Information Technology Security Threats to Modern e-Enabled Aircraft: A Cautionary Note *†

Marko Wolf and Moritz Minzlaff and Martin Moser
{marko.wolf,moritz.minzlaff,martin.moser}@escrypt.com
ESCRYPT GmbH – Embedded Security, Germany

Most passengers, airlines, and the aircraft industry in general are used to very high safety standards and precautions surrounding aircraft systems. As the computerization of aircraft steadily progresses, the question of security, i.e. the protection against intentional manipulations, becomes increasingly relevant. This article focuses on these security challenges. In particular, it adds the following contributions: It assesses the current state of public research on aircraft IT security and contrasts it with an evaluation of the threat-level through a discussion of recent attacks and vulnerabilities. This shows that many attack vectors are not protected against by the state-of-the-art technology implemented in today's aircraft. In addition, increasing digitalization, connectivity, and similar developments of modern ("e-enabled") aircraft are shown to cause an ever larger attack surface. This results in challenges to the aircraft industry which are discussed in the final part of this paper and lead to a requirement for additional technical, organizational, educational, and regulatory counter-measures.

1 Introduction

Digital network connectivity and electronic data exchange have been identified by Ken Dunlap [32], Director of Security of the International Air Transport Association (IATA), as the basis of future efficiency gains in the aviation industry. According to Dunlap, these new 'all-electric' aircraft will have a whole range of systems operating electronically and data will be communicated and updated automatically in real time. However, the increasing computerization of and digital communication between formerly mechanically driven and isolated systems carries great risks, too: As became apparent in the automotive domain [18], this process opens the door to potentially malicious encroachments by hackers and malware that can jeopardize an aircraft system's availability and overall aircraft safety. A series of recent incidents [28, 57, 42]

*Parts of this article have been already presented at the 13th German IT Security Congress in May 2013.

†This document is an author version. The original article has been published at Journal of Aerospace Information Systems, Vol. 11, No. 7 (2014), pp. 447-457. DOI: 10.2514/1.I010156.

shows that vulnerability of aircraft information technology (IT) is not only an academic possibility but already harsh reality. "The likelihood of this sort of threat is low, because of the complexity [of launching such an attack]", concedes Ty Miller, CTO of an IT security company specialized in penetration testing, "but the impact is extreme" [59]. In fact, he sees cyber attacks as the second largest threat to airlines directly after natural disasters.

Our contribution: The aim of this paper is to raise awareness for aircraft IT security and to point out the relationship between technological progress and an increasing threat-level. To begin, we give an overview of the current state of research on the topic in Section 2. Then, in Section 3, we provide a state-of-the-art analysis of recent attacks and incidents that happened to civil and military aircraft. These sections prove that there is currently insufficient protection of on-board IT systems. Despite its importance, public research in the area of aircraft IT security is not keeping pace with recent developments towards e-enabled aircraft. In Section 4, we analyze what has changed over the past decades and how these changes might have affected the information security of modern aircraft. Based on this analysis, we discuss in Section 5 open challenges that have to be addressed to ensure the information security of modern e-enabled aircraft and to minimize the risks due to security vulnerabilities. We close our findings in Section 6 with a summary and an outlook on the future of aircraft IT security.

2 Related Work

One of the first to discuss the topic was Neumann [44]. His article focuses on security-relevant problems of computer usage in aviation and gives a review of past incidents. Furthermore, he lists potential future incidents, many of which have occurred since the article was published in 1997. More recent work was done by Sampigethaya et al. [52]. They discuss the problems arising from the high complexity of modern "e-enabled" aircraft's IT systems. The discussion involves an analysis of vulnerabilities of such systems as well as possible security solutions. Another paper by Sampigethaya et al. [53] gives an outlook on the opportunities and upcoming security challenges related to the computerization of aircraft in the next 20 years. While these papers provide a theoretical analysis of the developments in the first place, they do not discuss the current threat-level based on real-life attacks. An adaptive architecture that enforces the security of e-enabled aircraft is introduced by Mahmoud et al. [37]. At the center of their architecture is the "Security Manager", a component designed to control the aircraft's data traffic. The architecture's usability is checked by a detailed performance study. Finally, the authors conclude that such an architecture requires an aviation-adapted public key infrastructure in order to provide authentication for the increasing number of civil aircraft. Alomair et al. [7] propose to use digital signatures for securing air-ground communications. They introduce several possible signature protocols using a forward-secure digital signature scheme. Concrete secure message protocols are analyzed and compared by Thanthry et al. [62]. They propose to use a SSL/TLS based security mechanism since it has almost the same security level as IPSec but does not suffer from the same service quality issues. A more general approach is used by Nuseibeh et al. [46] who developed a framework for a security requirement analysis of air traffic control projects. Similarly, a systematic approach via Common Criteria is supported by Robinson et al. [51]. Additionally, research and standardization is also driven by official committees and authorities. For example, the Airlines Electronic Engineering Committee (AEEC) develops "engineering standards and technical solutions for

avionics, networks, and cabin systems that foster increased efficiency and reduced life cycle costs throughout the aviation community" [5]. It has published several standards such as the ARINC Report 811 [12] which describes a framework for the information security process of aircraft (cf. [48] for a comprehensive overview). IATA is also aware of the problems arising from the use of complex IT systems in aircraft and has published an overview discussing the related security threats and challenges [32].

The next section will show that many vulnerabilities exist and are already being actively exploited. This leads the authors to conclude that despite the above mentioned research, risk awareness for IT security in the aviation industry lacks behind other industries, e.g. the automotive industry where public projects and standardization committees have made tremendous progress. The later sections of this paper will explore the underlying reasons for this gap between serious security threats on the one hand and research and implementation of countermeasures on the other hand.

3 Recent Security Incidents and Threats

While safety of aircraft IT systems is a well-established field, their protection against systematic manipulation has only recently started to attract attention. However, as the following examples demonstrate, aircraft IT security is already a big challenge today. Moreover, the authors expect a considerably higher actual number of security incidents than the following list suggests since some organizations may consider it in their best strategic or commercial interests not to disclose information about any incidents. Each of the examples discusses the incident/threat itself, identifies who attacked or might carry out similar attacks in the future, and derives conclusions for the system operators. To aid in the identification of attackers, let us first discuss distinct attacker profiles. Generally speaking, the sophistication of attackers, i.e. their expertise, technical equipment, target knowledge, access perimeters, and financial and temporal resources, varies between types of attackers. Moreover, it varies within a certain type depending on the specific attack target. Finally, as Stuxnet proved [24], an attacker may have vast resources available. Given these difficulties in assessing possible attackers, we extracted the following broad classification.

Military forces will try to launch attacks with a direct impact on the enemy in the battlefield such as thwarting an attack by airplanes or interfering with or destroying enemy airplanes. Hence, they will be "close" to the target and, e.g., try to intrude on aircraft communications using equipment on site (cf. Predator drone incident [28]).

Intelligence services may support troop operations in the battlefield or gather information at home or abroad on personal, business, military, or political developments [64]. Their methods may include exploitation of systematic security weaknesses, organizational, or backend security vulnerabilities (cf. Sentinel drone incident [57] or Stuxnet incident), or monitoring airspace (e.g., via globally unique ICAO (International Civil Aviation Organization) aircraft identifier).

Terrorists usually try to sabotage a particular aircraft or aircraft control system for politically motivated extortion or intimidation. Terrorists will likely use COTS equipment, but nonetheless their actions can have serious impact. Among the fatal accidents involving commercial

aircraft with at least ten passengers between 1950 and 2009, a purported 9% are due to aircraft tampering or sabotage (by terrorists and non-terrorists alike) [50].

Business competitors intrude on aircraft IT systems developed or used by a particular company for industrial espionage [39] similar to intelligence service motives above [64]. Less likely but still possible is limited sabotage with the intent to damage a competitor's reputation or to increase their costs due to flight delays or cancellations.

