AVIATION CYBER SECURITY STUDY

K. Kainrath[1], K. Gebeshuber[2], M. Fruhmann[2], M. Gruber[1]
1 FH JOANNEUM, Institut Luftfahrt, Alte Poststr. 149, 8020 Graz, Österreich
2 FH JOANNEUM, Institut Internet-Technologien & -Anwendungen, Werk-VI-Straße 46, 8605 Kapfenberg, Österreich

Zusammenfassung

Das Projekt „Aviation Cyber Security Study“ (ACySS) zielt darauf ab, aktuelle Angriffsmethoden auf ein Avionik-Netzwerk anzuwenden und dessen Sicherheit zu analysieren. Moderne Zivilflugzeuge wie der Airbus A380, oder die Boeing 787 sind mit der Netzwerktechnik „Avionics Full-Duplex Switched Ethernet“ (AFDX) ausgestattet. Eine weitere Entwicklung für sicherheitskritische Kommunikation bietet Time-Triggered Ethernet (TTEthernet). Den kritischen Datenverkehr im Flugzeug regeln Netzwerk Switches, aufbauend auf dem Ethernet IEEE 802.3 Netzwerkstandard, jedoch mit zusätzlichen Quality-of-Service (QoS) Features. Im gesamten Luftfahrzeug existieren unterschiedliche Bussysteme als Kommunikationsbackbone. Es stellt sich die Frage, ob kritische Elemente wie z.B. die Flugsteuerung (Cockpit Domäne) eventuell das gleiche Netzwerk wie die Kabinenkontrolle (Kabinen-Domäne) oder das In-flight Entertainment System (IFE, Passagier-Domäne) nutzen.
Ziel des Projekts ist es, anhand von Cyber-Angriffsmethoden die Sicherheit des Avionik-Netzwerkes basierend auf AFDX und TTEthernet zu überprüfen. Für die Simulation der unterschiedlichen Domänen (kritisch/unkritisch) wird ein Testbed aufgebaut. Damit soll getestet werden, ob die Möglichkeit besteht, durch Manipulation des Netzwerks ausgehend vom unkritischen Bereich der Passagier/Kabinen-Domäne Fehlfunktionen zu erzeugen, die bis hin zur Kontrolle der kritischen Cockpit-Domäne reichen könnten. Die daraus generierten Ergebnisse sollen Aufschlüsse für eine mögliche Überarbeitung des Netzwerkdesigns bzw. von Applikationen geben. Als Applikation gilt hier z.B. eine Funktion wie die Fahrwerksteuerung, die im Netzwerk ausgeführt wird. Dabei wird auch ein besonderes Augenmerk auf Safety-Maßnahmen in Bezug auf mögliche Security Updates gelegt.

1. EINLEITUNG

In den letzten 30 Jahren hat sich in der Luftfahrtindustrie die Integrierte-Modulare-Avionik, kurz IMA, als Avionik-Architektur durchgesetzt. Das Konzept der IMA sieht es vor, funktionelle Einheiten zu bilden. Ursprünglich wurden etwa die Flugsteuerung, die Kommunikationseinheit, oder die Navigationseinheit als Module mit standardisierten Schnittstellen entwickelt. Diese Module nennt man Line Replaceable Units (LRU). Jedes dieser Subsysteme ist funktionell in sich abgeschlossen. Geschützt werden diese Module durch Gehäuse, die nach den Gehäusebauformen für Avionik-Systeme wie ARINC 404A [1] (Aeronautical Radio Incorporated) und ARINC 600 [1] gebaut werden. Da für jedes Subsystem alle benötigten Funktionen innerhalb eines Gehäuses implementiert werden, kommt es häufig vor, dass gleiche Funktionen mehrfach bei unterschiedlichen Modulen existieren. Redundanz erreichte man hiermit durch die mehrfache Nutzung gleicher LRUs. Daraus entstand das Line Replaceable Module (LRM). Die Idee dabei ist, nicht mehr gesamte Teilsysteme, sondern nur einzelne Teilfunktionen als Module zu entwickeln. Diese Module werden dann ein Teil eines IMA-Racks. Innerhalb dieser Racks sind alle Module miteinander über ein Kommunikationsnetzwerk verbunden. Der Vorteil dieses Ansatzes ist die Möglichkeit, Ressourcen zu teilen. So werden Funktionen nicht mehr mehrfach implementiert und mehrere Teilsysteme können sich nun eine Funktionalität (z.B einen GPS-Empfänger) teilen. Das System kann dadurch auch leichter modernisiert werden, da man Module einfach durch weiterentwickelte Versionen ersetzen kann. Über einen aeronautischen Datenbus werden diese Module miteinander verbunden. Zuvor waren die einzelnen und zum Teil völlig unabhängigen Teilsysteme zu einem komplexen Gesamtsystem verbunden worden. So gab es für jeden Flugzeugtyp eine eigene Avionik.

