kaspersky

# Faults in digital avionics systems threaten flight safety

Vasily Buzoverya

17.07.2025 Version 1.0

# Contents

# Introduction

Like many other industries, civil aviation is undergoing a digital transformation. This transformation involves enhancing the information connectivity between aircraft and ground-based digital infrastructure, which introduces new cybersecurity risks. These issues are specifically mentioned in the International Civil Aviation Organization (ICAO) Aviation Security Manual[1].

In the context of information security, onboard systems are of particular interest because in earlier generations of aircraft, they were isolated from ground systems and featured limited and controlled interconnectivity. Modern onboard systems are digital avionics (derived from the words "aviation" and "electronics") systems that are used to perform various tasks during flight, including engine control, navigation, communication, and interaction with ground services. In this article, the term "avionics systems" refers specifically to digital onboard systems or digital subsystems of onboard systems. Avionics systems are integrated into the aircraft's avionics suite, also known as the Integrated Avionics System.

As the interconnectivity and openness of onboard systems increase, so does the need to protect them from cyberattacks – intentional unauthorized interference with systems via digital interfaces (note that electromagnetic or other analog effects are not considered cyberattacks). Cyberattacks can lead to failures in avionics systems and cause aviation occurrences, including aviation incidents and accidents[2].

To date, there have been no publicly available reports of confirmed cyberattacks targeting avionics systems or of vulnerabilities in such systems. However, there have been incidents and accidents caused by faults in the hardware and software of such systems. Analysis of the causes and consequences of these incidents can, to some extent, provide insight into the nature of potential cyberattacks and support assumptions about possible vulnerabilities in digital avionics systems, as well as the consequences of their deliberate exploitation by malicious actors familiar with functions, technical aspects, and weaknesses of avionics systems.

---

[1] Important ICAO documents worth reviewing:

- Resolutions adopted at the 40th Session of the ICAO Assembly, 2019;
- Cybersecurity Culture in Civil Aviation, 2022;
- Cybersecurity Action Plan, 2022.

[2] Aircraft accidents refer to events that result in serious injury or death, or in serious damage to, loss of, or complete destruction of an aircraft. Aircraft incidents include all other events that had or could have had a negative impact on flight safety.
Source: Annex 13 to the Convention on International Civil Aviation: Aircraft Accident and Incident Investigation, ICAO, Edition 11, July 2016.

In this article, we consider only at aviation occurrences involving civil commercial aircraft referred to as transport category airplanes in the U.S. and large airplanes in the European Union. These include, for example, the Boeing 787, Boeing 737, Airbus A350, Airbus A320, SSJ-100 (RRJ-95), MC-21, and Comac C919. However, the examples provided may also be useful in analyzing cybersecurity risks for other types of aircraft, including light aircraft, helicopters, and unmanned aerial systems.

This article does not cover issues related to Positioning, Navigation, and Timing (PNT) functions, including those involving satellite navigation technologies (GPS, GLONASS) and protocols used for automatic data exchange with ground services (ADS-B and ACARS). These issues involve the interaction between onboard, ground-based and satellite systems, and require separate consideration; therefore, they are excluded from the scope of this article.

# Modern digital avionics suites

From an information security perspective, key features of the latest (fifth) generation[3] avionics suites include high levels of connectivity and openness. Digital avionics systems are connected to the core onboard computing network using the Internet Protocol (IP), with certain systems linked to the ground-based information infrastructure of airlines and airports[4]. Figure 1 illustrates several digital systems of the Boeing 787 Dreamliner, the first aircraft to feature a fifth-generation avionics suite, which completed its first commercial flight in October 2011.

[3] Fifth-generation avionics suites are installed on such aircraft as the Boeing 737 NG/MAX, Airbus A320neo, RRJ-95, and MC-21.
[4] The term "connected aircraft" is sometimes used to describe aircraft with digital avionics systems.

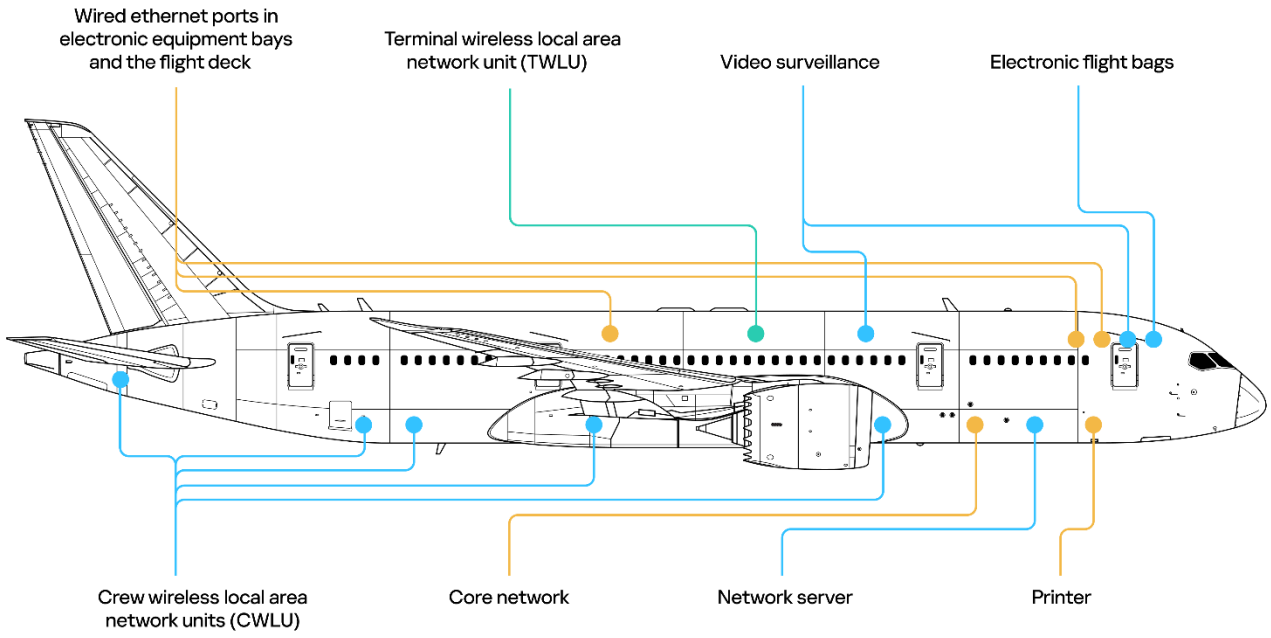


**Figure 1. Digital onboard systems of the Boeing 787 Dreamliner**

The fifth-generation avionics suites implement the concept of Integrated Modular Avionics and the aircraft systems are controlled by software. For example, the Airbus A350 XWB, equipped with a fifth-generation avionics suite, contains 1,200 software components with individual part numbers assigned. In addition to bespoke (purpose-built) components, these modern avionics suites use commercial off-the-shelf (COTS) hardware and software. These are another two key features of modern avionics from cybersecurity perspective.

## Essential and supporting systems of the avionics suite

The systems of an aircraft's avionics suite can be categorized as essential (primary) and optional (supporting). Primary systems are critical for performing the flight and for ensuring safety. These include, for example, the electrical power system, flight control system, and fire protection system. Supporting systems are not used for aircraft control or safety assurance, yet efficient commercial operation is virtually impossible without them. Such systems include, for example, the in-flight entertainment system and the pilots' portable electronic flight bags (EFB).

Aviation authorities worldwide require[5] that supporting systems must not have any adverse impact on the primary systems. Portable devices are not part of the approved aircraft design for which the type certificate is issued.

### Note 1. Electronic Flight Bags for Pilots and Technicians

Electronic flight bag (EFB) provides pilots with the information required to perform a flight, including navigation data (charts and procedures, including approach charts), weather briefings, and operations manuals. When using EFB, having the equivalent paper documentation on board is not required.

EFB runs applications for calculating flight parameters, including takeoff and landing performance data, takeoff weight and aircraft center of gravity, as well as fuel reserves.