Hackers in this context range from single persons with little specialist knowledge to powerful underground groups such as Anonymous. The former may simply be interested to abuse, e.g., on-board Wi-Fi, but may also be interested in crashing a plane to commit suicide or enact personal revenge on a passenger. Hacker groups may try to attack the security or privacy of aircraft IT systems for reasons such as fun, fame, politics, revenge, or profit.

3.1 Intercepting Video Feeds of Drones (2009)

Already back in 2009 the Wall Street Journal reported that militants in Iraq and Afghanistan intercepted live video streams of U.S. predator drones [28]. The enemies of the U.S. forces used commercial-off-the-shelf (COTS) hard- and software that cost less than 100 USD to exploit unprotected communication links. Generalizing this situation, anyone with an interest to gain insight into enemy operations may pursue such an attack. This includes military forces, intelligence services, and terrorists. But the situation is not exclusive to the military domain: The FAA Modernization and Reform Act of 2012 [23] allows the commercial use of drones in U.S. skies starting in 2015. In this context, one may also think of hackers and business competitors that may want to gain access to restricted data. The security leak of predator drones was apparently known to the U.S. military since the 90s, but as the Wall Street Journal writes, it was assumed that enemies would not find out to exploit it. As this example demonstrates, blind faith is not enough when dealing with confidential data.

3.2 Spoofing GPS Navigation of a U.S. RQ-170 Sentinel Drone (2011)

The latest known cyberwar incident is the downing of a U.S. RQ-170 Sentinel drone in Iran in December 2011. Allegedly, a spoofed GPS signal mislead the drone to automatically land on Iranian soil, while its GPS navigation actually believed to be near a U.S. military location [57]. Even though there are doubtful voices regarding those claims, it is clear that capturing hostile drones is extremely valuable to one's own forces and intelligence services: The goals of such an attack may range from the immediate blow to enemy forces on the battlefield to the possibility of reverse engineering the drone. It is not clear what really caused the drone to land, but manipulated navigational data seem to be part of the reason. To prevent such an incident from happening again, integrity and availability of such data must be guaranteed.

3.3 Spoofing GPS Navigation of Civilian Drones (2012)

In contrast to the RQ-170 incident, the research of Humphreys et al [31] has publicly proved that integrity of civil GPS navigation is easily violated. Using equipment that cost only around 1,000 USD, they demonstrated that "these drones nav systems are hackable by their exposed

GPS stream, and once you spoof it, you can have your way with a drone" [42]. Attackers that may want to exploit this security hole are manifold: Hackers may try to gain control of drones for amusement or, just like terrorists, to wreak havoc. Depending on the drone operator, business competitors may be interested in damaging or irritating drones. Considering that more and more applications rely on accurate GPS data there is an urgent need to enable authenticity & integrity validation (and to ensure availability) of GPS data.

3.4 Spoofing Aircraft With Faked ADS-B Messages (2012)

The situation of information security in commercial aircraft is not much better as a look at the automatic dependent surveillance-broadcast (ADS-B) system reveals. ADS-B messages are digital aircraft beacons containing an aircraft's unique identity, position, speed, heading, and other data. They are broadcast to make aircraft digitally visible in real-time to nearby aircraft and ground control for purposes such as air traffic control, air traffic alert, and collision avoidance. Automated ADS-B technology is already used by over 70% of all commercial aircraft and is expected to replace radar as the primary surveillance method. However, current ADS-B specifications are without any authenticity or integrity protection against malicious manipulations or spoofing. In fact, "solutions for verification of position information received in A2I/A2A-In applications do not currently exist" [52]. With ADS-B transponders freely available from 2,000 USD, everyone can spoof aircraft and ground control. In fact, Costin et al. [20] demonstrated at the Black Hat 2012 that "[ADS-B] attacks are both easy and practically feasible, for a moderately sophisticated attacker". Plausible attack scenarios are hackers or terrorists that put phantom aircraft in the sky to launch a denial-of-service attack on airports by overwhelming traffic control capacity or causing airplanes to take dangerous evasive maneuvers. As with navigational data, integrity of ADS-B messages is important, but to thwart the above attacks, authenticity needs to be ensured as well.

3.5 Tracking of Hidden BARR Aircrafts (2012)

Current ADS-B specifications are also without any protection against unauthorized eavesdropping or tracking – even if the aircraft movements are blocked from public dissemination upon "Business Aircraft Registration Request (BARR)" to the National Business Aircraft Association (NBAA). As Hoffmann et al. [29] demonstrated at DEFCON 20, ADS-B messages (or even speech contents) that are always sent out unprotected (i.e. without encryption or signature) enables eavesdropping and tracking of any aircraft equipped with ADS-B transponders. This could be interesting for espionage (e.g., tracking important CEO travels) or preparation of other (sabotage) attacks (e.g., tracking *Air Force One*). To stop such exploits, ADS-B needs to be enhanced with confidentiality protecting measures.

3.6 Attacking the Flight Management System of Aircraft (2013)

At the "Hack in the Box 2013" security conference in Amsterdam, security consultant and pilot Hugo Teso demonstrated that it is possible to control an aircraft with equipment available on Ebay [61, 68]. His attack exploited the unprotected ADS-B and ACARS (Aircraft Communications Addressing and Reporting System) communication interfaces, which allow

not only to eavesdrop messages, but also to manipulate them and send malicious code. Such effective attacks on the flight management system (FMS) of aircraft would be interesting to all types of attackers, especially by military and terrorists, to cause damage and to further their goals. To prevent this, at minimum strong access control needs to be implemented at all external communication interfaces of aircraft. For his demonstration, Teso used a laboratory environment with real aircraft soft- and hardware:

- Different flight management systems, both old and new ones, all including real aircraft code according to their manufacturers.
- A sophisticated simulation software normally used to train pilots. The software allows to simulate multiple aircraft, flying routes etc. under different conditions.
- A ground-based tool that is used to simulate the data-link between an aircraft and ground stations, again based on actual software used in real aircraft. It can be used to create, send and receive ADS-B and ACARS messages.

Although these conditions might not exactly map to an actual aircraft, they come as close as possible without causing a huge safety risk during the experiment. So while Teso's exploits cannot be used directly for an attack on actual aircraft, the vulnerabilities and potentially dangerous attack paths they identify do exist in current avionics. His attack is performed in several steps:

1. Use ADS-B messages to locate an aircraft.
2. Use ACARS messages and vulnerabilities in the FMS to upload malicious code ("SIMON") to the FMS. This is possible due to the unprotected nature of ACARS which allows real-time data transmission to the FMS.
3. Use SIMON to manipulate the FMS, e.g. change flight plans, weather forecasts, aircraft information etc. which at least disturbs the pilots, but can also lead to serious consequences and safety issues.
4. As long as the autopilot is active, SIMON can be used to actually remotely control the aircraft, possibly even to crash it.

Note that even while Teso demonstrated these features with an Android application ("PlaneSploit"), a smartphone would not be able to perform an attack on actual aircraft. Instead, an attacker would need a more powerful sender with an appropriate long-range antenna.

3.7 Attacking Mission-Critical Systems via In-Flight Entertainment Systems

A different avenue of attack from the above incidents is via in-flight entertainment (IFE) systems. Even though they are insecure legacy systems [63], they have become connected to mission-critical aircraft systems as in the example of the new Boeing 787 [67]. In some cases, there are even plans to allow passengers to hook up their own computer to the IFE [21]. Attackers in this scenario start with a curious passenger looking for security holes, but also include hackers and terrorists that install manipulated software before take-off or use established vulnerabilities to gain control of or crash an aircraft while in flight. To thwart these intrusions

in the face of increasing connections and communications between aircraft components, new security measures have to be put into place to ensure continued security [27]. They should include secure memory, secure communication, and secure run-time environments.

