

**Fachtagung
„'Neue' Technologien & ,neue' Bedrohungen“**

Frankfurt, 24. November 2017

Gesellschaft
für Informatik



Dr. Gunther Grasmann, Fraunhofer IOSB

© Fraunhofer IOSB

1



Fraunhofer
IOSB

Inhalt

- Einleitung und kurze Vorstellung des Fraunhofer IOSB
- Drohnen – Nutzen und Gefahren
 - Aktuell verfügbare Drohnen und ihr Nutzen
 - Gefahren durch Drohnenmissbrauch
 - Möglichkeiten der Drohnerdetektion
 - Schutz vor durch Drohnenmissbrauch entstehenden Gefahren
- Das Projekt ArGUS
 - Motivation und Zielsetzung
 - Vorgehen und Konsortium
 - Arbeitspakete und Ergebnisdefinition
- Zusammenfassung & Ausblick

© Fraunhofer IOSB

2



Fraunhofer
IOSB

Einleitung

Drohnen – ein dynamisch wachsender Markt:

Heute bereits leistungsfähige Consumer-Drohnen im Low-Cost-Bereich verfügbar

Extreme Leistungen und sehr leichte Handhabung im Kostenbereich 10k

Hohe Leistungsfähigkeit und hoher Nutzen bei vielen Transport- und Schutzaufgaben

aber

Hohes und schwer abschätzbares Bedrohungspotenzial

Standorte des IOSB

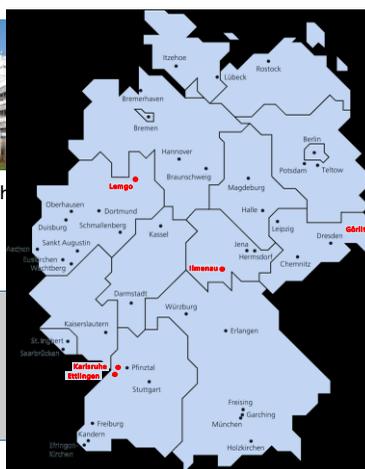
www.iosb.fraunhofer.de



Standort Ettlingen



Standort Karlsruhe



Lemgo



Ilmenau



Beijing



FH Zittau / Görlitz

Betriebs- u. Investitionshaushalt 2016	52 Mio €
Stammpersonal	500
davon Wissenschaftler und Ingenieure	321
Wissenschaftliche Hilfskräfte	179

Das IOSB ist mit dem Karlsruher Institut für Technologie KIT eng verbunden
 Fakultät für Informatik, Institut für Anthropomatik,
 Lehrstuhl für Interaktive Echtzeitsysteme IES

Kernkompetenzen des IOSB



Optonik:

Elektrooptische Systeme und Verfahren zur Signal- und Bildgewinnung vom Ultravioletten bis zum thermischen Infrarot



Systemtechnik:

Fähigkeit der Analyse, des Verständnisses, der Modellierung, der Entwicklung und Beherrschung komplexer Systeme



Bildauswertung:

Aufbereitung, Echtzeitverarbeitung sowie automatische und interaktive Informationsgewinnung aus Bildern und Videos



Kompetenzen Fraunhofer IOSB

Optonik:

- Vermessung und Bewertung optischer Sensoren und Optiken (speziell IR)
- Nachtsichtlabor & Reichweitenmodelle
- „Gated Viewing“

Bildauswertung:

- Bildbasierte Detektion & Klassifikation
- „On Board“ Bildverarbeitung

Systemtechnik:

- Systemarchitektur, -design, Prototyping
- Heterogene Sensorik
- Sensordatenfusion
- Beratung, Erprobung und Tests
 - IOSB-eigener Drohnenpark
 - Kontrollstationen/Lagezentren
 - Diverse Sensorsysteme



Drohnen: vielseitige unbemannte Fluggeräte

Einsatzgebiete (großer und kleiner) Drohnen:

- als Testplattform für (neue) Flugsysteme oder als Zieldarstellungsdrohne
- Erkundung, Aufklärung und Überwachung, Inspektion
- mit Waffen bestückt in Kampfeinsätzen
- Foto- und Videoaufnahmen, Vermessung, Logistik, Kommunikation (Relais)
- Wissenschaft (Meteorologie, Archäologie, Geologie, Biologie,...)
- zur Unterhaltung

Steuerung:

- Fernsteuerung (Funk- oder Infrarotsignale)
- Automatisch

Abmessungen:

- Abmessungen: von einigen Millimetern bis zur ca. 60 m.



