automatisierungsgrad ist als sehr hoch einzuschätzen, da das aufgenommene Bild durch Video Analytics behandelt wird. [29]

### Einsatz der Künstlichen Intelligenz in der Flughafensicherheit

Die zuvor beschriebenen Prozesse sind komplex, mit Personalaufwand verbunden und müssen sich in Zukunft auf sich verändernde Bedrohungslagen anpassen können. Dabei müssen auf hohem Sicherheitsniveau Qualität, Komfort und Effizienz erhöht werden. Durch den hohen Kostendruck muss die Ausgestaltung der Prozesse ökonomisch sinnvoll erfolgen.

Die Verwendung von KI bietet einen Ansatz, um diesen Herausforderungen entgegenzutreten. Im Gegensatz zu Menschen, kann KI schnellere Entscheidungen treffen, Probleme mit weniger Unsicherheit in kürzerer Zeit lösen und ständig verfügbar sein. [32] Außerdem ist die menschliche Entscheidungsfindung mit Fehlern behaftet. Diese Fehler können durch den Einsatz von KI reduziert werden. [33] Ein Nachteil besteht in der fehlenden Flexibilität bei veränderten Rahmenbedingungen.

Aktuell wird KI in bestimmten Bereichen unabhängig voneinander eingesetzt. Nachfolgend werden Beispiele über die in den Prozessbeschreibungen hinausgehende Einbindung von KI am Flughafen dargestellt.

Eines davon stellt die intelligente Videoüberwachung dar, die durch KI interpretiert wird. Dabei lernt das System selbstständig, Unregelmäßigkeiten im Sicherheitsbereich zu erkennen und zu melden. [34]

iBorderCtrl als weiteres Beispiel stellt ein KI-basiertes System zum psychologischen Profiling dar. Dabei geht es um die automatische Erkennung von Täuschungen in Echtzeit durch die Analyse der nonverbalen Mikroausdrücke von Menschen. [35]

Ein weiteres KI-basiertes System ist die Überwachung der Hochsicherheitsbereiche, die nur für befugtes Personal zugänglich sind. Dieses System verwendet elektronische Tore in Verbindung mit Bewegungssensoren und verschiedene Arten von Kameras. [36]

Diese sowie die zuvor beschriebenen Beispiele agieren unabhängig voneinander und stellen somit Insellösungen dar. Zwischen den einzelnen KI-Systemen ist kein Informationsaustausch vorgesehen. Somit kann kein Gesamtbild der Sicherheitslage erstellt werden. Um diese Herausforderung zu überwinden, wird nachfolgend eine KI-Lösung vorgeschlagen, die Zugriff auf alle sicherheitsrelevanten Systeme hat.

### Gesamtheitliches KI-System für die Flughafensicherheit

In Bild 4 ist ein Schema des Informationsflusses der KI dargestellt. Es sind verschiedene Bereiche des Flughafens mit Sensoren (blau) und Aktuatoren (grün) abgebildet. In der oberen Hälfte befinden sich die o.g. Security-Prozesse. Durch die Einbeziehung von Safety (in der unteren Hälfte) ist die KI in der Lage, gegenseitige Auswirkungen zu erkennen.

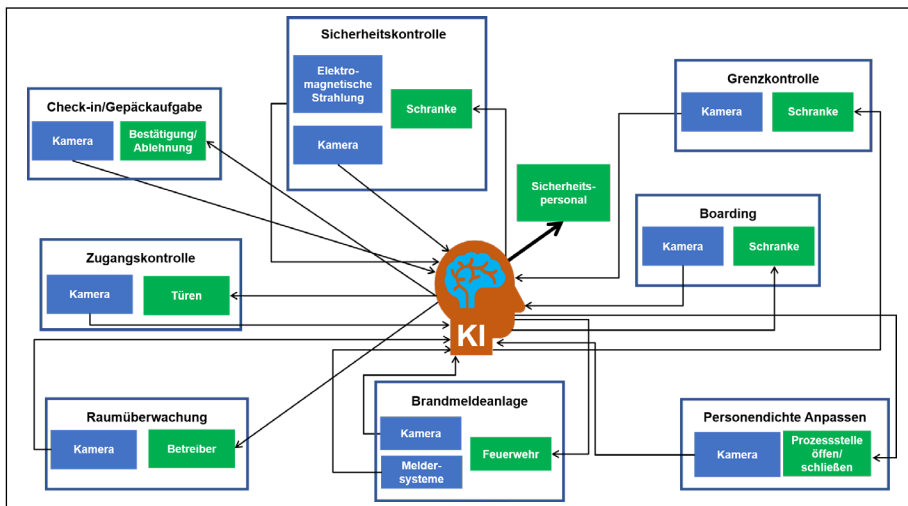


Bild 4: Schema zum Einsatz von KI in verschiedenen Bereichen von Security und Safety  
Eigene Darstellung

