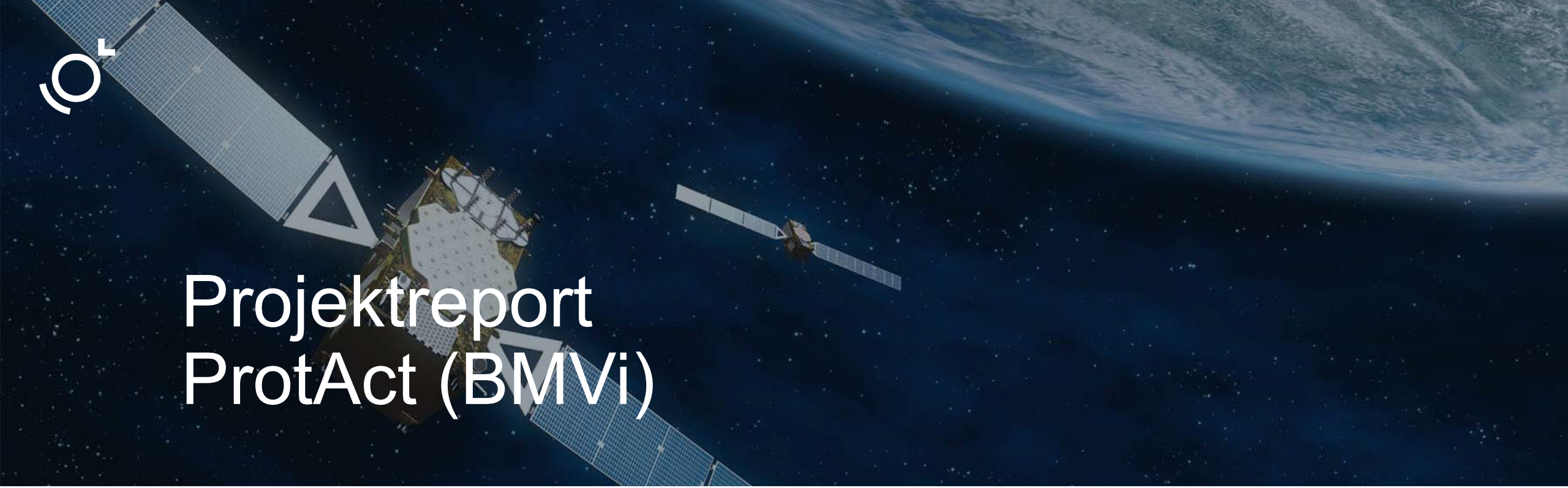
DLR Gesellschaft für
Raumfahrtanwendungen



Projektreport ProtAct (BMVi)

ProtAct

Referenzverfahren zum Schutz kritischer Infrastrukturen vor unbemannten Luftfahrtsystemen – *Bundesministerium für Verkehr und digitale Infrastruktur*

a company of DLR

Projektreport.

- ProtAct (BMVi)
  - Zuwendungsbescheid in 2019
    - Entwicklung eines Referenzverfahren zum Schutz kritischer Infrastrukturen vor unbemannten Luftfahrtsystemen
    - High-Level Workshop zum Thema Drohnendetektion und Drohnenbetrieb (GCC - Januar 2020)
    - Publikationen (Print/Online) für fachfremdes Publikum sowie vom Experten für Experten
    - Öffentlichkeitsarbeit – Podiumsdiskussion im Rahmen der Messe UT-Sec. Nürnberg (COVID 19 bedingt abgesagt -> Entwicklung eines neuen Konzeptes)

    - Realisierung einer Onlinekampagne zum Thema Drohnendetektion und Drohnenbetrieb

Inhaltsverzeichnis

1. Gefährdung kritischer Infrastrukturen (KRITIS) durch nicht kooperative Drohnen
2. Anwendungen
3. Regularien
4. Anforderungen an das System
5. Risikobewertung (Schutzmaßnahmen und potenzielle Anwendungen)
6. System Architektur
7. Referenzverfahren
8. Übersicht Systemhersteller