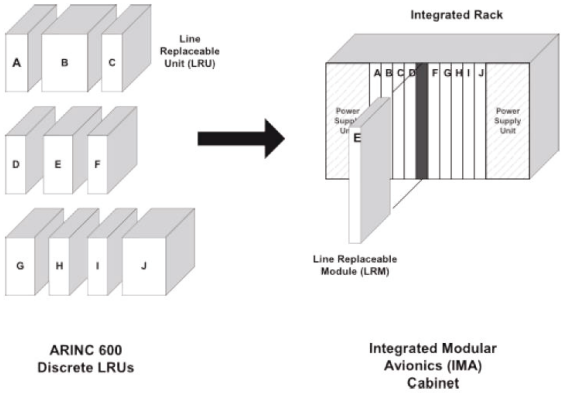

BILD 1. LRU und LRM [2]

Das IMA-System ist, wie der Name schon sagt und zuvor beschrieben wurde, modular aufgebaut, und kann entsprechend den Anforderungen problemlos erweitert werden. Das bedeutet, man kann das System einfach um

neue Funktionen erweitern, oder auch bestehende Funktionen leicht redundant ausführen und es so an die unterschiedlichen Voraussetzungen des jeweiligen Flugzeugtyps anpassen.

2. DATENBUS

Für eine reibungslose Kommunikation der Module ist der Datenbus verantwortlich. In den 70ger Jahren wurde für die allgemeine Luftfahrt der ARINC 429 Datenbus [2] zum Standard erhoben. Dieser unidirektionale Datenbus arbeitet zwar sehr langsam (12 bis 100 kbit/s), ist jedoch sehr zuverlässig. Andererseits war durch die Tatsache, dass der Bus unidirektional ist, der Verkabelungsaufwand enorm. Von Boeing wurde Anfang der 80ger Jahre ein weiterer Datenbus entwickelt, der 1989 zum ARINC 629 Standard erhoben wurde [3] und bis heute eingesetzt wird. Dieser Bus arbeitet als serieller bidirektionaler Bus (multiple Source, multiple Sink [4]) und hatte eine weit höhere Datenrate von 2 Mbit/s. Der Flugzeughersteller Airbus hat im Zuge der Entwicklung des A380 aufbauend auf der ARINC 664 Spezifikation Part 7 und dem IEEE 802.3 Netzwerk, allgemein als Ethernet bekannt, das Avionics Full-Duplex Switched Ethernet Netzwerk (AFDX) entwickelt und patentiert. Dieser Avionik-Datenbus wurde von der TU Wien und TTTech mit der TTEthernet Technologie erweitert und ist derzeit der fortschrittlichste, besitzt geringe Latenzen und hat eine hohe Datenrate von 100 Mbit/s.

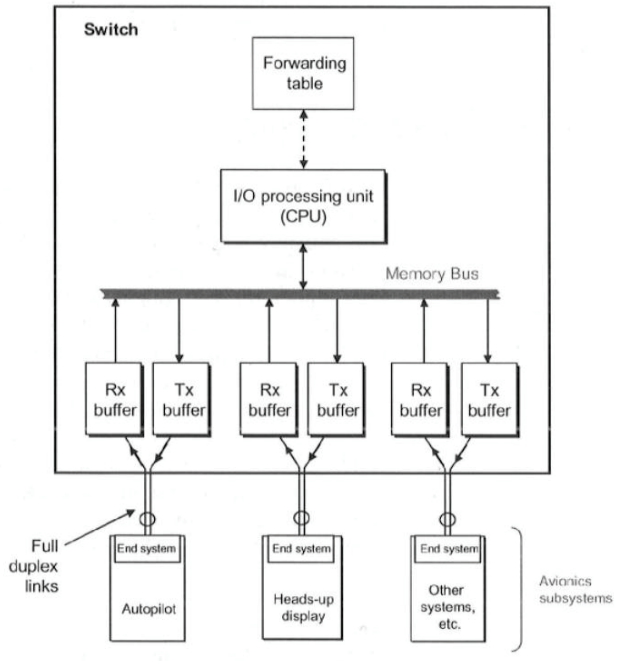

BILD 2. AFDX Switch [4]