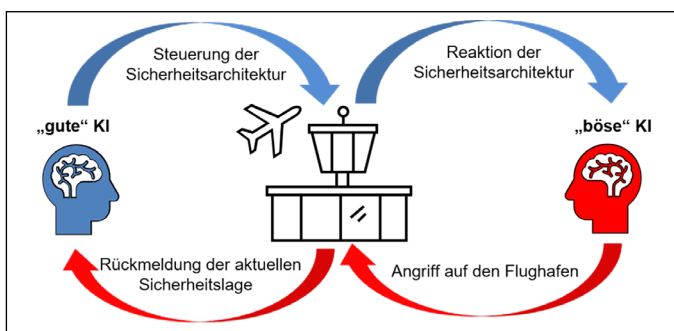


Bild 5: E<sup>2</sup>S<sup>2</sup>AI Methode, zwei KI-Systeme treten zur Verbesserung der Sicherheit am Flughafen gegeneinander an.  
Eigene Darstellung

Safety (Unfallvermeidung) und Security (Kriminalprävention) sind per Definition zwei getrennte Bereiche. Safety kann jedoch Auswirkungen auf Security haben und umgekehrt. Aus diesem Grund ist ein Gesamtkonzept nötig, das im Kontext des Managements – insbesondere von kritischen Infrastrukturen wie einem Flughafen – beide Bereiche abdeckt. Unser Vorschlag für ein solches Konzept besteht aus einem zentral zu steuernden und interpretierenden KI-System. Dieses soll durch die Auswertung der oben genannten Sensoren und deren Interpretation koordinierte Angriffsvektoren erkennen und adäquat reagieren. Dies bedeutet, dass der Angreifende an mehreren Stellen des Sicherheitssystems ansetzt. Durch die Steuerung mithilfe eines zentralen KI-Systems kann die Regelung der Aktuatoren über Bereichsgrenzen hinweg angepasst werden.

Ein Beispiel für die Notwendigkeit des Einbeziehens von Safety ist das fälschliche Auslösen eines Feueralarms mit anschließender Evakuierung in einen durch Angreifer gefährdeten Bereich. Rauchmelder bieten die Möglichkeit, mittels Lasersensoren, Temperaturmessung und Kameras bzw. Videotechnik, auf Brandspuren in der Luft zu reagieren. Dadurch werden Fluchtwegtüren und Rauchabzugsöffnungen im Fall eines

Brandes automatisch geöffnet, wichtige Türen geschlossen und eine Notbeleuchtung eingesetzt. [37] Die Sensoren können jedoch bspw. durch den Stand der Sonne in einem ungünstigen Winkel einen Fehlalarm auslösen. [38] Somit besteht die Möglichkeit, dass Terroristen durch die Manipulation dieser Sensoren einen Alarm auslösen und die Reaktion für einen Anschlag ausnutzen. Dieses Ausnutzen kann z. B. aus dem gezielten Platzieren eines Sprengsatzes – getarnt als NzG – entlang des Evakuierungsweges der Passagiere bestehen. Eine KI, die Zugriff auf Informationen der Rauchmelder besitzt, kann durch Abgleich von Daten verschiedener Sensoren eine mögliche Manipulation erkennen. Zusätzlich kann eine solche KI durch den Zugriff auf Informationen der Raumüberwachung eine Zeitgleichheit des Auftretens eines Feueralarms und eines NzG im Evakuierungsweg erkennen. Auf Basis dieser Erkenntnis werden die zuständigen Stellen mit Handlungsempfehlungen alarmiert.