Quelle: androidmag.de

Gängige Abkürzungen:

UAV - Unmanned **A**erial **V**ehicle

RPAV - Remotely **P**iloted **A**erial **V**ehicle

UAS - Unmanned **A**ircraft **S**ystem

RPAS - Remotely **P**iloted **A**ircraft **S**ystem

Die Bezeichnung umfasst das Gesamtsystem des fliegenden UAV, der (Boden)Station zum Start und ggf. Landung, sowie der Station zur Führung und Überwachung des Fluges.

UAVs: Klassifizierungsbeispiel

Class of UAV	Weight	Size	Typical Altitude
Standard	>25kg	>2m	>2000m
Small-scaled (S-class)	2-25kg	0,5m - 2m	0-2000m
Micro-scaled (M-class)	0,05kg-2kg	15cm – 50cm	0-500m
Nano-scaled (N-class)	<50g	< 15cm	0-20m



Quelle: Fa. HiSystems



Quelle: Fa. DJI



Quelle: coolthings.com



Quelle: www.aecinfor.com



Quelle: Clear Flight Solutions

Drohnen Nutzlasten: Kamera mit Gimbal

Gimbal – Stand der Technik:

- Motoren: Brushless DC Motor (getriebelos)
- Sensoren: Acc, Gyro, Kompass, Barometer, GPS
- Datenübertragung: WLAN, 4G
- Freiheitsgrade: 2x 180° (roll, pitch), 1x 360° endlos (yaw)



- 4K onboard Videoaufzeichnung
- Full HD-4K Video Downstream
- Kameras im sichtbaren sowie Infrarot- und Multispektralbereich
- 3 fache Bildstabilisierung
- 30x optischer Zoom



- AMFIS V4 Gimbal: < 980g, WLAN, 4G, 30x optischer Zoom

Einige zivile Einsatzgebiete kleiner UAVs

- Luftaufnahmen (Video oder Infrarot) für
 - Kino/Videoproduktion (auch Paparazzi)
 - wissenschaftliche Zwecke (Meteorologie, Archäologie, Geologie, Biologie,...)
 - Landwirtschaft (Pflanzenzustand, Schädlingsbefall, Auffinden von Tieren, ...)
 - Inspektion großer und/oder schwer zugänglicher Objekte (Gebäuden, Denkmäler, Hochspannungsleitungen, Dämme,...)
 - Lageerkundung bei polizeilichen Einsätzen, Rettungsarbeiten, Katastrophenschutz,...
- Für 2D- und 3D-Vermessung unterschiedlicher Objekte
- In der Logistik
- Als Träger für spezielle Sensoren:
 - Gassensoren, Strahlungssensoren,...
- Und natürlich als Hobby...



Quelle: Wikipedia



Kleine UAVs

Vorteile:

- Kostengünstiger als Einsatz von Helikoptern
- Fern- und Programmsteuerung möglich
- Schnell einsatzbereit
- Leicht zum Einsatzort zu transportieren
- Können auch im Gefahrenbereich eingesetzt werden – ggf. als Einwegequipment



Quelle: Fa. DJI



Nachteile:

- Witterungsabhängigkeit
- Relativ geringe Nutzlast
- Begrenzter Aktionsradius und Flugzeit
- Müssen von Menschen betreut werden
- Nicht optimale rechtliche Rahmenbedingungen für gewerblichen Einsatz



Einsatzbeispiel AMFIS: „Das Fest“ in Karlsruhe (2010-2015)