Dadurch wird es möglich, IMA größeren Umfangs zu realisieren. Durch die Verwendung von Full-Duplex Ethernet [5] erreicht man eine Kollisionsvermeidung. Zusätzlich wird durch ein Quality-of-Service (QoS) Feature sichergestellt, dass kritische Nachrichten priorisiert werden und dadurch schneller an ihrem Ziel ankommen. Die Endgeräte werden über je ein twisted pair-Kabel zum Senden und Empfangen mit dem AFDX bzw. TTEthernet Switch verbunden. Innerhalb des Switches ist für jedes Subsystem ein Sende- und Empfangspuffer als FIFO Speicher implementiert. Der Switch regelt den Datenverkehr, indem er die Nachrichten aus den Puffern holt und mit Hilfe der Forwarding-Tabelle an die Zieladresse weiterleitet. Dieses Routing geschieht über eine Virtual Link ID, welche im AFDX Frame übertragen wird, analog einer MAC-Adresse einer Ethernet Nachricht. So wird der Typ der Nachricht über die Virtual Link ID identifiziert, welche sich aus einem 16-bit unsigned integer Wert zusammensetzt. Davor steht für Identifizierungszwecke eine konstante Bitfolge aus 32-Bit. Zusammen ergeben sie eine 6 Byte große Zieladresse. Der Switch ist nun so realisiert, dass er eine AFDX oder TTEthernet-Nachricht an exakt ein genau vorgegebenes Endsystem routet. Die moderne IMA, wie sie zum Beispiel im A380 Anwendung findet, wird nun folgendermaßen aufgebaut: Aus einer LRU wird eine “avionics application“ (z.B. Navigations Applikation). Diese Applikation ist über mehrere Integrated Avionics Modules – IAMs verteilt. Die IAMs stellen Rechenleistung, Speicher und I/O zur Verfügung. Externe Komponenten wie Displays, Sensoren und Aktuatoren können über standardisierte Interfaces angeschlossen werden. Eine Funktion wird auf einem oder mehreren Core Processing and I/O Modules (CPIOM) in einer partitionierten Umgebung ausgeführt. Dabei werden mehrere Module für eine Funktionalität verwendet, wodurch eine höhere Integrität und bessere Verfügbarkeit erreicht wird. Das Interface zwischen Ethernet-Netzwerk und bestehenden Datenbussen (ARINC 429, CAN, diskrete oder analoge Signale) wird durch ein sogenanntes I/O-Modul (IOM) hergestellt, welches jedoch keinen Host der Applikation darstellt.

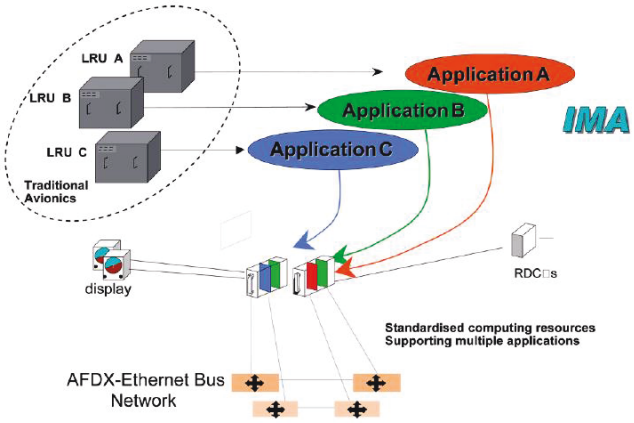

BILD 3. Konzept einer IMA [6]

Die IMA hat sich mittlerweile in drei Entwicklungsstufen weiterentwickelt. Die „First Generation IMA“ wird zum Beispiel bei der Boeing 777 als elektrische Einheit des Electrical Load Management System (ELMS) eingesetzt. Bei dieser ersten Generation gibt es einen Systemhersteller je Flugzeug [7], der dafür auch die Software zur Verfügung stellt. Der Aufbau der IMA ist verhältnismäßig einfach implementiert. Es wird eine Platine (PCB) als Backplane [8] verwendet und die einzelnen LRUs werden dediziert verkabelt und mit Spannung versorgt. Bei der „Second Generation IMA“ gibt es mehrere Hersteller für ein Modul des Gesamtsystems. Die Softwarefunktionalität kann zusätzlich zum System-Integrator auch von spezialisierten Modul-Herstellern zur Verfügung gestellt werden. Die Funktionalität wurde insgesamt verbessert und es wird eine teilweise offene Architektur für das Rack/Cabinet [9] verwendet. Für den

Datenaustausch wird eine serielle Backplane wie zum Beispiel ARINC 429 verwendet und die Spannungsversorgung wird wiederum mittels dedizierten Power Supply Units realisiert. Anwendung findet diese IMA-Generation etwa in der Boeing 777 als Feuermeldesystem oder zur Hydrauliksteuerung.

Die „Third Generation IMA“ besteht mittlerweile aus vielen standardisierten Modulen unterschiedlicher Hersteller. Sie bietet weitaus verbesserte Funktionalitäten im Vergleich zu den Vorgängergenerationen. Die Backplane wird hier aus Commercial off-the-shelf (COTS) [10] Komponenten aufgebaut, welche auch im gesamten Flugzeug für die Anbindung an das Netzwerk Verwendung finden. Diese Generation der IMA wird aktuell im A380 [7] verwendet. Dabei wird auch AFDX als Netzwerktechnik eingesetzt.

3. IN-FLIGHT ENTERTAINMENT

Um den Komfort der Flugreise zu erhöhen werden nahezu alle Mittel- und Langstreckenflugzeuge mit In-flight Entertainment-Systemen (IFE) ausgestattet. Die meisten dieser Systeme basieren auf einem einfachen Client Server Modell. Ein Server hat hierbei die gesamten Mediendaten gespeichert und kann diese an die Clients weitergeben. Das Client-Modul setzt sich meist aus einer Seat Electronic Box (SEB), in der die meiste Hardware untergebracht ist (meist unter dem Sitz montiert), und einem Bildschirm zusammen. Darüber kann der Fluggast sich gewünschte Medieninhalte aussuchen. Weiters besteht auch die Möglichkeit, sich diverse Flugdaten wie die aktuelle Geschwindigkeit, Höhe und Position auf einer interaktiven Karte anzeigen zu lassen. Da das IFE System auch in das Avionik-Netzwerk integriert ist, kann es auf diese Flugdaten zugreifen. Somit gehören zu einem Avionik-Netzwerk alle flugrelevanten Systeme genauso wie Kabinen- und Energiemanagement und auch das IFE. Um die Flugsicherheit zu gewährleisten, sind daher sicherheitskritische Betrachtungen des gesamten Avionik-Netzwerkes essentiell.

