Security Requirements for SATCOM Datalink Systems for Future Air Traffic Management

Karin Bernsmed, Christian Frøystad, Per Håkon Meland
Department of Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway

Tor André Myrvoll
Department of Connectivity Technologies and Platforms
SINTEF Digital
Trondheim, Norway

***Abstract*—Aircraft equipped with satellite communication (SATCOM) systems will enable advanced Air Traffic Management (ATM) operations over datalink on a global basis. A key concept of future ATM is 4D trajectory management, which aims to ensure an optimal path and designated arrival time for the flight by integrating time as a fourth dimension into the aircraft trajectory. However, the increase reliance on digital information exchange needed for implementing 4D implies that cyber security will be a key concern. The goal of the Iris Service Evolution programme is to provide a secure and reliable datalink for air-ground communication in oceanic and remote environment based on satellite. This paper provides an overview over ongoing work on cyber security in the Iris programme. We discuss the need for security for future datalink services in the aircraft control domain and, based on a security risk and threat analysis, provide a number of security requirements that future SATCOM datalink systems for ATM should fulfil.**

***Index Terms*—cyber security, security requirements, Air Traffic Management, satellite communication**

I. Introduction

The introduction of new technology will change Air Traffic Management (ATM) significantly over the next 15 years. 4D trajectory management, also referred to as "time-based operations", will be a key concept in future ATM [1]. The goal is to ensure an optimal path and designated arrival time for the flight by integrating time as a fourth dimension into the aircraft trajectory. By synchronizing trajectory information between the aircraft avionics and the Air Traffic Control (ATC), the arrival sequence at the airports can be optimized, hence reducing costs and emission while increasing the capacity of the airports.

Implementing the future ATM will bring new types of challenges [2]. Datalink will be the normal means of communication between the aircraft and the ground at cruising altitude. Broadcast transmissions will give way to unicast communications and standardized pre-formatted text-messages will replace voice-based instructions. Together with the ongoing technological changes in the aviation industry, such as the increased reliance on software, new vulnerabilities will appear and a new threat picture arise. Security will be a key enabler to ensure safe and reliable services in future ATM [2], [3].

Iris [4] is a European Space Agency program, which has been launched to support the development of a satellite-based communication system for European Air Traffic Management. Iris aims to make aviation safer by developing a new satellite communication (SATCOM) system, which will provide a robust and reliable air-ground datalink that can be used to enable advanced ATM operations in oceanic and remote environments. Iris will operate in a multilink environment, providing an oceanic and continental air-ground datalink as a supplement to existing surface communication systems in airports (AeroMACS [5]) and ground-based communication systems (LDACS [6]). Iris is anticipated to be fully operational in 2028, with an initial Precursor service foreseen to be launched in 2018.

This paper focuses on security requirements for future SATCOM datalink systems, which will enable advanced ATM operations based on datalink. The scope of our work is primarily Air Traffic Services (ATS) and Aeronautical Operational Control (AOC) datalink services intended to be included in the Aircraft Control Domain (ACD). We look into the security needs of these services, assess the security risks of a selected set of services, namely the envisioned Aeronautical Telecommunication Network Baseline 3 (ATN-B3) applications that will enable 4D trajectory management: CM, CPDLC and ADS-C [7], and propose a set of security requirements that will mitigate these risks and fulfil the needs, taking into account additional requirements originating from a number of other sources.

The methodologies used for deriving the requirements are through an ISO/IEC 27005 [8] compliant risk analysis, where information of threats, vulnerabilities and risks has been derived from a litterature study, a thourough analysis of existing SATCOM systems documentation and from elicitation workshops with selected stakeholders in the European aviation community.

The paper is organized as follows. Section II outlines related work and explains how they have been utilized in this paper. Section III presents the context of the paper by going into details of the future ATS datalink and AOC services and explaining how they will be delivered over SATCOM. In Section IV, we outline security goals for these services. Section V presents results from a security threat and risk analysis. Section VI presents the security requirements that we have derived. Section VII discusses the relation between security and safety requirements. Finally, Section VIII concludes the paper and outlines our future work.

II. Related Work

A. The SESAR program

The Single European Sky ATM Research (SESAR) program [9] is an initiative launched by the EU in 2004 to reform European ATM. The SESAR P15.2.4 project has delivered a specification of the Future Communication Infrastructure (FCI) [7], which includes SATCOM as an air-ground datalink for future ATM. Furthermore, the 15.2.4 project has performed a risk assessment of the FCI [10] and defined a set of mission requirements that will apply to SATCOM datalink systems that aim to be part of the FCI [3]. The scope of the work presented in our paper is based on the envisioned use of future ATM services as they have been described in [7]. While the scope of the risk assessment performed by the 15.2.4 project is wider than ours (the threats identified in [10] are generalized to cover all the air-ground radio links in the FCI), we have focused specifically on the ATN-B3 application data exchange over a SATCOM link.

B. Eurocontrol/FAA and NextGen

In 2007, EUROCONTROL [11] and the Federal Aviation Administration (FAA) [12] performed a study of future ATM in which they identified a number of requirements that future radio systems will need to fulfil [13]. Their study identified security needs for ATS datalink and AOC services and outlined a set of requirements for the FCI and its radio links. This study was the starting point for the SESAR 15.2.4 project, which used it to derive the SATCOM mission requirements in [3] and for NextGen [14], which is a collaborative effort between FAA and the aviation community. We have used the threat severity classification in [13] when discussing the security needs of future ATS datalink and AOC services (cf. Section 4) and we have cross-checked the SATCOM security requirements that we have derived with the requirements delivered by EUROCONTROL and FAA, to make sure that nothing has been overlooked in our analysis.