There are two types of EFBs: installed devices, which are integrated into the avionics suite, and portable devices. The former are developed in accordance with aviation equipment standards and are part of the approved aircraft design, while the latter are based on COTS products, such as the Apple iPad. In Figure 2, a pilot is shown using an iPad-based EFB running the Flysmart+ application[6].

There are portable devices for the cabin crew (Cabin Electronic Flight Bags of Electronic Cabin Bags) and maintenance technicians (Electronic Tech Logs or Electronic Log Books). These differ from pilot EFBs only in terms of installed applications. Applications for the portable devices can be installed via app stores (such as the Apple Store).

[5] Aviation regulations, Part 21 (aircraft certification):

- Federal Aviation Regulations "Certification of Aircraft, Aircraft Engines, Propellers, and Related Products; Certification of Designers and Manufacturers of Aircraft Products. Part 21." Ministry of Transport of the Russian Federation, 2014;
- The Code of Federal Regulations: Title 14 – Aeronautics and Space, Chapter I – Federal Aviation Administration, Department of Transportation, Subchapter C – Aircraft, Part 21 – Airworthiness Standards: Transport Category Airplanes, U.S. Government Publishing Office, 2022;
- Easy Access Rules for Airworthiness and Environmental Certification (Regulation (EU) No 748/2012), Part 21 (IR + AMC & GM), European Union Aviation Safety Agency (EASA), EASA eRules, May 2023.

[6] Technical information on the Flysmart+ application, developed by Navblue Inc., a subsidiary of Airbus (Flysmart+ in the Apple Store).

Although portable EFBs are officially classified as low-risk devices, errors in their design, implementation, and operation can lead to severe consequences. One should also take into consideration that COTS portable could be susceptible to cyberattacks. For instance, several zero-day vulnerabilities (CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990) were discovered in iOS in 2023, which were exploited in a targeted cyberattack on devices running that operating system. Kaspersky experts reported[7] on this issue. That same year, a vulnerability was identified in the Flysmart+ application and disclosed to the developer through a responsible disclosure process.

**Figure 2. Pilot electronic flight bag based on an Apple iPad**

[7] More articles by Kaspersky experts on the Operation Triangulation campaign.

# Examples of incidents involving failures of digital avionics systems

Cybersecurity researchers began to draw public attention to failures of onboard electronic (digital) systems as early as the late 20th century. Even then, there were assumptions that cyberattacks could cause similar results. For many years, the ACM SIGSOFT Software Engineering Notes journal has published articles in the Risks to the Public in Computers and Related Systems column, covering incidents and accidents involving computers and computerized systems, including avionics systems. In 1997, Peter Neumann, the long-standing editor of the column, presented a keynote address on emerging challenges in aviation cybersecurity at an international aviation safety conference organized by a U.S. government safety and security commission. He noted that many aviation occurrences involving avionics failures could have been caused by cyberattacks as well ("many of the past accidents could alternatively have been caused intentionally – and in some cases could be recreated maliciously today") and urged greater attention to the protection of ground and onboard systems, particularly from large-scale coordinated attacks.

In this article, we present six examples of failures in both primary and supporting avionics systems. The first two involve software errors in portable EFBs. The next three describe hardware and software failures in primary avionics systems of aircraft equipped with modern avionics suites. These cases are notable in that, as a temporary mitigation measure, the systems had to be periodically reset and rebooted by turning the aircraft power off and back on. The final example involves a fault in onboard flight data recorders, which resulted in incorrect recording of flight data.

The chronology of the considered and related events is presented in Figure 3.

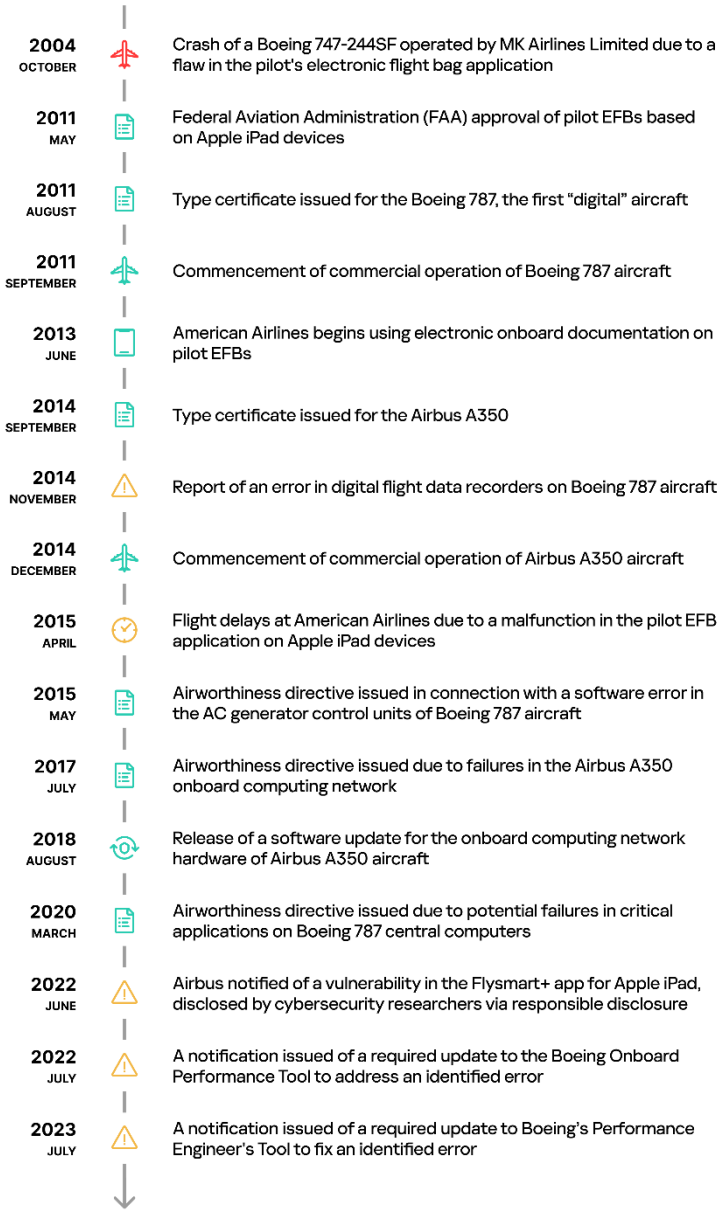


**Figure 3. Chronology of documented events**

# Flight delays at American Airlines

On the evening of April 28 and the morning of April 29, 2015, dozens of American Airlines flights were delayed at several U.S. airports due to issues with an application on pilots' EFBs running on Apple iPad devices. Passengers reported the delays in social media from Dallas, New York, Los Angeles, and

Chicago airports. In some cases, delays exceeded three hours. All affected flights were operated by Boeing 737 aircraft.

A spokesperson for the airline stated that a total of 74 flights were delayed, 24 on April 28 and 50 on April 29. At the time, American Airlines was the world's largest airline, operating an average of 6,700 flights per day. According to the company's 2014 financial report, its fleet included 928 aircraft, 246 of which (27%) were Boeing 737s. Thus, the issue affected approximately 8% of the airline's fleet.

The malfunction of the EFB application prevented flight crews from accessing the navigation charts and procedures required for flight. American Airlines had fully transitioned from paper navigation documents to digital versions[8] on pilot EFBs across all aircraft of the type.

A software flaw caused the Boeing Onboard Performance Tool application to fail. The application was developed by Jeppesen, a Boeing subsidiary and a leading global provider of aeronautical charts and procedures. According to Avionics International, citing a Jeppesen representative, the issue affected a dedicated version of the application used by American Airlines only and did not affect other versions.

The error occurred while processing an Instrument Landing System chart file for Ronald Reagan Washington National Airport. A new file with an updated approach procedure was uploaded to the electronic chart database in the EFB application. This new file had the same name and index number as the current chart file. As a result, two different versions of the file with the same index numbers were present on the devices. Attempting to open this file caused the application to crash.