Der US Government Accountability Office (GAO) “AIR TRAFFIC CONTROL” Bericht [11] zeigt die möglichen Gefahren von Cyber Angriffen in modernen Flugzeugen auf. Durch die immer stärker werdende Vernetzung mit Verbindung zum Internet bzw. Wireless LAN im Flugzeug öffnen sich auch neue Angriffsflächen. Moderne Flugzeuge haben im Gegensatz zu älteren Modellen nur mehr ein gemeinsames Netzwerk, mit welchem einerseits weniger sicherheitskritische Systeme (IFE) aber auch sicherheitsrelevante Systeme (Flugsteuerung) verbunden sind. Der Bericht zeigt zwar keine bekannten Sicherheitslücken auf, allerdings besteht aufgrund der vorhandenen Infrastruktur und der steigenden Komplexität derartiger Systeme immer die Möglichkeit, dass Schwachstellen vorhanden sind.

Das GAO-Albtraum-Szenario ist ein Hacker am Boden, der durch Ausnutzung einer Sicherheitslücke im flugzeuginternen WLAN oder IFE-System Zugriff auf das Netzwerk im Flugzeug erhält (BILD 4). Durch Ausnutzung einer Sicherheitslücke der Firewall ist ein Zugriff aus dem Passagiernetzwerk in das Avionik-Netzwerk möglich und damit ist Zugang zur Flugzeugsteuerung gegeben. Die hohen Qualitätsansprüche in der Luftfahrt erschweren einfache Angriffe. Jegliche eingesetzte Avionik muss langwierige Zertifizierungsprozesse durchlaufen. Für Hardware gibt es die DO-254 [12] und für Software die DO-178c. [13] Diese sogenannten „Design Assurance Guidance“ werden von der RTCA [14] in Kooperation mit der EUROCAE [15] entwickelt. Sie geben genau die Richtlinien für den Entwurf von zertifizierbarer und somit einsetzbarer Avionik vor.

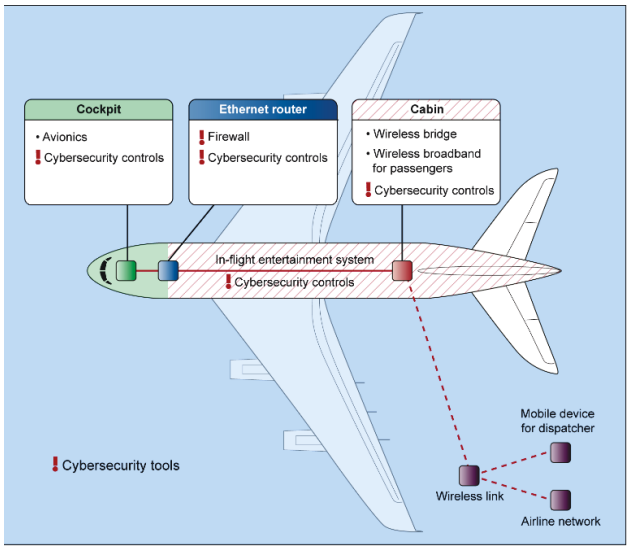

BILD 4: IP Konnektivität [11]

Standards im Bereich der Cyber Security sind DO-326A, und die Leitlinien in DO-355 und DO-356 bzw. die Europäischen Standards (ED-202A, ED-203 und ED-204). Diese Dokumente beinhalten allerdings nur einen ersten Satz von Leitlinien – eine Erweiterung der Standards wird auf Grund des verstärkten Bewusstseins derzeit geplant, konnte auf Grund der vielen offenen Punkte aber noch nicht abgeschlossen werden. [16], [17], [18], [19], [20]

Beispiele aus der Automobilindustrie zeigen allerdings, dass Angriffe durchaus möglich sind. So zeigen Miller und Valasek [21] anschaulich den Angriff auf ein Fahrzeug mit nachfolgender voller Kontrolle der internen Aktorik bis hin zur Beeinflussung des Lenk- bzw. Bremssystems. Ein Angriffsvektor aus dem Internet ist in diesem Fall durch Ausnutzung von Konfigurationsfehlern im von extern erreichbaren Telematik-System, über weitere Sicherheitslücken des internen Mediencenters bis hin zur Manipulation von Firmware auf Chipebene des Fahrzeugs möglich, um schlussendlich auf dem abgesicherten CAN-Bus des Fahrzeugs Steuerungsbefehle auszuführen. Die Hersteller haben darauf reagiert, bekannte Sicherheitslücken wurden geschlossen, wofür allerdings ein Rückruf von 1,4 Millionen Fahrzeugen notwendig war. [27]

4. TESTSZENARIEN

Um die strukturierte Vorgehensweise der Analyse sicherzustellen wird die Testmethodik in Anlehnung an das OSSTMM (Open Source Security Testing Methodology Manual V3) [22] gewählt. Eine umfassende Analyse muss gründlich erfolgen, hat alle vorhandenen Kanäle in das zu prüfende System zu berücksichtigen, muss nachvollziehbar und wiederholbar sein und

schlussendlich ist eine entsprechende Dokumentation des Testaufbaues und der Ergebnisse nötig.

