Informationssicherheit bei Flugzeugen – Eine Einordnung

HAMBURG AEROSPACE LECTURE SERIES (AEROLECTURES)

7. DEZEMBER 2023

V. HAFNER

https://doi.org/10.5281/zenodo.10342347

CODE Institut - Kurzvorstellung & Überblick

Übersicht über die Doktorvater / Mutter-Familie

Herr Prof. Dr. Wolfgang Hommel

Professur für IT-Sicherheit von Software und Daten mit Schwerpunkt u.a. auf Hardening, Implementation, Konzepte und Modelle

Herr Prof. Dr. Dieter Scholz

Professor für Flugzeugentwurf, Flugzeugsysteme und Flugmechanik

Leiter Aircraft Design und Systems Group (AERO)

Frau Prof. Dr. Dreo

Aufnahme und Beginn der Dissertation bis zwischen 2018 und 2022

Lehrstuhl für Kommunikationssysteme und Netzsicherheit

Angaben zum Doktorand V. Hafner

LMU M.A. (Magister Artium) in Sozial- und Wirtschaftsgeschichte, Psychologie und Rechtswissenschaften

IT-Akademie Ulm - Ausbildung zum Systemadministrator

Hochschule Aalen - M.Sc. (Master of Science) in IT-Sicherheitsmanagement

Uni Bw München - Doktorand zum Thema Standards der Informationssicherheit in der Luftfahrt (Thema seit 2018)

Zur Zeit Lead Expert für Informationssicherheit in Fürstenfeldbruck

BSI zertifizierter Berater für Standards der Informationssicherheit

TISP Zertifizierung nach TeleTrust

Lead Auditor Qualifikation nach IRCA für ISO 27001 und BITKOM Zertifizierung für Notfallmanagement

Die Präsentation im Überblick

1. Ziel des heutigen Vortrags

- Zwänge und Rahmenbedingungen

2. Ein Kontrast der Zeiten der Cockpitsteuerung am Beispiel von eingebetteten Geräten

- Basisbegriffe und Definitionen

3. Öffentliches Fachgespräch zur Informationssicherheit in Flugzeugen

- Warum?

4. Akzente aus dem Forschungsstand zur Informationssicherheit im Flugzeugumfeld

- Kurzer Überblick

5. Flugzeuge in der Interaktion mit dem Begriff der Informationssicherheit

- Abgrenzung, Dimensionen, künftige Entwicklungslinie

1. Ziel des heutigen Vortrags & Zwänge und Rahmen-bedingungen

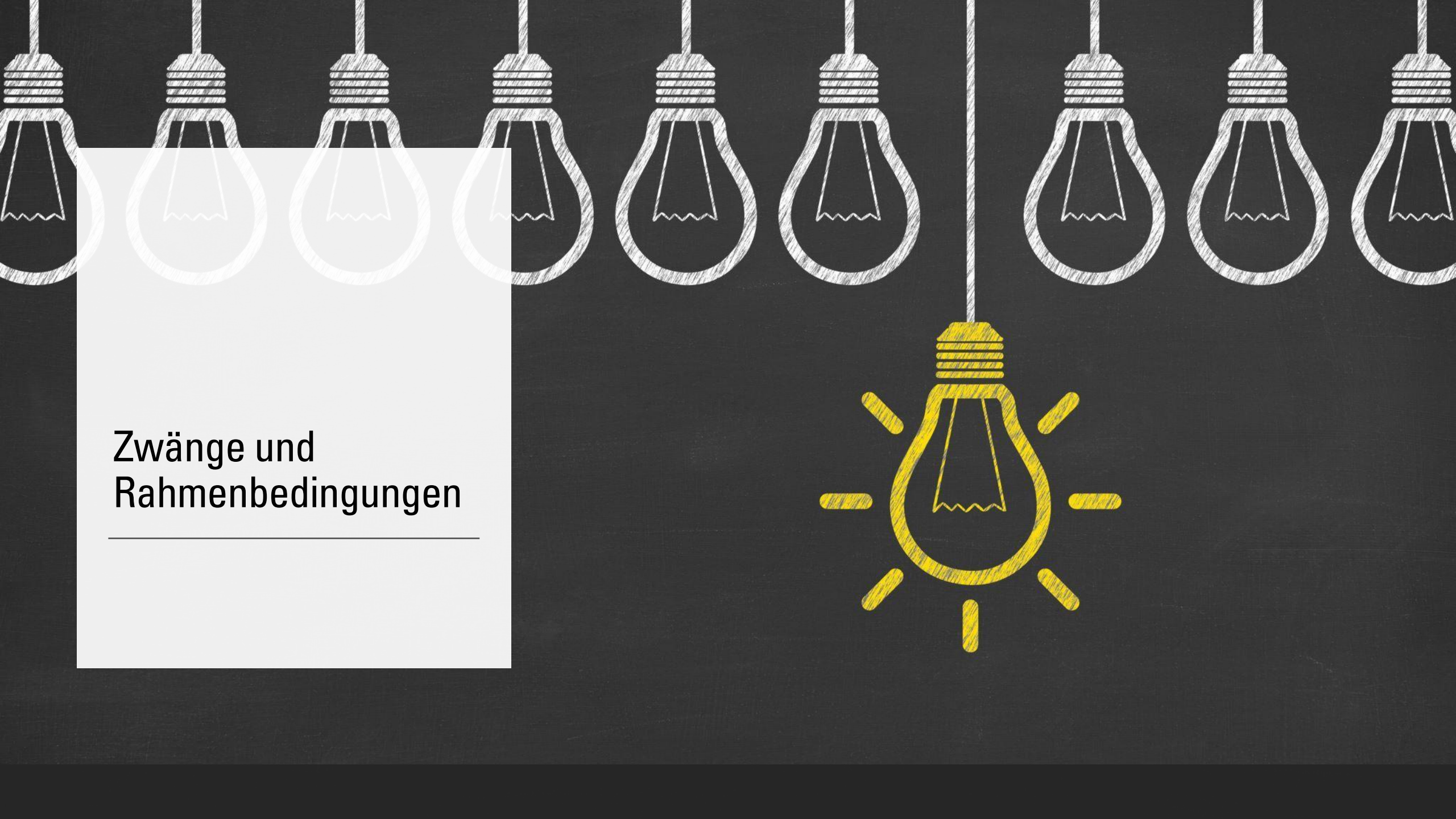
Darstellung entscheidender standardsbezogener Basisbegriffe, von denen die Debatte rund um Informationssicherheit bei Flugzeugen abhängt

❖siehe dazu die Anekdote von der AERO 2023 in Friedrichshafen zum Schluss

Hervorhebung der **Aspekte**, die für die Diskussion über die **Informationssicherheit bei Flugzeugen** von Bedeutung sind

Sensibilisierung im Zusammenhang zwischen Flugzeugen und Informationssicherheit

Zwänge und Rahmenbedingungen



Zwänge und Rahmenbedingungen

Keine Inhalte mit technischem Detaillierungsgrad in Form von Protokollen, technischen Detailzeichnungen und deren Erläuterungen

Alle verwendeten Quellen sind offen und frei zugänglich, sei es analog in Bibliotheken, im Online-Format im Internet oder auf Anfrage bei Institutionen

Das Abstraktionsniveau soll Fachleute und an diesem Thema Interessierte ansprechen

Grenzen der Auslegung

Die **Interpretation** der folgenden Aspekte der Informationssicherheit in und im Zusammenhang mit Flugzeugen **unterliegt der individuellen Subjektivität**

Kein Anspruch auf Deutungshoheit weder aus theoretischer noch aus konzeptioneller Sicht

Keine abschließender Behandlung der Informationssicherheit in Flugzeugen

Keine Nennung von Herstellern und ihren Produktmarken sowie von Zulieferern und ihren Produktmarken mit Klarnamen **zur Vermeidung unbeabsichtigter Assoziationen**

Der **Schwerpunkt** dieses Vortrags **liegt auf der übergeordneten Debatte** und nicht auf konkreten Flugzeugen oder eingebauten Produkten

Grenzen der Auslegung

Unbemannte Fluggeräte mit der **Problematik**

- Der **dauerhaften Online-Verbindung** zu einem Kontrollzentrum bzw. einer Kommando- und Kontrollinfrastruktur,
- der **Integrität der Informationen**, die in einem unbemannten System zur Verarbeitung vorgehalten werden müssen,
- der **Absicherung der Online-Schnittstellen**

sind **nicht Teil und Fokus dieses Vortrags**

Keine Vorstellung individueller Lösungen für Flugzeuge oder Flugzeugtypen

2. Ein Kontrast der Zeiten der Cockpitsteuerung am Beispiel von eingebetteten Geräten. Basisbegriffe und Definitionen

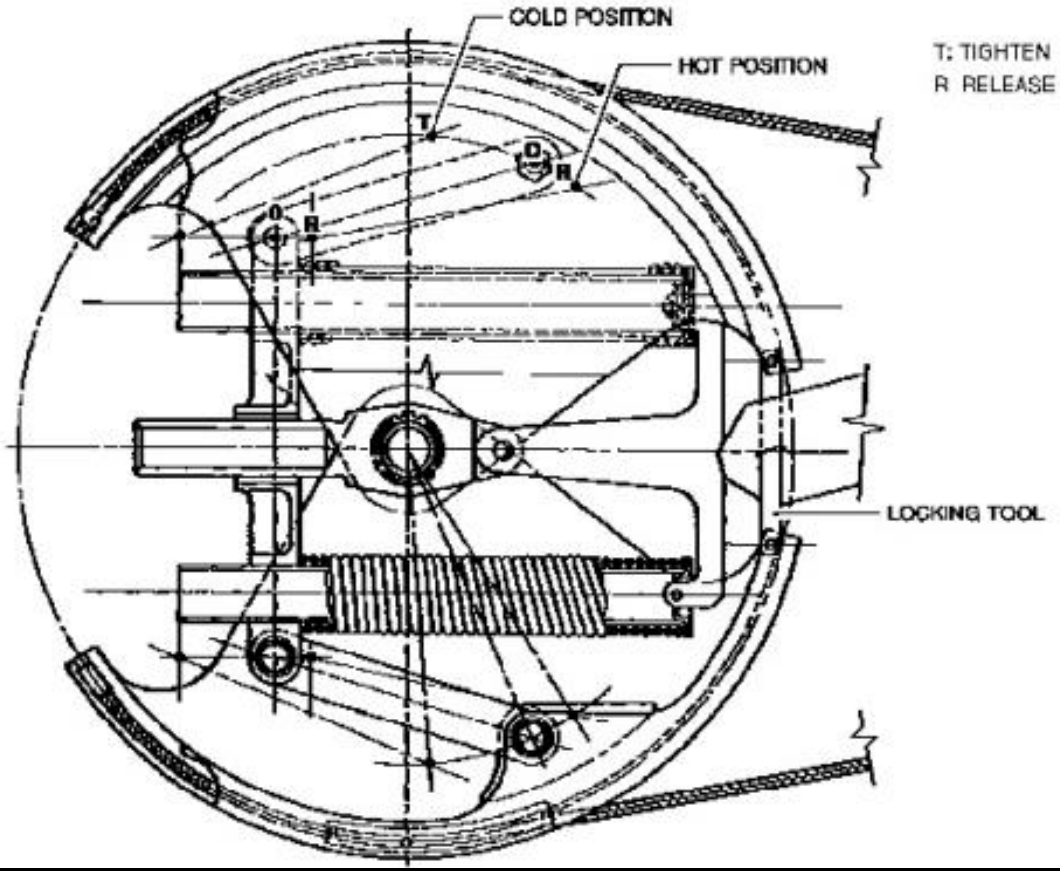
Ausgangslage

Vom Zugseil zum eingebetteten System am Beispiel der Cockpitsteuerung

Ursprünglich mechanische Flugsteuerung

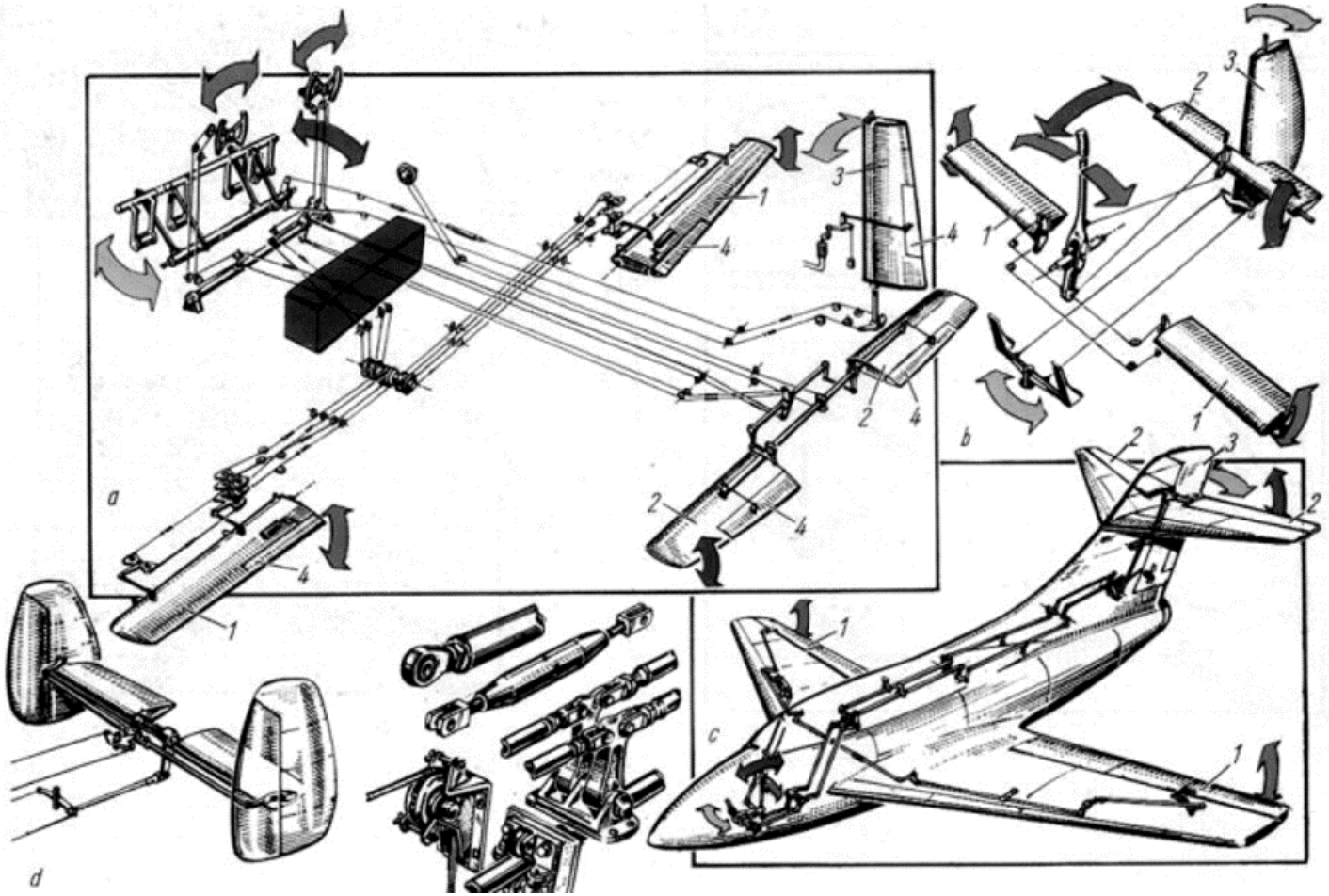
die **Übertragung der Steuerbefehle von den Steuersysteme** wie Steuersäule zu den Ruderflächen, **erfolgte** zunächst **mechanisch** (Seilzüge, Gestänge), später mit Unterstützung hydraulischer Übertragungssysteme

Frühere Cockpitsteuerung - Seilquadranten



Seilzügen und Stahlseilen
Seilführung unter dem Sitz (Rumpf) des Flugzeug

Dieses Foto von "Seilquadranten (Bild 6.29)" stammt von https://www.fzt.haw-hamburg.de/pers/Scholz/materialFS/FS_Skript_6-Flugsteuerung.pdf.