Gefährdung kritischer Infrastrukturen durch nicht kooperative Drohnen

Die Gefährdung von kritischen Infrastrukturen durch nicht kooperative Drohnen, wie beispielsweise die eines Flughafens o.a., wird auf Grund der stetig anhaltenden positiven Marktentwicklung im Bereich unbemannter Fluggeräte wie Drohnen, zukünftig Betreibern kritischer Infrastrukturen vor sicherheitskritischen Aufgaben und Herausforderungen stellen. Eine Implementierung von entsprechenden Drohnenabwehrsystemen wird somit unabdingbar, welche nicht nur für den Schutz von kritischen Infrastrukturen verantwortlich sein werden, sondern auch eine Vielzahl von Drohnenanwendungen innerhalb des geschützten Bereiches, wie beispielsweise Monitoring Aufgaben oder Überwachungsaufgaben, ermöglichen werden.

Das folgende Dokument beschreibt eine Handreichung für Betreiber von Testgeländen und/oder kritischen Infrastrukturen (KRITIS) um nach Best Practice ein Drohnenabwehrsystem zu gestalten, welches vor nicht kooperativen Drohnen schützt und eine Nutzung kooperativer Drohnen in einer sicheren und zuverlässigen Betriebsumgebung ermöglicht.

Potenzielle Gefährdung kritischer Infrastrukturen durch nicht kooperative Drohnen

KRITIS (Beispiel)	Gefährdung	Effektoren
Flughäfen	• Nicht kooperative Drohnen im Endanflugbereich eines Flughafens • Nicht kooperative Drohnen im Sicherheitsbereich (§3) eines Flughafens • Überflug des Flughafengeländes generell	Durch den Einsatz eines spezifizierten Drohnenabwehrsystems
Primärsektor	• Landwirtschaft: Verbreiten von Schadstoffen mit der Hilfe von Drohnen	Durch den Einsatz eines spezifizierten Drohnenabwehrsystems
Quartärsektor	• IT-Dienstleistungen: Einsatz von Schadstoffen, giftigen Substanzen oder Sprengstoff in Kombination mit Drohnen	Durch den Einsatz eines spezifizierten Drohnenabwehrsystems

Potenzielle Anwendungen von Drohnen in Bereichen von kritischen Infrastrukturen

KRITIS (Beispiel)	Gefährdung	Effektoren
Flughäfen	• Nicht kooperative Drohnen im Endanflugbereich eines Flughafens • Nicht kooperative Drohnen im Sicherheitsbereich (§3) eines Flughafens • Überflug des Flughafengeländes generell	Durch den Einsatz eines spezifizierten Drohnenabwehrsystems
Primärsektor	• Landwirtschaft: Verbreiten von Schadstoffen mit der Hilfe von Drohnen	Durch den Einsatz eines spezifizierten Drohnenabwehrsystems
Quartärsektor	• IT-Dienstleistungen: Einsatz von Schadstoffen, giftigen Substanzen oder Sprengstoff in Kombination mit Drohnen	Durch den Einsatz eines spezifizierten Drohnenabwehrsystems