3.8 Vulnerabilities in COTS-Based Electronic Flight Bags

Electronic flight bags (EFB) are attractive due to their reduced weight and removal of paper from the cockpit. However, the use of COTS devices such as tablet PCs or laptops [30, 36] – including their external Wi-Fi connections and their inevitable, constantly vulnerable legacy operating systems – "at any point during the flight to access performance applications, electronic documentation of the airline's manuals, weather information, navigation, and airport charts" can lead to serious security problems especially if they are allowed to communicate with mission-critical flight control systems, for instance, via ARINC-429 or ARINC-717 interfaces (see Fig. 1). Potential security attacks, which can be carried out by hackers, malware, or terrorists, include for instance denial-of-service attacks on a EFB's functionality itself or, in case the EFB is connected to other on-board IT systems, malicious intrusions of the aircraft in general. In spite of these remarkable security threats, current EFB approval regulations such as FAA AC-120-76B [25] barely include precise IT security (testing) requirements. Instead they include vague and hardly verifiable requirements such as "demonstrate that adequate security measures are in place to prevent malicious introduction of unauthorized modifications". Hence, it is strongly required to develop reliable protection measures for secure EFB integration that are precisely specified, implemented, and approved.

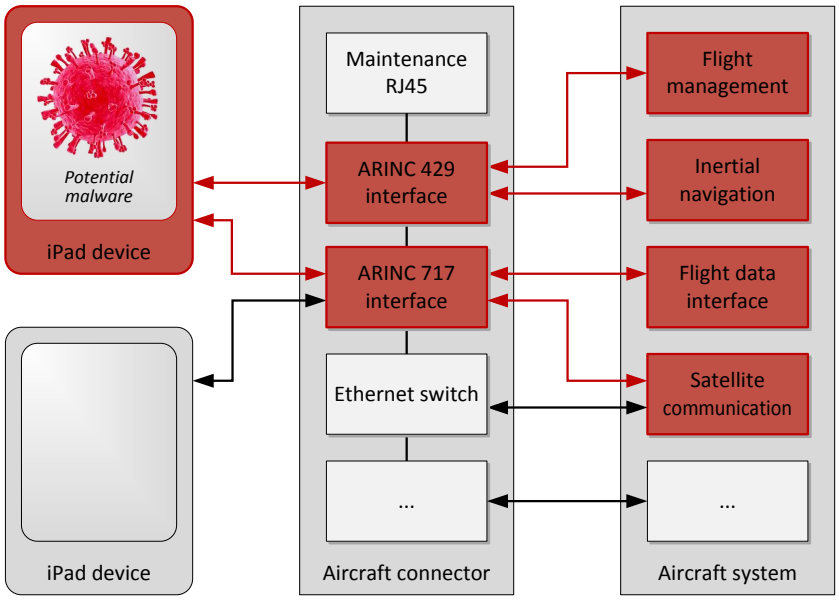

Figure 1: Integration of commercial FAA class-2 approved [25] COTS-EFBs (here: Apple iPad) into the flight control domain via ARINC 717 or 429 could enable malware to reach mission-critical aircraft domains misusing the COTS-EFB as *malware carrier*.

3.9 Malware Infection over Wireless External Interfaces (2012)

Another possibility is the automatic infection with malware from one aircraft to another using the external communication channels. This was demonstrated at the 2012 "Drone Games", where James Halliday introduced a virus spreading itself automatically from one drone to another [1]. Even if this kind of scenario seems unlikely today, it may be used by all kinds of attackers to dramatically increase the damage potential without much effort.

3.10 Attacking Aircraft via Compromised IT Infrastructures (2011)

Yet another security hole may exist in ground IT infrastructures such as airport, airline, or maintenance networks. Pascal Andrei, Director of Aircraft Security at Airbus, says: "It is not just a matter of ensuring that the channels of data transmission are secure, but also of ensuring that the information transmitted through those channels is correct. Aircraft have to rely on external data coming into the aircraft. If that information is not correct, it could jeopardize the safety of the flight" [32]. A related attack on Creech Air Force Base in Nevada has already been reported [56]. While it has not prevented pilots from controlling their drones, the virus has resisted various efforts at removing it from the system. But an attacker may have goals besides controlling the drones. They may want to gather intelligence, prepare denial-of-service attacks, or destroy the drone system. Hence, potential attackers may be found among intelligence services, terrorists, and hackers. With increasing external communication of aircraft, it does not suffice to secure the components of aircraft alone, but one has to make sure that everything connected to aircraft is secure as well.

4 Underlying Developments Affecting Information Security

Section 3 clearly showed that security vulnerabilities for modern computerized aircraft have left academic theory behind and have started to threaten real-world aircraft. One reason this could happen may be a still strong attitude that avionics is immune to serious security threats due to its isolated nature in the past. However, this is not the case anymore. This section takes a closer look at the underlying developments that increase the risk for IT security vulnerabilities. We analyze what has changed over the past decades and how these changes might have affected the information security of modern aircraft.

4.1 Increasing Digitalization and Automation

Modern aircraft have become more and more computerized with many analog systems being replaced by highly automated digital ones. In addition, these digital systems are increasingly digitally connected with each other using shared internal and external data communication links. On the one hand, growing digitalization and automation improves performance, functionality, efficiency, flexibility, reduces wiring, maintenance efforts and saves weight and costs. But on the other hand, it complicates manual supervision and increases risks for new security vulnerabilities and completely new attack paths (e.g., software attacks, remote attacks), hence making malicious manipulations (e.g., eavesdropping, information theft, information loss, and

digital sabotage) more likely and much easier to execute. Instead of costly, locally limited, analog modifications, it now could be sufficient for an successful attack by just changing the "right bit" within seconds – even from far remote without requiring physical access and without leaving any (physical) traces behind. Growing digitalization and automation further complicates also detection, fast and adequate containment, and prevention of information security attacks since, for instance, typical attack response and containment strategies such as blocking, resetting or deactivating an affected system would often not be an adequate response for most avionic systems.

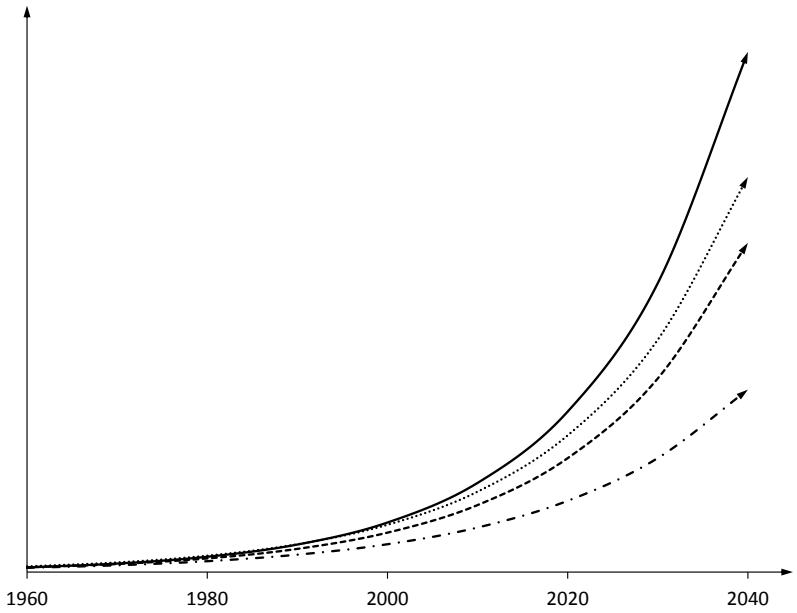

Figure 2: Exponential increase of code size (—), number of functions (···), number of digital interfaces (– –), and degree of connectivity (– ·) of modern avionic systems.

4.2 Increasing Complexity

Modern integrated modular avionics (IMA) architectures already consist of several dozens of digitally networked, highly interactive IT systems providing hundreds of thousands of software functions. As shown in Fig. 3, a today's Boeing 787 civil aircraft, for instance, processes already more than 8 million lines of code, while the recent F-35 II military aircraft uses even more than 22 million [41]. The code size of modern IMA therefore already reaches that of recent operating systems [47] and modern cars [17], both known to be constantly vulnerable to security issues [18].