Frühere Cockpitsteuerung - Seilführungen

Dieses Foto von "Bild 2.3: Beispiele konventioneller mechanischer Flugsteuerungssysteme [39]" stammt von https://www.opendata.uni-halle.de/bitstream/1981185920/10956/1/GunHaase.pdf

Vom Zugseil zum eingebetteten System am Beispiel der Cockpitsteuerung

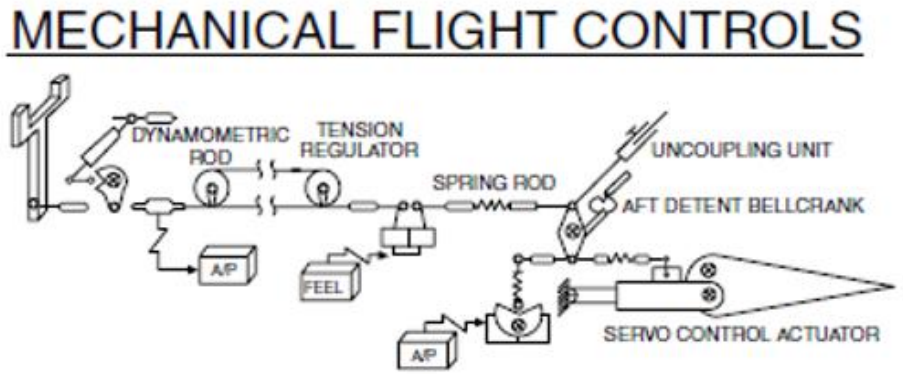
Antikes Cockpit

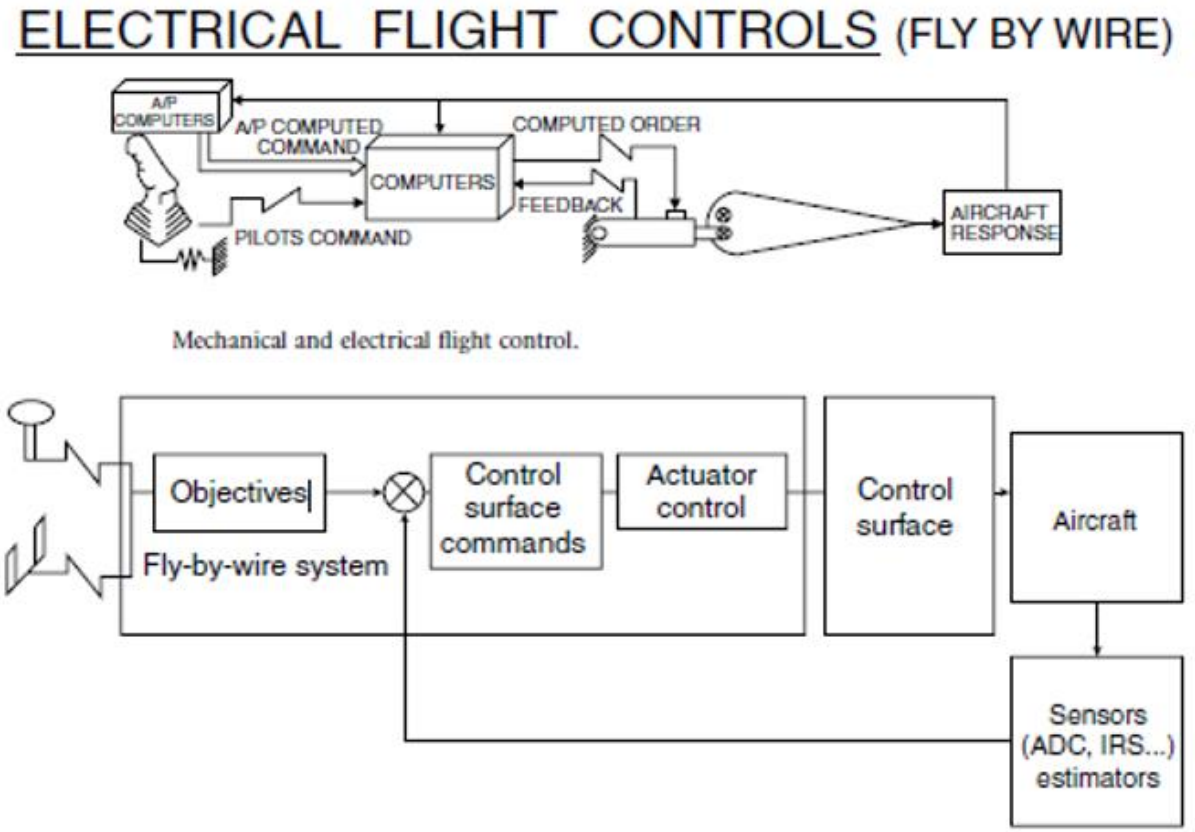
Frühere Flugzeuge - ausschließlich **manuell** geflogen und **terrestrisch**, d.h. mit **Kompass und Stoppuhr** navigiert

Steuerungskomponenten wie Leitwerk, Antriebshilfen oder Querruder **wurden auf analoge Weise** bzw. **manuell** betätigt

Vom Zugseil zum eingebetteten System am Beispiel der Cockpitsteuerung

Antikes B-17 Cockpit





Vom Zugseil zum eingebetteten System am Beispiel der Cockpitsteuerung

Eine **Abbildung im Kontrast** zwischen **mechanischer**, elektrischer und signalsgesteuerter Flugsteuerung basierend auf **digitale Komponenten**

Vom Zugseil zum eingebetteten System
am Beispiel der Cockpitsteuerung

Modernere Cockpits

*Anmerkung: aktuell gibt es weiterhin Flugzeuge deren **Cockpitsteuerung mit Seilzügen** realisiert wird und gleichzeitig über **moderne digitale Systeme** verfügen.

Vom Zugseil zum eingebetteten System am Beispiel der Cockpitsteuerung

Modernere Cockpits

Cockpit eines europäischen Hersteller

Die Veränderungen der Cockpit-Steuerung werfen zwei Fragen auf:

Erstens, welche konkreten Komponenten haben die Veränderung ermöglicht?

zweitens, ob bei der Einführung digitaler Komponenten aus Sicht der IT-Sicherheit ausreichende Rahmenbedingungen für deren Einsatz vorhanden waren bzw. sind?

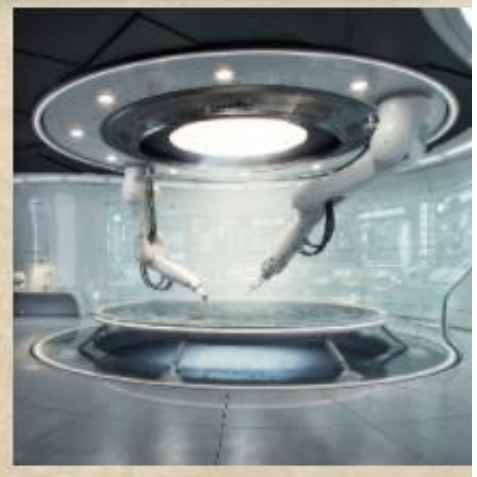
Ein Kontrast der Zeiten und flugzeugbezogene Basisbegriffe

Wann und wo genau begann der disruptive Wandel von der analogen zur modernen Cockpit- / Flugzeugsteuerung aus digitaler und vernetzter Sicht?

Der Einzug der Embedded Systems und digitaler Komponenten

ANSÄTZE FÜR EINEN DISRUPTIV EN UND SUBKUTANEN WANDEL

BASISBEGRIFFE, DEFINITIONEN UND ERLÄUTERUNGEN



Der Einzug digitaler Komponenten

nach Klaus Hünecke 2008 "Die Technik des modernen Verkehrsflugzeuges" und Cary R. Spitzer et al. 2015 "The Avionics Handbook"

mit Beginn der **80er Jahre d. 20. Jhd. weitreichende Veränderungen** an der Bauweise der Flugzeuge

Einzug des **ARINC-Vernetzungsstandards** (ARINC 419 Vorläufer zu ARINC 429) seit den späten 70er d. 20. Jhd.

Die Art und Weise der Bedienung und Ansteuerung der Steuerungssysteme wie z. B. Leitwerk, Antriebshilfen oder Querruder **wurde ab diesem Zeitpunkt sukzessive computergesteuert**

Computer in Flugzeugen

in Form und Größe eines **eingebetteten Systems (ES)**

Flugzeugbezogene Basisbegriffe

ES sind **informationsverarbeitende Systeme**, die in ein größeres System oder Produkt **integriert sind**

übernehmen Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben

nicht direkt von den Benutzenden wahrnehmbar

Bei Flugzeuge - Klasse (A) Heavy (**large wide body aircraft**) können **zwischen 50 und 100 eingebettete Systeme** in einer **Avionikarchitektur** integriert sein

Entstehung der Schicht der **vernetzten Systemumgebungen**

Flugzeugbezogene Basisbegriffe

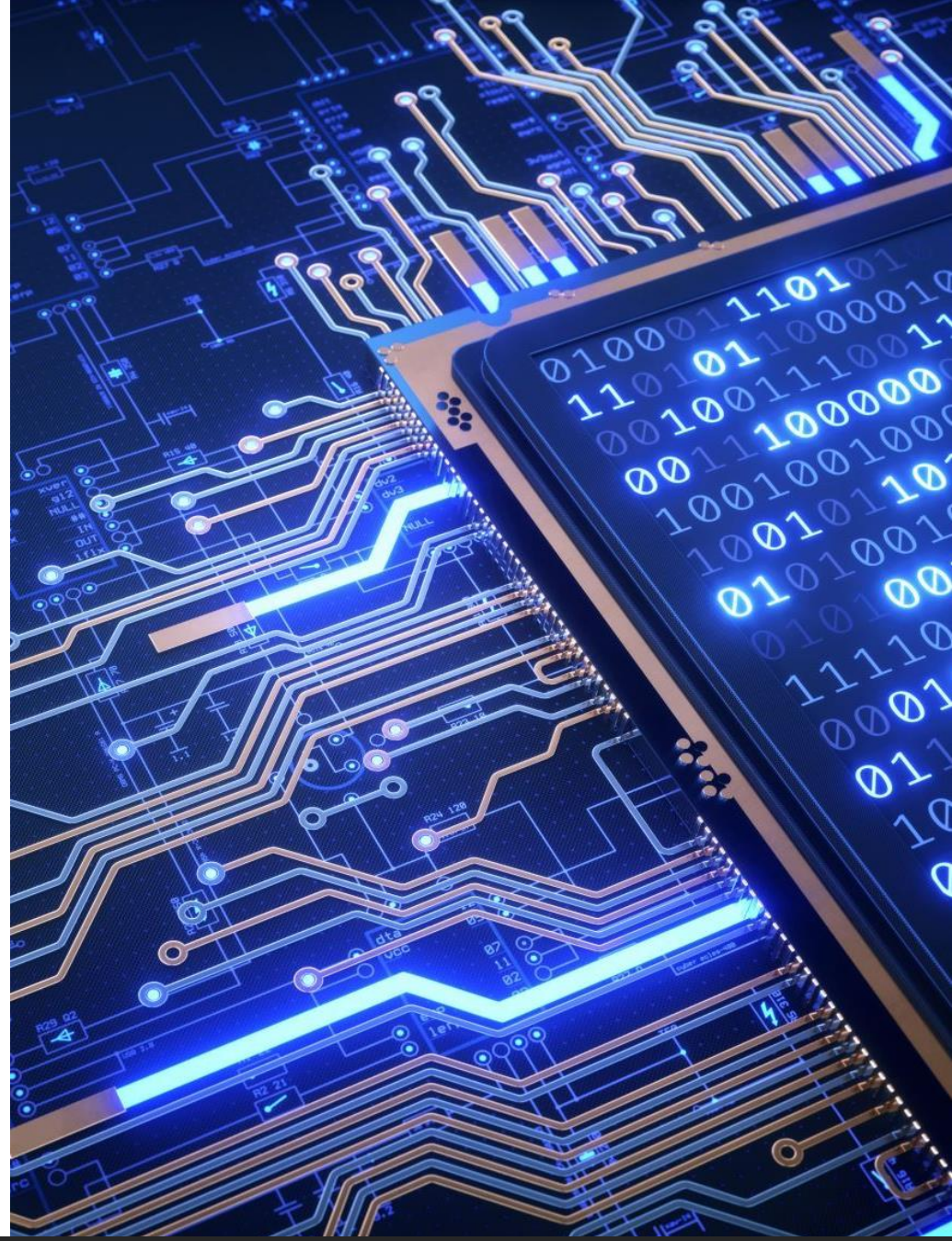
ES- Geräte bestehen aus Hardware und Software

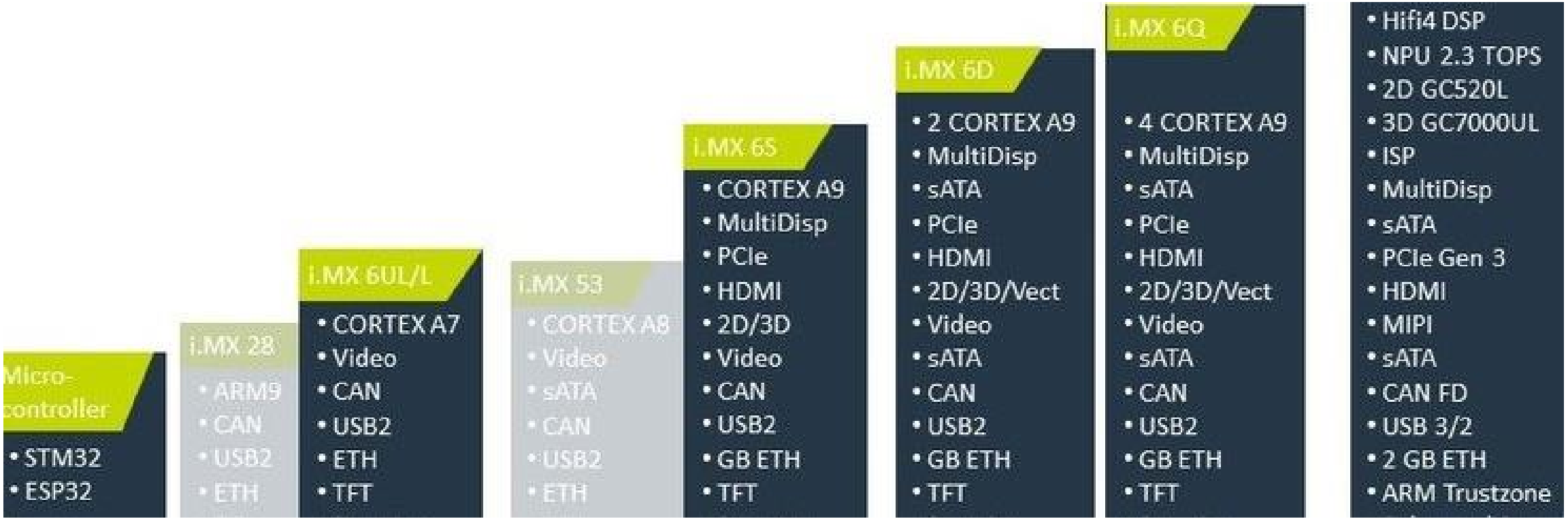
mit mehreren Kommunikationsschichten zwischen der Anwendungssoftware und der Schnittstelle zur Hardware

Schichten wiederum entsprechen dem k**lassischen ISO / OSI-Modell** in Bezug auf Transport und Zustellung von Datenpaketen

mit Kommunikationsprotokollen analog zur bekannten Client/Server-Architektur und integrierten Schnittstellen

Als **Betriebssystem** für eingebettete Geräte -**Linux oder ein Linux-Derivat** od. **proprietäre Applikation** als Betriebssystem oder **Firmware**





Dieses Foto stammt von "© 2023 Ginzinger" übernommen von https://www.ginzinger.com/de/technologie/embedded-hardware-und-software/.

Eine Übersicht über Schnittstellen bei ES

CAN, ETHERNET, USB U.A.

Flugzeugbezogene Basisbegriffe

Klassisches Beispiel für ES

Fly by Wire Technologie

Steuerbefehle (Eingabe mit Hilfe des so genannten“Side Sticks”) werden in Form von elektrischen, **digitalen Signalen** zu den Stellzylindern der Ruder **übertragen**

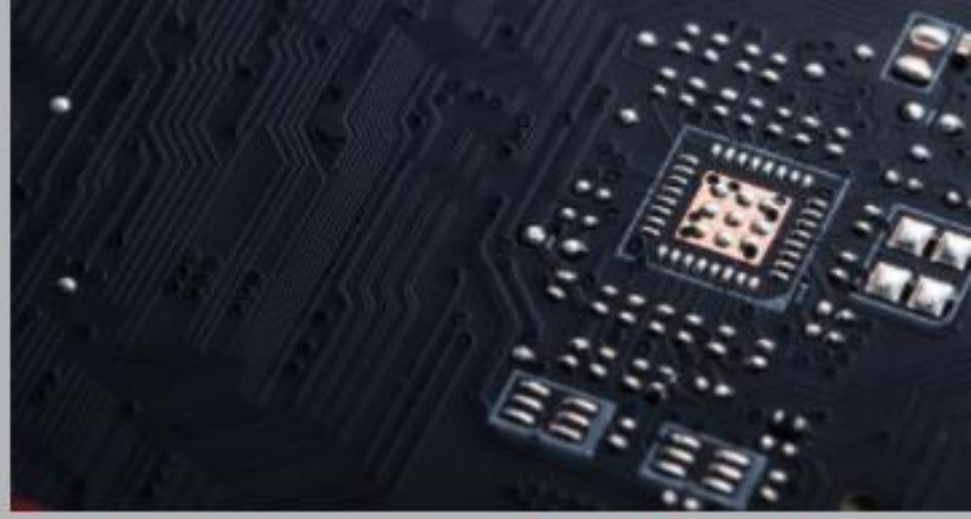
Hard- und Software zur Ansteuerung und Überwachung der Steuerflächen sind zur Verringerung der Ausfallhäufigkeit dissimilar und **redundant ausgelegt**