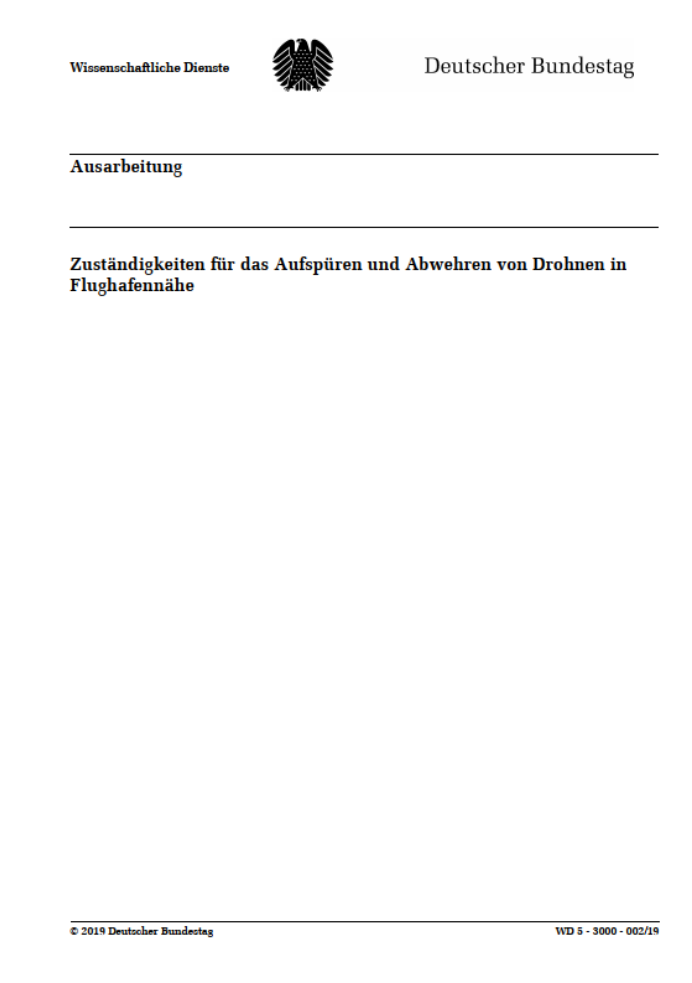
Regulatorische Neuerungen

Anlässlich der Ereignisse am Flughafen London-Gatwick (KRITIS) im Dezember 2018 wurden folgende Fragestellungen der Diskussion zum Schutz kritischer Infrastrukturen, in diesen Fall, vor Drohnen, zu Grunde gelegt:

- Wer ist zuständig für das Aufspüren von Drohnen an Flughäfen sowie in dessen Umkreis (auch außerhalb der 1,5 km-Zone)?
- Wer ist für die Abwehr von Drohnen an Flughäfen zuständig?
- Wer ist zuständig für die Anschaffung von entsprechender Abwehrtechnik?

Prognose: 600.000 Flugbewegungen von unbemannten Flugobjekten (Drohnen) im Jahr 2017 sollen sich bis zum Jahr 2020 verdoppeln.

Ein erhöhter Bedarf des Schutzes kritischer Infrastrukturen vor nicht kooperativen Drohnen ist somit von höchster Relevanz.



Wissenschaftliche Dienste — Deutscher Bundestag

Ausarbeitung

Zuständigkeiten für das Aufspüren und Abwehren von Drohnen in Flughafennähe

© 2019 Deutscher Bundestag — WD 5 - 3000 - 002/19

Regulatorische Neuerungen und Verantwortlichkeiten

Das Entfernen von nicht kooperativen Drohnen im Luftraum, setzt eine erfolgreiche und zuverlässige Detektion der Drohne voraus.

Aufgaben der Flugsicherung bei der Beobachtung des Luftraumes und dem Aufspüren von Drohnen (Drohnendetektion)

Nach EG Nr. 549/2004 (Abl. EG Nr. L 96 S.1) ist davon auszugehen, dass Flugsicherungen nicht nur Luftsicherungsaufgaben wahrnehmen, sondern auch Überwachungsaufgaben wie beispielsweise die Detektion von unbemannten Luftfahrtsystemen

Das Entfernen von Drohnen aus dem Luftraum als eine Form der Gefahrenabwehr ist grundsätzlich eine polizeiliche Aufgabe

Auf Bundesebene wird der Einsatz von Drohnenabwehrsystemen durch die Bundespolizei zum Schutz des Luftverkehrs nach §§4, 14 Abs. 1 Bundespolizeigesetz (BPoIG) sowie § 12 Verwaltungsvollstreckungsgesetz (VwVG) i.V. m dem Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (UZwG) für denkbar gehalten

Zielsetzung zur Integration von Drohnendetektionssystemen an KRITIS

- Integration eines wirksamen und einer wirtschaftlichen Systemkombination mit maximaler Reaktionszeit

Schrittweise **Integration** eines/r modularen Drohnendetektionssystems / Systemarchitektur:

- Analyse der Betriebsumgebung anhand einer UAV/UAS-Bedrohungsanalyse sowie die Betrachtung verschiedener Bedrohungsszenarien
- Herstellerunabhängige Technologiebetrachtung anhand der Ergebnisse aller vorhergehenden Analysen
- Vorbereitung der Testgestellung unter Berücksichtigung sämtlicher äußeren Einflüsse sowie spezifische Gegebenheiten der Betriebsumgebung zur optimalen Integration eines modularen Schutzsystems

Zielsetzung zur Integration von Drohnendetektionssystemen an KRITIS

Die verfügbare Reaktionszeit ist einer der entscheidenden Faktoren bei der Auswahl eines Schutzkonzepts.
Das Drohnendetektionssystem und dessen Managementsoftware sollte entsprechend so entwickelt werden, dass die Dauer zwischen dem Eindringen einer nicht kooperativen Drohne in den geschützten Bereich und der Alarmierung optimale Voraussetzungen für das Einleiten von Mitigationsmaßnahmen zulässt.