Beginnend mit einer Modellierung des Systems aus Sicht eines Angreifers (Analog Threat Modelling von Applikationen) werden Ziele, Angriffsflächen, Angriffskanäle, Risiken und Schwachstellen analysiert und dargestellt. Das System wird zuerst in seine Teilkomponenten zerlegt, Kommunikationswege, Vertrauensverhältnisse und Vertrauensübergänge innerhalb des Systems werden markiert. Dann erfolgt die Identifikation von Eingangspunkten über die ein potentieller Angreifer mit dem System interagieren kann. Weiters erfolgt die Identifikation von Informationen oder Bereichen an denen ein Angreifer interessiert sein kann. Einzelne Bedrohungen werden klassifiziert, dazu kann z.B. das STRIDE Threat-Model herangezogen werden. Die Klassifizierung erfolgt sowohl aus Sicht des Angreifers, als auch aus Sicht der Verteidigung. Nach Auswahl von möglichen, kritischen Angriffspfaden werden auf verschiedenen Netzwerk- und Applikationsebenen Security Tests durchgeführt. Dabei kommen gezielt Testmethoden (Penetration Testing), wie sie auch in anderen kritischen Domänen Anwendung finden, zum Einsatz.

Alleine die Anzahl der möglichen Eingangskanäle im Flugzeug ist beeindruckend: Radar, GPS, ADS-B, WLAN, Bluetooth, Netzwerkverkabelung, Internet, Wartungsdatenkanäle, physikalischer Zugriff, USB, Sprachfunk, Datenfunk, Satellitenkommunikation und weitere.

Die Norm ISO 27005 [23] definiert den Begriff „Vulnerability“ (Verwundbarkeit) als Schwäche eines „Assets“ (Vermögenswert), die von einer oder mehreren „Threats“ (Bedrohungen) ausgenützt werden kann. Die Ausnutzung von Verwundbarkeiten soll in diesem Projekt speziell im Bereich von unerlaubten Zugriff, Beeinflussung der Verfügbarkeit (Denial of Service) und Beeinflussung bzw. Manipulation der Funktionalität untersucht werden. Sollten bei den Security Analysen Auswirkungen auf die Betriebssicherheit (Safety) erkannt werden, so sind diese einer getrennten Betrachtung zu unterziehen.

4.1. Analyse der In-flight Entertainment Systeme

In-flight Entertainment Systeme sind ein fixer Bestandteil nahezu jedes neuen Zivilflugzeuges und leisten einen großen Beitrag zur Verbesserung der Reisequalität. Das Bemühen der Airlines, ihre Chancen im engen Wettbewerb um die Gunst der Flugpassagiere zu verbessern, führt zur Entwicklung und Installation von immer vielseitigeren und leistungsfähigeren Systemen. Aufgrund der steigenden Komplexität dieser Systeme steigt aber auch die Anfälligkeit bezüglich des Missbrauchs, unter anderem auch in Hinsicht auf ihre potentielle Vernetzung mit wichtigen Flugsteuerungssystemen.

Im Zuge dieses Projektes sollen aktuelle In-flight Entertainment Systeme auf potentielle Verwundbarkeiten untersucht werden und wie diese missbräuchlich verwendet werden können. Beispiel für die zu testende Möglichkeiten:

- Das System durch unerwartete Eingaben zu Fehlverhalten zu bewegen
- Physikalischen Zugang zu den verschiedenen Komponenten des Systems zu erhalten, um das System für eigene Zwecken zu modifizieren beziehungsweise dessen Netzwerkverbindungen mit eigenen Geräten zu missbrauchen
- Manipulation des Entertainment-Systems beim Passagier (Entfernung Schutzabdeckung, Rahmen, etc.)
- Verwundbarkeiten bezüglich manipulierter, eingeschleuster Medieninhalten zu finden
- Das System über Mobilgeräte und Notebooks über zur Verfügung stehende Wireless LAN oder Ethernet Verbindungen zu attackieren
- Finden von potentiellen Zugangspunkten durch Analyse von eingesetzter Firmware (Reverse Engineering)

Aus den potentiellen missbräuchlichen Zugangsmöglichkeiten sollen dann mögliche Gefährdungen des regulären Flugbetriebes eruiert werden, unter anderem:

- Störung oder Beschädigung einzelner oder mehrerer Entertainment-Systemkomponenten
- Einschleusen von nicht autorisierten Inhalten zur Manipulation des Verhaltens von Passagieren (Panik oder Einschüchternung)
- Manipulation (Störung, Beschädigung, Zugriff) potentiell erreichbarer Flugsteuerungssysteme