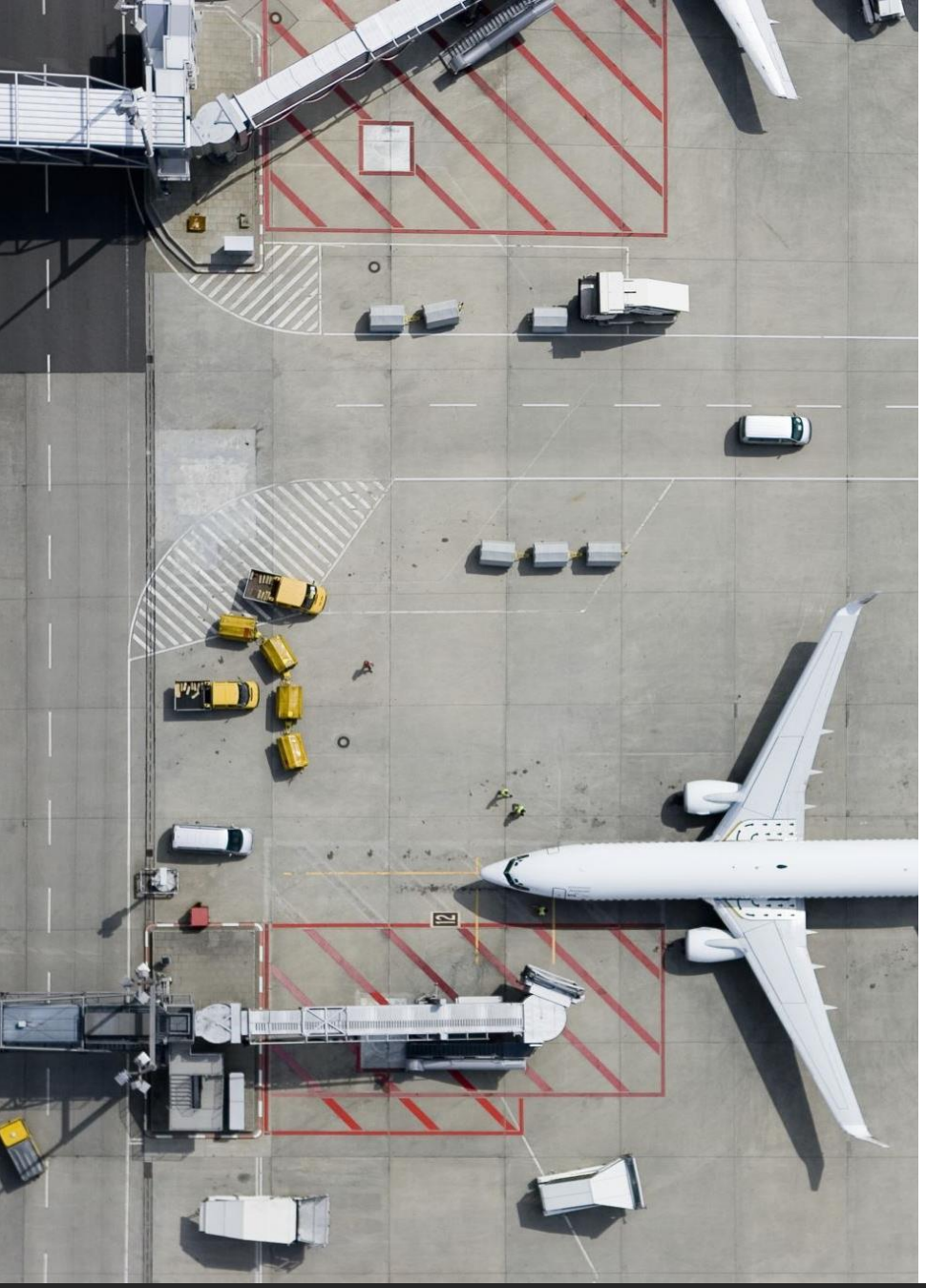
Side Sticks - kurzzeitiges Ein- und Ausschalten des Autopiloten

Flugzeugbezogene Basisbegriffe

Die sukzessive Einführung von digitalen Komponenten in die Avionik Architektur führte zur Entstehung einer flugzeugbezogenen digitalen Wirkungssphäre, deren Gravitation Flugzeuge erfasst





Eine Sicht der IATA auf die Vernetzungsschicht durch eingebettete Systeme

CIVIL AVIATION - EUR/NAT REGIONS 2022 MEETING (EUR/NAT-DGCA/2022-1)

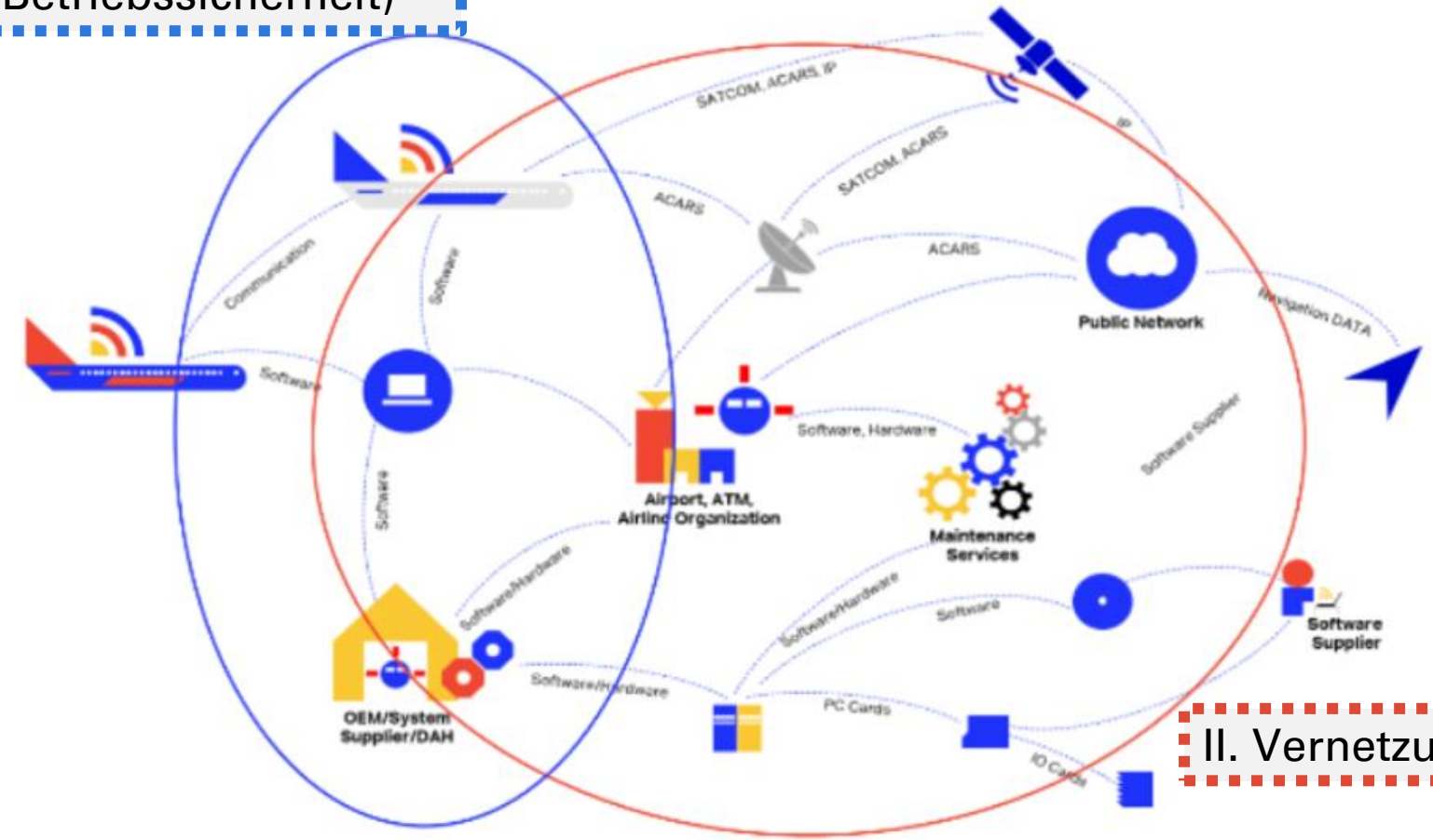
Paris, France, 10 May 2022

IATA Präsentation durch

Manon Gaudet - IATA, Assistant-Director Aviation Cyber Security

Angeles Romero - Assistant Director Airport, Passenger Cargo and Security Europe

I. Klassische Sphäre der Safety (Betriebssicherheit)



Die Gravitation zweier Sphären, welche auf einem Flugzeug heutzutage nach IATA wirken

II. Vernetzungsbasierte Sphäre

Dieses Foto stammt von "International Air Transport Association (IATA) übernommen von https://www.icao.int/EURNAT/Pages/EUR-and-NAT-Document.aspx.

Flugzeugbezogene digitale Wirkungssphäre

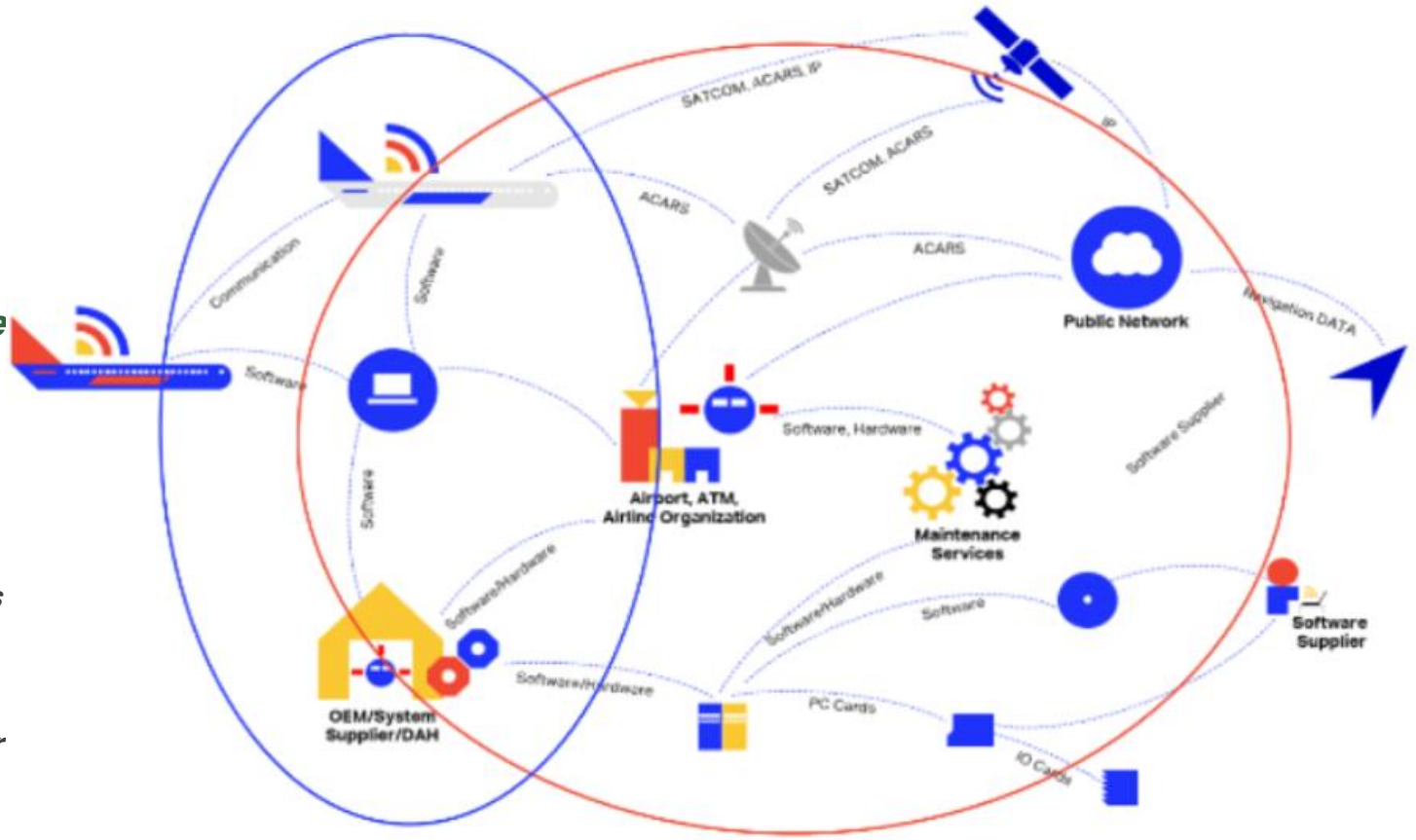
Kritische Informationen und Systeme, die

mit dem Luftfahrzeug oder seinen kritischen Funktionen verbunden sind, gewartet und/oder betrieben werden,

kritische Funktionen der Fluggesellschaft zur Unterstützung des kritischen Fluglinienbetriebs verwendet werden,

mit dem Luftfahrzeug oder seinen kritischen Funktionen verbunden sind, gewartet und/oder betrieben werden

müssen cybergeschützt, aktualisiert und überwacht werden.



Stufenartige Effekte durch Embedded Systeme bei Flugzeugen hinzu Vernetzung, zum Cyberumfeld und zur Debatte über Informationssicherheit

Basisbegriffe im Cyberumfeld

DEFINITIONEN UND ERLÄUTERUNG BEGLEITENDER BEGRIFFE

Basisbegriffe im Cyberumfeld

Gefährdung - Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. **Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt**.

Schwachstelle - **sicherheitsrelevanter Fehler eines IT-Systems** […] . Ursachen können in der **Konzeption**, den verwendeten **Algorithmen**, der **Implementation**, der **Konfiguration** […] liegen. **Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird** und […] ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

/ od. in eigener Formulierung

Eine oder die Summe unerwarteter, im Design nicht beabsichtigte Konfigurationsmöglichkeiten, können zu einer Schwachstelle führen

Basisbegriffe im Cyberumfeld

Angriff - eine **vorsätzliche Form der Gefährdung**, nämlich eine unerwünschte oder unberechtigte Handlung **mit dem Ziel**, sich Vorteile zu verschaffen bzw. einer dritten Person **zu schädigen**.

EASA Verwendung einer Begriffserweiterung im Kontext der Luftfahrtregulatorik - absichtlichen unbefugten elektronischen Interaktionen (IUEI) engl. ***"intentional unauthorised electronic interactions"***

Der Begriff "absichtliche unbefugte elektronische Interaktion (IUEI)" wurde gemeinsam von RTCA und EUROCAE eingeführt

Definition und Umfang von IUEI in EUROCAE ED-Standards

Basisbegriffe im Cyberumfeld

Plattform zur Manifestation der Gefährdung, Schwachstelle, Angriff, absichtliche unbefugte elektronische Interaktion (IUEI)

IT-System - technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Smartphones, Tablets, IoT-Komponenten, Router, Firewalls

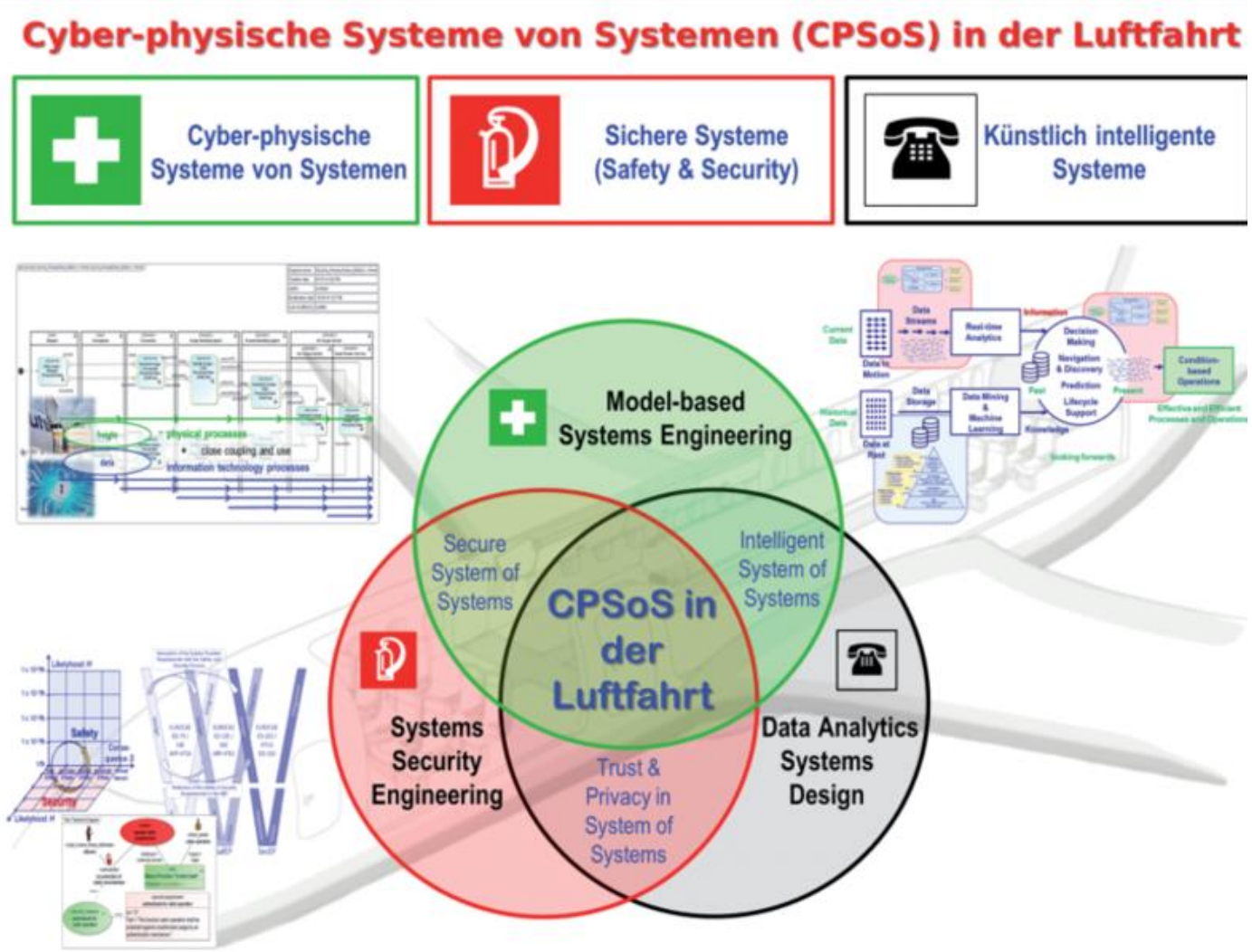
und demnächst wahrscheinlich auch Flugzeugen?

eingebettete Systeme als Erweiterung dieser klassischen Definition hinzu **Plattform** oder nach Prof. Dod **"System von Systemen"**

Ein Flugzeug in einer erweiterten Definition des Kompositums „IT-System“ als informationstechnologische Plattform

Eine Definition als „System von Systemen“

*„[…] **der Wandel heutiger Luftfahrtsysteme stellt eine für die Entwicklung herausfordernde Mischung aus** CPS (**cyberphysisches System**) **und** SoS (**System der Systeme**) **dar, die als cyberphysisches System von Systemen** (CPSoS) **bezeichnet wird** […]“.*



Flugzeug als cyber-physisches System nach Prof. Dod

Dieses Foto stammt von God, Ralf et al.: Digitale Transformation-Systeme in der Luftfahrt im Wandel, in: Ingenieur-Spiegel, Band 1, S. 36, Bingen 2019.