Typenabhängige Gefahreneinschätzung von UAVs

Eigenschaft \ Typ	Spielzeug	Hobby	Professionell (zivil)	Militärisch
Kosten	Niedrig (ab ca. 30 Euro)	Mittel (ab ca. 500 Euro)	Hoch (ab ca. 5000 Euro)	Sehr hoch
Zugänglichkeit	Hoch	Hoch	Mittel	Niedrig
Nutzlast	Sehr niedrig bis keine	Mittel	Mittel bis hoch	Mittel bis hoch
Flugweite	Niedrig	Mittel	Mittel	Mittel bis hoch
Wahrscheinlichkeit des Missbrauchs	Mittel	Hoch	Mittel	Niedrig
Gefährlichkeit	Niedrig bis mittel	Hoch	Hoch	Hoch bis sehr hoch

Missbrauchspotenzial kleiner UAVs - Grobeinteilung

Kategorie 1 – Störung

- „Kinderstreich“ – zufällig oder absichtlich
- Ausspähung, unerlaubte Erkundung
- Ablenkung (z.B. des Wachpersonals)



Kategorie 2 – Gesetzeswidrigkeit

- Fliegen in Flugverbotszonen
- Transport von Objekten
 - Gefährliche Objekte (Waffen, Munition, Sprengstoffe, Drogen,...)
 - Verbotsbereiche (Grenze, JVA, Militärobjekt etc.)
 - Bei Straftaten (Diebesgut, Hilfsmittel, Beseitigung von Beweisen)

Kategorie 3 - Gefährdung

- Durchführung von Anschlägen
 - Auf Personen
 - Auf Fahrzeuge, Flugzeuge, etc.
 - Auf Gebäude, Infrastruktur, etc.



Quelle: money.cnn.com

Mögliche Szenarien: Kategorie 3 - Gefährdung

Anschläge

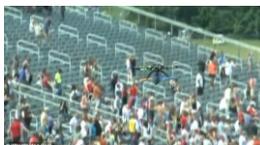
- Anschläge auf konkrete Personen
 - UAV muss i.d.R. präzise gesteuert werden – z.B. vom Piloten per Videolink oder automatisch videobasiert (noch nicht verbreitet)
- Terroristische Anschläge mit dem Ziel, so viel Schaden wie möglich anzurichten
 - Präzise Steuerung ist nicht immer erforderlich

Beispiele mit präziser Steuerung:

1. Landung eines UAV mit Schadstoffladung vor dem Ansaugrohr einer Klimaanlage
2. Besprühen eines fahrenden Wagens mit Farbe



Quelle: io9.com



Quelle: Washington Post



Quelle: i-HLS.com

Vier Phasen eines Angriffs

Ein „Angriff“ lässt sich in vier Phasen unterteilen:

1. Vorbereitung
 - Planung (ggf. mit Erkundung vor Ort)
 - Beschaffung notwendiges Equipments
 - Aufbau und Einschalten am geeigneten Startort
2. Anflug
 - Fluggerät ist gestartet und befindet sich im Anflug
3. Einwirkung
 - Durchführung der Wirkung am Zielort
4. Landen und Nachbereitung (falls geplant)
 - Flug zum Landestelle (evtl. Rückkehr zum Startposition)
 - Rückbau und ggf. Spurenbeseitigung
 - Abtransport

Zwischenfazit I

- Kleine UAVs unterschiedlich zivil und militärisch einsetzbar.
- Die Technologie entwickelt sich rasant.
- Immer neue Einsatzbereiche (legal und illegal).
- Erhebliches und ständig wachsendes Bedrohungspotenzial bei kleinen UAVs Wird aber häufig nicht ernst genommen.
- Gefährlichkeit der UAVs vom Typ und von der Anwendung abhängig.
- Mit der schnell wachsenden Zahl von UAVs wachsen auch allgemeine Risiken, die durch Verbesserung von entsprechenden Gesetzen und Kontrollmechanismen erheblich reduziert werden können.
- Die gesetzlichen Grundlagen für den Einsatz von UAVs und deren Überwachung sind noch lückenhaft und werden angepasst.