To resolve the issue, flight crews were advised to reinstall the navigation app on their EFBs. In some cases, aircraft had to return to the terminal from taxiways so that pilots could connect to the airport Wi-Fi. Additionally, crews could obtain printed charts and procedures at the airport. Shortly afterward, a software update was released to fix the file-loading issue. As a temporary workaround, crews could manually download the Reagan National Airport procedure in PDF format onto their EFBs.

A duplicate file appeared on the devices as a result of the airline's standard procedure: new approach charts were uploaded to the tablets one day before they were scheduled for use, allowing flight crews time to review them in advance. At this time, the old charts remained valid for one more day. At 7:00

[8] American Airlines was the first airline to receive regulatory approval (from the FAA) to use electronic documentation on portable electronic flight bags throughout all phases of flight in place of paper documentation.

p.m. Central Time on April 28, 2015, a new approach chart file was made available on the pilots' tablets, which led to simultaneous malfunctions on numerous devices at various airports. The first to encounter the issue were pilots who had favorited Ronald Reagan Washington National Airport.

It is important to note that all updates to aeronautical information, including approach procedures, are made in accordance with the ICAO's Aeronautical Information Regulation and Control (AIRAC) process and take effect on pre-established dates. These dates are set years in advance and published by ICAO and regulatory authorities. Updates always take effect on Thursdays, with a 28-day interval between successive updates. The exact time of activation is defined by the national regulator – in the United States, this is 09:00 UTC (which falls between midnight and 4:00 a.m. local time depending on the time zone). In April 2015, the next AIRAC update date was April 30. As mentioned above, the new approach chart file was uploaded the day before.

Public sources did not report the root cause of the error, including why it was triggered by that specific file, why it had not been detected earlier, and why it only affected the version of the app used by American Airlines. No official damage assessments were published, but the impact can be roughly estimated based on publicly available data. The failure caused 74 flight delays – approximately 1% of the airline's daily flights – with some delays exceeding three hours. Given American Airlines' average load factor in April 2015 (81.6%) and the average seating capacity of its Boeing 737 fleet (150 seats at the end of 2014 and 159 by the end of 2015), it can be assumed that about 10,000 passengers were affected by delays. For an airline of this size (carrying over 100 million passengers annually), the damage can be considered insignificant. Nevertheless, this case illustrates how such software errors can affect a large number of aircraft across various locations and time zones, disrupting airline operations.

Similar problems may arise due to compromised integrity and availability of software and data on EFBs and onboard information systems. This should be taken into account when assessing cybersecurity risks.

It should be noted that the EFBs in this case were based on Apple iPad devices running on the iOS operating system. Many EFB models are developed on this hardware platform. For example, Delta Air Lines, which operated the world's second-largest fleet (975 mainline aircraft) as of the end of 2024, also uses similar tablet-based EFBs.

Portable EFBs, including their system and application software, are not subject to certification by aviation authorities. Airlines and their vendors are responsible for ensuring the quality, reliability, and security of these devices.

This incident highlights the importance of supply chain management as part of holistic approach to cybersecurity assurance.

## Crash of a Boeing 747-244SF Operated by MK Airlines Limited

In October 2004, a cargo Boeing 747-244SF operated by MK Airlines Limited crashed during takeoff at Halifax Stanfield International Airport (Nova Scotia, Canada) due to insufficient engine thrust. All seven crew members on board were killed.

The accident investigation concluded that the cause of the crash was the crew using incorrect takeoff performance data, which stemmed from an erroneous takeoff weight value used in the calculations. The crew used a dedicated software application installed on a Boeing Laptop Tool device – a laptop-based electronic flight bag – to compute take-off performance data.

According to the report of the Transportation Safety Board of Canada (Report A04H0004), published in June 2006, the most likely primary cause of the accident was a feature of the pilot electronic flight bag application: it would automatically copy the estimated takeoff weight value from the weight calculation form into the main takeoff and landing performance calculation form without notifying the user and would automatically overwrite any entry in the planned takeoff weight field of the main form – even if the takeoff weight had not been recalculated (in such cases, the previously calculated value was copied). Figure 4 shows the performance calculation form of this application.

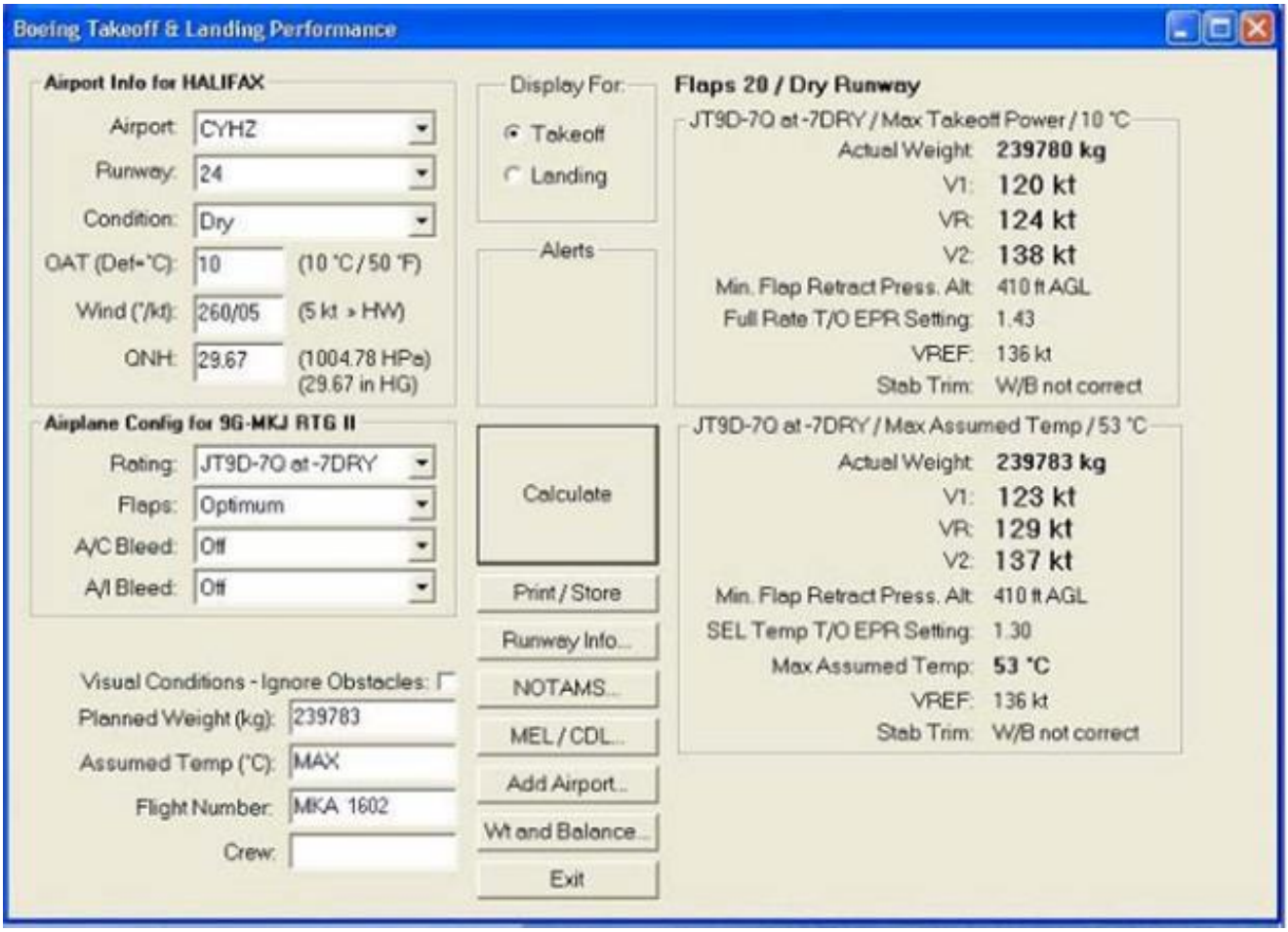


**Figure 4. Takeoff performance calculation form in the Boeing Laptop Tool[9]**

Because of this application feature, the takeoff performance data calculation before the departure from Halifax used the takeoff weight from the previous flight segment, from Bradley International Airport in Windsor Locks (Connecticut, USA) to Halifax.