4.2. Analyse der Netzwerkinfrastruktur

Dieser Themenbereich behandelt die Analyse der Netzwerkinfrastruktur in Bezug auf potentielle Verwundbarkeiten. Dabei werden einerseits Zugangsmöglichkeiten für Angreifer zum Netzwerk und anderseits die Ausnutzung von möglichen Sicherheitsschwächen analysiert. Die Funktionalität von vernetzten Systemen kann im OSI Schichtenmodell (ISO/IEC 7498-1 [24]) abgebildet werden. Es bietet sich an, die Security-Analyse auch auf Basis der einzelnen Netzwerkschichten aufzubauen. Dabei unterscheiden sich Analyse- und Angriffsmethoden auf den transportorientierten Schichten (Layer 1-4) [24] merklich von den Methoden auf den anwendungsorientierten Schichten (Layer 5-7). Im **ersten** Schritt soll die Analyse des Aufbaues und der Konfiguration des Netzwerkes erfolgen:

- Analyse der Netzwerkarchitektur
- Analyse der Gemeinsamkeiten/Unterschiede von AFDX und TTEthernet zu Standard-Ethernet
- Analyse der Gemeinsamkeiten/Unterschiede zu Standard-IP-Netzwerken

- Analyse von möglichen Netzwerkübergängen zwischen Passagier- und Avionik Netzwerk und deren Absicherung
- Analyse der Konfigurationsdaten von Switches, Router, Firewalls
- Analyse der eingesetzten Netzwerk-Protokolle (Routing, Redundanz, Management)
- Analyse der Firmware von Netzwerkgeräten (Reverse Engineering)

Der **zweite** Schritt umfasst umfangreiche Tests auf den verschiedenen Netzwerkschichten:

- Die Untersuchungen des Netzwerks auf der physikalischen Ebene (L1) [24] können grob in 2 unterschiedliche Bereiche unterteilt werden:
  1. Angriffe ohne mechanisch-physikalischen Zugriff auf jedwede Teile des Netzwerks
  2. Angriffe mit mechanisch-physikalischen Zugriff auf einzelne oder mehrere Teile des Netzwerks

Dabei werden sämtliche am Netzwerk angeschlossenen Geräte ebenso wie die Verkabelung (inklusive Steckverbindern) als zu untersuchende Bestandteile des Netzwerks definiert. Der Versuch, mechanisch-physikalischen Zugang zum Netzwerk zu erhalten soll dabei auf folgende Arten (abhängig von der jeweiligen Netzwerk-Sicherheitsdomäne) erfolgen:

- Suche nach frei zugänglichen Netzwerk-Steckverbindern
- Physikalische Anzapfung des Übertragungskanals (wiretapping)
- Attacken ohne mechanisch-physikalischen Zugang zum Netzwerk werden unspezifisch (räumliche Nähe einzelner Netzwerk-Komponenten) oder spezifisch über drahtlose Netzwerktechniken (im Speziellen WLAN gem. IEEE 802.11x) durchgeführt.

Grundsätzlich soll untersucht werden, welche der folgenden fundamentalen Kategorien an sicherheitsrelevanten Netzwerk-Störungen durch Angriffe auf den Physical Layer hervorgerufen werden können:

- Teilweise oder vollständige Inoperabilität des Netzwerks (denial of service)
- Belauschen des Datenverkehrs am Netzwerk (eavesdropping)
- Manipulation der transferierten Daten/Signale
- Einschleusen von Daten/Signalen

Dabei sollen folgende (Angriffs-) Techniken Anwendung finden:

- Applikation von Störsignalen unterschiedlicher Intensität und Frequenzen (→ Untersuchung EMV-Verträglichkeit)
- Applikation von Störsignalen über USB (USB-Bomb → Untersuchung EMV-Verträglichkeit)
- Applikation von zusätzlichen Signalen, die den L1-Spezifikationen des Netzwerks entsprechen, logisch-inhaltlich jedoch außerhalb des Übertragungskontext stehen (Paket-Injektion → Untersuchung Datenintegrität, Echtzeitverhalten unter Last/Störung)
- L1-Repeat-/Echo-Attacken (→ Untersuchung Datenintegrität, Echtzeitverhalten unter Last/Störung)
- Überflutung (flooding) des Netzwerks durch vom Angreifer generierte Pakete (→ Untersuchung Datenintegrität, Echtzeitverhalten unter Last/Störung)
- Test des Systemverhaltens bei Kurzschluss bzw. Unterbrechung einer oder mehrerer Übertragungsstrecken (→ Untersuchung Systemstabilität/-redundanz)

Zur Bewertung der Ergebnisse der o. a. Untersuchungen erfolgt eine Risikoanalyse, welche die Angriffsszenarien nach (Eintritts-) Wahrscheinlichkeit und Auswirkung quantifiziert. Ist ein physikalischer Zugriff auf das Netzwerk möglich, so stehen einem Angreifer in den höheren Netzwerkschichten zahlreiche Möglichkeiten zur Verfügung um Daten am Netzwerk mitzulesen bzw. auch Nachrichten einzuschleusen und zu manipulieren. Ob diese Schritte im konkreten Fall ausnutzbar sind, hängt sehr stark von der Konfiguration der Netzwerkkomponenten bzw. auch von installierten Alarmierungs- und Monitoring-Systemen ab. Grundsätzlich gilt es zu untersuchen, ob die Ursache etwaig aufgetretener Schwachstellen im Bereich der Implementierung, Konfiguration oder dem zugrundeliegenden Regelwerk liegt.