Over the last 20 years the amount and complexity of embedded software in aircraft has grown exponentially and usually involves several dozens of different vendors. However, according to the internationally accepted security expert Schneier [54] "complexity is the worst enemy of security" since complex systems:

– have more code, and therefore more bugs that might affect security,

– are increasingly modular, and therefore have more interactions that increase the risk of security flaws,

– are harder to test, to analyze, and to evaluate adequately regarding security,

– are harder to design securely, to implement securely, to configure securely, and to be use securely, and

– are harder to understand for developers and users.

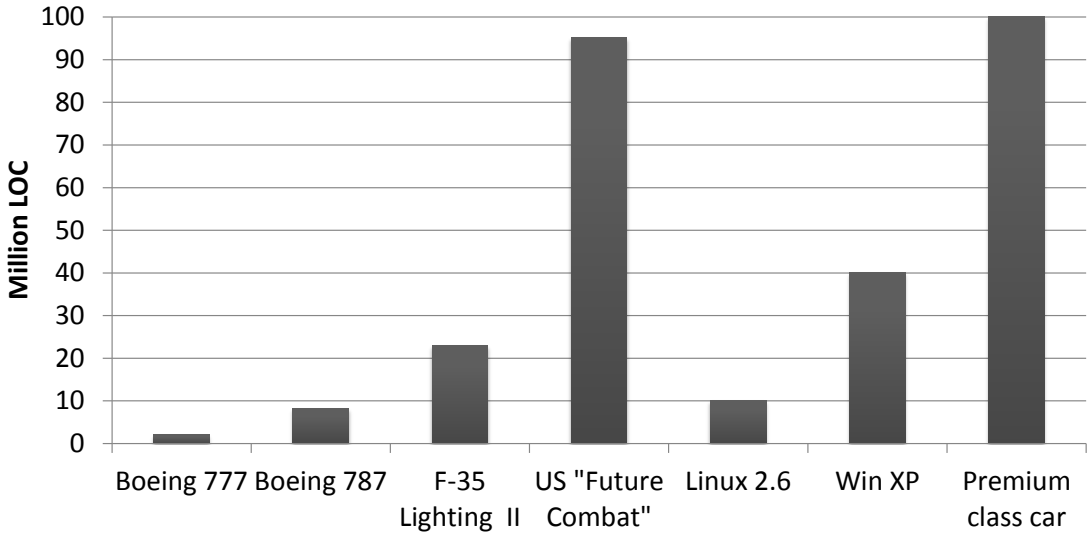

Figure 3: Increasing code size of modern avionic systems [41] in comparison with recent operating systems [47] and cars [17].

4.3 Increasing Resources Sharing and Inter-Domain Connections

Another development that comes with the IMA approach is the increased sharing of aircraft IT resources and the corresponding introduction of inter-domain communication connections (cf. Fig. 4). In particular, the ongoing parallel execution of software applications with different safety certifications (e.g., "level A" certified flight control function vs. only "level E" certified comfort function) executed on the same processor via virtualization technologies. Thus, a compromised subsystem might now easily affect or "infect" other connected subsystems. This development from dedicated, closed systems towards shared, connected systems extends existing or creates even new attack paths (cf. for instance attacks based on a weakness of the implemented memory management unit used for PCI Express (PCIe) devices as recently presented by Isfort et al. [33]) and hence multiplies the security risks already introduced through increasing complexity (cf. Section 4.2) and requires additional (complex) protection measures.

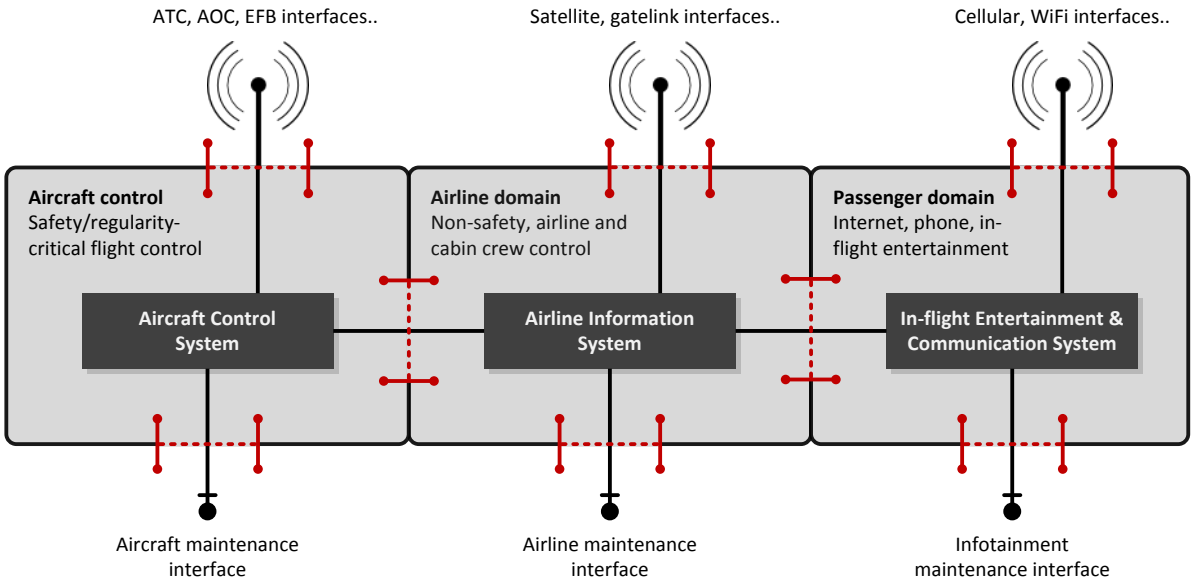

Figure 4: Open IMA architecture showing all potentially vulnerable inter-domain communication connections and external interfaces of a modern aircraft and hence superseding the former aircraft IT security paradigm based on closed systems and physical "air gap" isolation.

4.4 Increasing Number of Communication Interfaces to the Outside World

For a long time, the only aircraft communication interface to the outside world was analog radio either directly or (since 1990) indirectly with the help of satellite-based relay stations (SATCOM). These radio transmitters allowed only analog voice communication and the analog transmission of short telegraphs (airline teletype message). The first digitally processed aircraft data interface was introduced in the 1980s based on the "Aircraft Communications Addressing and Reporting System (ACARS)" [8]. The ongoing integration of ACARS with on-board IT systems made possible the interactive coupling of the internal flight management system (FMS) with external operators (e.g., airports, airlines) for automated air traffic control (ATC), administrative airline communication (AAC), maintenance data exchange, and interactive crew communication ("aircraft email") [9].

Today's aircrafts however are virtually non-stop online. They continuously communicate weather data, flight routes, infotainment data, passenger list, operating & maintenance data up to remote/cloud computing of vital flight parameters (cf. "Remote Processing: Cockpit Calculations" in [3]). Therefore today's aircrafts make use of (wireless) digital communication interfaces to other aircrafts (e.g., ADS-B), to global satellite navigation systems (e.g., GPS, GLOSNASS), to cellular networks (e.g., GPRS, LTE), to passenger devices (e.g., on-board Wi-Fi, on-board cellular radio), to backends of airports and airline (e.g., Gatelink [13]), and to their airborne weapon systems (for military aircrafts). Moreover, current aircrafts are more and more directly connected to the internet [43]. Even if they are not always directly internet-connected, they are usually equipped with various wireless network interfaces that are regularly connected to internet-enabled, even Windows-operated devices, for information ex-

change, diagnosis, or maintenance reasons among others. In fact, according to Tom Anderson, JetBlue's senior vice president of technical operations and aircraft programs, "the cockpit will, in essence, become a node within the company network" [40].

As depicted in Fig. 5, the enormous increase of digital communication interfaces leads to significantly growing numbers of potential attack points and attackers from very different domains, which cannot always be treated as fully trustworthy. Moreover, the typically deep integration of these digital interfaces with the aircraft's on-board IT systems – including the mostly fully automated processing of those systems – increases the potential impact of attacks notably. Possible attackers can mount their attacks from remote locations targeting multiple aircraft in parallel with little cost and little risk of becoming detected.