The investigation found that the error in the input data used for performance calculations combined with several other reasons led to the accident. One of these reasons was that the crew failed to verify the computed performance data according to the airline's standard operating procedures. Besides, the airline did not have a formal training and testing program on the application. Anyway, the identified feature of the application silently overwriting the weight

[9] Screenshot of the takeoff performance calculation form in the Boeing Laptop Tool application is taken from a report by the Transportation Safety Board of Canada.
Source: Transport Safety Board of Canada. Aviation Investigation Report A04H0004. Reduced Power at Take-off and Collision with Terrain, MK Airlines Limited, Boeing 747-244SF 9G-MKJ, Halifax International Airport, Nova Scotia, 14 October 2004.

data in the main form should be viewed as a flaw in the application[10]. One should consider such flaws in human-machine interfaces, which can be introduced during design and implementation, as security weaknesses and take them into account when assessing cybersecurity risks.

The report also stated that, at the time of the accident, no systems or procedures were in place to alert the crew to insufficient aircraft acceleration during takeoff. In light of this, the Transportation Safety Board of Canada recommended that aviation regulators, in cooperation with ICAO, establish a requirement to equip aircraft with takeoff performance monitoring systems designed to alert the crew when parameters are not within allowable thresholds. No recommendations were made regarding the procedures or tools used to perform takeoff and landing performance calculations. Boeing released a message to all users of the Boeing Laptop Tool with a review of the feature and a call to ensure the crews were properly trained on it.

Flaws in the design and use of the pilot EFB application led to a fatal accident: lives were lost, and the aircraft and its cargo were destroyed. Regulators issued directives requiring the airline to revise its operating procedures. Notably, under existing aviation regulations and guidelines, portable pilot EFBs are not considered capable of affecting flight safety. In this case, however, the actual harm did not match the expectation.

### Note 2. Errors in Boeing EFB Applications

In connection with the software flaw in the EFB performance calculation application that led to the crash of the MK Airlines Boeing 747, it is worth mentioning that similar flaws have been discovered recently.

In July 2023, Boeing issued SAFO (Safety Alert for Operators) 23004 for operators of Boeing 737 aircraft (models prior to the NG family), Boeing 747, Boeing 757, and Boeing 767. The alert announced the need to update the Performance Engineer's Tool software to eliminate errors in calculating maximum takeoff weight, which could result in insufficient engine thrust during takeoff. Although these aircraft are equipped with previous-generation avionics suites, they are operated using modern information systems.

[10] Werfelman, L. Fatal Calculation: Bad Weight Computation Dooms Takeoff // Aviation Safety World. Volume 1, Issue 4 (October 2006). – P. 18–24.

A year earlier, in July 2022, Boeing issued SAFO 22002, a safety alert for users of the Boeing Onboard Performance Tool running on iOS devices. The application, developed by Jeppesen, is used across all Boeing aircraft types. The alert described two flaws identified in one version of the application that caused it to malfunction under certain conditions. This resulted in incorrect runway lengths being used in landing performance calculations: in one case, the parameters of the departure airport's runway were used instead of those for the destination airport; in another, the full runway length was used even when the takeoff was initiated from a taxiway intersection rather than from the runway threshold. In both cases, the crew was provided with incorrect distance values, critical for flight safety. Users were advised to either follow specific instructions to prevent malfunctions or to install an updated version of the application, which fixed the issues.

All types of available runway lengths are classified in civil aviation as critical data from the standpoint of data integrity.

The report indicated that similar aviation occurrences, including fatal accidents, had already occurred due to the use of incorrect takeoff performance data. The report mentioned twelve events, four of which took place within the three years preceding the crash under discussion. Two of these four incidents took place on consecutive days and involved Boeing 747 aircraft. In one of these incidents, a Boeing 747-300 operated by South African Airways sustained damage during takeoff (a tail strike occurred) because the flight engineer used an incorrect takeoff weight when calculating takeoff performance using an EFB. In the other case, a Boeing 747-412 operated by Singapore Airlines also experienced a tail strike, because of insufficient thrust and critically low initial takeoff speed. The reason was the pilots had entered into the Flight Management System incorrect takeoff performance data. Although the input values differed significantly from the values computed by the system itself, the system accepted them without issuing any warning about the discrepancy and a possible error.

The issue of using incorrect takeoff performance data has been under discussion for several decades. After two incidents, in 2004 and 2006, caused by calculation errors, specialists from the Applied Anthropology Laboratory at Paris Descartes University conducted a study on the underlying causes of such errors, commissioned by French government agencies, the Bureau of Enquiry and Analysis for Civil Aviation Safety (Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile, BEA) and the Directorate General for Civil Aviation (Direction générale de l'aviation civile, DGAC). The findings formed the basis for further research on this topic. In 2011, the Australian Transport Safety Bureau

(ATSB) published a report on take-off performance calculation and entry errors, and a similar study was conducted by the U.S. National Aeronautics and Space Administration (NASA)in 2012. In September 2021, the European Union Aviation Safety Agency (EASA) released a safety information bulletin on the use of erroneous parameters at take-off, referencing those three studies.

The findings of these investigations indicate that flight crews fairly often make mistakes in calculating takeoff performance data or entering values into the Flight Management System (FMS). It is evident that specific risks are associated with the use of EFBs and similar devices for such calculations. For example, in the NASA report, errors related to the use of tablets for calculating takeoff and landing performance data were classified as a separate category.

**Note 3. Malfunction of Pilot EFBs Due to Low Temperatures**

The NASA report on the causes of takeoff and landing performance calculation errors mentions a case involving a laptop that had been exposed to low temperatures (cold-soaked). Although the pilots entered the correct data, the calculation results were incorrect. The crew failed to detect the error, and during the takeoff roll, an uncontrolled liftoff began, forcing the takeoff to be aborted at high speed.

In modern avionics suites, software applications for calculating takeoff and landing performance data are installed on application servers that are part of the onboard information and maintenance systems, as well as on integrated and portable EFBs.

The majority of fatal aviation accidents occur during takeoff, initial climb, approach, and landing. According to Boeing, between 2013 and 2022, about 67% of all fatal accidents occurred during these phases, even though they represent only 6% of the total flight time. An Airbus annual analytical report also emphasizes that approach and landing are the most complicated phases of flight. These stages are characterized by high crew workload and an increased likelihood of encountering unexpected conditions. Together, these factors can lead to hazardous situations.

EFBs serve as the primary source of navigation information and performance data for flight crews. Any EFB malfunction, or deletion or distortion of the information stored on them, can significantly increase the crew's workload during critical flight phases. Some cybersecurity researchers do believe that cyberattacks on applications used to calculate takeoff and landing performance data may lead to hazardous situations.

Based on the above, it can be concluded that errors in systems used to calculate performance data, even if they do not directly lead to adverse consequences, should be treated as security weaknesses in the context of security risk assessments and assumed to be potentially exploitable by malicious actors.

## Software error in the AC generator control units of Boeing 787 aircraft

In May 2015, the U.S. Federal Aviation Administration (FAA) issued an airworthiness directive[11] (FAA-2015-0936) requiring Boeing 787 operators to fully power down the aircraft at regular intervals (no less than once every 120 days) to prevent a hazardous condition caused by a malfunction in AC generator control units (GCUs). The power-off duration had to be at least 15 seconds (a "cold and dark" state), it was not necessary to disconnect the aircraft's two onboard batteries though.

Laboratory testing by Boeing (the aircraft manufacturer and type certificate holder) identified a software flaw in the GCUs: after 248 consecutive days of uninterrupted generator operation, a software counter overflowed, and each of the aircraft's six generators switched to a failsafe mode regardless of the current phase of flight. As a result, AC power generation would cease, potentially leading to a loss of aircraft control. This means that a software error in the generator control unit could cause a catastrophic failure at the aircraft level[12].