C. Iris Precursor

The Iris Precursor project [15], which is part of the Iris program, has developed enhancements to existing aeronautical SATCOM for delivering ATS datalink services. Iris Precursor introduced security gateways in the air and ground segments, which are used to set up IP-sec tunnels between the aircraft and the satellite ground station and to ensure that safety services are prioritized over other data from the cockpit and cabin. In addition, Iris Precursor added enhancements to the radio access network to increase the network performance and availability for ATS datalink applications. While the scope of the Iris Precursor was to enable a robust and secure means for delivering ATN/OSI traffic over the satellite link, the scope of the Iris Service Evolution study (in which the research presented in this paper was performed), is to enable future ATN services that will be delivered over the IP suite: ATN/IPS. The security architecture of Iris Precursor, which is described in [16], has been used as the target of evaluation when we assessed the security risks of future ATN-B3 services delivered over SATCOM (cf. Section V-D).

D. Other Work

Security for future ATM has also been studied by the research community. Casado et al. [17] discuss the need for information security in future ATM. They outline and analyze the impact of a number of threats to flight and surveillance information. Sampigethaya et al. [18] provide an overview over state-of-the-art research and standardization efforts to ensure cyber security capabilities of future datalink-enabled aircraft and point out a number of open challenges that need to be addressed. Security threats to ADS-B have been studied by e.g., [19] and [20]. A number of other sources have also pointed out vulnerabilities and threats to existing and future ATM systems [21]–[25]. Most of these threats will be highly relevant for the future ATN-B3 services and have therefore been included in our study as well.

III. SATCOM Datalink Systems for Future Air Traffic Management

In this section, we briefly outline how SATCOM datalink systems are envisioned to support future ATM, as envisioned by the SESAR and Iris research programs. An overview is provided in Figure 1, which illustrates how ATS datalink systems, AOC systems and voice systems can utilize an IP-based communication link set up between an Air Security Gateway (ASGW) on the aircraft and a Ground Security Gateway (GSGW) in the ground segment, hence enabling Air Navigation Service Providers (ANSPs), which are the organizations providing Air Traffic Control (ATC), and Airlines to securely exchange information with the aircraft over a satellite datalink.

By 2028, it is envisioned that ATM will be completely digitalized [4]. ATN/IPS is an air-ground Aeronautical Telecommunication Network (ATN) operating over a new network infrastructure based on the Internet Protocol Suite (IPS), which is currently being standardized by ICAO [26]. The purpose of ATN/IPS is to provide an efficient and robust network infrastructure to both ATS, which includes ATN-B3 applications[1], and AOC applications in the Aircraft Control Domain (ACD), which will support safety and regularity of flight [27]. The ICAO ATN/IPS specification is still only a draft, but our understanding of how the standard will enable future IP-based services to be delivered over SATCOM to the aircraft is illustrated in Figure 2. As can be seen in the figure, both ATS datalink and AOC (ACD) applications will be delivered over the ATN/IPS network. Whether cockpit voice (VoIP) should be included in ATN/IPS or delivered over "general IP" is still under discussion in the research programs.

SESAR has defined a set of ATN datalink services that will be necessary to support 4D trajectory management [7]. These ATN-B3 applications, as foreseen today, are:

[1]The concept of "ATS datalink applications" includes both existing FANS-1/A applications as well as future ATN-B2 and ATN-B3 applications; however, the scope of our study is restricted to security analysis of the ATN-B3 applications.

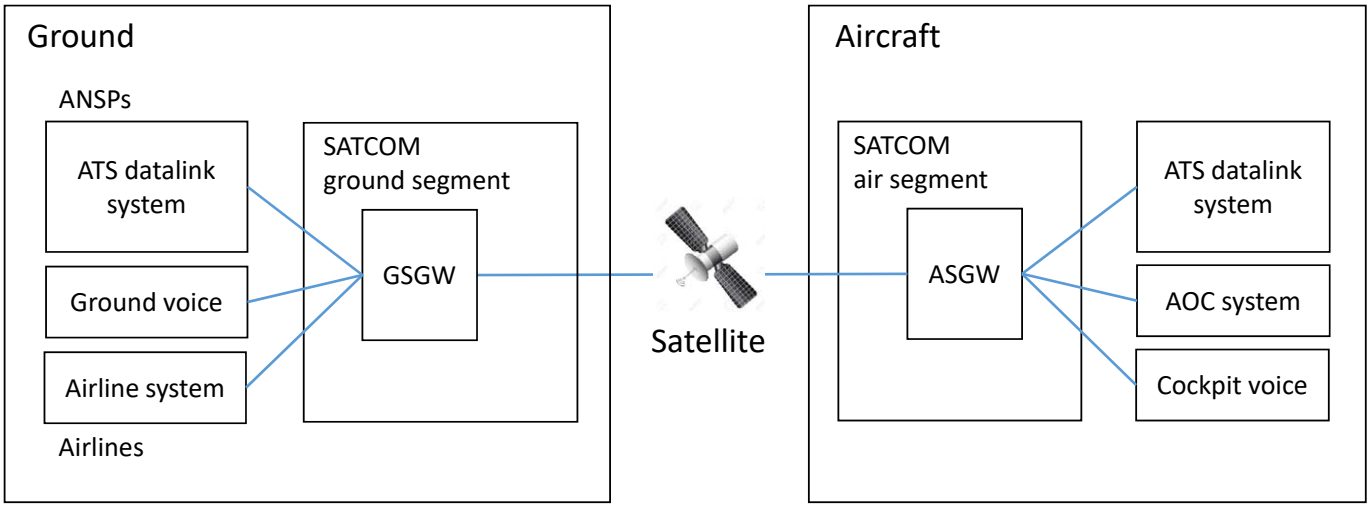

Fig. 1. End-to-end context of future ATM over SATCOM.

