Airworthiness Security: Zuverlässigkeit ist nicht mehr genug!

Sicherheit in der Luftfahrt

Sicherheit meint die Abwesenheit von Gefahren, d.h. die bestmögliche Vermeidung von inakzeptablen Risiken. Der Mensch strebt nach Sicherheit und versucht einen relativen Zustand der Gefahrenfreiheit zu erreichen. Gerade bei Hochtechnologiesystemen wie in der Luftfahrt ist daher das Erreichen und Aufrechterhalten von Sicherheit ein seit jeher intensiv verfolgtes Ziel. Beginnend mit dem Pariser Luftfahrtabkommen von 1919 und der dort initiierten *Commission Internationale de Navigation Aérienne* (CINA) und gefolgt vom Chicagoer Abkommen im Jahr 1944, steht die in Chicago ins Leben gerufene und am 13. Mai 1947 gegründete *International Civil Aviation Organization* (ICAO) für Sicherheit in der Luftfahrt. Traditionell kümmert sich die ICAO insbesondere um die Zuverlässigkeit (engl. *Safety*), also die funktionale Sicherheit der Luftfahrtsysteme. „Immer das Geforderte leisten, auch beim Auftreten von Fehlern" lautet das Motto. Dann jedoch, und einhergehend mit den seit Beginn der 70er Jahre zunehmend aufkommenden terroristischen Angriffen auf das Lufttransportsystem, veröffentlichte die ICAO im Jahr 1975 die erste Ausgabe des ICAO Annex 17 mit dem Titel *Safeguarding International Civil Aviation Against Acts of Unlawful Interference* [1]. Seitdem spielt auch der Schutz des Systems vor physischen Angriffen (engl. *Security* oder auch *Aviation Security*) eine wichtige Rolle. Als am 11. September 2001 Passagierflugzeuge erstmals als Waffen gegen Bodenziele eingesetzt wurden, im Englischen als sog. Renegade-Fall bezeichnet, erreichte der Schutz des Systems vor physischen Angriffen nochmals eine völlig neue Dimension. Sehr schnell musste dann durch entsprechende Maßnahmen und Verordnungen zum Schutz des Systems reagiert werden [2].

Systemische Informationssicherheit als aktuelles Thema

Ein vergleichsweise neues Thema der Luftsicherheit sind mögliche Angriffe auf die informationstechnischen Systeme. Aktuell kann sich die Luftfahrt der Digitalisierung und der Öffnung des *Cyberspace* nicht mehr völlig verschließen. Schließlich sollen auch im Lufttransport mit durchgängiger Konnektivität, digitaler Kommunikation, gesammelten Daten und zeitnah übertragener Information in Zukunft noch mehr Effizienz bei den Fluggesellschaften und Komfort für die Passagiere erzielt werden. Datenanalyse und künstliche Intelligenz sollen hier die neuen Potenziale erschließen. Bei der rasanten Technologieentwicklung in diesem Bereich kann die ICAO kaum mehr Schritt halten. Erstmals im Jahr 2010 finden sich in der in der Ergänzung Nr. 12 zur 9. Ausgabe des ICAO Annex 17 [1] zwei kurze Empfehlungen zum neuen Bedrohungsszenario *Cyber Threats*: 1.) Es sollen Maßnahmen entwickelt werden, welche kritische Informations- und Kommunikationstechnologie-Systeme (IKT-Systeme) in der Zivilluftfahrt davor bewahren, die Zuverlässigkeit (*Safety*) zu gefährden, und, 2.) es sollen kritische IKT-Systeme und deren Bedrohungen und Schwachstellen identifiziert werden, um entsprechende Schutzmaßnahmen zu entwickeln. Aber erst auf der 39. Tagung der ICAO im September 2016 hat die ICAO die *Secretariat Study Group on Cybersecurity* (SSGC) eingerichtet, um alle Elemente und Bereiche des internationalen Luftverkehrs zu beleuchten, die von Cybervorfällen und Angriffen betroffen sein könnten. Aufgrund der Dringlichkeit und Komplexität des Themas ist es nicht verwunderlich, dass sich auch *Bottom-up*, d.h. von der Technik ausgehend, inzwischen viele Stakeholder zusammengefunden und Initiativen gebildet haben, welche sich intensiv mit dem Thema *Aviation Cyber Security*, also der systemischen Informationssicherheit in der Luftfahrt, auseinandersetzen. In diesem Kontext existieren heute die drei wesentlichen Bereiche (1) *Airport* und *Airline Cyber Security*, (2) *Aircraft Cyber Security* und (3) *Air Traffic Management* (ATM) *Cyber Security*.