At the time of the directive publication, 28 Boeing 787 aircraft in the United States were subject to the directive (with over 100 operating globally). According to the FAA, the cost of a single power cycle event, considering only the labor time of maintenance personnel, was estimated at $85.

In its operator bulletins, Boeing stated that a software update was scheduled for release in the fourth quarter of 2015. In October 2018, a new airworthiness directive (FAA-2017-0771) was issued, mandating the installation of the updated GCU software, thereby superseding the earlier directive. Thus, it took more than three years to fully address a flaw that could have caused a serious failure.

[11] An airworthiness directive is a document issued by a regulator when a decrease in flight safety levels is identified. It describes the safety threat and prescribes actions to restore an acceptable level of safety.
[12] Catastrophic failure conditions at the aircraft level include any conditions resulting from system failures that prevent continued safe flight and landing.
Source: ARP4761A: Guidelines for Safety Assessment Methods for Systems and Avionics Equipment of Civil Aircraft, Interstate Aviation Committee, Aviation Register, 2010.

The FAA estimated the labor-only cost of installing the software update at $510 per aircraft. This included installing the software itself and performing the associated power-down and power-up procedures. Additional work was also required, with the total estimated labor-only cost amounting to $1,360 per aircraft. At the time the directive was issued, 55 aircraft in the U.S. were affected. Boeing provided the software update free of charge, but the installation work was not covered under warranty in this particular case.

The overall estimated costs for operators to comply with the airworthiness directives mentioned seem quite low, but they do not include the expenses of developing and certifying the software update incurred by the aircraft manufacturer.

No aviation occurrence took place because of the issue. However, this example demonstrates that fixing avionics software errors can take a considerable amount of time, and one should take this into account when considering vulnerability management in the course of cybersecurity risk assessments.

## Software error in the central computer applications of Boeing 787 aircraft

In March 2020, the U.S. Federal Aviation Administration (FAA) issued an airworthiness directive (FAA-2020-0205) requiring Boeing 787 operators to fully power down the aircraft at least once every 25 days. The directive was based on Boeing's service bulletin (B787-81205-SB420045-00) and was issued to prevent catastrophic failure conditions at the aircraft level due to an undetected failure of the central computer system. According to the bulletin, the issue was discovered during internal analysis and testing. We were unable to find any public notices regarding the cancellation of the directive.

At the time the directive was issued, 196 aircraft registered in the U.S. were subject to its requirements. Based solely on the cost of maintenance labor hours, the FAA estimated the expense of performing a power cycle (power-down/power-up) to be $85 per aircraft. This means that the total annual cost of compliance per aircraft would amount to approximately $1,275. However, some experts have pointed out that aircraft are typically “rebooted” at least once a week as part of routine operations, so no additional costs would be incurred to comply with the directive.

The central computer system of Boeing 787 aircraft is called the Common Core System (CCS). It is the foundation on which the Integrated Modular Avionics (IMA) architecture is based. The CCS runs software applications that implement flight-critical functions such as flight management, navigation,

landing gear control, and more. A software error in this system can lead to catastrophic failure conditions.

Data communication between the software applications running on the CCS and the aircraft's avionics systems is conducted via the ARINC 664 Avionics Full-Duplex Switched Ethernet[13] onboard network, referred to in the Boeing 787 as the Common Data Network (CDN). The IP protocol is used at the network layer, and the UDP protocol is used at the transport layer. The physical data transmission layer based on the Ethernet standard is implemented in the CDN using commercial off-the-shelf (COTS) components, while the logical layer is built on Application-Specific Integrated Circuits (ASICs). On the Boeing 787, a proprietary protocol developed by Boeing, Error Detection Encoding (EDE)[14], is used at the logical layer to ensure message integrity and timestamp verification. The EDE protocol extends the message integrity control features of ARINC 664 The UDP packet data field structure when using the EDE protocol is shown in Table 1.

| Field Length (bytes) | Field Name |
|---|---|
| 2 | EDE sequence number |
| 6 | EDE timestamp |
| Variable | Data |
| 2 | CRC-X checksum |
| 2 | CRC-Y checksum (incl. CRC-X) |

**Table 1. UDP packet data field structure when using EDE protocol**

As stated in the directive and service bulletin, after 51 days of continuous operation of the CCS server, the EDE timestamp verification function becomes silently disabled, that is, without detection and notification to the crew. If a hidden failure of a CDN network switch were to occur at the same time, the applications running on the CCS central computer could receive outdated (stale) data inputs. For example, the primary displays for both pilots could show

[13] See the ARINC 664P7standard: ARINC Specification 664P7. Aircraft Data Network, Part 7, Avionics Full-Duplex Switched Ethernet Network, Aeronautical Radio, Inc., 2009, 150 p. Networks conforming to this standard are sometimes called AFDX networks (AFDX is a registered trademark of Airbus).

[14] See the following specifications and articles:

- MX Foundation 4 API, ARINC 664 Frames, Max Technologies Inc. (Updated 10/23/2023);
- Santamarta, R. A Reverse Engineer's Perspective on the Boeing 787 '51 Days' Airworthiness Directive, IOActive, May 6, 2020;
- AMCX-FDX-2, 2 Port 10/100/1000Mbit/s, AFDX®/ARINC664P7, Test, Simulator and Monitor, Module for PMC, Data Sheet, AIM, 2023.

incorrect values of flight-critical parameters (such as altitude, airspeed, attitude indicator readings, and engine performance parameters), while stall and overspeed warnings would not be triggered. Pilots would be flying the aircraft based on incorrect data and would be unable to maintain continued safe flight and landing, which would be a catastrophic failure condition. The directive estimates the likelihood of a hidden failure in the CDN network switch to be Extremely Remote. Therefore, the probability of a catastrophic failure after 51 days of uninterrupted CCS server operation is also Extremely Remote. However, it is still two orders of magnitude higher than the acceptable threshold, because aviation regulations and guidance stipulate that catastrophic failure conditions must be Extremely Improbable. Moreover, such a condition is possible as a result of a single point of failure, which is inadmissible.

**Note 4. Probabilities of Failure Conditions**

Extremely Remote failure condition: a failure condition that is not expected to occur during the service life of a single aircraft of the given type. At the same time, it may occur several times during the service life of all existing aircraft of the given type. Probability: between $10^{-5}$ and $10^{-7}$ per flight hour for an average-duration flight.
Extremely Improbable failure condition: a condition that is not expected to occur during the lifetime of all existing aircraft of the given type. Its probability is estimated to be $10^{-9}$ or less per flight hour.
A catastrophic failure condition must be Extremely Improbable and must not result from any single point of failure.

After the airworthiness directive was published, Ruben Santamarta, an information security expert who was working at IOActive at the time and was conducting cybersecurity research on the Boeing 787, offered his opinion on the possible root cause. He suggested that a flaw in the implementation of the data link layer in the application-specific integrated circuit (ASIC) used in the CDN network might have led to the failure of the network message age validation function.

## Message delivery errors in the main onboard computing network of Airbus A350 aircraft

In June 2017, the European Union Aviation Safety Agency (EASA) issued an airworthiness directive, EASA AD 2017-0129, based on a service bulletin from Airbus. The directive required Airbus A350 operators to perform a complete power shutdown of the aircraft on a regular basis (at least once in every 149

hours) to prevent a failure of the onboard computing network. The directive stated that operators had reported instances of loss of communication between avionics systems over the main onboard computing network, with a variety of failures reported, from failures of backup systems to malfunctions in specific aircraft functions implemented via software applications running on the central computer. However, the directive did not provide any details on the exact nature of the failures.

An analysis conducted internally by Airbus revealed that after 149 hours of continuous avionics system operation, the delivery of messages to software applications on the central computers via the ARINC 664[15] standard network could become disrupted. This could lead to failures in safety-critical systems.

A software update that eliminated the root cause of the failure was issued a year after the directive was released along with a service bulletin with installation instructions (Airbus SB A350-42-P010). Another year later, in July 2019, the directive was amended (EASA AD 2017-0129R1): power shutdowns were no longer required for aircraft on which the software had been updated.