Ein weiterer Vorteil dieses Gesamtsystems ist das in Beziehungsetzen von unterschiedlichen Security-Aspekten. So kann z. B. die durch KI angereicherte Raumüberwachung ein NzG im Terminal mit dem Verhalten des Verursachers in Verbindung setzen. Der Verursacher wird durch das System

mittels Raumüberwachung detektiert und zeitgleich erkennt die KI verdächtiges Verhalten des Verursachers. Das zentrale KI-System erfasst eine kritische Situation und führt eine Gesichtserkennung des Verursachers durch. Mit Hilfe der durch die Gesichtserkennung ermittelten Daten wird in zur Verfügung stehenden Datenbanken nach Ähnlichkeiten gesucht. Ein Bild des Verursachers zusammen mit den Ergebnissen dient als Basis für die Aktionsempfehlung für die Aktuatoren, in diesem Fall das Sicherheitspersonal.

Ein solches Gesamtsystem muss auf jeden Flughafen zugeschnitten sein, da jeder einzelne Flughafen, z. B. im Hinblick auf Layout und Sicherheitsarchitektur, individuell gestaltet ist. Die Verantwortlichen für die Sicherheit eines Flughafens können so ein Gesamtsystem realisieren, indem sowohl die Auswertung als auch die Steuerung zentralisiert werden. Um ein System zu erhalten, welches die Interpretation der Daten übernimmt, schlagen wir ein an die Sicherheitsarchitektur angepasstes KI-System vor. Damit dieses KI-System etwaige Bedrohungen erkennt und adäquat darauf reagiert, ist ein Lernprozess notwendig. Dieser kann z. B. mithilfe von Szenarien erfolgen. Im DLR-Projekt E<sup>2</sup>S<sup>2</sup>AI (Evaluation and Evolution of Safety and Security with Simulation Based Artificial Intelligence) wird ein anderer Ansatz verfolgt. Das KI-System lernt, indem es unterschiedliche Aktionen innerhalb der Sicherheitsarchitektur ausführt. Die Rückmeldung an das KI-System über den Erfolg oder Misserfolg der Aktion versetzt dieses in die Lage, zu lernen. Um das Potenzial dieser Lernmethode zu nutzen, ist es vorteilhaft, eine Symmetrie herzustellen, sodass das System gegen sich selbst in einen Wettbewerb treten kann. Aus diesem Grund wird ein weiteres System eingeführt, um die Schwächen der Reaktion des ersten zu testen. Beide Systeme lernen, indem sie auf die Aktion des anderen reagieren (s. Bild 5). Da beide KI-Systeme an die Sicherheitsarchitektur eines Flughafens angepasst sind, können sie wertvolle Hinweise zur Verbesserung von Safety und Security eines Flughafens geben.

### Fazit und Ausblick

Die Abwehr von kriminellen und terroristischen Operationen gestaltet sich zunehmend komplexer. Neue Methoden der Angriffe – insbesondere durch Digitalisierung und Automatisierung – stellen eine große Herausforderung dar. Digitalisierung und Automatisierung bieten gleichzeitig eine Chance, dieser Herausforderung zu begegnen.

In diesem Beitrag wird ein Konzept dargestellt, welches sicherheitsrelevante Infor-



mationen mithilfe einer KI zentral interpretiert und adäquat agiert. Zur Beschreibung des Konzepts werden die Sicherheitsprozesse am Flughafen, die identifizierten Sensoren und Aktuatoren sowie bereits verfügbare Anwendungen von KI dargestellt. Aus der Schilderung der Sicherheitsprozesse wird deren Automatisierungsgrad eingeschätzt.

Die Analyse der Sicherheitsprozesse zeigt in vielen Bereichen einen fortgeschrittenen Automatisierungsgrad und eine verbreitete Anwendung von KI. Jedoch handelt es sich dabei um Insellösungen für spezielle Aufgaben, wie z. B. Gesichtserkennung. Die eingesetzten Systeme sehen keinen Informationsaustausch zwischen den einzelnen KI-Anwendungen vor.

Im Gegensatz zu den aktuell eingesetzten KI-Systemen ist das in diesem Beitrag vorgestellte Konzept in der Lage, koordinierte Angriffsvektoren zu erkennen und adäquat zu reagieren. Durch KI erweiterte Raumüberwachung kann z. B. eine Verbindung zwischen einem NzG im Terminal und dem Verhalten des Verursachers herstellen. Die ermittelten Informationen und entsprechende Handlungsempfehlungen werden unmittelbar den Verantwortlichen zur Verfügung gestellt.

