Das Projekt KI-Inspektionsdrohne

Christian Bachmeir

Short Facts

Projektlaufzeit: *01.01.2018 – 31.12.2021*
Fördersumme: *623.000 €*

1 KURZZUSAMMENFASSUNG UND PROJEKTZIEL

Das Verbundvorhaben KI-Inspektionsdrohne, im Rahmen des Luftfahrtforschungsprogramms V [1], hat als Ziel Maintenance-, Repair- und Overhaul-(MRO-)Prozesse in der Luftfahrtindustrie zu beschleunigen, und damit die MRO-Industrie noch wettbewerbsfähiger zu machen. Im Vorhaben wird ein sicheres System zur Schadensdetektion und -bewertung von äußeren Flugzeugstrukturen unter Berücksichtigung aktueller Instandhaltungs-Anforderungen der Luftfahrtbranche entwickelt. Der entwickelte Prototyp integriert vernetzte UAV (Unmanned Aerial Vehicles – Unbemannte Flugsysteme), autonome Navigation und Schadensaufnahme und KI-gestützte Auswertung und stellt ein Decision Support System zur Verfügung bzw. fällt eigenständig Entscheidungen. Forschungsschwerpunkt der FHWS ist, bzw. Forschungsschwerpunkte sind industriespezifische Ende-zu-Ende-Security, KI, Safety, und insbesondere die Absicherung der mobilen, mit Cloud oder Edge verbundenen Einheiten gegen Cyberattacken.

Abbildung 1: Inspektionsdrohne mit Lidar und Kamera

2 AUSGANGSSITUATION UND ZIELSETZUNG

Der zu beschleunigende Prozess ist die Inspektion von Flugzeugen im Hangar. Diese findet meist in regelmäßigen Intervallen statt, kann aber auch anlassbezogen, beispielsweise nach einem Flug durch ein Gewitter, gewährleistet werden. Bisher wird diese Inspektion rein manuell durchgeführt: Fachpersonal schiebt verschiedene Aufbauten, Leitern und Gerüste zum Flugzeug, inspiziert gestützt durch Arbeitskarten das gesamte Flugzeug und meldet gefundene Schäden. Die Kosten eines stehenden Flugzeugs sind hoch, daher existiert hier ein Einsparpotenzial, das nun genutzt werden soll.

Ziel des Projektes ist es, eine Drohne zu entwickeln, die autonom um das Flugzeug im Hangar fliegen soll und das gesamte Flugzeug nach Schäden scannt. Diese gefundenen Schäden sollen dann KI-gestützt identifiziert und klassifiziert werden.

2.1 Konsortium

Das Projektkonsortium besteht aus der Lufthansa Technik, IBM und den drei wissenschaftlichen Partnern HSU, TUM und FHWS.

3 SCHWERPUNKTE DER FHWS

Ziel der FHWS ist die Verbesserung der IT-Sicherheit für das Gesamtsystem »KI-Inspektionsdrohne« gegenüber Cyber-Angriffen. Dazu wird ein Ende-zu-Ende-Security-Konzept entwickelt und auf das im Verbund entwickelte Gesamtsystem angepasst.

- Zunächst wird über einen Security-by-Design-Ansatz, angepasst an das Gesamtsystem, eine möglichst hohe Hürde für Cyber-Angriffe aufgebaut. Dies geschieht durch die Isolierung von Aviation- und Non-Aviation-Funktionalität.
- Die verbauten Sensoren werden auf Schwachstellen und Fehleranfälligkeit untersucht. Dazu werden Situationen analysiert, bei denen die Sensordaten unzuverlässig werden. Im Anschluss werden Mitigationsstrategien vorgeschlagen und umgesetzt.
- Die Kommunikation mit der Bodenstation wird nach Stand der Technik gesichert.
- Verbaute Komponenten werden nach Sicherheitskriterien bewertet und ausgewählt.
- Betriebs- und Notfallkonzepte werden zusammen mit den anderen Partnern entwickelt.
- Die KI wird sowohl im Hinblick auf Fehleranfälligkeit, als auch im Hinblick auf gezielte Angriffe analysiert. Insbesondere wird hier ein Augenmerk auf Adversarial Attacks gelegt.

4 EINORDNUNG IN DEN KONTEXT DER HOCHSCHULE

Im Rahmen des Projektes KI-Inspektionsdrohne werden zahlreiche Kompetenzen der Hochschule genutzt und weiter ausgebaut. Das Projektziel der Hochschule besteht in der Entwicklung eines sicheren, autonomen Drohnensystems, welches eine automatisierte KI-gestützte Inspektion im Rahmen eines MRO-Prozesses in einem besonders sensiblen Bereich (Flughafen) realisiert.

Mit dem Kompetenzzentrum für Künstliche Intelligenz und Robotik (CAIRO – Center for Artificial Intelligence and Robotics) und dem Kompetenzzentrum Industrial IoT, Security, kognitive-CPS/UAV bringt das IDEE die Kompetenzen in den Bereichen Künstliche Intelligenz und Security ein.

5 AKTUELLER STAND DES PROJEKTS

Das Projekt befindet sich auf der Zielgeraden. Im September 2021 wird eine Demonstration der Projektergebnisse stattfinden. Die entwickelte Drohne verfügt über ein SLAM-Modul, welches das Erkennen und vollständige Scannen eines stehenden Flugzeugs autonom ermöglicht. Die Daten werden auf eine Bodenstation transferiert und von einer KI analysiert.

Der Drohnen-Operator hat die Möglichkeit, mittels einer Fernsteuerung jederzeit einzugreifen und die Kontrolle über die Drohne zu übernehmen.