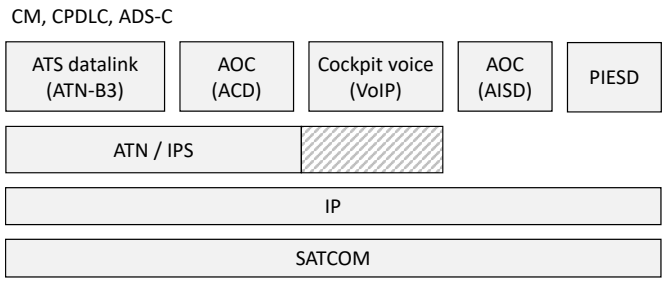

Fig. 2. Future IP-based services delivered over SATCOM.

- Context Manager (CM), which will provide services relevant for establishing the communication context of a session, including exchanging information about available services, communication methods and security requirements between the involved parties.
- Controller Pilot Data Link Communications (CPDLC), which will will replace most of the radio communication between the pilot and the controller. CPDLC includes the transmission of standardized textual messages and will enable the possibility of automating parts of Air Traffic Control (ATC).
- Automatic Dependent Surveillance - Contract (ADS-C). ADS enables tracking the aircraft in a given airspace by broadcasting information about position, altitude, speed, etc. ADS-C will enable data to be transmitted based on an explicit contract between the ANSP and the aircraft, stating when and what information should be reported.

For Aeronautical Operational Communication (AOC), we distinguish between applications in the Aircraft Control Domain (ACD) and applications in the Aircraft Information Service Domain (AISD). AOC applications in the ACD domain will support the safety and regularity of flight and may include 1) applications supporting flight operations, for example Digital Automatic Terminal Information Service (D-ATIS), 2) meteorological reports, 3) systems monitoring, for example Aircraft Condition Monitoring System (ACMS) and 4) aircraft tracking, for example Position Reports (POSRPT) [21]. In addition, the RTCA Special Committee 206: EUROCAE WG 76 is in the process of standardizing a modernized set of Aeronautical Information Services (AIS) and Meteorological (MET) Information Services [28], referred to as AIS/MET, which will be available to the flight crew via SWIM [29]. A subset of these is also expected to be included in the ACD domain. AOC services that support more airline-specific information exchange will be delivered in a separate AISD domain [27].

It is important to note that the current draft of ATN/IPS is a point-to-point (unicast) protocol. However, many of the future ATM services will need to have broadcast capabilities, so that an ATC can efficiently reach all aircraft within a certain region or area. The SESAR 15.2.4 project has therefore stated that the FCI must support multicast communication at the IP level for ground-air communication [7]. This requirement may apply to SATCOM datalink systems as well. At the time of writing, it is unclear which of the aforementioned services will need broadcast capabilities; however, AIS/MET is a likely candidate.

The ultimate goal of the Iris program is to enable ATN-B3 applications for full 4D trajectory based operations as a safe and reliable service, alongside with IP-connectivity for AOC applications. The Iris Service Evolution study comprises preparation activities for the transition of existing SATCOM datalink systems (including the Iris Precursor solution described in Section II) to support this vision, and this includes analyzing the security needs and deriving security requirements, which is the scope of this paper.

IV. Security Goals for Future ATS Datalink and AOC Services

In this section, we present some fundamental security goals for future ATS datalink (ATN-B3) and AOC (ACD domain)

applications. Our conclusions in this section have been derived from an analysis of the reports from the SESAR 15.2.4 project [10] and EUROCONTROL and FAA [3].

A. Confidentiality

Confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Ensuring the confidentiality of information includes making sure that only intended recipients are able to access and read the information. A breach of confidentiality is the unauthorized disclosure of information [30].

Confidentiality is a cornerstone in cyber security, but has traditionally not been an issue in aviation. Anyone can listen in on current ATC voice communication with the help of equipment easy to access. It is also relatively easy to record and decode unencrypted air-ground data transmissions [21], [22], [24]. In voice based ATC no attempt has been made to keep the communications confidential and neither is there any intent to make the existing ATC datalink confidential [7], [31].

Whereas little or none of the ATC information exchanged between the aircraft and ground is classified as confidential today, this does not mean that sensitive data is not transferred over the SATCOM network. Regarding AOC applications in the AISD domain, we are aware of examples of e.g. credit card data being transmitted openly over ACARS[2], placing the airline in direct violation of the PCI DSS standard[3]. Even though application specific solutions, such as SecureACARS [32], exist, they have not yet been widely adopted. Moreover, the aircraft and onboard crew systems also hold large amounts of flight operational data that could potentially be made available to relevant personnel on the ground if proper confidentiality was ensured. Ensuring proper confidentiality of such information will prevent information disclosure to unintended recipients - potentially illegally listening in on the communication link. Additionally, an open communication channel will allow eavesdroppers to map any potential vulnerabilities of the datalink system, which may undermine its security [10].