Informationssicherheit

EINE DEFINITION

Informationssicherheit

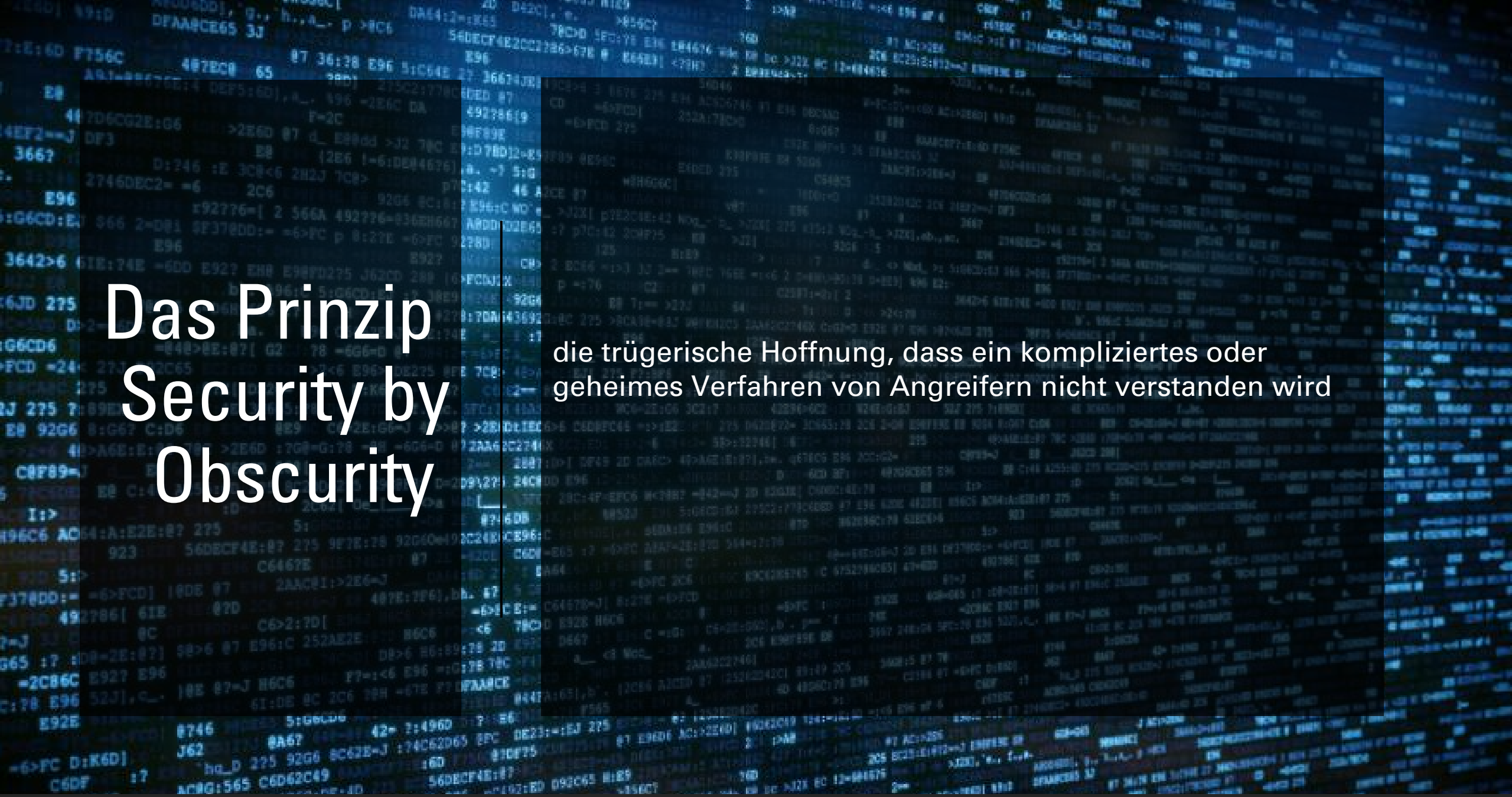
ist Teil der Oberbegriffe erstens Compliance, zweitens Sicherheit

hat den **Schutz von Informationen als Ziel**. Dabei können **Informationen** […] **in IT-Systemen** […] **gespeichert sein**. Die **Schutzziele** oder auch Grundwerte der Informationssicherheit sind **Vertraulichkeit, Integrität und Verfügbarkeit**,

umfasst den umfangreicheren Bereich des Schutzes von Informationen zwar in und mit IT und ohne IT bzw. über IT hinaus.

IT-Sicherheit – **Untermenge** der Informationssicherheit und beschäftigt sich **an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung**

Das Prinzip Security by Obscurity



Das Prinzip Security by Obscurity

die trügerische Hoffnung, dass ein kompliziertes oder geheimes Verfahren von Angreifern nicht verstanden wird

3. Öffentliches Fachgespräch zur Informationssicherheit in Flugzeugen

DIE FRAGE NACH DEM WARUM UND ANTWORTEN DURCH REFERENZEN IN FORM VON PUBLIKATIONEN, ANSÄTZEN UND BEISPIELEN

Referenz 1
Jeep Cherokee Hack aus dem Jahr 2015

Hack über das Entertainment-System mit Fernsteuerung von außen

Das Infotainmentsystem des Fahrzeugs **enthielt eine kritische Schwachstelle**, **die es einer Entität ermöglichte**, **das** damit ausgestattete **Fahrzeug** über das Internet und über Remoteverbindung anzusprechen und **zu übernehmen**

folgende Fahrzeugsysteme übernommen werden: Kontrolle über Bremsen, Beschleunigung, Türverriegelung, Klimaanlage und Scheibenwischer

Im Rückwärtsgang war die Übernahmen des Lenkrads möglich

Möglichkeit zur Ortung* (genauen Standort) des betroffenen Fahrzeugs ohne Einwilligung des Fahrzeughalters (*Nebeneffekt)

über das Entertainment-System mit Fernsteuerung von außen

Hack durch die Sicherheitsforscher **Charlie Miller und Chris Valasek gegenüber WIRED** (Computerzeitschrift) vorgeführt

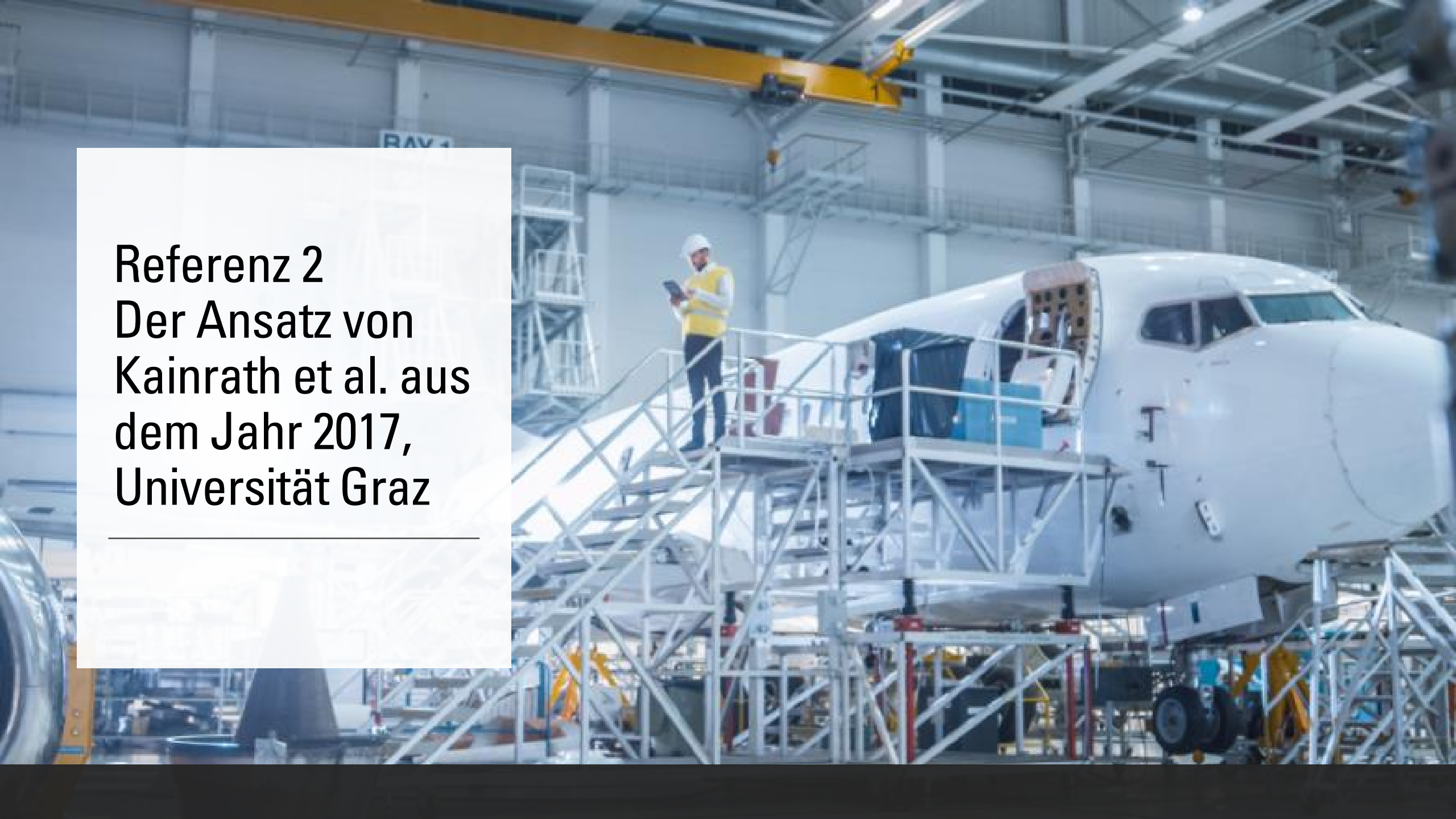
mit einem Fahrer, der in die Prozedur eingeweiht war

Vorführung sukzessiver Verlust der Fahrzeugkontrolle

Das kompromittierte Fahrzeug ist schließlich in einem Graben gelandet

Point of Entry war die Diagnoseschnittstelle (CAN-Bus) via Remoteverbindung

Kompletter Berichts des Hacks liegt online vor



Referenz 2
Der Ansatz von Kainrath et al. aus dem Jahr 2017, Universität Graz

Der Ansatz von Kainrath et al. aus dem Jahr 2017

Projekt **„Aviation Cyber Security Study“** (ACySS) - **aktuelle Angriffsmethoden auf ein Avionik-Netzwerk anzuwenden und dessen Sicherheit zu analysieren**

Moderne Zivilflugzeuge - mit der Netzwerktechnologie „Avionics Full-Duplex Switched Ethernet“ (AFDX) ausgestattet

Kritischer Datenverkehr im Flugzeug regeln Netzwerk Switches, aufbauend auf dem Ethernet IEEE 802.3 Netzwerkstandard

Kritische Elemente wie z.B. die **Flugsteuerung** (Cockpit Domäne) **nutzen das gleiche Netzwerk** wie die **Kabinenkontrolle** (Kabinen-Domäne) oder das **In-flight Entertainment System** (IFE, Passagier-Domäne)

Im gesamten Luftfahrzeug existiert im Wesentlichen ein Netzwerk als Kommunikationsbackbone

Der Ansatz von Kainrath et al. aus dem Jahr 2017

Untersuchung potenzieller Schwachstellen von Bordunterhaltungssystemen mit folgenden zu testenden Möglichkeiten u.a.

Das System durch **unerwartete Eingaben** zu Fehlverhalten zu bewegen

Analyse von **möglichen Netzwerkübergängen zwischen Passagier- und Avionik Netzwerk**

Analyse der eingesetzten Netzwerk-Protokolle

Umfassendere Tests in einer zweiten Phase, wie z.B. **Angriffe mit und ohne mechanisch-physikalischen Zugriff auf** alle Teile des **Flugzeugnetzes**

Ergebnisse sollen Aufschluss über mögliche Überarbeitungen des Netzwerkdesigns oder der Applikationen geben

Der Ansatz von Kainrath et al. aus dem Jahr 2017

Lehren und Aussichten

Die in modernen Flugzeugen verwendete technische Ausstattung ist für allgemeine Forschungszwecke sowohl schwer zugänglich als auch äußerst kostspielig

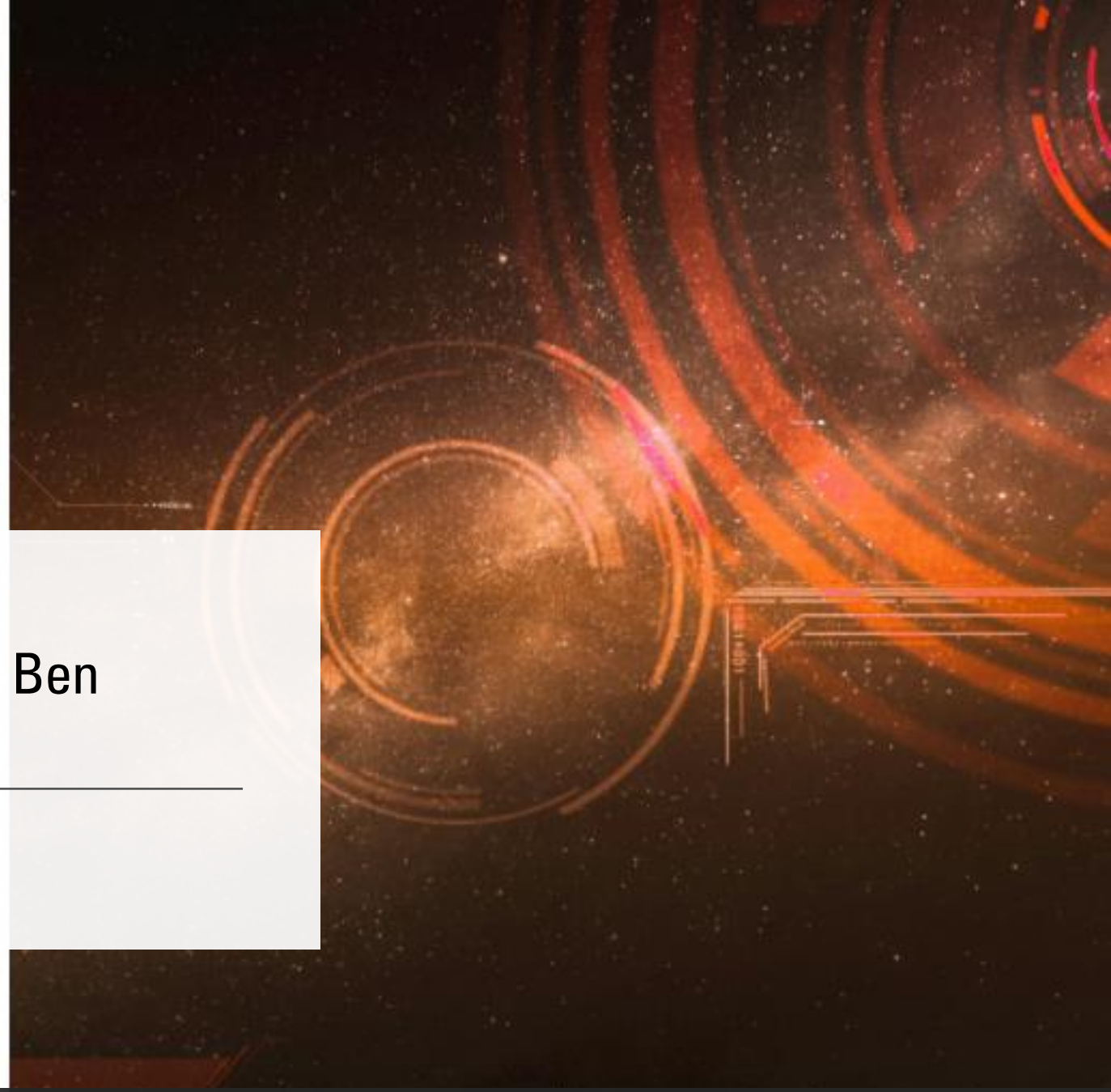
hoher Sicherheitsanforderungen und langwierigen Zulassungsprozederen (DO-254 (Hardware) DO-178c (Software) [13] als Safety- und z.B. die DO326A als möglicher IT-Security-Standard) sind kein Surrogat gegenüber einer dedizierten Betrachtung

Es bedarf nach Kainrath et al. eine dedizierte und regelmäßigen Untersuchungen der Avionik-Bussysteme

Der Ansatz von Kainrath et al. aus dem Jahr 2017

„[…] 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 […]“.