„State-of-the-art“

- Es gibt mehrere Anbieter unterschiedlicher Systeme und Technologien zur Detektion, Lokalisierung, Tracking, Klassifikation und Neutralisierung der Bedrohung durch Drohnen
- Das Angebotsspektrum reicht von einfachen Detektion- und Alarmierungssystemen mit einem Sensor bis zu komplexen multisensoriellen Lösungen
- Immer mehr neue Anbieter kommen hinzu - der Markt boomt
- Bei mehreren Systemen sind leider keine konkreten Informationen verfügbar



Quellen: SCG, DroneDetector, Airbus Group, Selex ES, Diehl Defence, Lockheed Martin, Blighter, Telespazio-Vega

Die wichtigsten Tendenzen

Immer mehr multisensorielle Systeme –
meistens modular und erweiterbar

Systemtechnische Lösungen nicht nur mit mehreren Sensoren und Wirkmitteln, sondern auch mit Lagedarstellung, Signaturdatenbanken für die Klassifikation von UAVs, Interfaces zu bestehenden Sicherheitssystemen,...

Staatliche Institutionen weltweit bereiten Gesetzesänderungen vor, die die Detektion und Bekämpfung verändern können

Einwirkung auf Schwachstellen eines UAVs (kommunikationstechnisch)

Komponente	Einwirkung	Ergebnis
Fernsteuerung	Signal manipulieren	Andere Flugroute/Landung
	Signal unterdrücken	UAV automatisch fliegt zurück/landet
Autopilot	Falsche Werte übertragen	Andere Flugroute/Landung
	Virus einschleusen	Andere Flugroute/Landung/ Absturz
GPS Sensor	Signal manipulieren	Andere Flugroute
	Signal unterdrücken	UAV wartet/landet automatisch
Visualisierung bzw. Videoübertragung	Signal manipulieren	Steuert der Pilot videobasiert, kann es zu Kollisionen und Zerstörung des UAVs kommen
	Signal unterdrücken	Pilot kann nicht mehr videobasiert steuern

„Sanfte“ und „harte“ Gegenmaßnahmen gegen UAVs

„Sanfte“ Abwehrtechniken basieren auf gezielter schwacher Einwirkung auf UAVs und führen i.d.R. nicht zu ihrer Beschädigung oder Absturz.

Mögliche „sanfte“ Maßnahmen:

- Blendung der Kamera (z.B. mit Laser)
- Störung der Kommunikation/Navigation („Jamming“)
- Lokale Verfälschung GPS/Glonass („Spoofing“)
- Kontrollübernahme



„Harte“ Abwehrtechniken basieren auf relativ starken Einwirkungen auf UAVs, die zur Unterbrechung ihrer Mission oder Flugunfähigkeit führen.

Mögliche „harte“ Maßnahmen:

- Beschädigung elektronischer Komponenten mit schwacher (z.B. IR Laser) oder starker (z.B. EMP) energetischer Einwirkung
- Flugunfähigkeit verursachen (Kleber, Leine, starker Schall...)
- Abfang (z.B. mit anderer Drohne(n), bemannten Fluggeräten)
- Abschuss (z.B. Wasserstrahl, Laser, Feuerwaffen)



Quelle: Daily Mail

Auswahl passender Gegenmaßnahmen

Art des Missbrauchs	Gegenmaßnahmen
Kategorie 1 – Störung UAV verursacht Störungen und Unannehmlichkeiten, ohne das Gesetz absichtlich zu brechen bzw. Personen oder Objekte (direkt) zu gefährden.	1. <u>Gesetze</u> : Nutzungseinschränkungen und Flugverbotszonen für UAVs, Zertifizierung UAV-Benutzer etc. 2. <u>Kontrolle</u> : Detektion/Klassifizierung/Lokalisierung von UAVs, Lokalisierung der Piloten
Kategorie 2 – Gesetzeswidrigkeit Die Anwendung von UAVs ist zwar ordnungs- oder gesetzeswidrig, Personen oder fremdes Eigentum werden aber nicht (direkt) gefährdet.	1. <u>Kontrolle</u> : Detektion/Klassifizierung/Lokalisierung von UAVs und Nutzlast, Lokalisierung der Piloten 2. <u>„Sanfte“ Gegenmaßnahmen</u>
Kategorie 3 – Gefährdung Das Ziel der Anwendung von UAVs ist eine direkte Gefährdung von Personen oder Objekten.	1. <u>Kontrolle</u> : Detektion/Klassifizierung/Lokalisierung von UAVs und Nutzlast, Lokalisierung der Piloten 2. <u>Bekämpfung des UAV</u>