Des Weiteren sollten folgende Punkte besondere Beachtung finden:

- Für den Betrieb eines Drohnendetektionssystems an einer kritischen Infrastruktur wie die beispielweise eines Flughafens, sollten in der Regel passive Komponenten, welche ohne elektromagnetische Abstrahlung (z.B. Optische Sensoren, Kameras, passive Radarsysteme) zur Detektion zu bevorzugt werden

- Das System sollte in der Lage sein, eine dreidimensionale Position einer Drohne zur ermitteln

- Bei der Detektion einer eindringenden Drohne, sollte die Genauigkeit der Positionsbestimmung ausreichend sein, um andere Sensoren (beispielsweise Kameras) bzw. Effektoren automatisch darauf zu richten

Zielsetzung zur Integration von Drohnendetektionssystemen an KRITIS

- Das Drohnendetektionssystem sollte über eine ausreichende Detektionsauflösung verfügen, damit mehrere Drohnen, die in einem geringeren seitlichen Abstand zueinander oder voneinander fliegen, detektiert werden können

- Das Drohnendetektionssystem sollte schwebende ruhende/positionshaltende Drohnen oder die mit variierenden Geschwindigkeiten und Flugtrajektorien erkennen können

- Das Drohnendetektionssystem sollte die Korrektheit der Klassifikation einer Drohne mit einer Wahrscheinlichkeit beziffern. Dies ermöglicht die Festlegung unterschiedlicher Meldeketten bzw. Mitigationsmaßnahmen anhand der Zuverlässigkeit einer Detektion. Dadurch wird es möglich, den Automatisierungsgrad eines Systems zu erhöhen (Im Idealfall kommt es zu keinem Fehlalarm, jedoch ist im Real Fall mit Fehlalarmen zu rechnen)

Detektion und Mitigation von Drohnen

Detektion von Drohnen:

Sensorikbasierte Sammlung von Informationen des durch ein Drohnendetektionssystem zu schützenden Bereiches sowie entsprechende Festlegung von Anomalien (Soll- und Ist-Zustand) zur möglichen Klassifizierung des sich in der Betriebsumgebung befindlichen Objektes (Drohne).

Klassifizierung des Objektes/Drohne:

Ein Algorithmusbasierter Prozess entscheidet hier über die Kategorie des detektierten Objektes bzw. Drohne. Des Weiteren werden hier weitere Informationen (Zustand der Betriebsumgebung) überprüft, um u.a. weitere Aussagen (wie beispielsweise: Größe, Höhe, Richtung oder Geschwindigkeit) über das detektierte Objekt treffen zu können.

Neutralisierung/Mitigationsmaßnahme:

Nach erfolgreicher Lokalisierung des/der Objektes/Drohne sind diverse Möglichkeiten zur Neutralisierung bzw. Mitigationsmaßnahmen sind derzeit technisch realisierbar. Grundsätzlich finden **ballistische** sowie **RF-basierte** Mitigationsmaßnahmen ihre Anwendung.

Referenzverfahren zur Integration von Drohnendetektionssystemen

Integrationsphase I

Spezifische Gegebenheiten
Bedrohungsanalyse auf Basis der geografischen Lage
Analyse der Bebauungsstruktur und des Umfeldes
-> operatives Umfeld des Drohnendetektionssystems

Integrationsphase II

Durchführung einer spezifizierten Bedrohungsanalyse (SORA (JARUS))
Analyse potentieller Effektoren

Herstellerunabhängiges Analyseverfahren

Räumliche Betrachtung

- Identifikation der besonders zu betrachtenden Bereiche am und um den kritischen Infrastrukturen