5. AKTUELLER STAND UND AUSSICHTEN

Die in modernen Flugzeugen eingesetzte Hardware ist für allgemeine Forschungszwecke einerseits schwer erhältlich und andererseits sehr teuer. Es ist trotz hoher Sicherheitsanforderungen und langwierigen Zulassungsprozederen nicht auszuschließen, dass die Systeme kleine Fehler aufweisen. Auch wenn es in der Luftfahrt unter anderem die DO-254 (Hardware) [12] und die DO-178c (Software) [13] als Safety- und z.B. die DO-326A [16] als Security-Standards gibt, existiert kein absolut sicheres Betriebssystem, genauso wenig wie es absolut sichere Software oder Firmware gibt. Daher ist es auch in dem Bereich der Avionik-Bussysteme wichtig,

Systeme regelmäßigen Untersuchungen zu unterziehen, ob sie den aktuellen Sicherheitsstandards entsprechen.

ACySS setzt genau hier an. Mit der Firma TTTech [25] konnte ein Partner für das Projekt gewonnen werden, der in der Entwicklung von sicherheitsrelevanten Bauteilen für Avionik-Busse tätig ist. Hier ergibt sich die einmalige Gelegenheit, Avionik-Hardware aus erster Hand für Testzwecke zu beziehen. Weiters ist auch die Firma AMES [26] an dem Projekt beteiligt. Sie sind Systemintegratoren und rüsten Flugzeuge unter anderem mit aktuellen IFE Systemen nach.

Der Aufbau des Testlabors ist nahezu abgeschlossen. Für die Analyse der Netzwerkinfrastruktur wird ein TTE Development System der Firma TTTech eingestzt. Dieses System beinhaltet klassische PCs, die als Endpunkte fungieren, und einen zertifizierten TTE Switch. An diesem Aufbau werden die in 4.2 genannten Testszenarien durchgeführt. Um einen DoS hervorzurufen, wird massiver Daten Traffic erzeugt und an den Switch gesendet. Hierfür wurde ein spezieller Aufbau mittels Einplatinenrechnern (Single Board Computers – SBCs) gefertigt. Dabei erzeugen 20 Raspberry Pis Traffic (Bild 4).

BILD 5. Traffic Generator aus Raspberry Pis

Mit einem extra angeschafften Netzwerk-Test-access-port (TAP) soll auch an dem Traffic „gelauscht“ werden und in weiterer Folge auch getestet werden, ob eine Manipulation der transferierten Daten Störungen hervorruft.

Bezüglich In-flight Entertainment wurden eingehende Recherchen unternommen und bekannte Hersteller kontaktiert, um ein Testsystem zu erhalten. Es erklärte sich, nach anfänglichem Interesse kein Hersteller zu einer Kooperation bereit. Aus diesem Grund wurde ein IFE System mit Hilfe eines System-Integrators realitätsnah nachgebildet. Dieses System besteht aus einer Server Unit sowie Clients und befindet sich derzeit im Aufbau. Die Server Unit soll dabei hauptsächlich die Synchronisation und Aktualisierung der Client Software übernehmen, sowie deren Funktion überwachen. Anders als bei klassischen Server-Client Systemen, sind die Medien bei dem Testsystem auch lokal auf jedem Client gespeichert. Das hat den Vorteil, dass bei einem Ausfall der Server Unit, der Passagier weiterhin Medien konsumieren kann. Die Clients bilden die Schnittstelle der Passagiere zur Passagierdomäne des Netzwerks.

Der Aufbau des Testclusters ist nahezu abgeschlossen. In der nächsten Phase des Projekts werden die verschiedenen in Punkt 4.1 und 4.2 genannten Szenarien getestet. Idealerweise soll dieser Aufbau als Plattform für zukünftige Security Tests dienen. Security wird auch im Hinblick auf die zukünftige Integration von unbemannten Fluggeräten im öffentlichen Luftraum von großem Interesse sein. Hierfür wird mit der Aviation Cyber Security Studie eine Basis geschaffen, die in Zukunft sowohl für die bemannte sowie die unbemannte Luftfahrt als Referenz verwendet werden kann.