Regarding the ATS datalink services, the ATN-B3 applications will comprise CM, CPDLC and ADS-C, which are all high-criticality operational services. The risk assessment performed by SESAR 15.2.4 explicitly states that confidentiality is not applicable for ATS in FCI: "Safety monitoring and ANSP policy requirements mean that end-to-end encryption of ATS communications to protect confidentiality of data in transit is not permitted" [10]. The need for confidentiality has also been evaluated in the study by EUROCONTROL and FAA [3], which, in contrast to the SESAR 15.2.4 project, concluded that FCI should support encryption to mitigate eavesdropping when providing services with "high-severe" or "medium" confidentiality ranking, however, the only ATS service they have identified with this ranking is D-ALERT[4]. Based on the analysis in [10] and [3] we therefore conclude that

> *The current draft of ATS Datalink applications (ATN-B3) has no known confidentiality requirements.*

Future AOC applications supporting safety and regularity of flight will include some of the AOC services currently supported over ACARS, which will be adapted to support transmission over IP, and future AIS/MET and AOC services that will be delivered over SWIM [21]. Candidate existing AOC applications to be supported by ATN/IPS in the ACD domain include D-ATIS, ACMS and POSRPT (see previous section). The study by EUROCONTROL and FAA [3] has not identified any confidentiality requirements for D-ATIS or ACMS, i.e. their confidentiality rankings are "none", and POSRPT has been assigned confidentiality ranking "low".

Regarding the AIS/MET services, they intend to provide aeronautical and meteorological information that will create a common view of the airspace situation for all aircraft in the region [28]. As mentioned in Section 3, such information may be broadcasted to several recipients. At this point in time there are no foreseen confidentiality requirements associated with these services. We therefore conclude that

> *The current draft of AOC applications in the ACD domain has no known confidentiality requirements.*

The AOC applications in the AISD domain include airline specific information exchange. These services will require new datalinks that can handle large amount of data without causing unacceptable delays of ATS datalink applications [7]. The SESAR Study document "AOC Datalink Dimensioning, Ed01.00.00" [33] defines a large number of new AOC services, mostly related to the Electronic Flight Bag (EFB), such as Aircraft Briefing Cards, Crew Briefings, Flight Deck Duty Time registration, Flight Journal Documentation and Passenger Information List/Manifest. Many of these services will include business sensitive information, or personal data from passengers and crewmembers, and will therefore have strong confidentiality requirements. This view is supported in SESAR 15.2.4, which states "Confidentiality is only likely to be needed and applied for AOC services, and on a service-by-service level" [10]. Additionally, as discussed in the beginning of this section, many airlines are already today in need of protecting personal and business sensitive information that is being transmitted between the crew in the air and the ground and we do not expect this to change in the foreseen future. We therefore conclude that

> *Some AOC applications (AISD domain) will have confidentiality requirements.*

[2]Aircraft Communications Addressing and Reporting System (ACARS) is an existing digital datalink system for transmission of short messages between aircraft and ground stations via airband radio or satellite

[3]The Payment Card Industry Data Security Standard (PCI DSS) was created to ensure that merchants meet a minimum level of security when they store, process and transmit cardholder data.

[4]The D-ALERT service enables a flight crew to notify appropriate ground authorities when the aircraft is in a state of emergency or in an abnormal situation. It is worth noting that the Eurocontrol/FAA study [13] assesses the future use of D-ALERT service instances per aircraft to one per year, which means that this service is not expected to be frequently used.

Some of the new AOC services defined by SESAR [33] will also have direct influence on the operation of the aircraft; the examples provided in the report are "Passenger Medical Examination" and "Hijack Report". The report also states that a number of the AOC services (e.g., "Weather Information", "NOTAM", "De-Icing", "Flow Control" (including slot times), "Position Reporting" and "Airport Delay Information") will have direct influence on flight operations and should therefore be considered to be classified as ATS. Therefore, in contrast to our previous statement that ATS Datalink applications has no known confidentiality requirements, one cannot rule out that future ATS Datalink applications, which have not yet been defined as ATS, will have confidentiality requirements. This view is supported by the SESAR 15.2.4 project, which states that "requirements for confidentiality, integrity, and availability may evolve as the operational services develop" [10]. We therefore conclude that

Future ATS Datalink applications, which are yet to be defined, may have confidentiality requirements.

It is worth noting that SESAR has established that, in order to meet safety monitoring and ANSP policy requirements, full end-to-end encryption of ATS communications to protect confidentiality of data in transmit will not be allowed (see page 72 in [10]). However, the same report also points out that the air-ground communication link could be encrypted at the network level, or that specific services (primarily AOC) can be encrypted at the application layer. At the time of writing SESAR has not decided whether, and on what layer, they should recommend air-ground datalink encryption in the Future Communication Infrastructure (FCI).

B. Integrity and Authenticity

Ensuring the integrity of data includes maintaining and assuring its completeness and accuracy [30]. In the context of cyber security in the future ATM, this means that no actor should be able to intercept and modify a message between e.g. an aircraft and the ATC without this being detected. Thus, ensuring adequate integrity will prevent undetected tampering with data. Closely related to integrity is authenticity, which is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This includes verifying a claimed identity or confirming the source of information [30], [34]. Error detection mechanisms, such as hashing and cycle redundancy checks (CRCs), will not on their own, provide such guarantees.