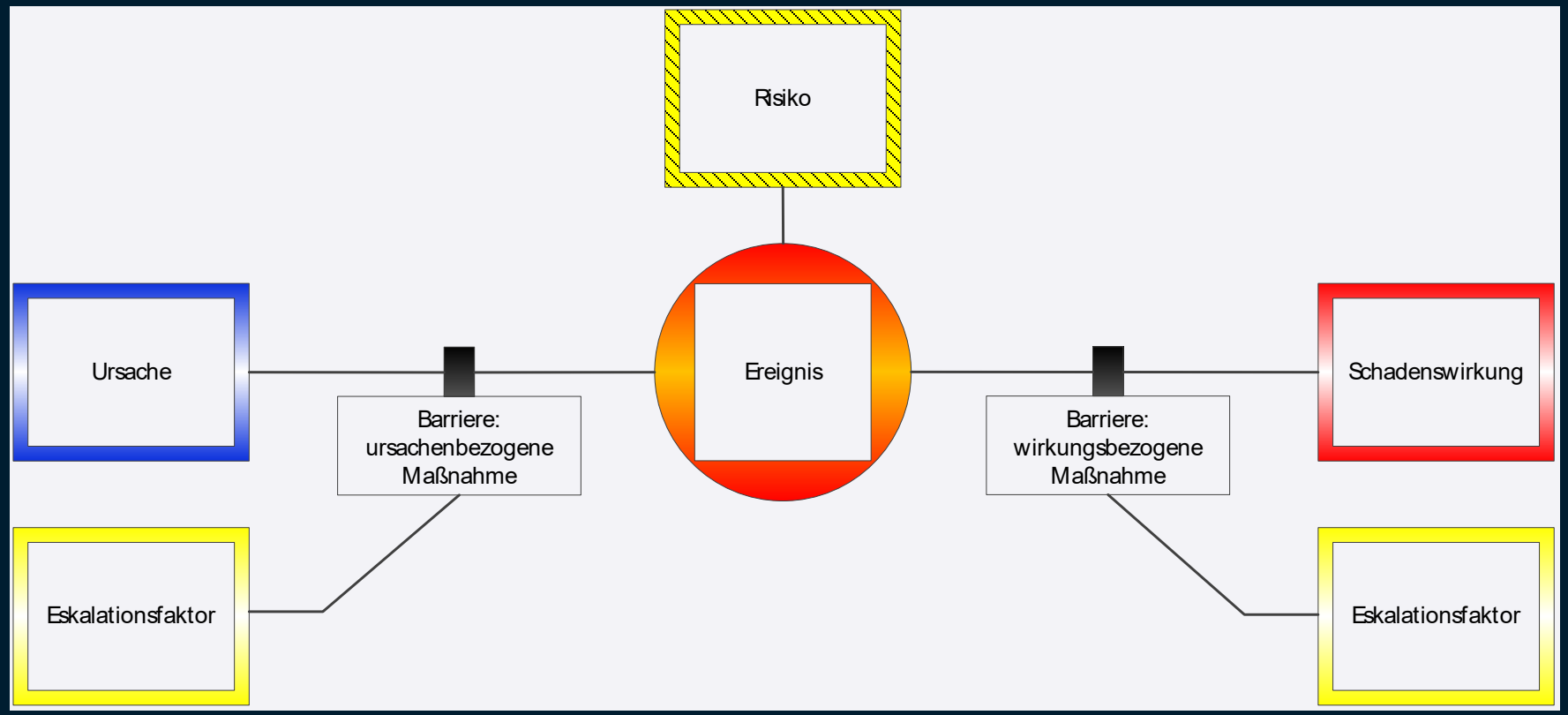
Bedrohungsanalyse

- Anlehnung an das „Specific Operations Risk Assessment“ von der „Joint Authorities for Rulemaking on Unmanned Systems“