Abkürzungen

AFDX – Avionics Full Duplex Switched Ethernet

ARINC - Aeronautical Radio Incorporated

CPIOM – Core Processing and I/O Modules

COTS – Commercial off-the-shelf

DoS – Denial of Service

ELMS – Electric Load Management System

GAO- Government Accountability Office

IFE- In-flight entertainment

OSI – Open System Interconnection

OSSTMM – Open Source Security Testing Methodology Manual

SBC – Single Board Computer

SEB – Seat electronic box

TAP – Test access port

TTE – Time Triggered Ethernet

Literaturverzeichnis

[01] ARINC Standards. http://www.aviation-ia.com/standards/, [Online, letzter Besuch 24.08.2017]

[02] ARINC429 Specification Tutorial, AIM GmbH https://www.aim-online.com/pdf/OVIEW429.PDF, 2012 [Online, letzter Besuch 24.08.2017]

[03] A. Gabillon, L. Gallon,: Availability of ARINC 629 Avionic Data Bus, http://gallon.perso.univ-pau.fr/publis/jnw2007.pdf Universität Pau 2006 [Online, letzter Besuch 24.08.2017]

[04] Helge Andreas Lauterbach: Avionik in Zivilflugzeugen, https://wuecampus2.uni-wuerzburg.de/moodle/pluginfile.php/667865/mod_resource/content/1/CivilAvionics_IntegratedMod

ularAvionics.pdf, Seminar Avionic Devices im SS2012 [Online, letzter Besuch 24.08.2017]

[05] IEEE 802.3 Ethernet Working Group. http://www.ieee802.org/3/, [Online, letzter Besuch 24.08.2017]

[06] R. Collinson: Introduction to Avionic Systems, Springer, Heidelberg, 3rd edition, 2011

[07] A380 Integrated Modular Avionics – The history, objectives and challenges of the deployment of IMA on A380 http://www.artist-embedded.org/docs/Events/2007/IMA/Slides/ARTIST2_IMA_Itier.pdf 2007 [Online, letzter Besuch 24.08.2017]

[08] ITWissen – Backplane http://www.itwissen.info/definition/lexikon/Backplane-BP-backplane.html [Online, letzter Besuch 24.08.2017]

[09] Jim Moore – Smiths Industries, Advanced Distributed Architectures Aerospace http://www.davi.ws/avionics/TheAvionicsHandbook_Cap_33.pdf, [Online, letzter Besuch 24.08.2017]

[10] ITWissen – COTS (Commercial Off-the-shelf) http://www.itwissen.info/COTS-commercial-off-the-shelf.html [Online, letzter Besuch 24.08.2017]

[11] United States Government Accountability Office. http://www.gao.gov/assets/670/669627.pdf, April 2015 [Online, letzter Besuch 24.08.2017]

[12] Dr. Paul Marriott, Anthony D. Stone: Synopsys, Inc Understanding DO-254 Compliance for the Verification of Airborne Digital Hardware, Whitepaper, October 2009 [Online, letzter Besuch 24.08.2017]

[13] Sven Nordhoff: DO-178C/ED-12C. The new software standard for the avionic industry: goals, changes and challenges, Whitepaper, 2012 [Online, letzter Besuch 24.08.2017]

[14] RTCA- Radio Technical Comission for Aeronautics. http://www.rtca.org/, [Online, letzter Besuch 24.08.2017]

[15] EUROCAE – European Organization for Civil Aviation Equipment. https://www.**eurocae**.net/,[Online, letzter Besuch 24.08.2017]

[16] DO-326A Airworthiness Security Process Specification, http://www.rtca.org/store_product.asp?prodid=1173, Aug 2014 [Online, letzter Besuch 24.08.2017]

[17] DO-355 Information Security Guidance for Continuing Airworthiness, http://www.rtca.org/store_product.asp?prodid=1170 June 2014 [Online, letzter Besuch 24.08.2017]

[18] DO-356 Airworthiness Security Methods and Considerations, http://www.rtca.org/store_product.asp?prodid=1176 Sept 2014, [Online, letzter Besuch 24.08.2017]

[19] ED-202A - Airworthiness Security Process Specification, https://www.eurocae.net/eshop/catalog/product_info.php?products_id=380 , [Online, letzter Besuch 24.08.2017]

[20] ED-204 - Information Security Guidance for Continuing Airworthiness, https://www.eurocae.net/eshop/catalog/product_info.php?products_id=374 [Online, letzter Besuch 24.08.2017]

[21] Dr. C. Miller, C. Valasek: http://illmatics.com/Remote%20Car%20Hacking.pdf, August 2015 [Online, letzter Besuch 24.08.2017]

[22] Open Source Security Testing Methodology Manual (OSSTMM). http://www.isecom.org/research/osstmm.html, 2010 [Online, letzter Besuch 24.08.2017]

[23] ISO/IEC 27005:2011 – Information technology -- Security techniques -- Information security risk management http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742, [Online, letzter Besuch 24.08.2017]

[24] OSI-Schichten-Modell http://www.netzwerke.com/OSI-Schichten-Modell.htm [Online, letzter Besuch 24.08.2017]

[25] TTTech: Robust Networked Safety Controls https://www.tttech.com/ [Online, letzter Besuch 24.08.2017]

[26] AMES - Aerospace and Mechanical Engineering Services http://www.ames.aero/ [Online, letzter Besuch 24.08.2017]

[27] Wired Magazine – Hackers Remotely Kill a Jeep on the Highway, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Online, letzter Besuch 24.08.2017]

[28] Threat Risk Modeling, https://www.owasp.org/index.php/Threat_Risk_Modeling [Online, letzter Besuch 24.08.2017]