Integrity and authenticity of ATC data transmissions are, and will continue to be, crucial in aviation. When losing the voice context there is nothing in a correctly formatted and in context datalink message that would reveal that the sender is anyone else than a genuine pilot or controller, or that the content of the message has not been changed during the transmission. This threat has been recognized by, for example, International Federation of Air Line Pilots, which lists "annoyance spoofing" of ACARS messages as one aspect that needs to be addressed in future solutions [21]. Messages of unverified origin could con the crew, by using technology readily available today, into performing potentially dangerous operations. With the reduced dependency on voice in the future ATM, being unable to verify the authenticity of a message or data packet could have much larger consequences than today.

The EUROCONTROL and FAA study [13] stated that the FCI shall support message authentication and integrity to prevent message alteration attacks when providing services for which a breach of security could have "severe" or "catastrophic" adverse effect on safety, flight regularity, or business interests. The study also stated that the FCI should support message authentication and integrity to prevent message alteration attacks when providing services with "medium" integrity ranking. This applies to a number of ATS Datalink application services, for example the aforementioned D-ATIS and D-ALERT[5]. Furthermore, the SESAR 15.2.4 project has formulated a dedicated requirement stating, "FCI systems shall employ security controls that authenticate the message source and mitigate message alteration attacks" [10].

Even though the impacts of a modification or replay attack will vary, depending on which service that is affected, both ATS Datalink applications and AOC applications clearly need to be secured against unauthorized tampering of messages and sender impersonation. We therefore conclude that

ATS Datalink application (ATN-B3) and AOC applications (ACD and AISD domains) will have high integrity and authenticity requirements.

C. Availability

From a cyber security perspective, availability means making sure all systems are operational and functioning when needed under any circumstances [30]. For most services envisioned to use the SATCOM link, availability will be a crucial factor. Ensuring that relevant information from the aircraft can reach the ANSPs and vice versa, will avoid disruption of the service and hence maintain the safety of the passengers.

Today, many airlines rely on AOC, and failure of the SATCOM data link means airlines will suffer from delays in their flight schedules. The SESAR 15.2.4 project [7] states that in the future even more applications will rely on the availability of the AOC services, and points out that new data links that can handle a large volume of data without delaying the CPDLC and ADS-C services will be required. Similarly, the EUROCONTROL and FAA study [13] has evaluated the severity of threats towards availability and states that the impact on many of the ATS datalink services will be high-severe.

Availability is a well-known concept in ATM and is usually included in existing safety and performance assessments and requirements. However, safety hazard analysis usually only consider unintended losses of messages and random system component failures. Design solutions derived from safety analysis therefore do not include protection against

[5]Note that [13] was an early attempt at defining future ATS requirements. The preliminary safety assessment for ATN B3 done by SESAR does not have hazards of the same level of criticality.

malicious actions, such as inter alia denial of service attacks or intentional jamming of the SATCOM link.

D. Non-repudiation

Non-repudiation provides protection against denial by one of the entities involved in a communication of having participated in all, or part of, the communication. Non-repudiation therefore prevents either the sender or the receiver from denying the origin and/or delivery of a transmitted message. Ensuring non-repudiation also includes being able to prove, with legal bearing, whether an event has occurred or not, as well as if a party was involved or not [34]. Even though authenticity and non-repudiation are closely related concepts, mechanisms that provide authenticity does not necessarily include non-repudiation, and vice versa.

Non-repudiation is not a well-known concept in ATM, most likely since it is not directly related to safety. SESAR has pointed out that, in the FCI, the actions of an entity should be traced uniquely to that entity so that it can be held responsible for its actions, and introduces accountability of actions performed as a dedicated requirement [10]. On the other hand, the EUROCONTROL and FAA study [13] has not identified any requirements, or evaluated any threats, related to non-repudiation for future ATS datalink services.

From a security perspective, one can foresee many cases where the parties involved in an ATS datalink or AOC application data transmission would like to prove, in hindsight, that a certain actor transmitted a certain message. For example, if an AOC message related to flight operations, which is sent to an aircraft from the ground, results in some form of financial impact on the airline (severe delays, or the like), it could be important for the airline to be able to prove the involvement of the responsible ATC. Even though it may not be necessary from a safety perspective, non-repudiation could therefore be important from a legal perspective. We therefore conclude that

> *Some ATS Datalink applications (ATN-B3) and AOC applications (ACD domain) may have non-repudiation requirements.*

E. Summing up

To summarize, our analysis in this section indicates that ATS datalink and AOC (ACD domain) application data exchange will have high integrity, authenticity and availability requirements. In addition, it may be necessary to implement confidentiality and non-repudiation on an application-by-application basis. The conclusions derived in this section will be used as input to the requirements on future SATCOM datalink systems that we present in Section 6.

V. Security threats and risks

A. Security Threats to Aviation

The envisioned transition of ATM operations to support full 4D trajectory based operations based on ATN-B3 will challenge the traditional way of thinking security in several respects. The aviation industry is accustomed to an era in which the equipment and competence to execute an attack was both expensive and rare. This era ended with the software-defined radios and the easy access to inexpensive transmitters and receivers, which provide anyone with the capabilities of listening and interfering with air traffic communication at will.

Having access to the communication channel and being able to interfere with it at a technical level is seldom enough to cause any serious problems. Both ATC controllers and pilots have been trained to identify perpetrators and know how to respond. Additionally, unless the perpetrator is using a specifically directed antenna, both real parties would notice the conversation and can immediately negate and correct the false instructions. These inherent countermeasures of ATC will become less effective as the communication moves from analogue to digital, from broadcast to unicast and from voice to text. It will be easier for a perpetrator to address only one party, making it difficult for the others to detect malicious activity. In addition, preformatted text messages will make it easier for a perpetrator to impersonate another actor by only changing specific fields in the messages.