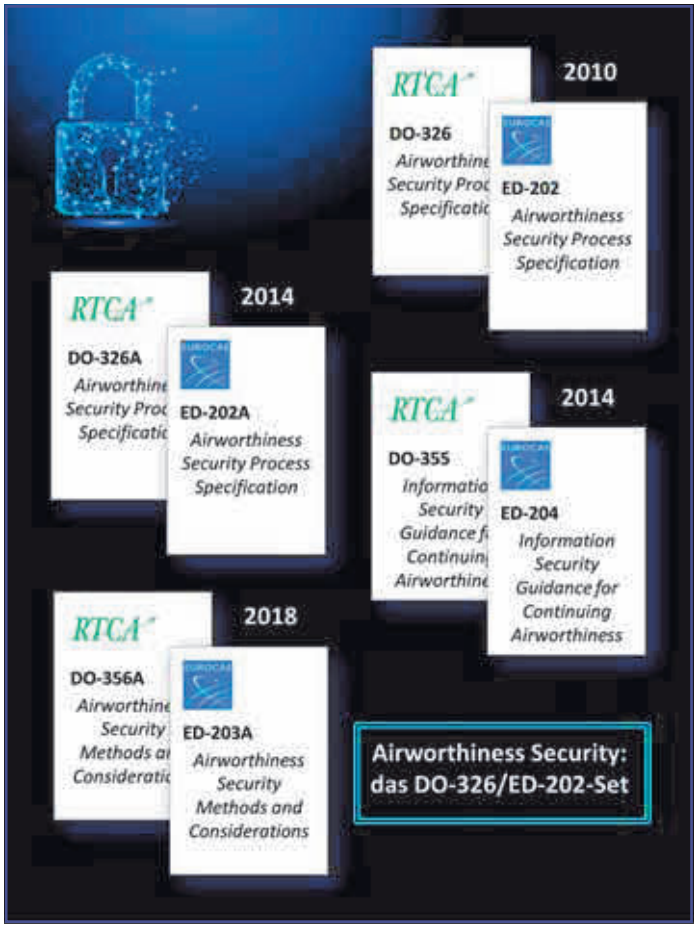

Bild 1: Das DO-326/ED-202-Set mit seinen zwischen 2010 und 2018 entstanden Dokumenten behandelt den Schutz eines Flugzeugs und seiner Systeme vor vorsätzlichen nicht autorisierten elektronischen Interaktionen. Mit anderen Worten: den Schutz vor Angriffen aus dem Cyberspace.

Jeder dieser Bereiche nutzt diverse IKT-Systeme, welche potenziell angegriffen werden können. Auch wenn sich ein solcher Angriff nicht zu einer Gefahr für das gesamte Lufttransportsystem ausweiten muss, so geht damit jedoch immer ein kommerzieller Schaden oder ein Vertrauensverlust in die Technik und deren Betreiber einher.

Airworthiness Security für die Entwicklung und den Betrieb

Ein extrem wichtiges Thema ist in diesem Bedrohungsumfeld die Sicherstellung der informationstechnischen Angriffssicherheit des Luftfahrzeugs, was landläufig gerne mit dem englischen Begriff *Aircraft Cyber Security* bezeichnet wird. Dieser bezieht sich auf das gesamte Fluggerät mit seiner Betriebsumgebung und meint die Resilienz des Luftfahrtgeräts gegenüber möglichen Angriffen aus dem *Cyberspace*. Möchte man definitionsgemäß hervorheben, dass von einem zugelassenen und informationstechnisch angriffssicher entwickelten bzw. betriebenen Flugzeug oder Flugzeugsystem die Rede ist, so spricht man korrekterweise von der so genannten *Airworthiness Security*. Grundsätzlich existieren hierbei immer die beiden Phasen, 1.) ein Flugzeug bzw. seine Systeme sicher (d.h. *secure*) zu implementieren und 2.), die oft schwierigere Phase, das Flugzeug und seine Systeme über drei bis vier Jahrzehnte hinweg sicher zu betreiben.