The Airbus Service Bulletin contains instructions on updating the software of the ARINC 664 onboard network switches (Common Remote Data Concentrator, CRDC) and the central computer units (Core Processing Input Output Modules, CPIOM), as well as explanations regarding the nature of the error. After 149 hours of continuous aircraft power supply, the internal timer built into each ARINC 664 network endpoint device would reset. If, during this short reset interval, any system or device attempted to transmit a message over the network, it would then be unable to send any further messages until the aircraft was fully powered down and restarted.

The European Union Aviation Safety Agency (EASA) directives did not include cost estimates for the power-down and restart procedure. However, a similar Federal Aviation Administration (FAA) airworthiness directive employed the same cost estimation methodology used for the Boeing 787 aircraft. Based solely on labor hour costs for technical maintenance, annual expenses could reach up to $5,185 per aircraft. At the time of the directive publication, two Airbus A350 aircraft were registered in the U.S. According to the service bulletin, the installation of the software update took four labor hours. This estimate did not include time for preparation, planning, or verification of results. Airbus covered these costs under its internal warranty labor rate, provided that certain conditions were met.

A noteworthy aspect of this error is that it was discovered only after operator reports of failures, despite its potential to cause catastrophic failure

[15] On Airbus aircraft, ARINC 664 standard networks are referred to as Aircraft Full Duplex (AFDX) networks.

conditions. Nevertheless, the direct financial impact on airline operators resulting from this error was insignificant. From a cybersecurity perspective with vulnerability management in mind, it is worth noting that it took about a year to develop and release a software update to correct the flaw.

## Error in the flight data recorders of Boeing 787 aircraft

Problems with incorrect message timestamps in ARINC 664 standard onboard networks bring to mind another avionics issue in the Boeing 787, which was identified during the investigation into the 2013 lithium-ion battery fire incident.

A lithium-ion battery caught fire on a Japan Airlines Boeing 787 at Logan International Airport in Boston, Massachusetts, shortly after the passengers had disembarked. According to the investigation report, the initial analysis faced difficulties due to issues with the Enhanced Airborne Flight Recorders (EAFR). It was discovered that after the data source had stopped providing valid flight data, the recorders continued to write stale data, that is outdated buffered data, as if it were valid. The report noted that using such stale data from the recorders to evaluate aircraft technical condition or perform maintenance and repairs could compromise airworthiness. In this connection, the U.S. National Transportation Safety Board (NTSB) recommended that the Federal Aviation Administration (FAA) and Boeing take appropriate measures.

Modern integrated avionics suites collect large volumes of performance and monitoring data on various aircraft systems and transmit them to airline operational teams. These data are used not only to diagnose individual aircraft but also for fleet-wide maintenance, including predictive maintenance.

No specific information has been made available on direct financial damage to airlines caused by the recorder flaw or related flight safety issues. However, violations of collected data integrity resulting from such flaws or from attacks on avionics systems, can have serious consequences and should be taken into account when assessing cybersecurity risks.

# Existing approaches to cybersecurity certification of digital avionics systems

A series of standards aimed at protecting aviation equipment from cyberattacks has been published in the United States and the European Union since 2014, with the goal of ensuring and maintaining aircraft airworthiness. A working group under the Aviation Register of the Russian Federation

(Aviaregister of Russia) is currently developing national regulatory and methodological documents for ensuring the information security (cybersecurity) of aviation equipment based on these standards. The working group includes representatives from leading Russian aviation industry enterprises, such as Yakovlev, National Helicopter Center Mil & Kamov, Ilyushin Aviation Complex, the Ural Works of Civil Aviation, Advalange (Laboratory of Secure Systems), the State Research Institute of Aviation Systems, and Kaspersky.

The existence of standards for protecting aviation equipment against cyberattacks to ensure and maintain airworthiness indicates that an internationally recognized approach has evolved in this domain. In this part of the article, we examine airworthiness in terms of its susceptibility to cyberattacks, define cybersecurity objectives for aviation equipment, and provide an overview of the main regulatory and methodological documents (standards, guidelines, etc.) used in international practice in the process of designing and operating aircraft.

### Note 5. Security, Safety, Airworthiness, and Flight Safety

For the purposes of this article, the term **Security**, when used without further clarification refers to information security or cybersecurity.
**Safety** refers to the absence of unacceptable risk of harm to human life and health, property, or the environment.
**Airworthiness** (fitness for flight) refers to the technical condition of an aircraft in which it conforms to its type (approved) design and ensures safe operation.
**Flight safety** refers to the condition of civil aviation or its individual components in which the safe operation of aircraft is ensured.

The primary objectives in ensuring the cybersecurity of avionics systems for civil aircraft are:

- Protection of airworthiness (i.e., protection of the aircraft's technical condition compliant with airworthiness standards);
- Protection of flight safety;
- Protection of the aircraft's technical condition in accordance with the airline's internal requirements (in addition to airworthiness standards);
- Protection of the airline's business operations.

Protection of airworthiness and flight safety are the highest-priority goals, as they have to do with risks to human life, health, and the environment.

We will examine each objective in detail and provide a brief overview of the relevant regulatory and methodological documents. Some of these documents

are used by leading international aircraft manufacturers and aviation regulators in the U.S. and the EU. American and European regulatory and methodological documents on the cybersecurity of aviation equipment are largely based on information security standards for general-purpose systems, particularly those developed by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the United States National Institute of Standards and Technology (NIST). A list of the main cybersecurity-related regulatory documents used in the U.S. and EU for the development and operation of aircraft is provided in Appendix A.

## Protection of airworthiness

National regulatory authorities such as the Aviaregister of Russia, the U.S. Federal Aviation Administration (FAA), and the European Union Aviation Safety Agency (EASA) establish requirements for protecting airworthiness from cyberattacks. These requirements are included in the certification basis of an aircraft type[16].

Protecting airworthiness involves designing and implementing cybersecurity measures at the development stage (in the process of ensuring airworthiness), as well as security measures during operation (in the process of maintaining airworthiness).

In the past, onboard systems that are critical to flight safety, as well as data transmission networks, were either physically isolated from external environments and from one another or had limited and controlled connectivity. In modern digital avionics suites based on IP data networks, these systems may be connected (directly or indirectly) to external systems and networks, as well as to cabin systems. From type certification perspective, the resulting interconnectivity and openness are treated by aviation authorities as new and unusual design features that affect airworthiness. Such design features may introduce novel threats to both airworthiness and flight safety.

The primary documents governing aircraft certification are the airworthiness standards. They define a set of baseline requirements that an aircraft must meet to obtain a type certificate. Occasionally, the certification authorities may impose additional requirements for the aircraft design under consideration in the course of certification, beyond those in the airworthiness standards. This may be necessary, for example, when an exemption from airworthiness

[16] The certification basis is a document that defines the airworthiness and environmental protection requirements applicable to a specific aircraft model.
Source: Federal Aviation Regulations "Certification of Aircraft, Designers and Manufacturers of Aircraft Products. Part 21", Ministry of Transport of the Russian Federation, 2014.

requirements is necessary or when the standards do not address certain novel or unusual design features not covered by the standards that could impact airworthiness. Such additional requirements are listed as Special Conditions (SC) in the aircraft type certification basis alongside the regular airworthiness requirements. It is up to the certification authority to decide on the structure, contents, and language of SCs. Examples of SCs on cybersecurity for the Boeing 737 are given in the Appendix B.

If airworthiness standards contain cybersecurity requirements, the certification authority must consider cybersecurity regardless of whether any onboard digital system or functionality is formally designated as a novel or unusual design feature.

U.S. airworthiness standards, developed by the Federal Aviation Administration (FAA), do not yet include specific cybersecurity requirements. Therefore, when certifying aircraft with advanced onboard systems, the FAA establishes SCs related to cybersecurity. In July 2020, European airworthiness standards were amended to contain a requirement to protect onboard systems from cyberattacks, based on an cybersecurity risk management[17] approach. The type certificates European Union Aviation Safety Agency (EASA) issued before that include cybersecurity-related SCs as well. Russian airworthiness standards currently do not include cybersecurity requirements, so the Aviaregister of Russia used SCs on cybersecurity.