***Hersteller von In-flight Entertainment Systemen**



Referenz 3
Edan Habler, et al. aus dem Jahr 2023, Ben Gurion Universität, Negev

Edan Habler, et al. aus dem Jahr 2023, Ben Gurion Universität, Negev

"Bewertung der Sicherheit von Luftfahrzeugen: Ein umfassender Überblick und eine Methodik zur Bewertung" als Zusammenstellung

Edan Habler, et al. aus dem Jahr 2023, Ben Gurion Universität, Negev

Raffinesse und Komplexität von Cyberangriffen und die Vielfalt der Zielplattformen in den letzten Jahren zugenommen

In den letzten Jahren **verschieden Angriffe** auf Verkehrssystem, darunter **auch auf Flugzeuge**

Schadenspotenzial von Angriffen aufgrund des Mangels an Sicherheitsmaßnahmen in bestehende Bordsystemen ist hoch (Wortlaut „enorm“)

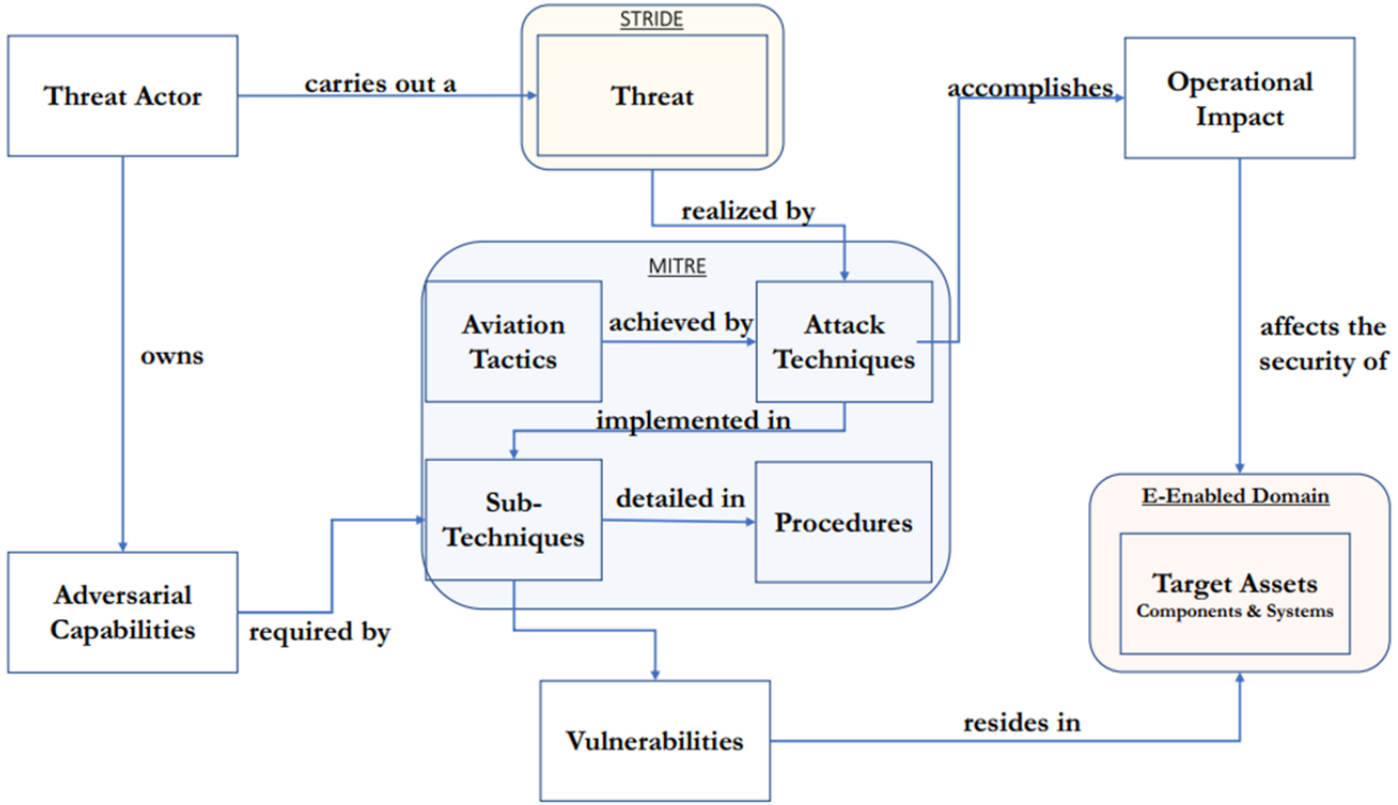
Intention von **Edan Habler, Ron Bitton und Asaf Shabtai** – ein umfassender Überblick über Flugzeugsysteme und Komponenten in deren netzwerktechnische Umgebung und welchen Cyberbedrohungen diese ausgesetzt sind, zu geben

Schwerpunkt auf Cyberbedrohungen bei Flugzeugen

Edan Habler, et al. aus dem Jahr 2023, Ben Gurion Universität, Negev

Vorstellung einer Taxonomie (einheitliches Verfahren oder Modell) die das Wissen und das Verständnis von Cybersicherheit im Bereich der Avionik aus der Sicht eines Angreifers standardisiert

Das vorgestellte Modell **kategorisiert Techniken in relevante Taktiken**, die in **verschiedenen Phasen des Lebenszyklus** eines gegnerischen **Angriffs** sich widerspiegeln und bildet bestehende Angriffe gemäß der MITRE ATTACK-Methodik ab verknüpft bzw. **angewandt auf dem Plattformtyp Flugzeug**



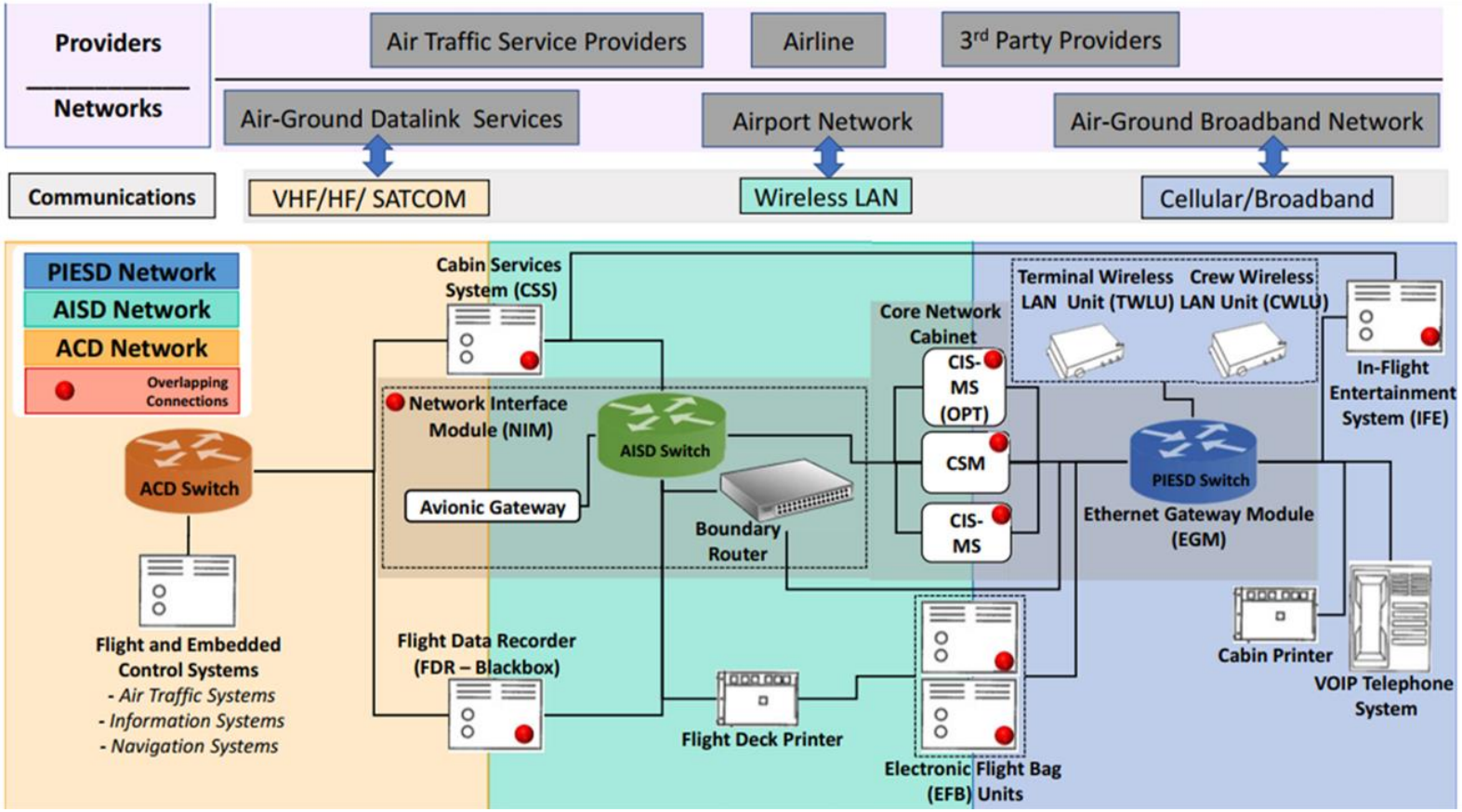
Edan Habler,
et al. aus dem Jahr 2023,
Ben Gurion Universität, Negev

PROZESSARTIGE DARSTELLUNG VON ANGRIFFSPFADE BEI FLUGZEUGEN DURCH EDAN HABLER, ET AL.

Dieses Foto stammt von Habler, Edan et al.:https://arxiv.org/pdf/2209.04028.pdf.

Edan Habler, et al. aus dem Jahr 2023,
Ben Gurion Universität, Negev

PROZESSARTIGE DARSTELLUNG VON ANGRIFFPFADE BEI FLUGZEUGEN DURCH EDAN HABLER, ET AL.



Dieses Foto stammt von Habler, Edan et al.:https://arxiv.org/pdf/2209.04028.pdf.

Referenz 4

Untersuchung durch R. Santamarta aus dem Jahr 2016

Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

Aktivität im Umfeld der Flugzeuge durch forschungsorientierte Initiativen

Nicht nur institutionelle Akteure, sondern **auch forschungsorientierte Initiativen** wie das EPIC - Electronic Privacy Information Center und **vereinzelt auch einzelne Forscher** haben sich mit den Möglichkeiten der Remote-Verbindung bzw. mit dem Eindringen in Flugzeugsystemen von einem Point of Entry oder Point of Entrance beschäftigt

Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

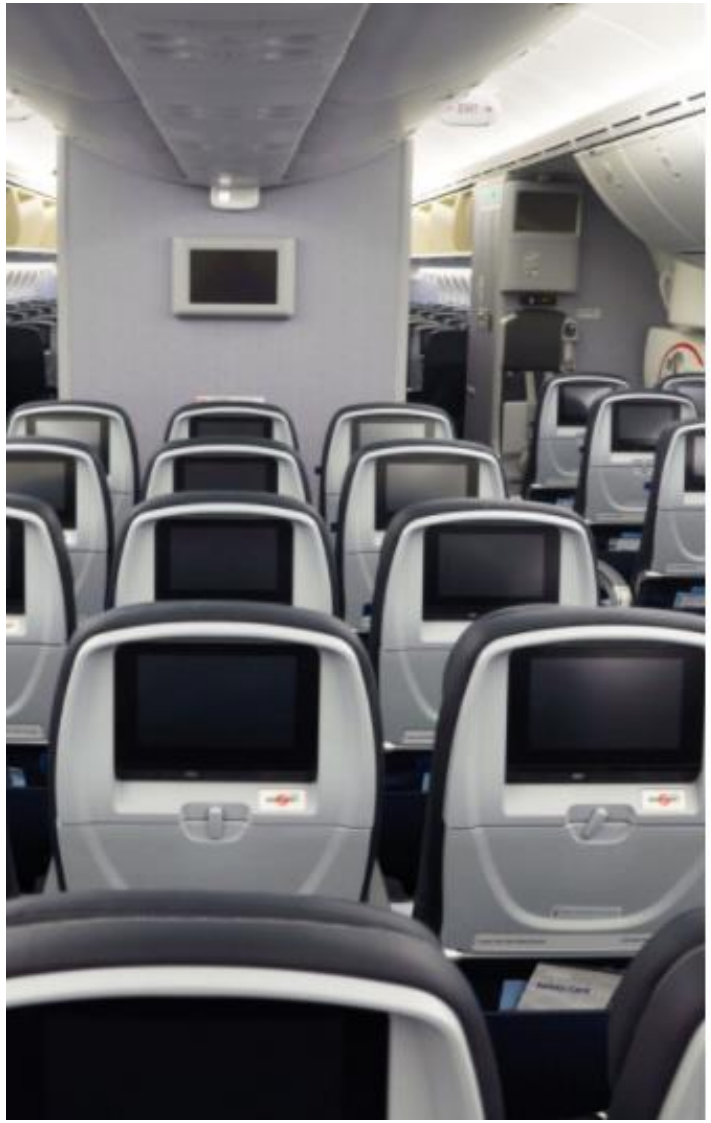
nach eigenen Angaben war R. Santamartas Antrieb der Wunsch zu verstehen, wie die Technologien in einem Flugzeug ineinandergreifen

Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

In seinem beruflichen Kontext entdeckte er während eines Fluges ein Bordunterhaltungssystem eines Herstellers, das er in der vorgefundenen Konfiguration einer technischen Analyse unterzog

Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

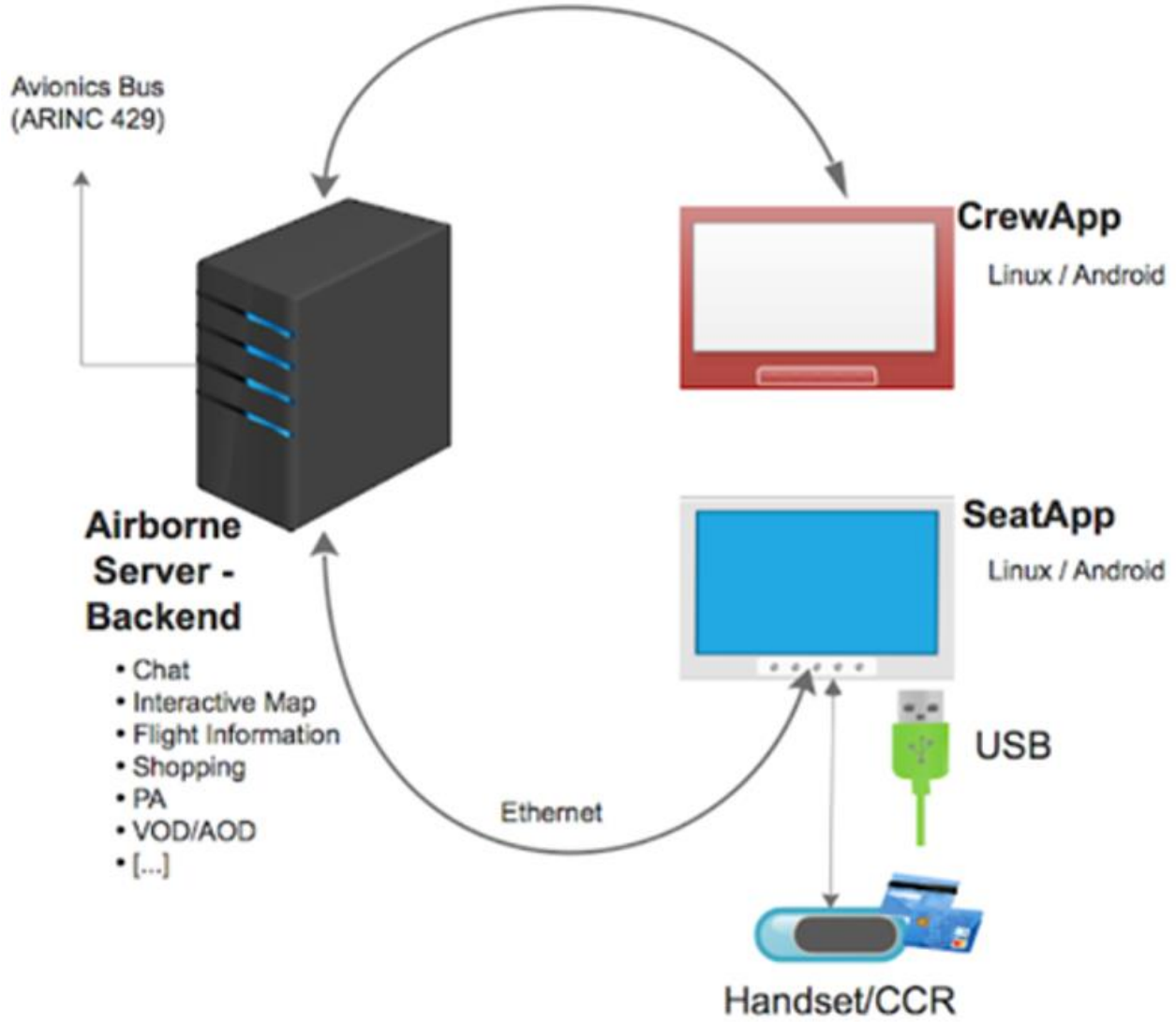
„[…] Die Schwachstellen in diesen Systemen könnten es Hackern ermöglichen, die Borddisplays der Passagiere zu „kapern“ […] […]".



Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

Angaben zum Einstiegsendpunkt und zu den Betriebssystemen online verfügbar

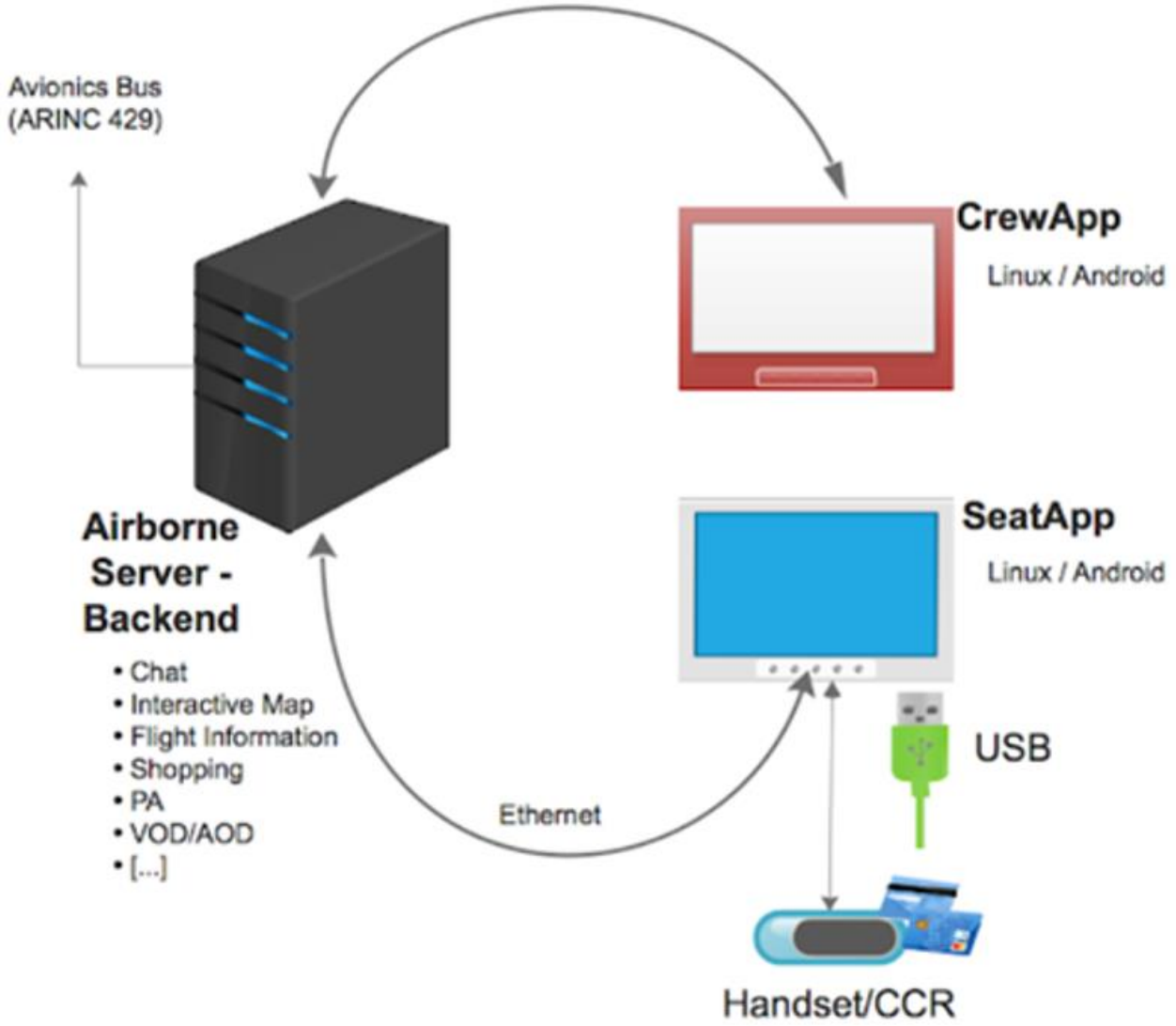
R. Santamarta gibt jedoch nicht im Detail an, welche Tools und welche Befehle in welcher sequentiellen Abfolge auf dem Zielsystem ausgeführt wurden, um in die Flugzeugsysteme einzudringen

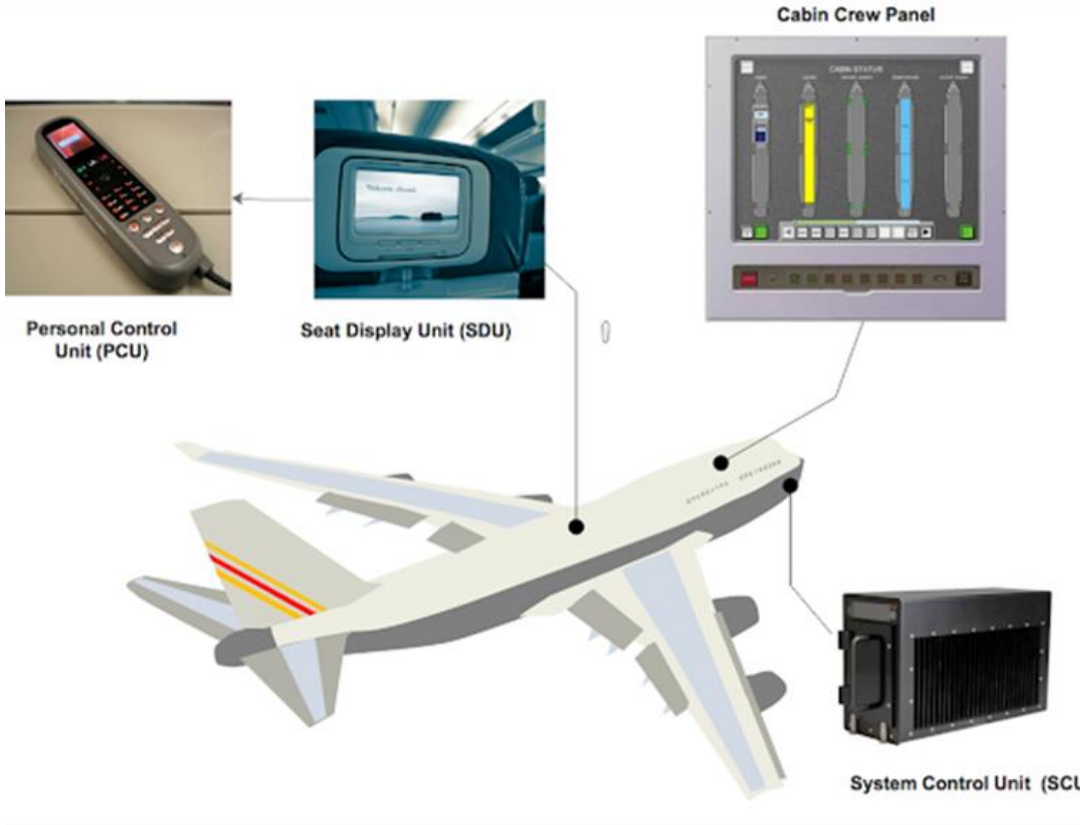


Dieses Foto stammt von Santamarta, Ruben: In Flight Hacking System, Seattle 2016. Online in Internet: https://ioactive.com/in-flight-hacking-system/.

Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

Gemäß der veröffentlichte Pressemitteilung von IOActive vom 20. Dezember 2016 hätten die genutzten ***„[…] […] Schwachstellen je nach Systemkonfiguration in einem Flugzeug möglicherweise auch als Einstiegspunkt in das breitere Netzwerk fungieren […]“*** können.





Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

Ein Effekt - Störung des Bordunterhaltungssystem während des Fluges

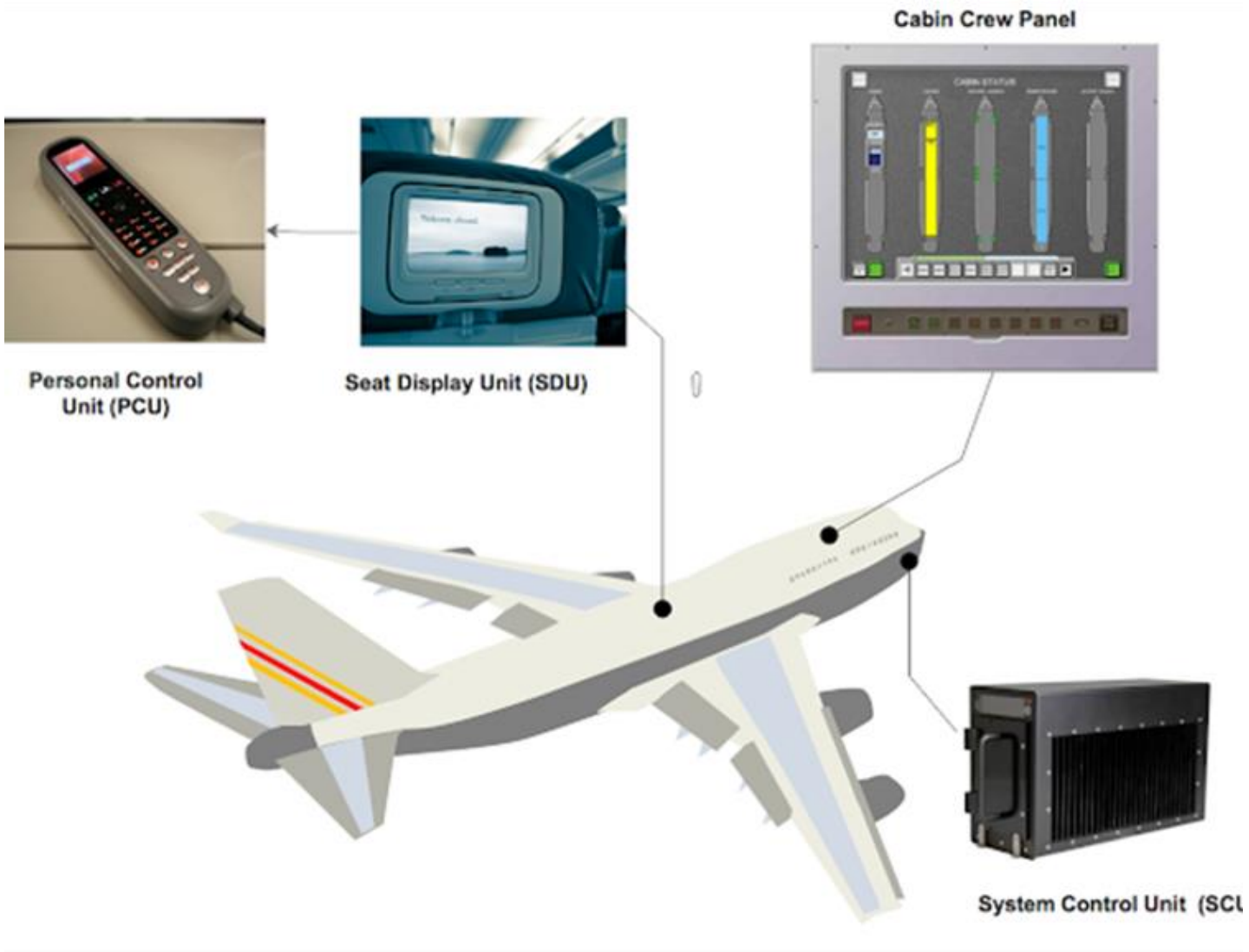
Die System Control Unit (SCU) empfängt normalerweise Echtzeitinformationen wie Windgeschwindigkeit, Breitengrad, Längengrad, Höhe und Außentemperatur

SCU – **kein kritisches System**, aber essentielles System in der Gesamtavionik

Dieses Foto stammt von Santamarta, Ruben: In Flight Hacking System, Seattle 2016. Online in Internet: https://ioactive.com/in-flight-hacking-system/.

Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

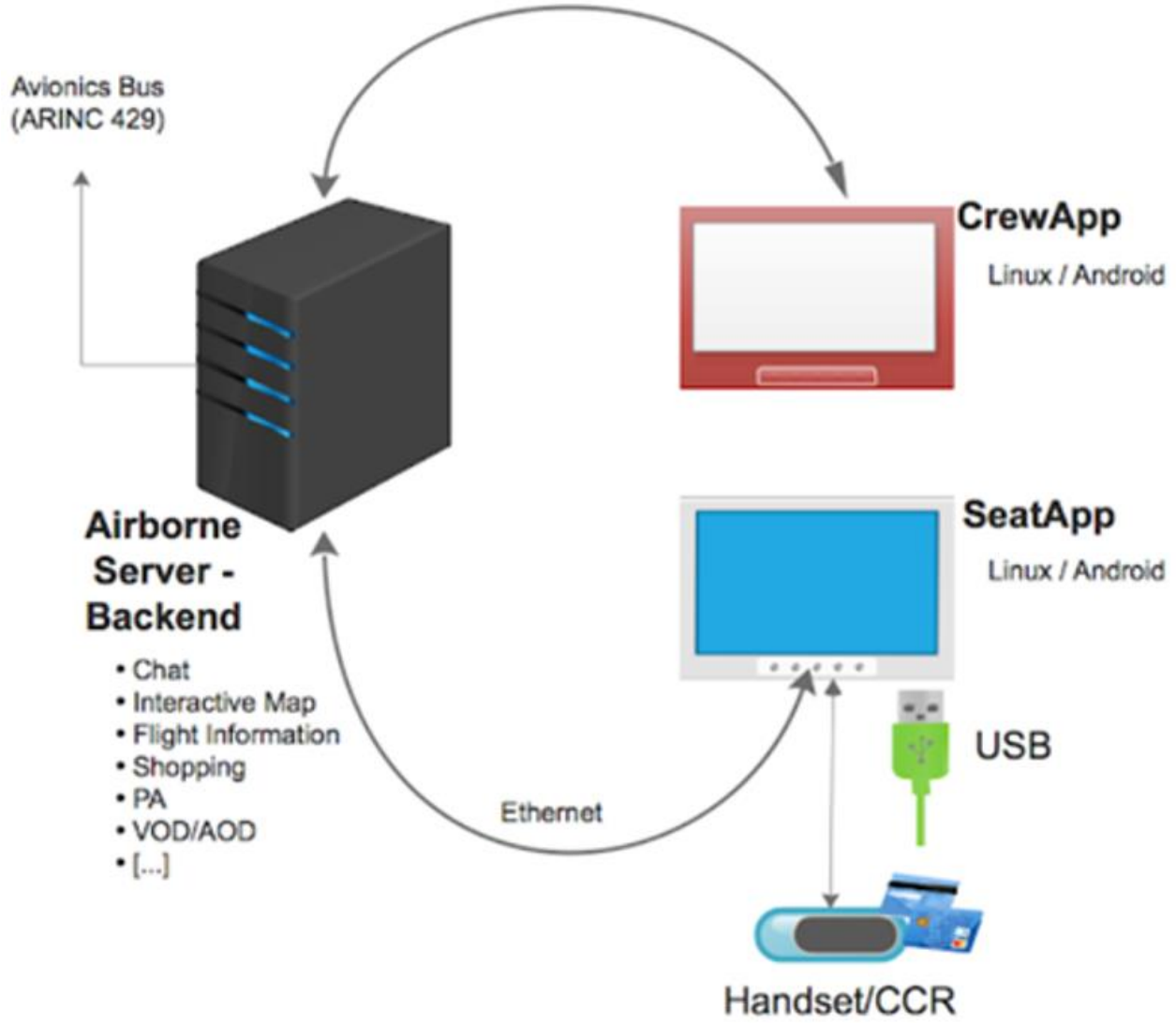
Diese **Parameter der SCU** wiederum werden, unter anderem, **über** den **Avionikbus ARINC 429 von der Luftfahrzeug-Kontrolldomäne in die Domäne der Informationsdienste übertragen.** Diese Informationen werden dann über **eine Ethernet-Verbindung am Seat Display Unit (SDU) direkt am Passagiersitz** zur Verfügung gestellt, so dass dort sich der Kreis in die Domäne der Fluggastinformations- und Unterhaltungsdienste schließt.



Referenz 4
Untersuchung durch R. Santamarta aus dem Jahr 2016

Eigene Einschätzung

Es ist auch davon auszugehen, dass der ausgeführte Code / Kommandos keine komplexe Syntax enthielt



Referenz 5
Untersuchung der us-amerikanischen Behörden
DHS und die CISA aus dem Jahr 2021

Referenz 5 Untersuchung der us-amerikanischen Behörden DHS und die CISA aus dem Jahr 2021

Programm FY17-21

Zwischen 2017 und 2021 wurde in einem Laborversuch versucht, Flugzeuge einer spezifischen Klasse einem Hacking-Test zu unterziehen.

Laut Angaben der DHS konzentrierte sich die Untersuchung darauf, die Hypothese zu bewerten, ob ein Remote-Cyber-Angriff auf Verkehrsflugzeuge **durch nicht-kooperative** (**nicht veröffentlichte**) Penetration (**Angriffstechniken**) möglich ist.

Während des FY17 erwarb das Programmteam einen Luftfahrzeug-Testartikel (TA) und führte erste Planungs- und Evaluierungsarbeiten durch.

Die im FY17 durchgeführte, angewandten non-kooperative Remote-Cyber-Penetration des Testartikels war erfolgreich.

Darauf aufbauend erfolgt im FY17-21 eine Bewertung der Systemschwachstellen und die Entwicklung von Empfehlungen zur Schadensbegrenzung.