With the continuous effort from aircraft manufacturers to reduce the cost of operation and the CO2 emissions of their aircraft, weight reduction plays a crucial part. One approach to reduce weight is to move from physical separation of domains and systems to software-based separation. This opens for a completely new category of potential vulnerabilities that can be exploited. Also the Flight Management System (FMS) is nowadays utilizing standardized hardware, which runs software modules that earlier were implemented a separate hardware modules. This reduces or removes the physical separation, which earlier provided additional security, by rather relying on logical separation and containerization. Thus, if an attacker gains logical access to one system, the possibility of gaining access to other systems increases.

In recent years, we have seen an increased interest in ATM security outside the aviation domain. Researchers have demonstrated that it is both easy and inexpensive to manipulate existing ATC transmissions such as ADS-B [19], [20], thus posing a direct threat to safety due to lack of security. In 2014, IOActive [22] conducted tests on SATCOM firmware from a number of different vendors and found multiple vulnerabilities including hardcoded credentials, undocumented protocols, insecure protocols, backdoors, and weak password reset mechanisms. According to IOActive, these vulnerabilities may allow an attacker to take control of the SATCOM link, which is currently used for e.g. FANS and CPDLC. Numerous other examples exist as well.

Looking 20 years ahead, additional threats are likely to emerge. If the 4D trajectory data were compromised, this could lead to severe safety hazards, such a loss of separation of aircraft, increased workload for the flight crew and the staff on the ground and, in the worst case, be a contributing factor to midair collisions. With the introduction of single-pilot systems or entirely unmanned aircraft, such threats will become even more serious. A malicious actor aiming to hijack a remotely piloted aircraft could do this from the ground, hence avoiding exposing himself to both the risk of being physically harmed

and the risk of being caught.

B. Threat Actors

In this section, we highlight some potential threat actors and discuss their motivations, intentions and capability to attack a SATCOM datalink system used for ATM. Note that this list is not meant to be exhaustive, but to demonstrate that there are actors with the motivation and capability to pose a cyber threat to the aviation industry.

Insiders will generally have a low motivation for actively attacking a system, but this motivation might increase significantly if the insider is extorted or coerced by another actor. What makes the malicious insider threat so serious is the extensive access to and knowledge about the relevant systems that, for example an employee, might possess. While the malicious insider usually is a more severe threat actor, negligent users might unintendedly cause problems as well. Depending on the maturity of the existing security mechanisms in the organization, there might be few, if any, mechanisms in place for detecting insider attacks. Terrorist organizations have demonstrated, over the last couple of years, their commitment and high motivation for their cause although said causes differ. Both Boeing and NATO ranks cyber-terrorism as one of the foremost threats to international aviation [23]. Foreign intelligence services and their role in the never halting race for military power and advantage makes them highly motivated threat actors. Disrupting the air traffic in a country or region might serve to demonstrate such capacity and power. In the event of a military conflict, grounding all air traffic of the opponent might be of strategic importance. Another motivating factor could be the promotion of national industry over a competitor. Hackers, ranging from simple script kiddies and activist hackers to security researchers conducting testing of vulnerabilities on live systems without regard to the ethics of endangering the passengers, could cause both intentional and unintentional problems. Criminals will always find new ways in which they can enrich themselves. If this can be done through posing a threat to aviation, there is a real possibility that someone will explore the option. However, criminal acts against the aviation industry is likely to be taken very seriously by the authorities and thus receive higher priority than more traditional crime. This could be a mitigating factor. Finally, legitimate organizations, e.g. suppliers, airlines or ANSPs, are often in a state of competition and could thus be tempted to have the competitor be perceived to be unable to operate a safe and secure service.

Looking ahead, future scenarios may motivate threat actors in ways that are difficult to foresee today. For example, while the aviation industry already is a likely target of ransomware, the aircraft themselves could also become targets of virus infections or ransom attacks, as the aircraft become increasingly advanced and connected.

C. Mitigating Factors

Even though the security threat picture in future ATM is severe, some mitigating factors already exist [24]. Safety has always been the primary concern of the aviation community and many of the safety mechanisms that are in place in today's aircraft and ground systems will also reduce the risks of security incidents. There already exist numerous procedures and practices for both controllers and pilots to deal with different sorts of failures in their technical systems. Most pilots have already experienced incorrect instrument readings and instructions and are trained to check and double-check every instruction they receive. Similarly, ATC controllers that notice "ghost aircraft", or aircraft that use multiple or incorrect identities already know how to handle such situations. Moreover, redundancy has always been an important mechanism to prevent safety incidents within aviation. If one system fails, or is compromised, another will take its place. These mechanisms will, to some extent, mitigate security threats as well. However, the move to digitalized communication will make both detecting and reacting to attacks on the communication channel much more difficult. A determined attacker may very well target multiple systems simultaneously, and will at the same time trying to hide any trace of ongoing malicious activity.