Das DO-326/ED-202-Set

Aufgrund des dringenden Bedarfes nach einer *Airworthiness Security Process Specification* veröffentlichten erstmals im Jahr 2010 das RTCA *Special Committee* 216 (SC-216) und die EUROCAE *Working Group* 72 (WG-72) unter den beiden Bezeichnern DO-326 und ED-202 ein gleichnamiges Dokument[3] (siehe Bild 1). Dieses war stark an den bekannten SAE-ARP4754-Leitfaden für *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*[4] und an die bekannte Normenreihe ISO/IEC 27000 mit Standards zur Informationssicherheit[5] angelehnt. Eine zweite harmonisierte Veröffentlichung der Dokumente DO-326A und ED-202A[6], welche sich unter gleichnamigem Titel nochmals auf die *Airworthiness Security Process Specification* zur 1.) sicheren Implementierung eines Flugzeugs bzw. seiner Systeme bezog, erfolgte im Jahr 2014. Ebenfalls im Jahr 2014 veröffentlichten die Arbeitsgruppen unter dem Titel *Information Security Guidance for Continuing Airworthiness* die Dokumente DO-355 und ED-204[7] zum 2.) sicheren Betrieb eines Flugzeugs und seiner Systeme während des Lebenszyklus. Ein drittes Dokumentenpaar zum Thema *Airworthiness Security Methods and Considerations*, welches erst in seiner zweiten Auflage als DO-356A bzw. ED-203A[8] harmonisiert wurde, folgte im Jahr 2018. Insgesamt spricht man bei dieser Dokumentenzusammenstellung zur *Airworthiness Security* vom sog. „DO-326/ED-202-Set“ (siehe Bild 1).

Werkzeuge und Methoden zur Implementierung dieses De-Facto-Standards

In den vergangenen Jahren wurden diese zum großen Teil neuen Leitlinien Schritt für Schritt in den Entwicklungsprozess von Flugzeugen und deren Systeme integriert und auch auf die Betriebsphase angewendet. Wenngleich im Ergebnis das wichtige Ziel der sicheren Implementierung eines Flugzeugs bzw. seiner Systeme erreicht wurde, so besteht bei stetig steigender Systemkomplexität dennoch eine Herausforderung hinsichtlich eines jederzeit detaillierten Überblicks zu den vielfältigen Wechselwirkungen von sowohl funktionalen, Safety-bezogenen als auch Security-bezogenen Anforderungen, wenn diese rein textuell spezifiziert werden. Dieser Herausforderung widmet sich das Institut für Flugzeug-Kabinensysteme an der Technischen Universität Hamburg methodisch mit Hilfe der modellbasierten Systementwicklung. Innerhalb des durch die DO-331[9] für die modellbasierte Entwicklung von Flugzeugsystemen vorgegebenen Rahmens, wurde ein Ansatz erarbeitet, bei dem die modellbasierte Security-Analyse ein integraler Bestandteil des Systemmodells ist. Als formale Sprache zur Modellerstellung wird die *System Modeling Language* (SysML)[10] verwendet. Das so genannte Drei-V-Modell (siehe Bild 2), welches in Form eines Vorgehensmodells die Interaktion zwischen dem Systementwicklungsprozess (SEP) zusammen mit dem Safety- und dem Security-Entwicklungsprozess (SafEP und SecEP) beschreibt[11, 12], dient als Grundlage für diesen Ansatz. Ausgehend vom Drei-V-Modell wurde, in Anlehnung an die CORAS-Methode[13] und einer Security-Ontologie folgend, die Möglichkeit geschaffen, konform mit den Forderungen des DO-326/ED-202-Set und innerhalb eines SysML-Modells auf allen Systementwicklungsebenen, eine Risikoanalyse modellbasiert durchführen zu können. Auch die nötige Konservierung der Analyseergebnisse in Form einer Risikomatrix erfolgt letztlich in diesem einen Modell. Der