Die rechtliche Situation

• Detektion

- Genehmigungserfordernisse hinsichtlich der Frequenznutzung
- Frequenzrechtliche Probleme bei der Verwendung von SDR-Technologie ?
- Anforderungen des Telekommunikationsgesetzes
- Werden personenbezogenen Daten vom Sensorsystem erhoben ?
- Möglichkeiten zur Anpassung des Systems für die Nutzung durch unterschiedliche Akteure (staatliche und nicht-staatliche)

• Gegenmaßnahmen

- Verwendung durch Hoheitsträger (Ermächtigungsgrundlagen und Grundrechtsbindung)
- Verwendung durch Private (straf- und zivilrechtliche Konsequenzen und mögliche Rechtfertigungstatbestände)
- Verwendung durch Mischkonstellationen (von der öffentlichen Hand beherrschte Unternehmen/privat- und zivilrechtliche Kooperationen)
- Haftungsfragen (Zivilrecht)

Zwischenfazit II

- UAVs haben diverse Schwachstellen und können auf diese Weise bekämpft werden.
- Bekämpfung von unerwünschten UAVs situationsabhängig (nur „Man-in-the-Loop“)
- Hauptproblem ist Zeitmangel:
Schnelle und richtige Entscheidungen nur durch spezielle Informationssysteme
- Gegenmaßnahmen können nur dann sicher und effizient sein, wenn sie rechtzeitig eingeleitet werden und genau auf die Situation abgestimmt sind
- Besonders schwierig ist gleichzeitige Bekämpfung mehrerer UAVs, die durch spezielle Angriffstaktiken zusätzlich erschwert werden kann
- Im militärischen und zivilen Kontext sind die Entscheidungsmöglichkeiten und möglichen Gegenmaßnahmen oft sehr unterschiedlich
- Im zivilen Kontext ist eine rechtzeitige Detektion des Piloten (möglichst vor dem eigentlichen Abheben des UAVs) meistens die beste Lösung
- Im zivilen Kontext ist eine rechtliche Betrachtung der Situation unabdingbar, was die erlaubten Detektionsmaßnahmen betrifft und die erlaubten Gegenmaßnahmen. Auch Fragen der Haftung spielen dabei eine Rolle.

Das Projekt „ArGUS“

Assistenzsystem zur situationsbewussten Abwehr von Gefahren durch UAS
Gefährdung durch Drohnen begegnen durch:

- Frühzeitige Detektion



- Einschätzung der Lage durch umfassende Klassifikation
- Auswahl der Maßnahmen durch Simulation und Bewertung der möglichen Szenarien

→ Assistenzsystem zur Entscheidungsunterstützung

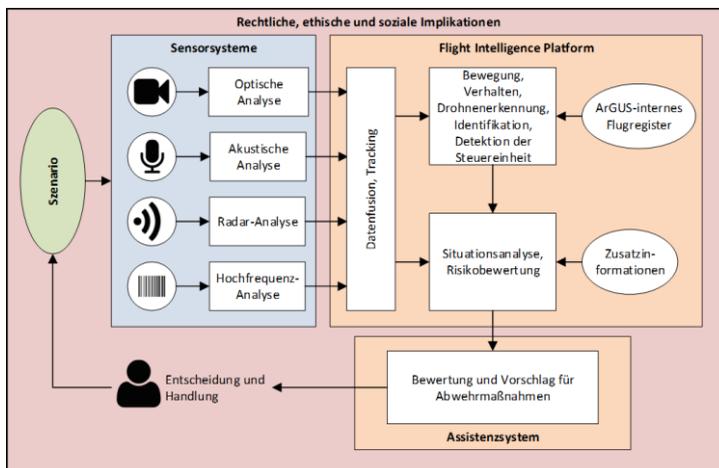
Gefördert vom BMBF in der Bekanntmachung
„Zivile Sicherheit Aspekte und Maßnahmen der Terrorismusbekämpfung“
im Sicherheitsforschungsprogramm der Bundesregierung