D. Risk Assessment of ATN-B3 Services over SATCOM

As part of the Iris Service Evolution study, we have performed a risk assessment of potential security threats against a SATCOM datalink system that will be used to deliver future ATN-B3 services. In the risk assessment, we have used the Iris Precursor security architecture as the target of evaluation (cf. Section II-C and [16]) and we have evaluated the likelihood and impact of a number of potential attack scenarios against this system. The likelihoods have been determined based on the existence of known vulnerabilities (or lack of security controls) in the system, the strength of existing mitigating countermeasures, the expected time and expertise required to perform the attack, and the "window of opportunity", which is the time period during which the target will be available to an attacker. The impacts have been assessed in terms of their effect on the flight operations, their effect on the occupants (passengers) and air crew, and their effect on ATS, which is in accordance with the requirements for aircraft airworthiness provided by EUROCAE [35]. In total 26 threat scenarios were identified and assessed. Due to its sensitive nature, we cannot reproduce all the details from the risk assessment here, but below we summarize the main results.

All the identified risks were evaluated using the safety hazard classes defined in the EUROCAE standard ED-78A [35]. None of the risks were evaluated to be hazardous (hazard class 2) or catastrophic (hazard class 1). The most serious risks that we identified, which will all lead to a significant increase in workload for the flight crew and, in worst case, also to a significant reduction in separation (hazard class 3) were derived from scenarios related to injection of false CPDLC messages from ATS, weaknesses in the selected cryptographic keys or algorithms, compromise of the private root keys, and unauthorised access to the Ground Security Gateway (GSGW, cf. Figure 1). Despite the potential severe consequences, these scenarios were all assessed as very unlikely to manifest.

The most likely threats that we identified were related to unavailability; for example, a jamming attack against the air-ground SATCOM network or a targeted DoS attack against PKI Ops, which is the organization that will operate the Public Key Infrastructure used for mutual authentication and establishment of a secure communication link between the ground segment and the aircraft in the Iris Precursor security solution, may prevent aircraft to establish an IP-sec tunnel to the satellite ground station and hence lead to delays for aircraft waiting to take-off (hazard class 4).

It should be noted that the use of safety hazard classes to evaluate the impact of the threat scenarios does not include other types of unwanted effects that do not affect safety, such as breach of legislation, a reduction of the public perception of the ATM or the SATCOM datalink system, or additional costs for any of the involved organizations. Many of the threat scenarios will lead to a severe breach of security, even though they have received a minor safety hazard classification in the risk assessment. For example, "aircraft masquerading", which means that an attacker pretends to be an authorized airborne user of the SATCOM link, may have little safety impact in itself, but would represent a serious breach of security in the Iris Precursor trust model and could be devastating for the reputation of the SATCOM datalink system provider and the affected ANSPs and Airlines.

Based on the results from the security risk analysis, we have proposed a number of countermeasures that should be implemented to strengthen the security of the Iris Precursor solution (these have been documented in [36]). In the following section, we have used the results to derive a number of security requirements that future SATCOM datalink systems should fulfil.

VI. Security Requirements for Future Air-Ground SATCOM Datalink Systems

This section presents a number of security requirements for future air-ground SATCOM datalink systems that will be used to deliver ATN-B3 services. We have derived these requirements based on the following sources:

- The need for confidentiality, integrity, authenticity, availability and non-repudiation for future ATS datalink and AOC services, as identified in Section IV.
- The Iris Precursor security architecture, which has been documented in [16].
- The results from the Iris SE security risk assessment, as outlined in Section V-D and documented in [36].
- Security requirements for the Future Communication Infrastructure (FCI), which have been identified by SESAR [3].
- Security requirements for future radio systems supporting ATS and safety related AOC communications, which have been identified by EUROCONTROL and FAA [13].
- Security requirements from applicable European and international regulation [37]–[40].
- Input and feedback from key stakeholders involved in the Iris Service Evolution consortium

The security requirements for future air-ground SATCOM datalink systems (hereafter referred to as "the system") are presented in Table I. The requirements are formatted as follows:

- The Req Id "Sys-xxx-yyy" contains "xxx" for requirements category ("Sec" indicates that it is a security requirement) and "yyy" for requirement number.
- The Phase column indicates when the capability is required to be in service. The phases have been defined by the Iris program and comprise: Phase 1 (2018), in which ACARS and dual-channel voice services will be delivered to the cockpit using the Iris Precursor security architecture; Phase 2 (2020), which introduces ATN/OSI, ATN-B1 and ATN-B2 to be operating on the SATCOM link; Phase 3 (2024), which introduces initial ATN/IPS capability to support ATN-B2 applications over IP and the migration of AOC services in the ACD from ACARS to ATN/IPS; and finally Phase 4 (2028), which completes the introduction of ATN/IPS in the European continental airspace and introduces ATN-B3 applications to be used for full 4D trajectory operations.
- The requirements column uses "shall" to indicate a mandatory requirement and "should" to indicate an optional requirement.
- The color green (G) means that the requirement is stable and justified by on-going programs, amber (A) indicates a potential requirement that needs further justification or clarification, and a red (R) requirement is not stable and needs further assessment.

Note that the last three requirements apply to the organization that will operate a future air-ground SATCOM datalink system, and not to the system itself.

As indicated in Table I, requirement Sys-Sec-205 is still unstable; the reason is that how (and if) ground-air multicast capability should be implemented is still being discussed. In addition, two of the requirements (Sys-Sec-225 and Sys-Sec-230) will need further clarification from the aviation community before they can be considered stable.

These 12 requirements are currently undergoing review by the Iris consortium and will, once they have been stabilized, be included in the final set of SATCOM datalink system requirements that the Iris Service Evolution study will deliver to the European Space Agency (ESA).

VII. A Note on Security versus Safety

The aviation community has long experience in analyzing safety threats, defining safety requirements and certifying the safety characteristics of aircraft. Once the aircraft has been certified, it is considered to be safe as long as no changes are made to its architecture, design or operation. These assumptions are problematic from a security perspective [41].