Many active type certificates for modern aircraft issued in the U.S. and the EU contain SCs on cybersecurity. For example, the type certificates for the following aircraft have such SCs:

- Boeing 787 (version dated January 31, 2025);
- Boeing 737 MAX (version dated January 28, 2025);
- Airbus A350 (version 31, dated April 10, 2025);
- Airbus A320 (version 86, dated April 4, 2025).

SCs typically require an assessment of cybersecurity threats and related risks that may affect the safe operation of the aircraft. The cybersecurity requirements included in type certificates issued by U.S. and EU regulators are very much alike. These requirements generally fall into three categories:

- requirements for protecting onboard systems and networks against unauthorized access by remote and local entities;

[17] See section CS 25.1319 in Amendment 25 to the European airworthiness standards (Easy Access Rules for Large Aeroplanes (CS-25) (Amendment 25), European Union Aviation Safety Agency (EASA), EASA eRules, June 24, 2020.

- requirements for assessing cybersecurity threats that exist during the operation of the aircraft onboard systems and networks, including threats associated with maintenance and repair, and for implementing cybersecurity risk management measures;
- requirements for developing manuals for aircraft operators on ensuring the cybersecurity of onboard systems and networks in order to maintain airworthiness (for continued airworthiness).

The first aircraft to receive a type certificate containing cybersecurity-related SCs was the Boeing 787. It was certified by the Federal Aviation Administration (FAA) in August 2011, and its commercial operation began the following month. At the time, no formal standards or recommendations existed regarding demonstrating compliance with cybersecurity-related SCs, so the FAA developed its own guidelines and criteria based on the specific architecture and design of the aircraft avionics suite.

Later, leading international aviation organizations, RTCA (U.S.) and EUROCAE (EU)[18], jointly developed a series of cybersecurity standards for aviation systems to ensure airworthiness. These standards are published in the U.S. and EU under different identifiers, but having the same contents. The first standard in the series was released in 2010 by EUROCAE as ED-202 and subsequently by RTCA as DO-326. It is commonly referred to as ED-202/DO-326. The other standards in the series follow similar dual identification scheme. The ED-202/DO-326 standard lists cybersecurity measures for design and modification of aviation equipment. The ED-203/DO-356 standard providing recommendations on implementing the measures followed a few years later. In 2014, the ED-204/DO-355 standard was published, supplementing the previous standards with recommendations on ensuring cybersecurity to maintain airworthiness. In 2015, the ED-201 standard was released, defining the overall context for the entire series.

Currently, updated versions of these standards are in effect: ED-202A/DO-326A (released in 2014), ED-203A/DO-356A (2018), ED-204A/DO-355A (2020), ED-201A/DO-391 (2021). U.S. and EU regulators accept compliance with these standards as evidence of conforming to cybersecurity-related SCs. For instance, the type certificate for the Boeing 737, issued by EASA, includes notes recommending that cybersecurity risk assessments be conducted in accordance with ED-202A/DO-326A.

[18] RTCA is a non-profit organization in the United States that develops technical manuals and standards in collaboration with regulatory authorities from various countries.
EUROCAE (European Organization for Civil Aviation Equipment) is a European organization involved in the standardization of both onboard and ground-based aviation systems and equipment.

Since July 2020, when the EU airworthiness standard were amended to include a requirement to protect onboard systems from cyberattacks, compliance with ED-202A, ED-203A, and ED-204A is required by EASA.

In addition to the ED/DO series of standards on cybersecurity, ARINC[19] specifications are also used to meet cybersecurity requirements and address cybersecurity needs. ARINC specifications include technical specifications for onboard electrical and electronic equipment and data transmission protocols. The specifications were developed in a joint effort of major manufacturers of aircraft and aircraft equipment, and aircraft operators. The ARINC 664 Specification (Aircraft Data Network) defines technical specifications for IP-based onboard data networks and recommends certain technical cybersecurity measures.

Airworthiness security requires ensuring that, should any supporting system (such as an EFB) be compromised, this will not adversely affect primary systems. This requirement is included in airworthiness standards or the relevant cybersecurity SCs. The U.S. Federal Aviation Administration (FAA) has issued advisories (advisory circulars) for certain aspects of using supporting systems, namely for electronic documentation and EFBs. Similar regulations have also been issued by the Australian Civil Aviation Safety Authority (CASA).

## Protection of flight safety

Flight safety is achieved through a range of measures, including activities aimed at ensuring and maintaining airworthiness, managing air traffic, and providing up-to-date information to flight crews (flight plans, electronic charts and maps, weather and wind data, passenger and cargo information) and maintenance personnel (system configuration, status, and failure data, as well as maintenance manuals). Thus, in addition to protecting airworthiness, a variety of operational processes and procedures require protection to ensure flight safety.

Ensuring flight safety requires interaction, sometimes automatic, between onboard and external systems. For example, modern air traffic management technologies such as ADS-B[20] (Automatic Dependent Surveillance-Broadcast) rely on onboard, ground-based, and satellite systems. In the United States, work is underway on the Next Generation Air Transportation System (NextGen). In 2015, the U.S. Government Accountability Office submitted a

[19] Aeronautical Radio, Incorporated (ARINC) was founded in 1929 and is now a division of Collins Aerospace. ARINC publishes technical standards and specifications for aviation equipment, developed by the Airlines Electronic Engineering Committee (AEEC). The committee includes representatives of leading aircraft manufacturers and operators.

[20] See article: New Air Traffic Surveillance Technology, Quarter 2 (QTR_02 10), pp. 7–13.

report to Congress stressing the need for a comprehensive approach to information security in the NextGen system, particularly due to the high level of interconnectivity between avionics and external systems. In 2020, the U.S. Government Accountability Office released another report assessing cybersecurity risks associated with onboard communication, positioning, and weather data systems. Both documents highlighted the need for an enhanced approach to avionics system security assessment by regulators.

At present, there are no dedicated flight safety standards considering cybersecurity. However, the ED-201A/DO-391 standard touches upon the issue of flight safety by outlining the context for cybersecurity risk assessment in civil aviation. The standard outlines the industry as a framework with multiple stakeholders and shared responsibility among them for ensuring cybersecurity.

In the U.S. and the European Union, the development of security measures in this area is based on applicable standards and guidelines issued by the U.S. National Institute of Standards and Technology, such as NIST SP 800-30 and NIST SP 800-53, as well as international ISO/IEC 27000 series standards.

## Protection of aircraft technical condition as defined by airline requirements

Airworthiness standards are established by regulators to ensure the safe operation of aircraft. At the same time, airlines may have their own additional requirements for the technical condition of their aircraft. These requirements typically concern such onboard systems as in-flight entertainment systems, onboard information systems, and portable EFBs. Reliable and secure operation of these systems is vital for commercial efficiency.

Such additional requirements on the aircraft technical condition may vary from airline to airline as they are based on the airline's business model, the service level maintained, and other factors. An airline bears full responsibility for maintaining the technical condition of aircraft. It is worth noting that any issues related to the potential exploitation of such supporting systems for cyberattacks against primary systems are addressed within the context of airworthiness security. For example, any potential impact of a compromised in-flight entertainment system on airworthiness falls under the domain of airworthiness security, while ensuring its stable operation falls under aircraft condition protection according to airline requirements.

To meet these airline-specific requirements related to protecting aircraft technical condition, airlines and manufacturers typically rely on cybersecurity

standards and regulations for general-purpose systems, since aviation-specific standards and regulations in this area are missing.

## Protection of the business interests of airlines

In a market economy, the protection of business interests is a relevant concern both at the level of individual aviation stakeholders – airlines, aircraft manufacturers, passengers, and suppliers of goods and services – and at the industry level.