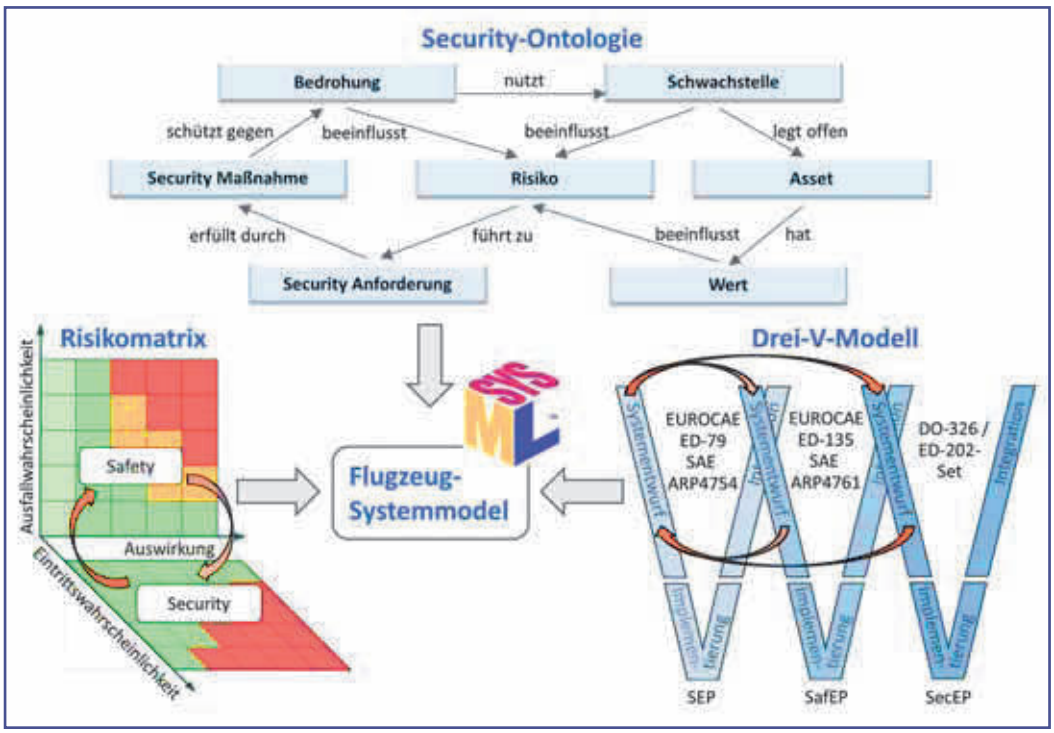

Bild 2: Methodische und werkzeugtechnische Integration des DO-326/ED-202-Set zur Erstellung eines Flugzeug-Systemmodells: Ausgehend vom Drei-V-Modell, welches die Interaktion zwischen dem Systementwicklungsprozess (SEP) mit dem Safety- und Security-Entwicklungsprozess (SafEP und SecEP) beschreibt, wird, einer Security-Ontologie folgend, die Security-Analyse modellbasiert durchgeführt. Die Konservierung der Ergebnisse in Form einer Risikomatrix ist integraler Bestandteil des Flugzeugsystemmodells.

Vorteil dieses Ansatzes, die nach dem DO-326/ED-202-Set geforderten Security-Entwicklungsaktivitäten in das Modell des Systementwicklungsprozesses zu integrieren, besteht darin, dass über dieses eine Modell eine feste Kopplung der spezifizierten funktionalen Safety- und den Security-Anforderungen innerhalb der beiden Prozesse SafEP und SecEP entsteht. Damit werden die Auswirkungen von Anforderungsmodifikationen unmittelbar erkennbar und nachvollziehbar. Auch bleibt damit die Konsistenz der Anforderungen innerhalb der komplexen Zusammenhänge in einem Gesamtsystemmodell erhalten. Im Ergebnis unterstützen die am Institut für Flugzeug-Kabinensysteme entwickelten Werkzeuge und Methoden die aktuell erforderliche Implementierung und Handhabung des DO-326/ED-202-Set-De-Facto-Standards und bieten damit erstmals eine modellbasierte Lösung zu dessen technischer Umsetzung bei der Flugzeug- und Systementwicklung.

Dipl.-Ing. Hartmut Hintze,
Prof. Dr. Ralf God,
Institut für
Flugzeug-Kabinensysteme
Technische Universität
Hamburg
www.tuhh.de/fks

Literaturverzeichnis

[1] ICAO-Annex 17 Security – Schutz der internationalen Zivilluftfahrt vor illegalen Eingriffen; aktuell 10. Ausgabe, April 2017.

[2] Verordnung (EG) Nr. 2320/2002 des europäischen Parlaments und des Rates vom 16. Dezember 2002 zur Festlegung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt; Verordnung (EG) Nr.300/2008 vom 11. März 2008.

[3] DO-326 / ED-202 (2010): Airworthiness Security Process Specification.

[4] SAE ARP4754: Certification Considerations for Highly-Integrated Or Complex Aircraft Systems; SAE ARP4754A (neu seit 2010): Guidelines for Development of Civil Aircraft and Systems.

[5] ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

[6] DO-326A / ED-202A (2014): Airworthiness Security Process Specification.

[7] DO-355 / ED-204 (2014): Information Security Guidance for Continuing Airworthiness.

[8] DO-356A / ED-203A (2018): Airworthiness Security Methods and Considerations.

[9] DO-331 (2011): Model-Based Development and Verification – Supplement to DO178C and DO-278A.

[10] The Object Management Group® (OMG®) Systems Modeling Language (SysML) http://www.omgsysml.org

[11] H. Hintze, R. God (2012): Ansatz für einen Systems Security Engineering Prozess zur Entwicklung eines Kabinenmanagementsystems der nächsten Generation, Deutscher Luft- und Raumfahrtkongress, Berlin, 10.-12. September 2012.

[12] H. Hintze, B. Wiegraefe, R. God (2013) A Security Engineering Process Approach for the Future Development of Complex Aircraft Cabin Systems, in: L.J. Janczewski, H. Wolf, S. Shenoi (Hrsg.) Security and Privacy Protection in Information Processing Systems, Springer-Verlag, IFIP AICT 405, 190-202.

[13] M.S. Lund, B. Solhaug, K. Stølen (2011): Model-Driven Risk Analysis, The CORAS Approach, Springer-Verlag.