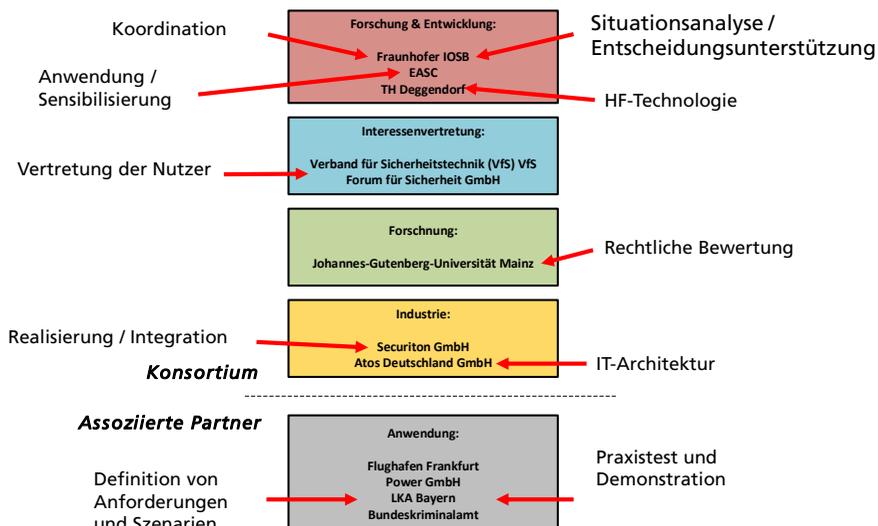
Herausforderungen

- Zuverlässige Detektion und Klassifikation
 - Geringe Reaktionszeit
 - Rechtliche Bewertung hinsichtlich Monitoring unklar
 - Verifikation „Freund / Feind – Erkennung“
- Situationsanalyse abhängig von vielen Faktoren
 - Entscheidung hinsichtlich richtigem Vorgehen multikriteriell
 - Rechtlicher Klärungsbedarf hinsichtlich Intervention und Haftung

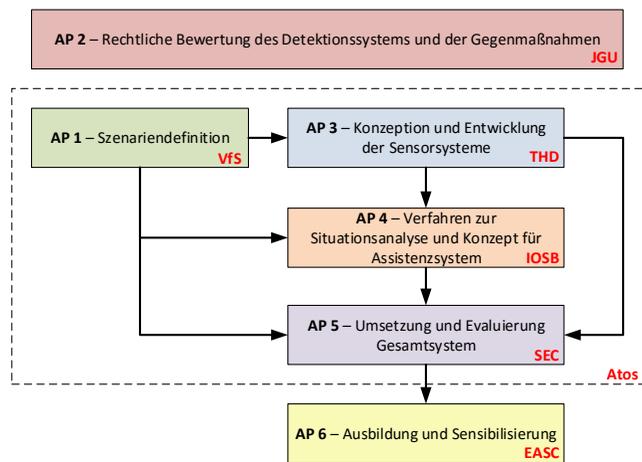
Projektübersicht



ARGUS-Projektpartner / Konsortium



Projektstruktur und Arbeitspakete



AP 1 – Szenariendefinition

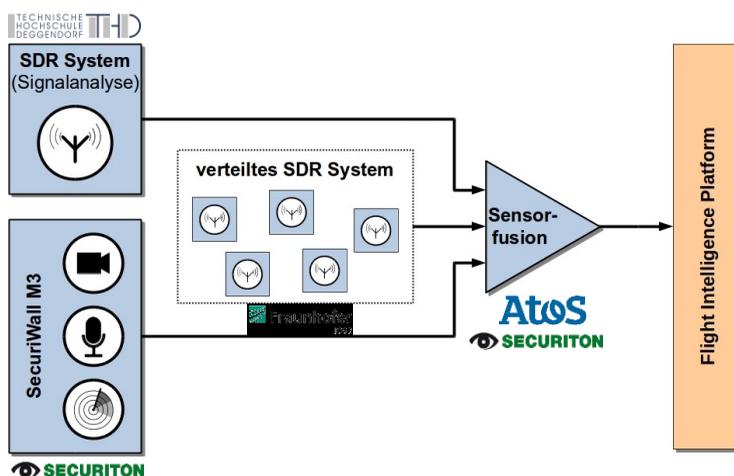


- Bestimmung des zu schützenden Objektes und der Schutzziele
- Analyse der Bedrohungen/Schadensszenarien
- Bewertung von Eintrittswahrscheinlichkeit und potenzieller Schadensschwere
- Entwicklung von Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit und Schadenshöhe
- Planung von Maßnahmen und Bereitstellung von Mitteln zur Schadensbekämpfung und –eindämmung
- Analyse der Risikotragbarkeit und Genehmigung des Restrisikos
- Priorisierung der Szenarien