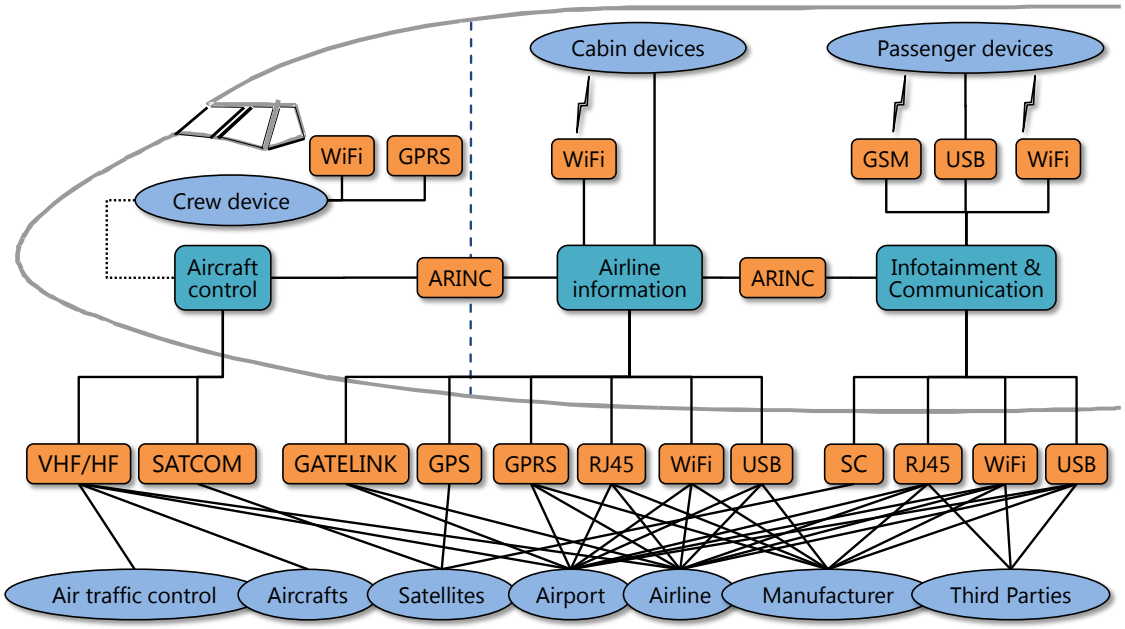

Figure 5: Increasing number of digital communication links of modern aircraft.

4.5 Increasing Deployment of Homogeneous COTS Hardware and Software

To manage advancing complexity, to increase flexibility, and to save costs, modern IMA architectures massively deploy standardized COTS hardware and software (e.g., standard not specially avionics developed micro-controllers, operating systems, Ethernet connections, or IP network stacks). In fact, today's unmanned aerial (combat) vehicles, for instance, are virtually completely assembled from COTS components [41]. This does not only increase the risk of counterfeits or Trojans (cf. Subsection 4.6), it especially increases "coverage" and power of potential attack paths and malware since a once (even costly) developed attack path can be later used (cost-efficiently) again for thousands of similar systems (cf. enormous number of existing malware for the widespread Microsoft Windows operating vs. considerably smaller number of malware for less widespread operating systems like Apple's Mac OS).

4.6 Increasing Complexity of Supply Chains for Avionic Components

Modern aircraft usually contain several million components from suppliers, sub-suppliers, and sub-sub-suppliers all over the world. It is virtually impossible to track such complex supply chains to detect potentially malicious counterfeit components or "dubious" cross connections. Thus, counterfeit parts or aircraft components without a completely monitored supply chain are a serious security issue: They could contain security vulnerabilities or malware (e.g., Backdoors, Trojan) - unintentionally or even intentionally [60]. For example, according to Senator Charles Schumer [55], in 2010 the U.S. Navy purchased 59,000 counterfeit microchips and other military equipment from abroad. Furthermore, he cites a Department of Defense statement that such counterfeits decrease the reliability of weapon systems year over year.

4.7 Information Security is a New Field of Research and Regulation

Until now aircraft, like cars, industry control systems, and medical devices, have been thought to be immune against most information security threats. This was due to strong organizationally enforced access control and the "air gap" that prevents most remote attacks by physical means. Hence, genuine protection against malicious encroachments was rarely considered and seldom implemented, while security research and regulation is still in its beginnings (cf. Section 2). However, taking the hitherto lucky nonexistence of serious security incidents as a safe sign for the future is dangerous. Alerting examples are the recent security attacks against real-world automobiles [18] and industrial automation systems [24]. Both affected industries have undergone developments similar to those described in this section. The incidents have impressively demonstrated the enormous attack power that is already available and that attackers are able to mount their attacks virtually from any place in the world. Finally, concerted security attacks are real and can be used as political, economic, and even military weapons. Modern aircraft will not remain immune against these threats.

5 Open Challenges for Aircraft Information Security

In Section 3 we have seen that the current level of security measures is not sufficient and in Section 4 we have described developments in avionics that continue to increase the attack surface of modern aircraft. In this section we turn our focus on the resulting challenges for the aircraft industry.

5.1 Secure Software Development

The exponentially increasing deployment of software in avionics (cf. Section 4.2) make secure software design, secure coding, software security testing (also known as *penetration testing*), and independent software security evaluations obligatory. This requires not only corresponding software security development tools and technologies (e.g., automated source-code security analyzes [19]), secure coding standards (e.g., CERT secure coding standards [16], or internationally accepted (software) security evaluation and certification standards (e.g., Common

Criteria [34]), but in particular a constant awareness and double-checking for potential security weaknesses during all stages of the software development cycle.

5.2 Secure Software Distribution

Currently, most software-based aircraft components do not implement any security mechanisms (such as secure software updates via digital signatures) that enforce data authenticity or access control for the software update interface itself. In fact, most software and data is installed at the aircraft based on – only limited trustworthy [38] – manual distribution schemes without any secure access control or any secure user authentication at the maintenance interfaces (cf. Fig. 4) based on strong cryptographic schemes, for instance. Hence, to thwart the security risks introduced by the increasing amount of easy-to-manipulate avionics software and data, the increasingly complex supply chains, and the increasing number of digital aircraft interfaces, a secure software distribution and update process that enforces update authorizations (e.g., who, when, what) is required, data authenticity (for original software only, against any data manipulations), data confidentiality (if required against espionage or for privacy reasons), and secure update logging (for legal issues or security forensics).

5.3 Off-Board Aircraft Communication Security

The application of communication security and privacy protection measures is still often considered as not needed. Asides from upper command communications and combat commands for heavy military apparatuses, enforcement of confidentiality and authenticity even of military (aircraft) communication in general is rather rare [35], while commercial aircraft communication is generally in clear using open, shared communication links virtually without any measures to reliably verify the authenticity of the communication, the authenticity of the communication endpoints, or to enforce access control to communication link (cf. ADS-B example in Section 3). However, to thwart the security vulnerabilities introduced by the increasing off-board communication interfaces and increasing number of communication entities (cf. Fig. 5), efficient communication security measures are required, which enforce off-board communication authenticity, availability, confidentiality, and privacy (if required).

5.4 On-Board Aircraft Communication Security

Except redundancy and plausibility checks, which can improve safety, but are only to a little extend capable to ensure also IT security [1], the authors are not aware about any dedicated protection measure to ensure on-board communication security beyond "hopefully" strict logical isolation between flight control domain and all other on-board domains via gateway firewalls or inherent access control mechanisms of partitioned run-time environments (e.g., microkernel-based virtualization) [27]. However, as shown in Fig. 4, the safety-critical, strictly controlled air control domain and the less safety-critical, hence less strictly controlled airline/passenger

[1] Measures for redundancy and plausibility checks are usually implemented to thwart against technical failures, whose typical malfunction can be often foreseen and contained. Hence, these measures are also usually known to an intelligent attacker and can often easily bypassed or even misused [66].

domain are already physically interconnected and even share (wireless) off-board communication interfaces. Similar connections and parallel data processing can be assumed for military aircraft, which have to process civil data (e.g., while flying in civil-controlled airspace) and classified data (e.g., commands and way-points for a classified combat mission) in parallel but strictly separated. Hence, to thwart the security vulnerabilities introduced by the increasing resources sharing, inter-domain connections, and inter-domain communications, efficient communication security measures are required that enforce on-board communication authenticity, availability, confidentiality, and privacy (if required) together with a strict access and flow control over all aircraft communication links. Again, it would be possible to transfer prototype implementations for secure vehicle on-board communications [65] to the avionics domain.