Referenz 5 Untersuchung der us-amerikanischen Behörden DHS und die CISA aus dem Jahr 2021

Programm FY17-21

Dabei konnte gezeigt werden, dass **Flugzeuge über eine Remote-Verbindung** angesprochen und gehackt werden können

Es ist **derzeit unklar bzw. unbekannt**, ob **technische Inhalte** zu **Angriffswegen / Einbruchsvektoren und Schwachstellen** der breiten **wissenschaftlichen Öffentlichkeit** zur Verfügung gestellt werden

und ob diese von Herstellern bei Design und Produktion berücksichtigt werden können

Das verfügbare Dokument, welches veröffentlicht wurde, wurde **größtenteils reihenweise mit Vermerke anstatt Inhalt veröffentlicht**

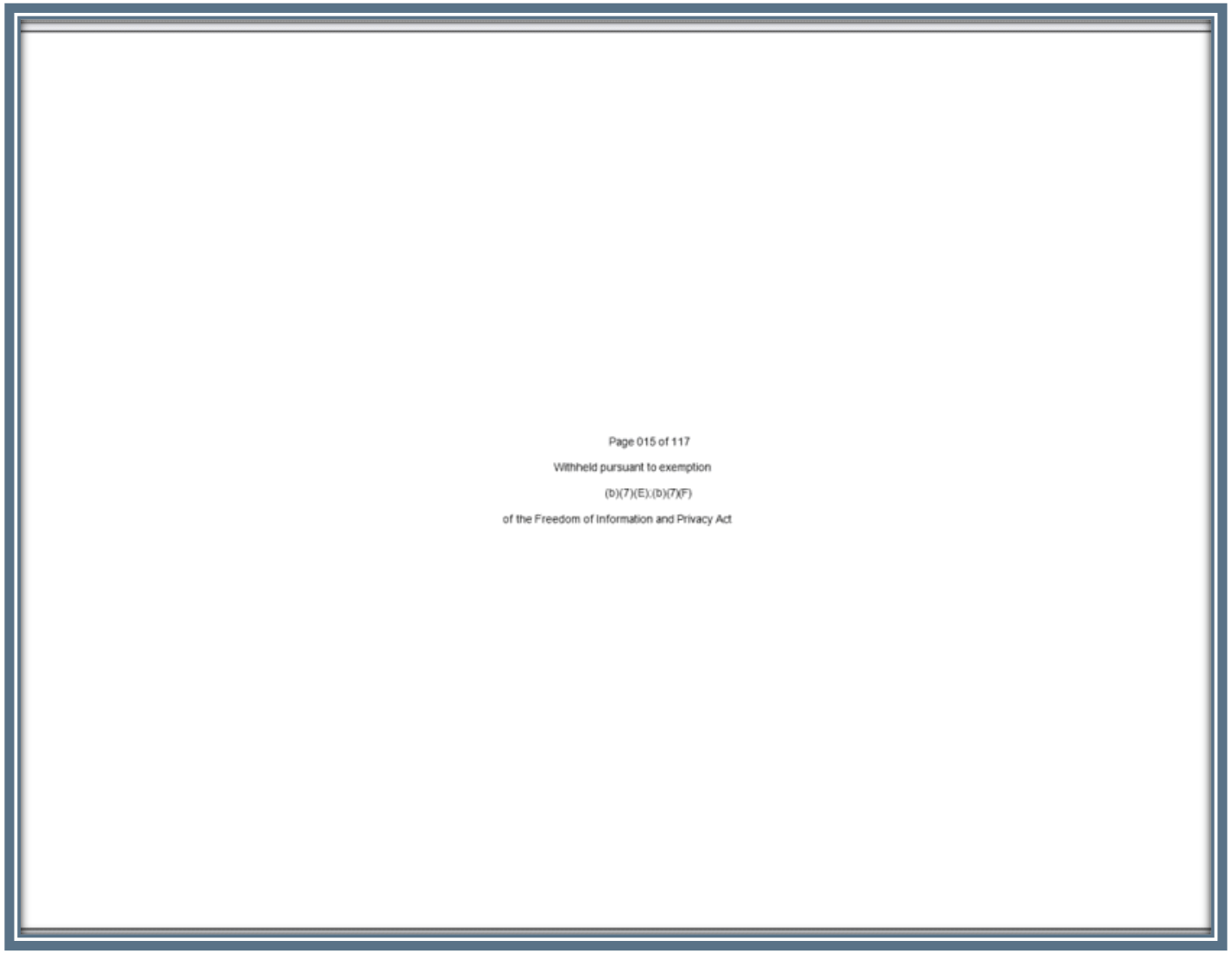
Referenz 5 Untersuchung der us-amerikanischen Behörden DHS und die CISA aus dem Jahr 2021

Programm FY17-21 - Veröffentlichung Gesetzes über Informationsfreiheit und Datenschutz

Seitenweise leer gelassen und wie folgt gekennzeichnet

Page 015 off 117withheld pursuant to exemption (b)(7)(E); (b)(7)(F) of the Freedom of Information and Privacy Act

Seite 015 von 117 z**urückbehalten gemäß Ausnahme** (b)(7)(E); (b)(7)(F) **des Gesetzes über Informationsfreiheit und Datenschutz**



Referenz 5 Untersuchung der us-amerikanischen Behörden DHS und die CISA aus dem Jahr 2021 **Screenshot**

4. AKZENTE AUS DEM FORSCHUNGSSTAND ZUR INFORMATIONS-SICHERHEIT IM FLUGZEUGUMFELD

KURZER ÜBERBLICK

Die Arbeit von Camilo Viveros von 2016

Titel **„Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts“**

Ein **Versuch, Informationssicherheitsvorfälle**, d.h. mit einem klaren Bezug zum Cyber-Bereich, darzustellen, in der die Ergebnisse auf der **Grundlage einer Befragung von Akteuren mit Expertise in der Luftfahrt** gewonnen wurden

Ausgangsbasis der Arbeit - **Befragung mit jeweils fünf identische Fragen für Fluglotsen und Piloten**

Die Antworten auf diese Fragen bildeten den Kern der Arbeit von Viveros. Dabei ist zu beachten, dass die Befragten die Fragen zwar aus ihrer fachlichen Sicht beantworteten, aber auch Situationen bewerten sollten

Die Arbeit von Camilo Andres Pantoja Viveros von 2016

Sein **Ziel war es, Cyberangriffe auf ADS-B-Geräte** und deren Funktionalität **systematisch zu analysieren** und mögliche Auswirkungen auf die Luftfahrt zu identifizieren

Der Versuch von Viveros, in eine Kernproblematik einzudringen, wurde zwar formal durchgeführt, die **Ergebnisse können jedoch nicht als validiert angesehen werden**.

Die **Befragung als systematisierte Analyse zu stilisieren ist mehr als gewagt** und verfehlt in der Darstellungsform die erkenntnisrelevanten Facetten. Dies mag auch ein **Grund für das geringe Rezipieren** der Arbeit von Viveros sein.

Die Arbeit von Elochukwu Ukwandu et al. von 2021

Titel **„Cyber Security Challenges in the Aviation Industry: An Overview of Current and Future Trends“**

Ähnlich wie bei Viveros wird der Begriff „Vorfälle“ mit Cybersecurity Bezug verwendet und die ausgesuchten Incidents als Studie zusammengefasst

Zwanzig Angriffe, die zwischen den Jahren 2000 und 2020 stattgefunden haben, wurden anhand von Quellen aufgelistet, mit der Angabe, **welches der drei abstrakten Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit** aus Sicht der Autoren **verletzt wurde**

Die Arbeit von Elochukwu Ukwandu et al. von 2021

Die zwanzig aufgelisteten Angriffe im Umfeld der Luftfahrt bilden den Basisdatensatz der genannten Studie.

Die **Studie zeigt aber auch die Schwächen** auf, sich einem komplexen Thema zu nähern, **ohne einen ganzheitlichen Rahmen zu entwerfen**

Obwohl die Verwendung der Basiswerte aus einem allgemeinen Verständnis der Begriffe der Informationssicherheit sich ableitet, haben die Autoren **weder direkt noch indirekt einen Bezug zu einem Standard der Informationssicherheit hergestellt**.

Die Arbeit von Elochukwu Ukwandu et al. von 2021

Es wird **nur auf die Arbeit von Viveros** aus dem Jahr 2016 **verweisen**

Ein **Bezug zur Problematik der Betriebssicherheit wird nicht hergestellt**. Damit ist der Leser gezwungen, um die Inhalte zu verstehen, selbst einen entsprechenden Rahmen gedanklich hinzuzufügen

Ebenso ist der Leser gezwungen, die in der titelgebenden Studie dargestellten Ausführungen zu akzeptieren, **ohne** dass die **Inhalte mit einer entsprechenden Begründung** versehen sind

Die Arbeiten von Mäurer et al. zwischen 2018 und 2023

Schwerpunkte veröffentlichter Publikationen

Sichere Kommunikation in der nächsten Generation digitaler aeronautischer Datenverbindungen

Flugversuch zur Demonstration eines sicheren bodengestützten Verstärkungssystems (GBAS) über das digitale L-Band-Luftfahrtkommunikationssystem (LDACS)

Eine Cybersicherheitsarchitektur für das digitale L-Band-Luftfahrtkommunikationssystem (LDACS)

Mit über **25 wissenschaftlichen Publikationen und einigen Best-Paper-Awards**

einem **Request for Comments (RFC) als Beitrag zur Standardisierung** als Mehrwert zur Erhöhung der Cybersicherheit in der Luftfahrt

Informationssicherheit in der Luftfahrt bei den Akkreditierungsbehörden (EASA)

Informationssicherheit in der Luftfahrt bei den Akkreditierungsbehörden (EASA)

EASA ED Decision 2020/006/R vom 01. Juli 2020

Ziel dieses Beschlusses ist es, die potenziellen Auswirkungen von Bedrohungen der Cybersicherheit auf die Sicherheit abzuschwächen. Solche Bedrohungen könnten die Folgen vorsätzlicher unerlaubter Handlungen des Zusammenwirkens mit den elektronischen Netzen und Systemen an Bord des Flugzeugs sein.

Informationssicherheit in der Luftfahrt bei den Akkreditierungsbehörden (EASA)

zwei weitere wesentliche Rechtsakte

DURCHFÜHRUNGSVERORDNUNG (EU) 2023/203 **vom 27. Oktober 2022**

in der EASA-Fachterminologie unter dem Begriff „**Part-IS Implementing Regulation oder Part IS.I.OR**“ subsumiert

ab dem **22. Februar 2026** gültig

DELEGIERTE VERORDNUNG (EU) 2022/1645 **vom 14. Juli 2022**

in der EASA-Fachterminologie unter dem Begriff „**Part-IS.D.OR**“ subsumiert

ab dem **16. Oktober 2025** gültig

Informationssicherheit in der Luftfahrt bei den Akkreditierungsbehörden (EASA)

zwei weitere wesentliche Rechtsakte

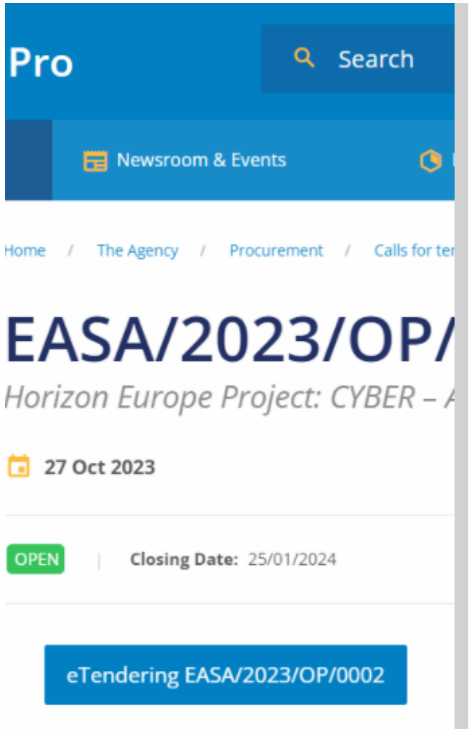
Part IS.I.OR und Part-IS.D.OR adressieren

- einerseits die Organisationen die unter EASA hoheitliche Fachlichkeit unterliegen
- andererseits die Agentur (EASA) selbst – einmaliges Beispiel

Informationssicherheit in
der Luftfahrt bei den
Akkreditierungsbehörden (EASA)

AUFBAU VON RAHMENWERKE ZUR STEUERUNG DER INFORMATIONSSICHERHEIT BEI FLUGZEGEN UND IN DER LUFTFAHRT

ORGANISATION	Beschreibung	AUTHORITY (Agentur)
IS.I.OR.100	Scope	IS.AR.100
IS.I.OR.200	Managementsystem für Informationssicherheit (ISMS)	IS.AR.200
IS.I.OR.205	Bewertung von Informationssicherheitsrisiken	IS.AR.205
IS.I.OR.210	Behandlung von Informationssicherheitsrisiken	IS.AR.210
IS.I.OR.215	Internes Meldesystem für die Informationssicherheit	
IS.I.OR.220	Vorfälle in der Informationssicherheit - Erkennung, Reaktion und Wiederherstellung	IS.AR.215
IS.I.OR.225	Reaktion auf die von der zuständigen Behörde gemeldeten Feststellungen	
IS.I.OR.230	Externes Berichtswesen zur Informationssicherheit	✓
IS.I.OR.235	Auftragsvergabe für das Informationssicherheitsmanagement	IS.AR.220
IS.I.OR.240	Anforderungen an das Personal	IS.AR.225
IS.I.OR.245	Aufbewahrung von Unterlagen	IS.AR.230
IS.I.OR.250	Information security management manual (ISMM)	
IS.I.OR.255	Changes to the information security management system	
IS.I.OR.260	Kontinuierliche Verbesserung	IS.AR.235

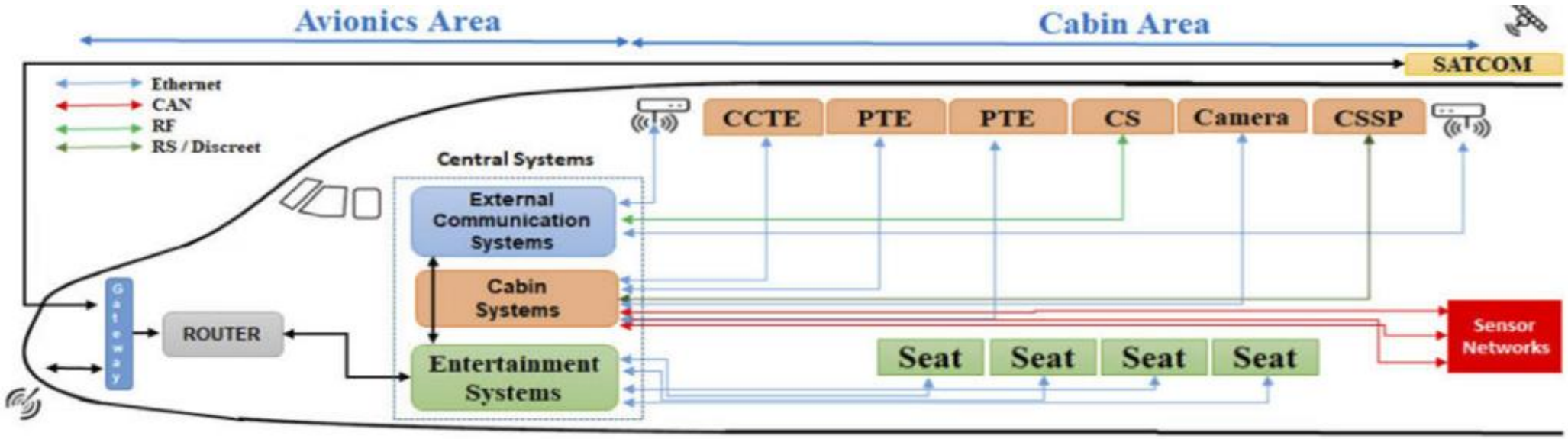


EASA/2023/OP/0002 Horizon Europe Project: CYBER – Aviation Resilience – Cybersecurity Threat Landscape

Ausschreibung - befasst sich mit folgenden Maßnahmen: Entwicklung einer Datenbank für Schwachstellen, die Informationen über entdeckte Schwachstellen sammelt, unterhält und verbreitet, und sich an wichtige Verkehrsinformations-systeme richtet.

5. Flugzeuge in der Interaktion mit dem Begriff der Informationssicherheit

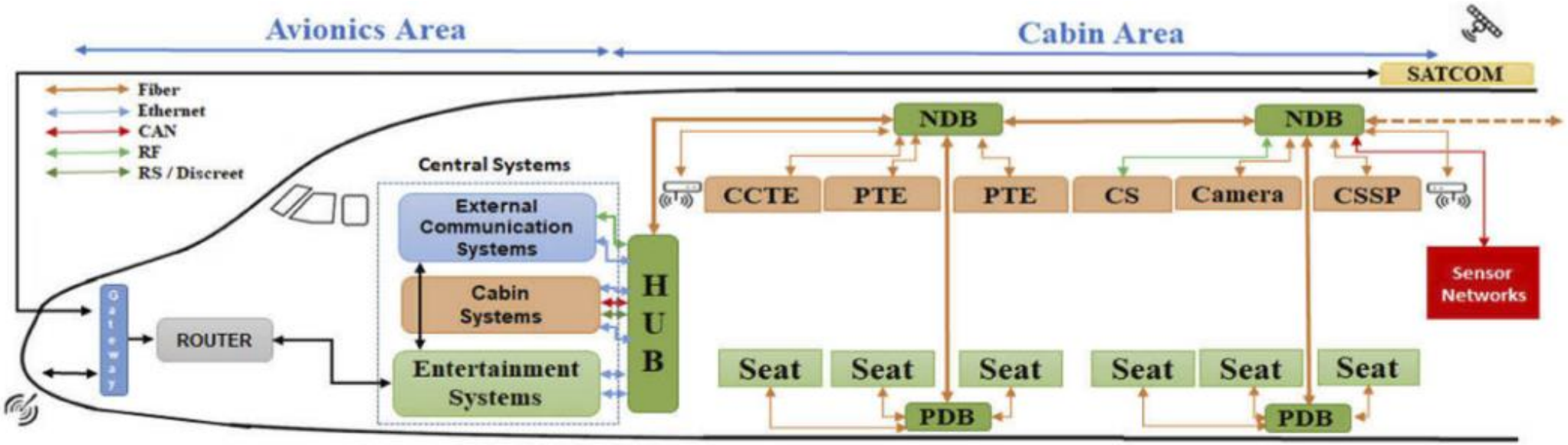
KÜNFTIGE ENTWICKLUNGSLINIE, ABGRENZUNG, DIMENSIONEN,



Künftige Entwicklungslinie im Zuge der dauerhaften und universellen Vernetzung

AKTUELLE KABINENNETZ-KUPFERARCHITEKTUR

Dieses Foto stammt von "Hamza Saadaoui et al." übernommen von https://opg.optica.org/optcon/viewmedia.cfm?uri=optcon-1-4-719&seq=0.