AP 2 – Rechtliche Bewertung

- Rechtliche Bewertung von Grundentscheidungen über die Funktionsweise des Detektionssystems, insbesondere zur Reichweite der Detektion (Was wird erfasst?)
- Abgrenzung der entscheidenden Normen für Detektions- und Gegenmaßnahmen
- Herausarbeitung der relevanten Rechtsregime für die einzelnen Szenarien und unterschiedlichen Nutzer (Private/Behörden/Mischformen)
- Rechtliche Anforderungen an die technische Gestaltung des Systems
- Rechtsgrundlagen für den Einsatz des Detektionssystems und von Gegenmaßnahmen in exemplarischen Verwendungsszenarien

AP 3 – Sensorsystem und Sensorsubsysteme



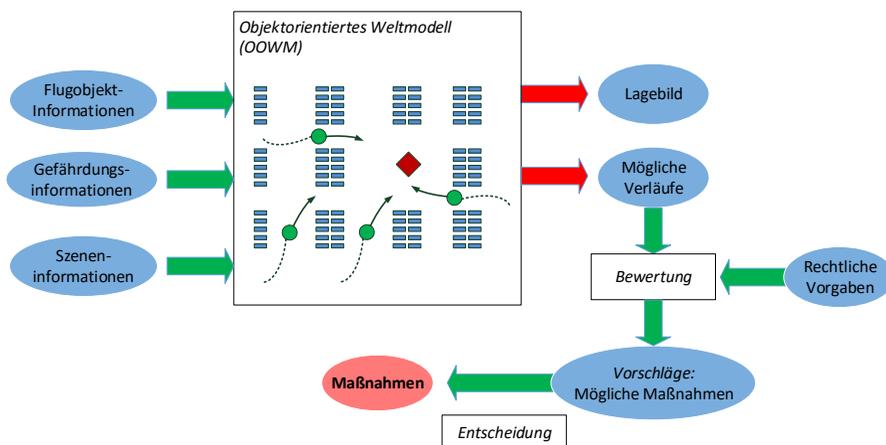
Konzept der Sensorsysteme

AP4 – Situationsanalyse 1 Feinklassifikation von UAVs

1. Erforschung und Festlegung der Parameter zur formalisierten Beschreibung von UAS
2. Erstellung einer UAS-Datenbank und Optimierung von Algorithmen für die Datenbanksuche
3. Entwicklung von Methoden zur Feinklassifikation von UAVs
4. Evaluierung der Klassifikationsmethoden
5. Parameter zur formalisierten Beschreibung einer Bedrohungslage und Erkennungsverfahren

Assistenz bei der Entscheidungsfindung im Falle einer potenziellen Gefährdung durch ein UAS

Situationsanalyse und Entscheidungsunterstützung



AP 5 – Umsetzung und Evaluierung Gesamtsystem



Arbeiten in AP5:

- Implementierung der Sensordatenfusion & UAV-Tracking
- Implementierung der Cloud- basierten modularen Flight Intelligence Plattform (FIP) mit Flugregister-Dienst
- Implementierung der Situations- und Risikoanalyse
- Kopplung der FIP mit dem Assistenzsystem zur Bewertung und Vorschlag von Abwehrmaßnahmen