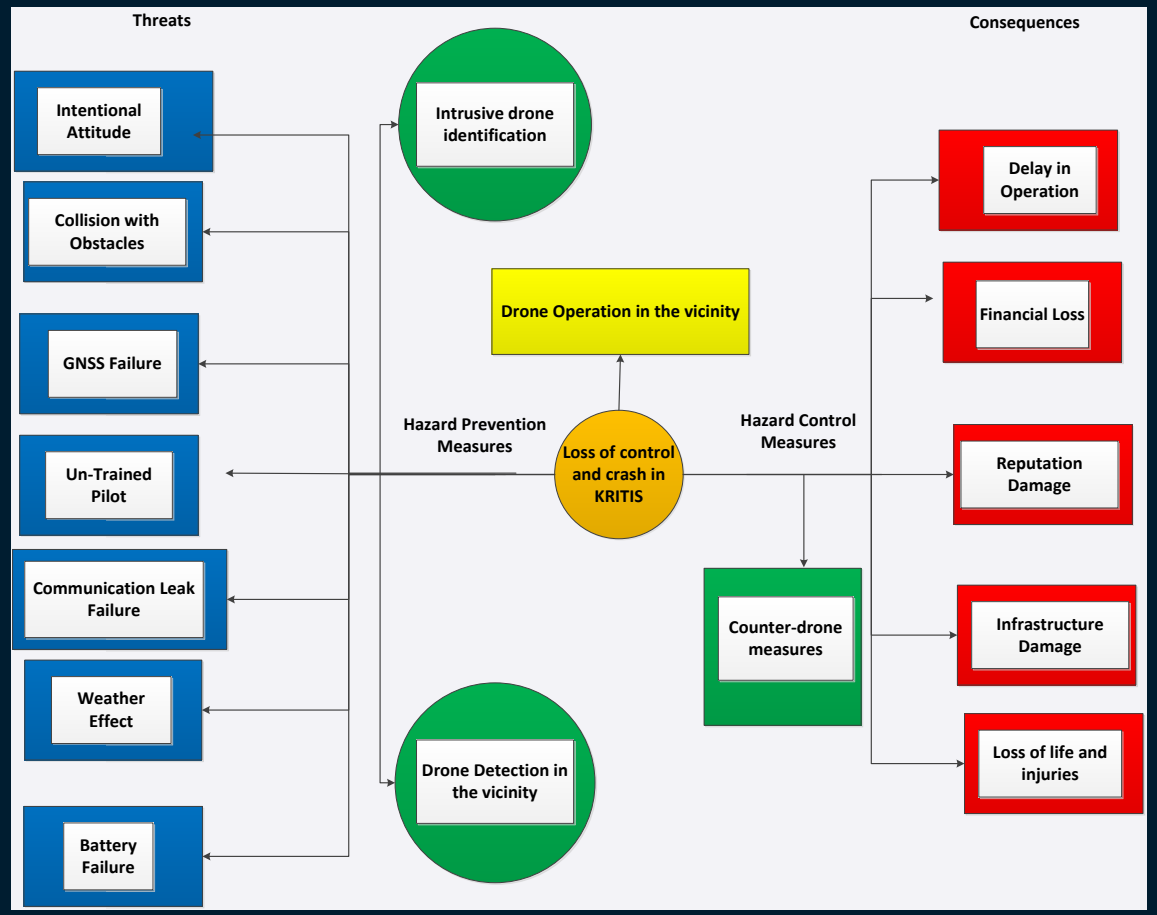
Gegenüberstellung der Detektionssysteme

- Technologie-betrachtung
- Erstellung eines Fragebogens bzgl. der Systemanforderungen zur Versendung an die Hersteller solcher Systeme
- Analyse der bereitgestellten Informationen und Datenblätter

Systematische Durchführung einer Bedrohungs-/Risikoanalyse



Systematische Durchführung einer Bedrohungs-/Risikoanalyse



Systematische Durchführung einer Bedrohungs-/Risikoanalyse

Aspekte	Beschreibung
Risiko	Die Aktivität, die eine Gefährdung darstellt. Das Risiko bildet den Ausgangspunkt für das abgebildete Diagramm. Die Risiken der höchsten Ebene innerhalb dieser Studie sind das Betreiben von UAS/UAV durch die kritische Infrastrukturen selbst sowie Behörden und Organisationen mit Sicherheitsaufgaben (BOS), durch kommerzielle Betreiber oder durch Privatpersonen. In der Abbildung handelt es sich beispielsweise um den privaten UAS/UAV Betrieb, der zum Risiko für kritische Infrastrukturen wird.
Ereignis	Beschreibt den Moment, in dem die Kontrolle über das Risiko verlorengeht. Es ist zu bedenken, dass das Ereignis nicht notwendigerweise den Verlust über die Kontrolle des UAS/UAV bedeutet (beispielsweise: stellt eine Drohne, die in den Bereich der kritischen Infrastruktur einfliegt, ein Ereignis das, obwohl die Drohne ggf. weiterhin unter Kontrolle ist). Dies wäre auch im oben erwähnten Beispiel der Fall, solange die Drohne nicht aus der Reichweite des Steuersignals herausfliegt.