Protection of business interests involves preventing financial losses and safeguarding reputation. The cybersecurity of all industry players directly affects the interests of airlines and should therefore be reflected in contracts and the relevant regulatory documents. For example, if it is possible that an issue with an electronic flight bag application causes flight delays, as in the case of American Airlines, the developer (vendor) of the application should share the responsibility with the airline for availability of the operation functions it enables. To avoid such problems at a systemic level, requirements for applications should be developed at the industry level, rather than being defined solely in private technical specifications. This applies not only to EFBs but also to other supporting systems in avionics suites, as well as external systems the aircraft communicates with, including airport and airline systems.

The area of responsibility of aviation authorities, however, is limited exclusively to airworthiness and flight safety and protecting the business interests of industry players is therefore out of scope of aviation cybersecurity standards at the moment. The notable exception is ARINC 811, which addresses aircraft cybersecurity in the context of commercial airline operations. This standard provides recommendations to airlines on structuring aircraft cybersecurity processes based on their business interests. As far as protecting aircraft technical condition is concerned, cybersecurity standards for general-purpose systems are adapted to aviation needs.

# Conclusion

A review of several aviation occurrences caused by hardware and software malfunctions in the avionics suites of modern civil aircraft demonstrates the need for cybersecurity risk assessment and the rationale for adequate protection from cyberattacks that could lead to such failures.

The aviation occurrences examined demonstrate that flaws and malfunctions in avionics suites can result in anything from minor disruptions to airline

operations to catastrophic outcomes. In aviation, multiple stakeholders share the responsibility for ensuring flight safety and maintaining the proper technical condition of aircraft, while each also protects its own business interests. The increasing interconnectivity and openness of avionics systems, driven by digitalization and integration with external systems, increases cybersecurity risks.

The current specialized approaches to evaluating the security of digital avionics suites used in the aircraft certification process are largely limited to verifying compliance with requirements for protection against cyberattacks aimed at ensuring and maintaining airworthiness. These requirements pertain solely to the technical condition of the aircraft and do not address flight safety holistically.

At the same time, the requirements for protecting flight safety against cyberattacks are broader in scope, as they involve the entire ecosystem of systems and technologies involved in managing air traffic. This domain is currently the most relevant area for the research and standardization of cybersecurity requirements in aviation systems.

As an essential industry of modern economy civil aviation involves various stakeholders, including airlines, aircraft and avionics manufacturers, suppliers of goods and services, and passengers. Rules for protecting the technical condition of aircraft to ensure efficient commercial operation, as well as protecting the stakeholders' interests against cyberattacks, have not been addressed at the level of industry standards and recommendations so far. General-purpose cybersecurity and risk management standards, supplemented by internal guidelines, have been considered sufficient. However, as the integration of airborne, space, and ground systems progresses and the information infrastructure of civil aviation becomes increasingly complex, it is likely that dedicated standards and guidelines will emerge to address cybersecurity risks in specific domains, for example, regulations governing use of artificial intelligence in avionics and digital twins of avionics systems and suites.

# Appendix A. List of international standards and directives on information security for civil aircraft

The European standard ED-201: Aeronautical Information System Security (AISS) Framework Guidance defines the overall context for securing onboard systems.

The following standards are used in the U.S. and EU in the process of aircraft design and manufacturing to meet airworthiness requirements and obtain a type certificate:

- European standard ED-202A: Airworthiness Security Process Specification, and its U.S. counterpart, DO-326A, which outline key requirements for ensuring the information security of aircraft and their systems.
- European standard ED-203A: Airworthiness Security Methods and Considerations, and its U.S. counterpart, DO-356A, which provide recommendations on implementing the provisions of ED-202A/DO-326A.

The following standards and directives (advisory circulars) are used to maintain airworthiness during operation:

- European standard ED-204A: Airworthiness Security Process Specification, and its U.S. counterpart, DO-355A.
- European standard ED-206A: Guidance for Security Event Management, and its U.S. counterpart. DO-392;
- FAA Advisory Circular AC 119-1: Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP), which addresses ensuring information security in onboard data networks to maintain airworthiness.
- FAA Advisory Circular AC 120-78B: Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals, which governs the use of electronic signatures and digital logs and manuals.
- FAA Advisory Circular AC 120-76E: Authorization for Use of Electronic Flight Bags, which defines the requirements for operational approval of Electronic Flight Bags (EFBs).
- FAA Advisory Circular AC 43-216A: Software Management During Aircraft Maintenance, which provides guidance for handling software during aircraft maintenance and repair.

In addition to the documents listed above, ARINC standards are used to ensure compliance with Special Conditions (SCs) for ensuring information security. When developing onboard data networks based on the IP protocol, the ARINC Specification 664: Aircraft Data Network is applied. One of its components, ARINC Specification 664P5, provides recommendations on defining logical network domains and outlines information security requirements for onboard data networks. Some ARINC standards include guidance on specific technical measures for ensuring and maintaining airworthiness:

- ARINC Report 852: Guidance for Security Event Logging in an IP Environment;
- ARINC Report 835-1: Guidance for Security of Loadable Software Parts Using Digital Signatures;
- ARINC Report 842-1: Guidance for Usage of Digital Certificates.

The ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework offers recommendations for airlines on ensuring the information security of aircraft. This document stands out because it explicitly or implicitly accounts for all four aircraft cybersecurity objectives.

When a specific standard is used to demonstrate compliance with Special Conditions (SC), it becomes part of the practical guidance (instructions) on maintaining the aircraft's airworthiness.

# Appendix B. Special Conditions for information security in type certificates for the Boeing 737

Below are the Special Conditions for information security listed in the type certificates for the Boeing 737 Next Generation modification (-600/-700/-700C/-800/-900/-900ER) and MAX (8/9/-8200), issued by the U.S. Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA).

## Special Conditions for information security in the FAA type certificate

In Type Certificate A16WE, version 73, dated March 15, 2023, issued by the U.S. Federal Aviation Administration (FAA), the following two Special Conditions for information security are specified:

25-550-SC "Airplane Electronic Systems Security Protection From Unauthorized External Access":

1. The applicant must ensure that the airplanes' electronic systems are protected from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity.

2. The applicant must ensure that electronic system security threats are identified and assessed, and that effective electronic system security protection strategies are implemented to protect the airplane from all adverse impacts on safety, functionality, and continued airworthiness.

3. The applicant must establish appropriate procedures to allow the operator to ensure that continued airworthiness of the airplane is maintained, including all post type certification modifications that may have an impact on the approved electronic system security safeguards.

25-551-SC "Isolation or Airplane Electronic System Security Protection From Unauthorized Internal Access":

1. Заявитель обязан реализовать в конструкции самолета изоляцию или защиту электронных систем от доступа из внутренних неавторизованных источников. Конструкция должна исключать возможность случайных и преднамеренных изменений, а также любые негативные воздействия на оборудование, системы, сети и другие компоненты, необходимые для безопасного полета и безопасной эксплуатации.

2. Заявитель должен разработать процедуры, позволяющие эксплуатанту поддерживать летную годность самолета, в том числе при внесении в сертифицированную конструкцию изменений, которые могут негативно повлиять на работу утвержденных мер обеспечения информационной безопасности электронных систем.

## Special Conditions for information security in the EASA type certificate

In Type Certificate IM.A.120, dated January 10, 2023, issued by the European Union Aviation Safety Agency (EASA), one Special Condition is listed for ensuring the cybersecurity of computing systems and networks, which in fact consists of three provisions:

a) The applicant shall ensure security protection of the systems and networks of the aircraft from any remote or local access by unauthorized sources if corruption of these systems and networks (including hardware, software, data) by an inadvertent or intentional attack would impair safety.

b) The applicant shall ensure that the security threats to the aircraft, including those possibly caused by maintenance activity or by any unprotected connecting equipment/devices inside or outside the A/C, are identified, assessed and risk mitigation strategies are implemented to protect the aircraft systems from all adverse impacts on safety.

c) Appropriate procedures shall be established to ensure that the approved security protection of the aircraft's systems and networks is maintained following future changes to the Type Certificate design.

The certificate also includes recommendations on methods of demonstrating compliance with this special condition, including guidance on verifying security mechanisms.

**Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT)** — is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com