Im DLR-Projekt E<sup>2</sup>S<sup>2</sup>AI werden methodische Grundlagen für dieses Konzept und dessen Machbarkeit untersucht. Dabei wird ein KI-System entwickelt, das die Sicherheit im Sinne von Safety und Security am Flughafen erhöhen soll. Dieses System besteht aus zwei Komponenten, die sich gegenseitig herausfordern. Dieses Vorgehen führt dazu, dass unvorhergesehene Angriffsarten und die passende Reaktion erlernt werden.

Anschließend ist angestrebt, die in E<sup>2</sup>S<sup>2</sup>AI entwickelte Methode mit den Gegebenheiten der Sicherheitslandschaft eines Flughafens zu testen. Darüber hinaus sollen der Datenschutz und die Akzeptanz eines solchen Systems evaluiert werden. ■

## LITERATUR

- [1] Neue Rhein/Ruhr Zeitung (2013): Millionenschaden wegen Evakuierung des Flughafens Düsseldorf nach Kofferfund. [www.nrz.de/staedte/duesseldorf/millionenschaden-wegen-evakuierung-des-flughafens-duesseldorf-nach-kofferfund-id8535800.html](http://www.nrz.de/staedte/duesseldorf/millionenschaden-wegen-evakuierung-des-flughafens-duesseldorf-nach-kofferfund-id8535800.html) (Abruf: 04.05.2022).
- [2] Flughafenverband ADV (2017): Kosten der Luftsicherheit. [www.adv.aero/wp-content/uploads/2017/05/Luftsicherheit-im-Blick\\_klein.pdf](http://www.adv.aero/wp-content/uploads/2017/05/Luftsicherheit-im-Blick_klein.pdf) (Abruf: 14.12.2020).
- [3] Flughafenverband ADV (2019). In: Kosten der Luftsicherheit. [www.adv.aero/fachbereiche/flughafen-management/luftsicherheitsgebuehren/](http://www.adv.aero/fachbereiche/flughafen-management/luftsicherheitsgebuehren/) (Abruf: 04.05.2022).
- [4] Amtsblatt der Europäischen Union (2008): Verordnung (EG) Nr. 300/2008 des europäischen Parlaments und des Rates. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0300&from=DE> (Abruf: 30.03.2022).
- [5] Gesetze im Internet: Luftsicherheitsgesetz (LuftSiG). [www.gesetze-im-internet.de/luftsig/BjNR007810005.html](http://www.gesetze-im-internet.de/luftsig/BjNR007810005.html) (Abruf: 14.12.2020).
- [6] Laskowski, J. (2017): Evolution of the civil aviation security standards in the European Union. In: Transportation Overview, DOI: 10.35117/A\_ENG\_17\_11\_03.
- [7] ACI Europe (2019): Why airports are investing in automation. [www.airport-business.com/2019/06/airports-investing-automation/](http://www.airport-business.com/2019/06/airports-investing-automation/) (Abruf: 26.10.2021).
- [8] Flughafenverband (2017): Luftsicherheit im Blick. [www.adv.aero/wp-content/uploads/2017/05/Luftsicherheit-im-Blick\\_klein.pdf](http://www.adv.aero/wp-content/uploads/2017/05/Luftsicherheit-im-Blick_klein.pdf) (Abruf: 26.10.2021).
- [9] TSA (2021): Security Screening. [www.tsa.gov/travel/security-screening](http://www.tsa.gov/travel/security-screening) (Abruf: 14.12.2020).
- [10] European Parliament (2016): Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&rid=5> (Abruf: 30.03.2022).
- [11] Baskas, H. (2021): Most airport visitor pass programs back up and running. In: The Points Guy. [www.thepointsguy.com/news/airport-visitor-pass-programs-running](http://www.thepointsguy.com/news/airport-visitor-pass-programs-running) (Abruf: 03.04.2022).
- [12] Flughafen München (2021): Ihr Weg durch die Kontrollstellen. [www.munich-airport.de/sicherheits-und-passkontrolle-3897036](http://www.munich-airport.de/sicherheits-und-passkontrolle-3897036) (Abruf: 14.12.2020).
- [13] Europäische Kommission (2010): Mitteilung der Kommission an das europäische Parlament und den Rat über den Einsatz von Sicherheitsscannern auf EU-Flughäfen.
- [14] Munich Airport (2021): The quickest way to your gate: Security screening – smoother than ever.
- [15] Kroschwald, S. (2012): Sicherheitsmaßnahmen an Flughäfen im Lichte der Grundrechte. In: FORUM Wirtschaftsrecht – Band 11.
- [16] Amtsblatt der Europäischen Union (2010): VERORDNUNG (EU) Nr. 185/2010 DER KOMMISSION. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32010R0185&from=PL> (Abruf: 30.03.2022).
- [17] Süddeutsche Zeitung (2009): Flüssigkeiten im Handgepäck. Shampoo oder Sprengstoff? [www.sueddeutsche.de/reise/fluessigkeiten-im-handgepaeck-shampoo-oder-sprengstoff-1.38520](http://www.sueddeutsche.de/reise/fluessigkeiten-im-handgepaeck-shampoo-oder-sprengstoff-1.38520) (Abruf: 30.03.2022).
- [18] Aero International (2018): CT-Scanner soll Handgepäck am New Yorker Flughafen untersuchen. [www.aerointernational.de/airports-nachrichten/ct-scanner-soll-handgepaeck-am-new-yorker-flughafen-untersuchen.html](http://www.aerointernational.de/airports-nachrichten/ct-scanner-soll-handgepaeck-am-new-yorker-flughafen-untersuchen.html) (Abruf: 30.03.2022).