Systematische Durchführung einer Bedrohungs-/Risikoanalyse

Aspekte	Beschreibung
Ursache	Ereignis, dass zum Kontrollverlust über das Risiko führt und dadurch möglicherweise zum Eintreten des Ereignisses führt. Im oben dargestellten Beispiel könnte dies die Unkenntnis des Drohnenpiloten bzgl. der Gefahren sein, die er durch sein Handeln herbeiführt, kombiniert mit der Abwesenheit geeigneter technischer Maßnahmen in der Drohnenelektronik (Geofencing), die solch einen Flug verhindern würde.
Schadens-wirkung	Effekt, der durch das Eintreten des Ereignisses hervorgerufen wird. Dies ist der mögliche schaden bzw. die Konsequenz, die aus dem eingetretenen Ereignis hervorgeht. Im Beispiel könnten eine solche Schadenswirkung neben der Verletzung von Vorschriften in der Beschädigung eines anfliegenden Luftfahrzeugs bestehen (Im Falle einer kritischen Infrastruktur wie die eines Flughafens)

Systematische Durchführung einer Bedrohungs-/Risikoanalyse

Aspekte	Beschreibung
Barrieren	Ursachen- oder wirkungsbezogene Maßnahmen, welche die verfügbaren Mitigationsmöglichkeiten darstellen, die darauf abzielen, das Eintreten des Ereignisses zu verhindern (ursachenbezogen), d.h. die Entstehung des möglichen Schadens zu verhindern. Im Beispiel könnte eine Maßnahme die Alarmierung der Polizei sein, um den Piloten zum Zurückfliegen bzw. sicheren Landen der Drohne zu bewegen.
Eskalations-faktoren	Randbedingungen, die die Effektivität der Barrieren herabsetzen. Zu kurze Reaktionszeiten, lange Meldewege oder schwierige Erkennung der Drohne könnten im genannten Beispiel solche Faktoren sein.

Fragebogen zur Versendung an Hersteller

Faktoren	Ihre Kommentare
Mit welchen Beschaffungskosten ist zu rechnen?	
Wie groß ist die Reichweite des Detektionssystems unter realen Bedingungen?	
Welche Arten von RPAS bzw. UAS können NICHT detektiert bzw. identifiziert werden (z.B. Drohnen kleiner als BxHxT oder leichter als X Kg, autonome Systeme ohne Verbindung zwischen dem Piloten und der Drohne, selbst gebaute Systeme usw.)?	
Ist ein Ausbau der Infrastruktur zu erwarten? Ist es möglich bestehende Infrastrukturen am Flughafen einzusetzen (z.B. Überwachungskameras)? Gibt es Synergien zu anderen Anwendungsbereichen (z.B. Vogelzugradar)?	
Sind alle Systemkomponenten (z.B. akustische Sensoren) für den Einsatz an einem Flughafen tauglich? Besteht das Detektionssystem aus aktiven Komponenten, die Luftfahrteinrichtungen stören und/oder von denen gestört werden könnten?	
Besteht die Möglichkeit, mobile Einheiten in das System zu integrieren (z.B. einen Sensor nach Bedarf versetzen)?	

Fragebogen zur Versendung an Hersteller

Faktoren	Ihre Kommentare
Wie ist der Automatisierungsgrad des Systems einzuschätzen? Ist ein Systemoperator erforderlich?	
Wie sind die Verfügbarkeit (z.B. Ausfallzeiten/-quoten und Redundanz) und Zuverlässigkeit (z.B. Freund-/Feind-Erkennung, Reaktionszeit und Fehleralarmraten) des Systems zu beurteilen?	
Wie wird das System Instand gehalten, damit es neue RPAS am Markt detektieren bzw. erkennen kann (z.B. RPAS-Signaturen in einer Datenbank)?	
Wie ist die Modularität des Systems einzuschätzen? Besteht die Möglichkeit, das System phasenweise in Bezug auf Ort und Funktionalität auszubauen?	
Besteht die Möglichkeit, ein eventuell später aufzubauendes Abwehrsystem an das RPAS-Detektionssystem anzuschließen?	