5.5 Strong Access Control on Digital Data, Functionality and Resources

The advanced sharing and deep integration of aircraft data and functions (cf. Section 4.3) makes critical data, functionality, computing or communication resources easy accessible to many entities, which could be other internal or external functions, components, device, backends, and persons. Even though commercial and military aircraft can, in contrast to most other IT systems, rely on organizationally enforced access restrictions that impede most direct unauthorized access attempts, they are still susceptible to indirect unauthorized access attempts over remote interfaces (e.g. wireless interfaces or interfaces to corresponding IT backends) or digital "intermediate transmitters" such as data storage media, maintenance devices, or electronic flight bags, which cannot a priori trusted since, for instance, they have previously been connected to the Internet. Already compromised components could "misuse" their inherent, often very extensive access rights to infect other components or to increase attack damage. However, current aircraft have usually very limited access control capabilities on digital data, functionality, and resources to enforce fine-grained access and usage restrictions. In fact, they apply only a few globally valid access roles, have only insufficient entity authentication mechanisms (e.g., by physical presence, global passwords), have seldom security firewalls, or security-related intrusion detection systems. This makes it difficult to dependably verify authorizations and to implement effective security policies in order to prevent unauthorized access and unauthorized exhaustion of resources (affecting the availability). Even if powerful quality of service (QoS) measures are implemented, they are often ineffective against systematic malicious encroachments as they are usually designed to prevent only technical failures, whose typical malfunction can be often foreseen and contained. In order to manage and enforce many different access and usage authorizations for many different entities, so called multiple independent levels of security (MILS) architectures [15] together with strict access control mechanisms on data, functionality, and resources based on efficient security policy interpreters and cryptography-based entity authentication might help to ensure strict isolation of entities and system resources with different levels of security.

5.6 Continuous Education of Maintenance Personnel

A challenge which is not directly linked to the IT-systems on board is the continuous education of maintenance personnel. With respect to the increasing use of software in aircraft it becomes necessary that the personnel has the relevant data security knowledge and awareness. To

guarantee a certain security level, it is not sufficient to implement security measures in soft- and hardware, but also essential to train the maintenance personnel with these, educate them continuously and regularly evaluate them accordingly.

5.7 Aircraft Information Security Regulations

Even though aircraft hardware and software components undergo a strong, mandatory safety evaluation [22], they are usually not mandatorily, systematically, and transparently evaluated regarding their IT security properties to thwart also potentially malicious IT encroachments. In fact, the U.S. Federal Aviation Administration (FAA) "currently does not have specific policy and guidance for aircraft avionics system security", but special conditions "may be issued when the current FAA regulations do not contain adequate or appropriate safety standards for protection and security of aircraft systems" [58]. These kinds of special conditions "contain additional safety standards" for "specific airplane models" and "address new or novel design features" [58]. For example, the FAA issued special conditions for the Boeing 787-8 airplane [27]. They contain additional regulations and state that "applicable airworthiness regulations do not contain adequate or appropriate safety standards for protection and security of airplane systems and data networks". So while aircraft hardware and software are thoroughly validated against random technical failures, they are not mandatorily validated against systematic malicious encroachments.

Of course there are many regulations related to aviation security, which however cover for instance access control to aviation infrastructures, baggage security screening, passenger handling, or airline/airport cooperate IT infrastructures, but which are usually not related to information security of aircraft and aircraft communications [4]. In fact, most standardization documents that define the regulations for (commercial) aircraft components such as DO-178B [22] do not consider any aircraft information security threats. The few information security related aircraft regularity documents such as ARINC 666 [11] for electronic software distribution, ARINC 823 [14] for aircraft-to-ground data link security [2], or ARNIC 653 [10] for spatial and temporal computing resource partitioning for integrated modular avionics (IMA) architectures, for instance, are still draft or non-mandatory guideline documents, respectively, with only little real-world application [2]. Solely, the ARINC report 811 [12] provides some more comprehensive but again non-mandatory guidelines "to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts" on a high-level manner. Hence, even though there are several aircraft information security regulations under development [6], today there exist no mandatory security regulations, branch-specific protection profiles, systematic integrated security engineering processes, or any mandatory security evaluations such as introduced for instance by the world-wide used Common Criteria [34] methodology. Developing and establishing mandatory, transparent security regulations for avionics will be one of the most important measures required to realize effective and sustainable data security and privacy protection.

[2] In contrast to for instance ADS-B messages [26], ARINC 823 "Aircraft Communications Addressing and Reporting System" (ACARS) messages are usually not used for air traffic control or automated safety systems such traffic alert or collision avoidance, but mostly for airline-to-aircraft communication for automated flight phase reporting, aircraft's operational performance reporting, and interactive crew communication.

5.8 Digital Forensics and International-Incident-Registration

The somewhat poor awareness of the data security problems discussed may also have its cause in the lack of a systematic central registration, analysis, and tracing of successful attacks and manipulations that have taken place. If incidents are discovered, then at first they are often treated as "functional errors" without considering a potential security attack. With respect to the enormous safety risks of security vulnerabilities in aircraft, the authors see the urgent necessity to (i) integrate an "IT forensics" process into the avionics-error-analysis to detect and analyze security incidents and (ii) a compulsory central registration of the incidents. The latter one can be controlled by an international authority (e.g., FAA or EASA) which collects critical security vulnerabilities, informs all affected parties (e.g., manufacturer, airlines, public authorities), forces a fast removal and issues emergency directives, if necessary. Fixed security vulnerabilities and the corresponding countermeasures should further become publicly available to a certain extend (e.g., similar to Microsoft Security Bulletins) to enable passengers and public research a meaningful risk evaluation.

5.9 Specific Constraints and Benefits for Security Implementations in Avionics

In addition to the general challenges for ensuring proper information security at the avionics domain, an avionic IT environment involves also some domain specific technical and organizational restrictions and constraints, which can considerably complicate or even impede the implementation of certain IT security measures. Some of them that have to be carefully considered are briefly described in the following.

Physically challenging environment that exposes airborne security hardware to strong mechanical stress, considerable radiation, big and frequent changes in temperature, pressure, and climate requires mechanically robust security solutions and comprehensive mechanical testing. *Multiplicity of international manufacturers, component suppliers, operators, and regulators* makes any changes of avionic components and related development and deployment processes slow, small, and costly. *Multiplicity of international mandatory international safety, legal, and interoperability regulations* makes any changes to existing regulations and related development and deployment processes slow, small, and costly. *Long product life-cycles with many different owners* require security solutions that provide adequate security over decades and can updated, upgraded, and comprehensibly reconfigured accordingly. *Limited off-board communication resources* require specially adapted security solutions that are offline-capable or can at least work properly also with only infrequent, sporadic, and low-bandwidth off-board communication capabilities. *Additional costs for aircrafts and infrastructures* created by security measures are without any apparent functionality that one can sell to his company and customers. *Security measures might come in conflict with strong safety measures or safety requirements* (e.g., security processing overhead vs. real-time requirements) as security solution are not always transparent to safety (e.g., most privacy ensuring measures) or even in synergy with safety (e.g., data authenticity enforcement). *Large, increasing system and infrastructure complexity, distribution, and diversification* makes security solutions complex, costly, and particularly vulnerable (cf. Section 4). *Dedicated avionic security departments and corresponding security experts are still seldom* so that there is currently still only little awareness and R&D regarding new area of aircraft information security.

However, in comparison with other typical information security application areas such as networks, servers, vehicles, mobile devices, or industrial automation, an avionic IT environment provides also some domain specific advantages, which can ease the implementation of information security measures considerably. Some of them are briefly described in the following.