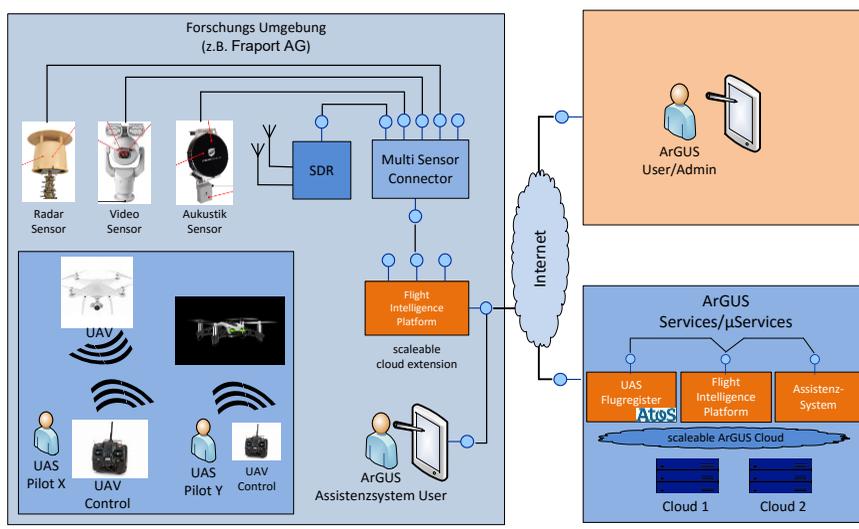
© Fraunhofer IOSB

35



Atos Deutschland

Möglicher ArGUS Demonstrator



© Fraunhofer IOSB

36



AP6 – Aus-, Fort- und Weiterbildung und Sensibilisierung



- AP6.1 Lehrinhalte „Schutz vor Drohnenmissbrauch“
 - Analyse des Status quo der derzeitigen Aus-, Fort- und Weiterbildung (Verbände und Dienstleister)
 - Evaluierung der notwendigen Ausbildungsinhalte
 - Erarbeitung möglicher Inhalte für Notfallszenarien und Alarmpläne
 - Erstellung eines Syllabus zur Implementierung

- AP6.2 Aktionsplan zur Sensibilisierung und Information der Bürgerinnen und Bürger
 - Ermittlung des Informations- und Sensibilisierungsbedarfs (Online-Umfrage)
 - Erarbeitung von Materialien, die geeignet sind Bürgerinnen und Bürger im Hinblick auf die von Drohnen ausgehende Gefahr zu sensibilisieren (Broschüre und Homepage)

Projektabschluss: Funktionsdemonstrator

- Realisierung als Funktionsmuster
- Demonstration in einem realistischen Szenario
- Nachweis der wesentlichen Eigenschaften:
 - Detektion
 - Klassifikation
 - Situationsanalyse
 - Entscheidungsunterstützung
- Dokumentation der rechtlichen Bewertung hinsichtlich Detektion und Reaktion
- Veranschaulichung der praktischen Relevanz

Zusammenfassung

- Drohnen sind vielfältig verfügbar und leicht zu beschaffen
- Der Nutzen ist hoch für viele Aufgabenbereiche
- Leider ist auch das Missbrauchspotenzial sehr hoch und die Gefahren schwer abzuschätzen
- Es gibt Ansätze dem zu begegnen durch Detektion, Klassifikation und Abwehrmaßnahmen
- Der Schutz durch geeignete Gegenmaßnahmen ist sehr hoch, wenn sie richtig gewählt und zeitnah angewendet werden

Ausblick

- Steigende Sensorqualität wird zu besseren Detektionsergebnissen und einer höheren Informationsqualität führen
- Steigende Kommunikationskapazität wird mehr Information verfügbar und nutzbar machen
- Bessere Simulationsverfahren werden zu besseren Prognosen und damit zu besserem Schutz führen
- Voraussichtliche Registrierungspflicht wird helfen
- Automatische Aktionen bleiben ausgeschlossen

Fachtagung
„'Neue' Technologien & ,neue' Bedrohungen“

Gesellschaft
für Informatik



Drohnen – Technologie, Einsatzgebiete und Risiken

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

FRAGEN?

Kontakt: Dr. Gunther Grasmann
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung
✉ Fraunhoferstraße 1, 76131 Karlsruhe
☎ +49 (0)721 6091-441
✉ gunther.grasmann@iosb.fraunhofer.de

© Fraunhofer IOSB

41



Fraunhofer
IOSB