Künftige Entwicklungslinie im Zuge der dauerhaften und universellen Vernetzung

NEUE ARCHITEKTUR DER OPTISCHEN KABINENNETZE MIT INTEGRIERTER MODULARER AVIONIK

Dieses Foto stammt von "Hamza Saadaoui et al." übernommen von https://opg.optica.org/optcon/viewmedia.cfm?uri=optcon-1-4-719&seq=0.

Absicherung ab
der Grenze der Schnittstellen
in Bezug auf vier Dimensionen

---

im das Ökosystem Luftfahrt gegenüber

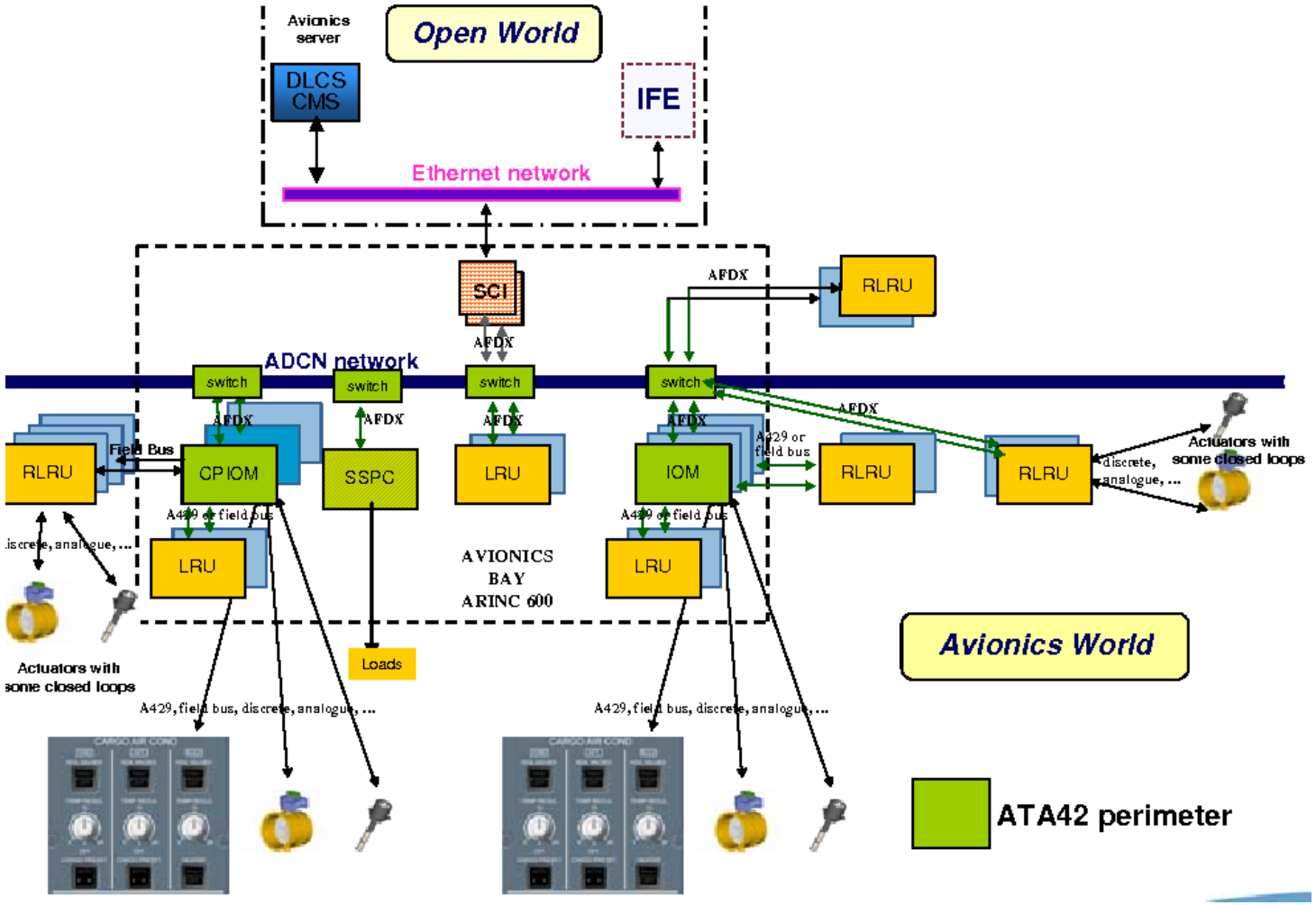
I. andere Flugzeuge,

II. Flughafen und

III. Bodensysteme,

IV. Satellitensysteme,

V. LTE



Absicherung eines IoT-Triebwerks

Remote-Verbindungen zur Wartungszwecken wie am Beispiel des vernetzten Triebwerks mit Remote-Funktion

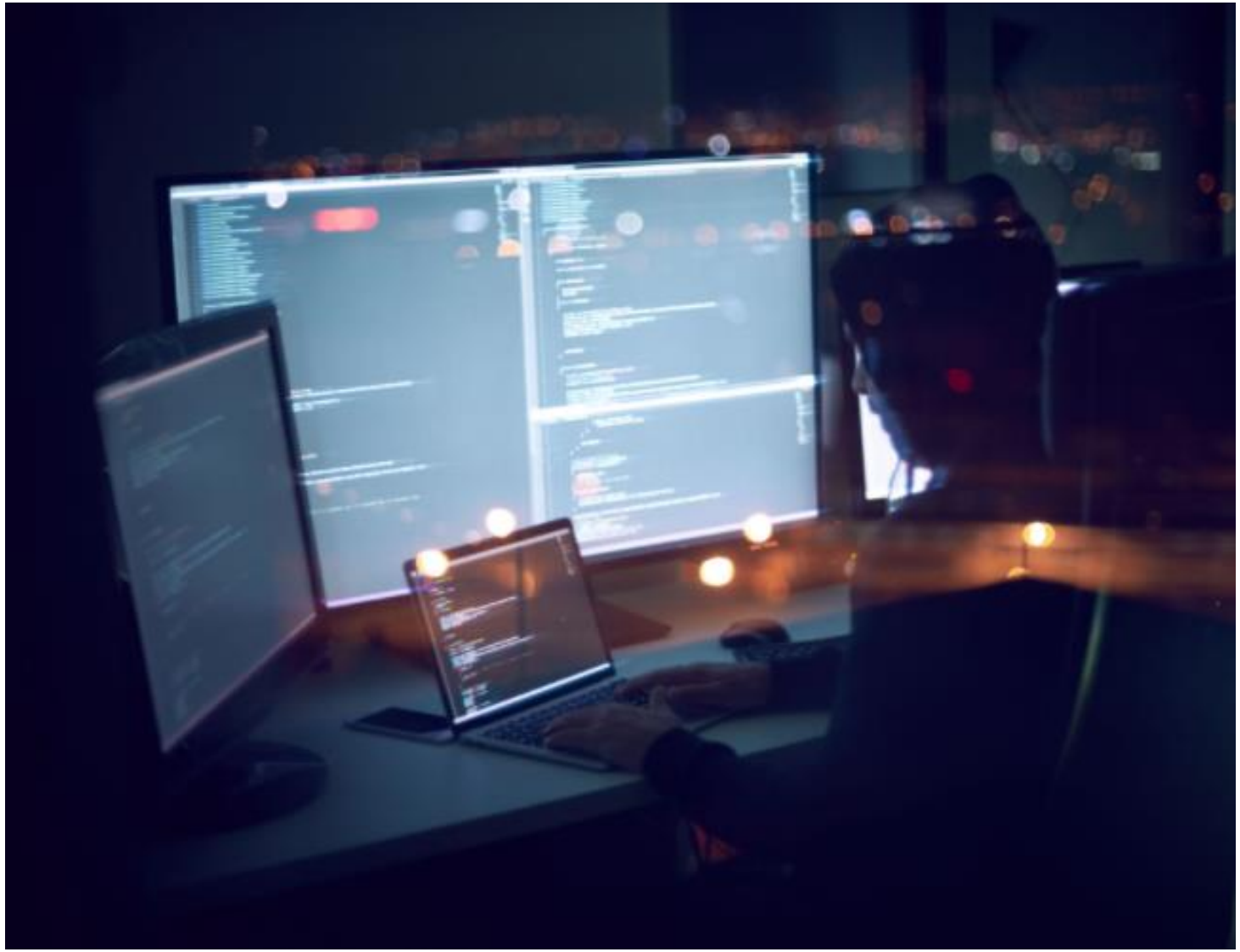
Absicherung eines IoT-Triebwerks

„[…] das neu entwickelte Triebwerk X wird in der neuesten Generation von großen Geschäftsreiseflugzeugen eingesetzt und nutzt ***mehr digitale Technologien als andere Triebwerke zuvor****. Dazu zählt etwa ein* ***Überwachungssystem****, das erstmals mehrere tausend Paramater der Triebwerke und wichtiger Anbauteile* ***während des Betriebs in Echtzeit erfasst****. Mittels eigens entwickelter Algorithmen kann in aufwendigen Rechenverfahren ein* ***etwaiger Wartungsbedarf noch in der Luft abgeleitet werden****. Zudem bietet das neue Überwachungssystem dank sicherer, bi-direktionaler* ***Kommunikation neuartige Möglichkeiten der Ferndiagnose*** *[…]“.*

Von Ammon, Cornelia: Was uns bewegt. Innovation der Woche KW 46/2018. Triebwerke werden digital, BDLI, Berlin 2018

Resümee - Flugzeuge in der Interaktion mit dem Begriff der Informationssicherheit Wechselwirkung

Wechselwirkung durch **elementare Bedrohungen**, durch **Vernetzung** und Digitalisierung, durch **Vorgaben** der Regulierungsbehörde, durch **Interaktion im Ökosystem Luftfahrt**



Resümee - Flugzeuge und Informationssicherheit

Die Interaktion mit der Informationssicherheit muss als Ziel die

I. Reifegradsteigerung der Implementierung der Informationssicherheit haben
II. Frage nach Prozessen der Informationssicherheit mit einem hohen Reifegrad

Reifegrad	Kennzeichen
0	Es existiert kein Prozess, es gibt auch keine Planungen hierzu
1	Es gibt Planungen zur Etablierung eines Prozesses, jedoch keine Umsetzungen
2	Teile des Prozesses sind umgesetzt, es fehlt jedoch an systematischer Dokumentation
3	Der Prozess ist vollständig umgesetzt und dokumentiert
4	Der Prozess wird darüber hinaus auch regelmäßig auf Effektivität überprüft
5	**Zusätzlich sind Maßnahmen zur kontinuierlichen Verbesserung vorhanden heißt PROZESS DER INFORMATIONSSICHERHEIT IST ETABLIERT UND WIRD KONTINUIERLICH VERBESSERT**

Möglicher Aufbau - Definition von Reifegraden in der Informationssicherheit

Laufende eigene Arbeiten

Laufende eigene Arbeiten am Beispiel eines klassischen Netzwerkansatzes

Die Aufteilung eines internen Netzes in verschiedene Zonen und die Gruppierung der Systeme nach **Funktion, Zuverlässigkeit und Schutzbedarf** mit entsprechenden Zugangsbeschränkungen zwischen den Zonen bewirkt, dass

Vorfälle und daraus resultierende Schäden in ihren Auswirkungen deutlich begrenzt werden können,

Angriffe auf Link-Ebene, wie z.B. Man-in-the-Middle-Angriffe, eingeschränkt werden können,

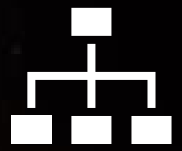
die Sichtbarkeit kritischer Systeme deutlich eingeschränkt werden kann.

Die Frage nach Systematik im Umgang mit Themen wie Bedrohungen, Schwachstellen

Laufende eigene Arbeiten am Beispiel eines klassischen Netzwerkansatzes

Ist ein solcher Ansatz bei Flugzeugen möglich? Zulässig? oder nur experimentell?

Welche Instrumente sollten eingesetzt werden?



Braucht es nur ein einmaliges Vorgehen oder kann eine Systematik vorgeschlagen werden?

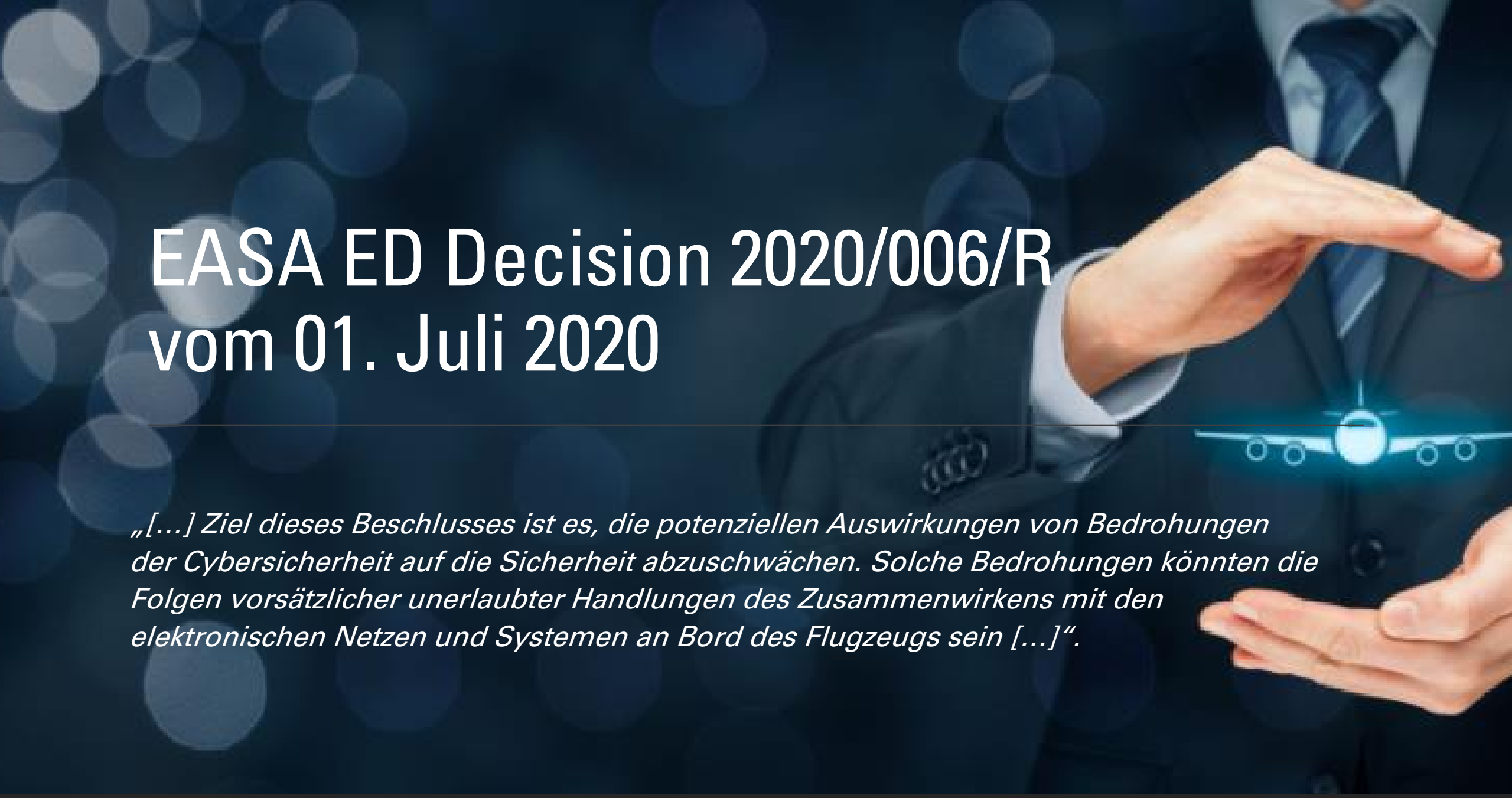
Im Rahmen der Dissertationsarbeit sollen u.a. Facetten dieser Fragestellungen untersucht werden.

Vor dem Abschluss eine Anekdote von der AERO 2023 in Friedrichshafen

DEMONSTRATION EINES VOLLSTÄNDIG DIGITALISIERTEN AVIONIK-SYSTEMS

Über Vorteile, Funktionen und Schnelligkeit einer komplett digitalisierten Avionik.
Kann das alles sein?

EASA ED Decision 2020/006/R vom 01. Juli 2020



„[...] Ziel dieses Beschlusses ist es, die potenziellen Auswirkungen von Bedrohungen der Cybersicherheit auf die Sicherheit abzuschwächen. Solche Bedrohungen könnten die Folgen vorsätzlicher unerlaubter Handlungen des Zusammenwirkens mit den elektronischen Netzen und Systemen an Bord des Flugzeugs sein [...]“.

Vielen Dank für Ihre Aufmerksamkeit

V. HAFNER