Strong safety regulations, evaluations, and certifications already involve deep analysis, validations, and testing that could be reused and extended to all information security requirements that might affect safety. *Usually strictly checked personnel* makes attacks by unauthorized persons more difficult and insider attacks at least somewhat more unlikely. *Usually extensively trained personnel* could be easily trained also for the proper application of complex security solutions. *Regular foreseeable and unforeseeable inspections* might at least contain the impacts of some security attacks and increase the chances for their detection. *Acceptable cost, size, weight, and power restrictions* provides, in contrast to very strict embedded devices such as smartphones or smartcards, adequate performance for most security solutions. *Changes and updates of aircraft's hardware and software* are possible, even if limited, to update or upgrade already deployed security solutions to a certain extend if needed.

5.10 Lessons Learned By the Automotive Industry

The problems presented in this article are not restricted to the avionics domain and many other industries are facing similar challenges like digitalization and increasing connectivity which imply new security risks. One example is the automotive industry, where security has been a key topic over the last 20 years. The developments in both industries are quite similar, although not always synchronous. Nevertheless, the awareness for security threats seems to be much higher in the automotive domain, which may have the following reasons:

- More public security research is done on cars, as they are much cheaper to get. Researchers can afford to analyze real-word cars instead of simulators or single components. If successful, the results are then published and spread throughout the media (e.g., [18]).
- Cars are produced in much higher quantities, so there is much more knowledge about technical details available and a lot more experts who understand the technology.
- Many people own a car whereas an aircraft is typically owned by an airline and quite abstract to the passenger.

The awareness of increasing problems has led to a rethinking in the automotive industry. Following are a few examples of important steps that have been taken lately:

- Since the 1980s there has been tremendous progress in the implemented security technology. From the first electronic car keys with static access code to today's cryptographic challenge-response protocols has been a long process that paid of in the end. Similar progress has been made in every other area, e.g. protection against mileage manipulation, virtualization of different domains, immobilizer, specification of hardware security modules just to name a few.
- Upon introduction of new technologies, security is considered throughout the complete development life-cycle. This leads the way from learning through incidents to a holistic security concept. One example is the communication between cars and infrastructure

(car-to-car communication, also vehicle-to-X). This communication is secured by cryptographic protocols, security software, a hardware security module and a dedicated public key infrastructure [49].

- Industry consortia like the AUTOSAR group or the Car-to-Car Communications Consortium have dedicated security working groups driving security topics and standardization.
- There are more and more research projects, funded publicly or privately, that explicitly deal with security. The results of the projects raise awareness, point to new problems, but also develop new technologies to secure future vehicles.

In contrast, much of the security research in the avionics industry is not publicly available [3]. Even though a lot of sophisticated work may be in classified research, the incidents presented in Section 3 show that there is room for improvements.

6 Conclusion

The international aviation industry is of great importance for the economy and security of our society. Hence, the society heavily relies on the safety and security of their "flying IT-systems". Even if the threat potential for the information security of aircraft seems to be comparably low today, this must not be misinterpreted as an insurance for the future. First real-world incidents presented in this article have shown that information security for modern aircraft is not only academic theory, but already a real threat. Nonetheless modern aircraft become increasingly computerized, standardized, and will continuously expand their digital on-board and off-board communications. All the while more and more business and safety critical systems process or even automatically act on fully computer-generated information which inherently increases also the security risks.

Considering the enormous importance of air transportation, avionics must not repeat the failures from other IT domains like the desktop world, the automotive industry, or industrial control systems where security requirements were ignored until increasing connectivity capabilities ruthlessly revealed various security vulnerabilities. Even though several typical avionics constraints make corresponding security implementations not necessarily easier, the industry needs - similar to or even combined with existing aircraft IT safety measures - adequate information security measures. These include systematic security engineering, mandatory inter-operable security standards and regulations, comprehensive security evaluations and certifications for all aircraft IT systems involved. As the avionics domain consists of a multiplicity of international actors, this overall goal is only feasible by a common approach by all responsible parties from industry, research, and administration to effectively avert critical dangers from people, economy, and society. Fortunately, the wheel does not have to reinvented: There already exist various effective and efficient embedded security solutions, for instance from modern automobiles, that can be transferred into airborne systems. Thus, security can and has to become ubiquitous for airborne IT systems.

[3] For instance, the FAA-2007-29305 amendment No. 91-314 states: "This assessment contains sensitive security information [...] its content is otherwise protected from public disclosure." This is in contrast to the *open design* principle that creates and ensures trust in a security solution by requiring that a system design needs to be secure independent of whether its implementation is known or not [45].

References

[1] E. Ackerman. AR Drone That Infects Other Drones With Virus Wins DroneGames. IEEE Spectrum robotic's blog, December 2012. Available online at http://spectrum.ieee.org/automaton/robotics/diy/ar-drone-that-infects-other-drones-with-virus-wins-dronegames.

[2] C. Adams. Securing ACARS: Data Link in the Post-9/11 Environment. *Avionics Magazine*, June 2006.

[3] C. Adams. Commercial Avionics Outlook. *Avionics Magazine*, January 2013.

[4] Aeronautical Radio, Incorporated (ARINC). Aviation security. Website, 2012. Available online at http://www.arinc.com/products/security/aviation_security.html.

[5] Airlines Electronic Engineering Committee (AEEC). Engineering Standards for Aircraft Systems. Website. Available online at http://www.aviation-ia.com/aeec/.

[6] Airlines Electronic Engineering Committee (AEEC). Data Link Security (DSEC) Subcommittee. Website, 2012. Available online at http://www.aviation-ia.com/aeec/projects/dsec/index.html.

[7] B. Alomair, K. Sampigethaya, A. Clark, and R. Poovendran. Towards trustworthy cryptographic protection of airplane information assets. In *AIAA Infotech@Aerospace Conference*, April 2009.

[8] ARINC 618-6. *Air/Ground Character-Oriented Protocol Specification*, 2006.

[9] ARINC 619-3. *ACARS Protocols for Avionic End Systems*, 2009.

[10] ARINC 653. *P1–P4: Avionics Application Software Interface*, 2006–2012.

[11] ARINC 666. *Electronic Distribution of Software*, 2002.

[12] ARINC 811. *Commercial Aircraft Information Security Concepts of Operation and Process Framework*, December 2005.

[13] ARINC 822. *Aircraft/Ground IP Communication*, June 2008.

[14] ARINC 823. *P1–P2: DataLink Security*, 2007–2008.

[15] J. Careless. MILS Operating Systems: Safety and Security. Avionics Today, March 2006. Available online at http://www.aviationtoday.com/av/military/MILS-Operating-Systems-Safety-and-Security_799.html.

[16] CERT. Secure Coding. Website, 2012. Available online at http://www.cert.org/secure-coding/.

[17] R. N. Charette. This car runs on code. *IEEE Spectrum*, 46(3):3, 2009.

[18] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Security*, 2011.

[19] B. Chess and G. McGraw. Static analysis for security. *Security & Privacy, IEEE*, 2(6):76–79, 2004.

[20] A. Costin and A. Francillon. Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Technical Report, EURECOM, Sophia-Antipolis, France, July 2012. Presented at Black Hat 2012, Las Vegas, USA.

[21] S. Deveau. WestJet develops new in-flight entertainment system. Financial Post, May 2012. Available online at `http://business.financialpost.com/2012/05/16/westjet-develops-new-in-flight-entertainment-system/`.

[22] DO-178B. *Software Considerations in Airborne Systems and Equipment Certification.* RTCA Inc., December 1991.

[23] F. A. A. (FAA). Automatic dependent surveillance-broadcast (ADS-B). Website, 2012. Available online at `http://www.faa.gov/regulations_policies/reauthorization/media/PLAW-112publ95[1].pdf`.

[24] N. Falliere, L. Murchu, and E. Chien. W32.Stuxnet Dossier. *White paper, Symantec Corp., Security Response*, 2011.