Checkliste zum Systemauswahlverfahren

Checkliste zum Auswahlverfahren eines ganzheitlichen modularen Drohnendetektionssystems (DD)

Kriterien	Relevante Aspekte	Erfüllungsgrad	Weitere Informationen
Detektionsmethode			
RF-Signaldetektor			
SigInt (Funksenoren)			
Radar	Radar Signatur		Detektion von RF Pulsen
Elektrooptisch/Optisch			
Akustisch	Identifizierung von Anomalien im regulärem Geräuschpegel der Betriebsumgebung. Datenbankqualität (Aktuell/Variation)		Hohe Genauigkeit und eine geringe Fehlalarm Quote
Infrarot/Thermo	Identifizieren der Drohne/UAV von anderen detektierten Objekten		Tag- und Nachtbetrieb möglich
Lokalisierungsmethode			
RF-Signaldetektor			
SigInt (Funksenoren)			
Radar			
Elektrooptisch/Optisch			
Akustisch			
Infrarot/Thermo			
Mitigationsmethoden			
Jamming			
Spoofing			
Block View			
Capture			
Laser			

Checkliste zum Systemauswahlverfahren

Checkliste zum Auswahlverfahren eines ganzheitlichen modularen Drohnendetektionssystems (DD)

Kriterien	Relevante Aspekte	Erfüllungsgrad	Weitere Informationen
Systemschnittstellen	Konfliktfreie Integration des ganzheitlichen Schutzsystems in die bereits bestehende Infrastruktur und deren vorhandenen Schnittstellen unter Berücksichtigung der einzuhaltenden und wirkungsvollen Reaktionszeiten des Gesamtsystems		

Checkliste zum Systemauswahlverfahren

Komponentenbeschreibung:

RF-Signaldetektor

SigInt (Funksensoren)

Radar

Optische Sensoren

Akustische Sensoren

Laser

Jammer /Spoofer

Checkliste zur Integration eines Drohnendetektionssystems

Checkliste zur Integration von Drohnendetektionssystemen

					Integrationsstatus	
Integrationsschritte	Relevante Aspekte	Hilfsmittel	Technische Durchführung	Weitere Informationen	In Progress	Final
Standortbestimmung verschiedener Sensoren zur Erreichung des optimalen Wirkungsgrades						
Installation der Sensorik, HW und SW						

Checkliste zur Integration eines Drohnendetektionssystems

Checkliste zur Integration von Drohnendetektionssystemen

					Integrationsstatus	
Integrationsschritte	Relevante Aspekte	Hilfsmittel	Technische Durchführung	Weitere Informationen	In Progress	Final
Integration des Systems an die interne Meldekette				Erreichen einer maximalen Reaktionszeit zur Minimierung aller Schadensereignisse		

High-level Workshop on drone detection – Eurocontrol
Ergebnisse vom 03. + 04.10.2019

- Sensibilisierung der Öffentlichkeit, Flughäfen- und Regierungsbehörden auf allen Ebenen über die Notwendigkeit von Gegenmaßnahmen Drohne
- Klärung der Rollen und Verantwortlichkeiten aller an der Planung und Ausführung von Mitigationsmaßnahmen beteiligten Akteure Drohnen-Maßnahmen
- Verbesserung der Risikobewertungsmethoden
- Definition der Anforderungsspezifikation für Maßnahmen zur Drohnenbekämpfung, einschließlich betrieblicher Maßnahmen
- Erarbeitung von Verfahren und technische Lösungen, welche mit vorhandener Infrastruktur kompatibel sind
- Erarbeitung einer Roadmap für einen integrativen Ansatz zur Bekämpfung von nicht kooperativen Drohnen in Bereichen von Flughäfen
- Prüfen der Rechtsgrundlage von Mitigationsmaßnahmen auf möglicherweise unzureichend Aspekte

Für weitere Informationen besuchen Sie unser Website: www.protact.eu

a company of DLR