6 ÜBERBLICK ÜBER DIE ERGEBNISSE

6.1 Redundanzen

Für den Anwendungsfall wurde ein Hexacopter für geeignet erachtet, welcher den Verlust von 2 bis 3 Rotoren ausgleichen kann, je nachdem wo diese relativ zueinander positioniert sind.

Die Hardware wurde so gewählt, dass 3 IMUs (Inertial Measurements Units) redundant vorhanden sind. Eine davon reicht aus, stabil (potenziell mit leichtem Drift) eine Position zu halten. Zusätzlich verfügt die Drohne über einen um 360-Grad rotierenden Lidar (Infrarot-Laser basierte Abstandsmessung), der nochmals geschwenkt wird, um den kleinen Öffnungswinkel in die dritte Achse auszugleichen. Die Daten des Lidars werden für ein SLAM-System verwendet, welches die Drohne nochmals unabhängig im Raum verortet und akkumulierende Fehler der anderen Systeme ausgleicht. Die Erkennung des Flugzeugs sowie die Pfadplanung erfolgen auf den Daten des Lidars. Als weiteres redundantes System kann der Operator angesehen werden, der über eine AR-Brille die Wahrnehmung und Einschätzung der Drohne angezeigt bekommt und auch eingreifen kann.

6.2 Kommunikationssicherheit

Die FHWS integrierte Security in das Gesamtsystem mittels eines Security-by-Design Ansatzes. Besonderer Fokus war hierbei die Redundanz von Sensorsystemen und die Beschränkung der Kommunikation der Computing Units mit der Bodenstation auf ein Minimum. Als Kommunikationsmethode wurde ein State-of-the-Art WLAN gewählt, das auch gegen Deauthentification-Angriffe geschützt ist. Zusätzlich wurde die Anforderung spezifiziert, dass ein menschlicher Operator jederzeit die Kontrolle übernehmen kann. Dazu wurden handelsübliche Fernbedienungen auf Security-Aspekte hin analysiert.

6.3 Analyse vorhandener Drohnenfernsteuerungen

Die Fernbedienungen DT 7 der Firma DJI [2] und die Taranis X9D [3] von FRSky wurden mittels Reverse-Engineering-Methoden auf Sicherheitsfeatures hin untersucht. Als erstes Ergebnis ist hier anzumerken, dass die Firmware der DT 7 nur verschlüsselt ausgeliefert wird. Auf der Fernbedienung selbst wird diese dann entschlüsselt und aufgespielt. Daher war es notwendig, das Protokoll über Black-Box-Tests und einen Logic-Analyzer zu rekonstruieren. Schlussendlich war es möglich, sich zwischen den Funkcontroller der DT7 und den Microcontroller zu schalten und das Protokoll soweit zu reverse engineeren, dass ein Replay-Angriff geplant und demonstriert werden konnte [4]. Auch die Taranis X9D war anfällig gegen eine Übernahme der Kontrolle durch eine sorgfältig konstruierte Fernsteuerung.

FrSky wechselte jedoch während der Projektlaufzeit auf das neue ACCESS Protokoll, welches sich als deutlich resilienter erwies [5].

Abbildung 2: DT7 & Taranis X9D

7 BETRIEBSKONZEPT UND NOTFALLMAßNAHMEN

Es wurde ein Betriebskonzept nach den Zielen Security, Safety und Betriebssicherheit entwickelt. Auf der technischen Seite existieren eine Erkennung des Verlustes der Verbindung zur Bodenstation oder Ausfall anderer Systeme sowie entsprechende Notfallprozeduren (Inform Operator, Hold Position, Return to Home, Return to nearest free Space, Slow Descent).

Zusätzlich wurde ein Mindestabstand berechnet, den anderes Personal minimal zu einer Drohne halten muss, damit die Drohne oder ein Operator im Fehlerfall genügend Zeit zum Reagieren hat. Dieser Operator kann mittels einer Augmented-Reality-Brille die Wahrnehmung der Drohne nachvollziehen und so von der Drohne unerkannte Gefahren oder Probleme rechtzeitig erkennen und mittels einer Fernbedienung, die eine unabhängige Frequenz nutzt, jederzeit die Kontrolle über die Drohne übernehmen.

8 KI

Die entwickelte KI wurde mittels XAI(eXplainable AI)-Methoden analysiert und bewertet. Auch die Anfälligkeit gegen Adversarial Attacks wurde nachgewiesen. Vorschläge zur Verbesserung der Resilienz und Treffergenauigkeit der KI wurden eingebracht und werden gerade umgesetzt.

LITERATURVERZEICHNIS

[1] o. A. (2019), »Luftfahrtforschungsprogramm V«, DLR, verfügbar in: https://www.dlr.de/pt-lf/desktopdefault.aspx/tabid-8363/

[2] o. A., »DT 7«, DJI, verfügbar in: https://www.dji.com/de/dt7-dr16-rc-system/feature

[3] o. A., »Taranis X9D Plus«, FrSky, verfügbar in: https://www.frsky-rc.com/product/taranis-x9d-plus-2/

[4] Namboodiri, V.; Aravinthan, V.; Mohapatra, S. N.; Karimi, B.; Jewell, W. (2013), »Toward a secure wireless-based home area network for metering in smart grids«, IEEE Systems Journal, 8(2), S. 509–520.

[5] o. A., »ACCESS – Protokoll«, FrSky, verfügbar in: https://www.frsky-rc.com/frsky-advanced-communication-control-elevated-spread-spectrum-access-protocol-release/