[25] Federal Aviation Administration (FAA). AC 120-76B - Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bag. Website, 2012. Available online at `http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%20120-76B.pdf`.

[26] Federal Aviation Administration (FAA). Automatic Dependent Surveillance-Broadcast (ADS-B). Website, 2012. Available online at `http://www.faa.gov/nextgen/portfolio/trans_support_progs/adsb/`.

[27] Federal Register. Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Protection of Airplane Systems and Data Networks From Unauthorized External Access. Website, 2007. Available online at `https://federalregister.gov/a/07-1838`.

[28] S. Gorman, Y. J. Dreazen, and A. Cole. Insurgents Hack U.S. Drones. Wall Street Journal, December 2009. Available online at `http://online.wsj.com/article/SB126102247889095011.html`.

[29] D. Hoffman and S. Rezchikov. Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. In *DEFCON 20*, 2012.

[30] C. Howard. Dell and Airbus deliver Electronic Flight Bag services to airlines worldwide. *Avionics Intelligence*, May 2013. Available online at `http://www.avionics-intelligence.com/articles/2013/05/Dell-Airbus-EFB.html`.

[31] Humphreys et al. Radionavigation Laboratory Spotlight. Website, 2012. Available online at `http://radionavlab.ae.utexas.edu/spotlight`.

[32] International Air Transport Assocation. Cyber Security - Access Denied. *Airlines International*, December 2011. Available online at `http://www.iata.org/publications/airlines-international/december-2011/Pages/cyber-security.aspx`.

[33] O. Isfort, K. Müller, D. Münch, and M. Paulitsch. Decreasing System Availability on an Avionic Multicore Processor Using Directly Assigned PCI Express Devices. In *European Workshop on System Security (EUROSEC2013)*, 2013.

[34] ISO/IEC 15408. *Information Technology – Security Techniques – Evaluation Criteria for IT Security*, 2009.

[35] J. Keller. Modernizing military cryptographic processors. *Military & Aerospace Electronics*, November 2011.

[36] J. Keller. Fokker Services certifies iPad electronic flight bag (EFB) for Bombardier Dash 8 twin-engine passenger turboprop. *Avionics Intelligence*, March 2013. Available online at `http://www.avionics-intelligence.com/articles/2013/03/Fokker-Bombardier-EFB.html`.

[37] M. S. B. Mahmoud, N., Larrieu, A. Pirovano, and A. Varet. An adaptive security architecture for future aircraft communications. In *Digital Avionics Systems Conference*, 2010.

[38] Mail Foreign Service. Fake Swedish air pilot flies passenger jets for 13 years without a license. Mail Online, May 2010. Available online at `http://www.dailymail.co.uk/news/article-1279083/Fake-Swedish-pilot-Thomas-Salme-flies-Air-One-jets-13-years.html`.

[39] Mandiant Corp. Exposing One of China's Cyber Espionage Units. Website, 2013. Available online at `http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf`.

[40] V. P. McConnell. Wireless Gatelink: Coming of Age. Avionics Today, July 2005. Available online at `http://www.aviationtoday.com/av/issue/feature/Wireless-Gatelink-Coming-of-Age_996.html`.

[41] E. McKenna. Embedded Overall. *Avionics Magazine*, November 2008.

[42] R. Merritt. GPS security a concern for university expert. Electronic Engineering Times Europe, July 2012. Available online at `http://www.electronics-eetimes.com/en/gps-security-a-concern-for-unniversity-expert.html?cmp_id=7&news_id=222913353&vID=209`.

[43] K. Moskvitch. Connected sky: Surfing the web above the clouds. BBC News, May 2012. Available online at `http://www.bbc.co.uk/news/technology-18021468`.

[44] P. G. Neumann. Computer security in aviation: Vulnerabilities, threats, and risks. Website, January 1997. Available online at `http://www.csl.sri.com/users/neumann/air.html`.

[45] NIST. Special Publication 800-123: Guide to General Server Security. Website, 2008. Available online at `http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf`.

[46] B. Nuseibeh, C. B. Haley, and C. Foster. Securing the Skies: In Requirements We Trust. *Computer*, 42(9):64–72, 2009.

[47] L. O'Brien. How Many Lines of Code in Windows? Knowing .NET, December 2005. Available online at `http://www.knowing.net/index.php/2005/12/06/how-many-lines-of-code-in-windows/`.

[48] M. L. Olive, R. T. Oishi, and S. Arentz. Commercial aircraft information security - an overview of arinc report 811. In *25th Digital Avionics Systems Conference*, 2006.

[49] P. Papadimitratos and J. Hubaux. Secure vehicular communication systems. *Encyclopedia of Cryptography and Security*, pages 1140–1143, 2011.

[50] PlaneCrashInfo.com. Causes of fatal accidents by sabotage: Statistics 1950–2009. Website, 2012. Available online at `http://www.planecrashinfo.com/cause.htm`.

[51] R. Robinson, M. Li, K. Sampigethaya, R. Poovendran, S. Lintelman, D. von Oheimb, J.-U.Buer, and J. Cuellar. Electronic distribution of airplane software and the impact of information security on airplane safety. In *International Conference on Computer Safety, Reliability and Security*, 2007.

[52] K. Sampigethaya, R. Poovendran, and L. Bushnell. Secure Operation, Control and Maintenance of Future eEnabled Airplanes. *IEEE Special issue on Aviation Information Systems*, 2008.

[53] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty. Future e-enabled aircraft communications and security: The next 20 years and beyond. In *Proceedings of the IEEE*, 2011.

[54] B. Schneier. Software complexity and security. Crypto-Gram Newsletter, March 2000. Available online at `http://www.schneier.com/crypto-gram-0003.html`.

[55] C. E. Schumer. Counterfeiting of military technology. Crypto-Gram Newsletter, July 2011. Available online at `http://schumer.senate.gov/record.cfm?id=333606`.

[56] N. Shachtman. Exclusive: Computer Virus Hits U.S. Drone Fleet. Wired Danger Room, July 2011. Available online at `http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/`.

[57] D. Shepard, J. A. Bhatti, and T. E. Humphreys. Drone hack. GPS World Website, August 2012. Available online at `http://www.gpsworld.com/drone-hack/`.

[58] P. Skaves. Cyber security issues related to aircraft systems. In *Digital Avionics Systems Conference*, 2011.

[59] L. Tay. Hacker: Avionics vulnerable to next-gen attacks. iTnews - For Australian Business, April 2011. Available online at `http://www.itnews.com.au/News/252981,hacker-avionics-vulnerable-to-next-gen-attacks.aspx`.

[60] M. Tehranipoor and F. Koushanfar. A survey of hardware trojan taxonomy and detection. *Design & Test of Computers, IEEE*, 27(1):10–25, 2010.

[61] H. Teso. Aircraft Hacking - Practical Aero Series. Hack in the Box Conference, April 2013.

[62] N. Thanthry, M. S. Ali, and R. Pendse. Security, Internet Connectivity and Aircraft Data Networks. In *Security Technology*, pages 251 – 255, 2005.

[63] H. Thompson. How to crash an in-flight entertainment system. Report, 2009. Available online at http://blogs.csoonline.com/how_to_crash_an_in_flight_entertainment_system.

[64] US Department of Defense. Military and Security Developments Involving the Peoples Republic of China 2013. Report, 2013. Available online at http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

[65] B. Weyl, M. Wolf, F. Zweers, T. Gendrullis, M. S. Idrees, Y. Roudier, H. Schweppe, H. Platzdasch, R. E. Khayari, O. Henniger, et al. Secure on-board architecture specification. *EVITA Deliverable D3.2*, 2010.

[66] M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In *Workshop on Embedded IT-Security in Cars*, 2004.

[67] K. Zetter. Faa Responds to Boeing Security Story. Wired Threat Level, September 2008. Available online at http://www.wired.com/threatlevel/2008/01/faa-responds-to/.

[68] Z. Zorz and B. Kucan. Hijacking airplanes with an Android phone. Help Net Security, April 2013. Available online at https://www.net-security.org/secworld.php?id=14733.