- [19] Milbredt, O.; Popa, A.; Doenitz, F.; Hellmann, M. (2022): Automation of Aviation Security. Outlook of Level of Automation of Security and its Impact. In: Journal of Airport Management, Volume 16 (2), Henry Stewart Publications. ISSN 1750-1958.
- [20] GIT Sicherheit (2013): Sicherheit für öffentliche Bereiche – von Retail bis Flughafen. [www.git-sicherheit.de/nachrichten/sicherheit-fuer-oeffentliche-bereiche-von-retail-bis-flughafen](http://www.git-sicherheit.de/nachrichten/sicherheit-fuer-oeffentliche-bereiche-von-retail-bis-flughafen) (Abruf: 26.10.2021).
- [21] Miami Airport (2021): Airport Security. [www.miami-airport.com/airport-security.asp](http://www.miami-airport.com/airport-security.asp) (Abruf: 14.12.2021).
- [22] CBP U.S. Customs and Border Protection (2021): Preclearance. [www.cbp.gov/travel/preclearance](http://www.cbp.gov/travel/preclearance) (Abruf: 14.12.2021).
- [23] German Federal Police (2021): EasyPASS-RTP.
- [24] Dormakaba (2021): Hoher Passagierkomfort. Mit sicheren Zugangslösungen für Flughäfen. [www.dormakaba.com/resource/blob/1165296/a9749fd3a98a055b046c64948237a4bd/dwl-200831-vertical-airport-de-data.pdf](http://www.dormakaba.com/resource/blob/1165296/a9749fd3a98a055b046c64948237a4bd/dwl-200831-vertical-airport-de-data.pdf) (Abruf: 21.11.2021).
- [25] SICK Sensor Intelligence (2021): Herausforderungen Detektieren. [www.sick.com/de/de/branchen/flughafen/c/g288273?q=Def\\_Type:Application](http://www.sick.com/de/de/branchen/flughafen/c/g288273?q=Def_Type:Application) (Abruf: 26.10.2021).
- [26] Bundespolizei Forschungs- und Erprobungsstelle (o. J.): Aktuelle Entwicklungen im Bereich Luftsicherheitskontrolltechnik. Präsentation.
- [27] Munich Airport (2022): Schmugglern auf der Spur. Zollfahnder am Flughafen München. [www.munich-airport.de/schmugglern-auf-der-spur-2478825](http://www.munich-airport.de/schmugglern-auf-der-spur-2478825) (Abruf: 03.04.2022).
- [28] Mörer-Funk, A.; Odrich, P. (2016): Fluggäste lassen sich per Bluetooth erfassen und zum Gate steuern. [www.ingenieur.de/technik/produkte/fluggaeste-lassen-bluetooth-erfassen-gate-steuern/](http://www.ingenieur.de/technik/produkte/fluggaeste-lassen-bluetooth-erfassen-gate-steuern/) (Abruf: 26.10.2021).
- [29] Bonn International Center for Conversion (2008): Innovationen zum Schutz deutscher Flughäfen vor Anschlägen 2008.
- [30] Bundespolizei (2022): Die Luftsicherheit. „Ein guter Platz, um seine Karriere zu starten.“. [www.komm-zur-bundespolizei.de/einsatzbereiche/luftsicherheit](http://www.komm-zur-bundespolizei.de/einsatzbereiche/luftsicherheit) (Abruf: 04.05.2022).
- [31] Bosch Security and Safety Systems (2021): Sicherheitslösungen für Flughäfen – Vorfälle managen, Abläufe unterstützen und die Sicherheit verbessern. [www.boschsecurity.com/de/de/industrie/flughafen/](http://www.boschsecurity.com/de/de/industrie/flughafen/) (Abruf: 26.10.2021).
- [32] Kikuchi, S. (2012): Artificial Intelligence Applications to Critical Transportation Issues, Transportation Research Board of the National Academies, <http://onlinepubs.trb.org/onlinepubs/circulars/ec168.pdf> (Abruf: 04.05.2022).
- [33] Mezher, T.; Asem, M.; Maarouf, B., (1998): Embedding critics in decision-making environments to reduce human errors. Knowledge-Based Systems, 11, pp. 229–237, DOI: 10.1016/S0950-7051(98)00072-0.
- [34] Donadio, F.; Frejaville, J.; Larnier, S.; Vetaut, S. (2018): Artificial Intelligence and Collaborative Robot to Improve Airport Operations. In M.E. Auer and D.G. Zutin (eds.): Online Engineering & Internet of Things, Lecture Notes in Networks and Systems 22, Springer International Publishing AG, Cham, Switzerland, pp. 973.
- [35] Jupe, L.M.; Keatley, D.A. (2019): Airport artificial intelligence can detect deception: or am I lying? In: Security Journal, DOI: 10.1057/s41284-019-00204-7.
- [36] Koroniotis, N.; Nour, M.; Schiliro, F.; Gauravaram, P.; Janicke, H. (2020): A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. In: IEEEAccess, Volume 8, DOI: 10.1109/ACCESS.2020.3036728.
- [37] IKZ (2008): Umfassende Brandschutzlösungen für Flughäfen, S. 32–33. [www.ikz.de/uploads/media/IKZF\\_200810\\_1775\\_Reportage.pdf](http://www.ikz.de/uploads/media/IKZF_200810_1775_Reportage.pdf) (Abruf: 04.05.2022).
- [38] Berliner Morgenpost (2021): Feueralarm am Flughafen BER – bei ungünstigem Sonnenschein. [www.morgenpost.de/flughafen-BER/article231725619/Brandmelder-fuehrten-zu-Fehlalarm-am-BER.html](http://www.morgenpost.de/flughafen-BER/article231725619/Brandmelder-fuehrten-zu-Fehlalarm-am-BER.html) (Abruf: 04.05.2022).



**Olaf Milbredt**, Dr. rer. nat.  
Wissenschaftlicher Mitarbeiter,  
Informationsgewinnung und  
Modellierung, Institut für Verkehrs-  
systemtechnik, Deutsches Zentrum  
für Luft- und Raumfahrt e.V.,  
Braunschweig  
[olaf.milbredt@dlr.de](mailto:olaf.milbredt@dlr.de)



**Andrei Popa**, Dipl.-Wirtsch.-Ing. (FH),  
M.A.  
Wissenschaftlicher Mitarbeiter, Design  
& Bewertung von Mobilitätslösungen,  
Deutsches Zentrum für Luft- und  
Raumfahrt e.V. (DLR), Institut für  
Verkehrssystemtechnik, Braunschweig  
[andrei.popa@dlr.de](mailto:andrei.popa@dlr.de)



**Friederike-Chantal Doenitz**, M. Sc.  
Absolventin Technologie-orientiertes  
Management, Carl-Friedrich-Gauß  
Fakultät, Technische Universität  
Braunschweig  
[friederike.doenitz@t-online.de](mailto:friederike.doenitz@t-online.de)



**Martin Hellman**, Dr.-Ing.  
Programm und Strategie: Sicherheits-  
und Verteidigungsforschung,  
Deutsches Zentrum für Luft- und  
Raumfahrt e.V. (DLR), Köln  
[martin.hellmann@dlr.de](mailto:martin.hellmann@dlr.de)