Due to the characteristics of malicious activities, the security risk picture is constantly changing. This means that the results from a security analysis have a very short lifetime; threats that are relevant today may be irrelevant tomorrow and new threats that cannot be foreseen may appear in the future. Hence,

TABLE I
SATCOM DATALINK SYSTEM SECURITY REQUIREMENTS FOR FUTURE ATM

Req ID	Phase	Requirement	S
Sys-Sec-200	3-4	The system shall enable integrity protection and data-origin authentication of ATS and AOC (ACD domain) unicast data exchange over the air-ground SATCOM network, to a level of confidence equivalent to a safety hazard classification of "Major" (SC3).	G
Sys-Sec-205	3-4	The system shall enable integrity protection and data-origin authentication of ATS and AOC (ACD domain) multicast data exchange over the air-ground SATCOM network, to a level of confidence equivalent to a safety hazard classification of "Major" (SC3).	R
Sys-Sec-210	3-4	The system shall be designed to support any additional overhead required by end-to-end cryptographic protection of datalink application messages.	G
Sys-Sec-220	3-4	The system shall perform separation and prioritization of ACD data from AISD and PIESD data over the air-ground SATCOM network.	G
Sys-Sec-225	3-4	The system shall prevent the SATCOM data network to be used as a means to inject malicious content into the ground or aircraft secure domains to a level of confidence equivalent to a safety hazard classification of Major (SC3).	A
Sys-Sec-230	3-4	The system shall be designed to withstand intentional attacks impacting the availability of ATS and AOC (ACD domain) data exchange to a safety hazard classification of 'Minor' (SC4).	A
Sys-Sec-240	3-4	The system shall detect and prevent aircraft and ground masquerading on the air-ground SATCOM network	G
Sys-Sec-250	3-4	The system shall prevent unauthorised physical and logical access to the ground segment	G
Sys-Sec-260	3-4	The system shall provide secure remote access to the ground segment for external terrestrial partners utilising the air-ground SATCOM network.	G
Sys-Sec-270	3-4	The system shall require a certain level of security to be implemented by external terrestrial partners connecting to the ground segment	G
Sys-Sec-280	3-4	The system shall operate in accordance with an Information Security Management System (ISMS).	G
Sys-Sec-290	3-4	The system shall implement and maintain a Security Information and Event Management (SIEM) system.	G

it is generally accepted in the security community that risk management must be an integral part of any organization and that the risk management must be an ongoing process in which threats are continuously assessed, monitored and responded to. An example of such a process is the ISO/IEC 27001 standard [42], which specified a framework for managing security risks. On the contrary, safety analysis tends to focus solely on unintentional actions and failures; the risk of malicious interference is often overlooked, even though there may be safety implications. An open question is therefore how existing standards and regulations on aviation safety can be adjusted to reflect this new reality. A recent document produced by the RTCA Special Committee SC216 [43] provides some guidance on this matter.

Security requirements may sometimes have an impact on safety. An example is encryption of controller-pilot communication in ATC, which is a security mechanism that cannot be implemented, since scrambled communication links could have a negative impact on safety. Aviation regulation specifically states "when security measures may adversely affect the safety of operations, the risks must be assessed and appropriate procedures developed to mitigate safety risks" (EC 216/2008, Annex IV, 8 [44]). Moreover, the partners in the Iris SE project has stated that safety must always precede security. Security requirements must therefore always be reviewed to ensure that they do not have any negative safety implications.

VIII. Conclusions and Future Work

In this paper, we have presented a study of security threats, risks and requirements that will apply to SATCOM datalink systems that will deliver ATS datalink and AOC (ACD) applications for future ATM. The requirements have been derived from existing work performed by e.g. SESAR, EUROCONTROL and FAA, from a security risk assessment of the Iris Precursor solution, from applicable aviation legislation and from discussions with key stakeholders in the Iris SE consortium. Our main conclusions are that SATCOM datalink systems must enable integrity protection and data-origin authentication of the datalink applications, whereas confidentiality and non-repudiation protection should be implemented on an application-by-application basis. Moreover, we foresee the need for secure ground-air broadcast capabilities, a strict separation between data in the ACD domain and the AISD domain, and that the organization(s) operating the SATCOM datalink system(s) operate(s) in accordance with an established standard for managing security risks. Our next step will be to provide an overall technical and operational security solution for the SATCOM datalink system that will be used to deliver ATN-B3 and AOC (ACD) datalink applications, as well as a schedule and migration path towards the proposed solution.

References

[1] L. H. Mutuel, P. Neri, and E. Paricaud, "Initial 4d trajectory management concept evaluation," in *Tenth USA/Europe Air Traffic Management Research and Development Seminar (ATM2013)*, 2013.

[2] SESAR, "The roadmap for delivering high performance aviation for Europe. European ATM master plan. Executive view," SESAR JU, Tech. Rep., 2015.

[3] e. a. S. L. Barbera, "SATCOM Mission Requirement Document," SESAR deliverable D104, edition 00.06.02," SESAR JU, Tech. Rep., 2016.

[4] "Satellite Communication for Air Traffic Management (Iris)." [Online]. Available: https://artes.esa.int/iris/overview

[5] A. Malaga, K. A. T. Murugan, A. Roy, and D. Farah, "Aircraft installation amp; operational aspects of the aeronautical mobile airport communications system (aeromacs)," in *2012 IEEE Aerospace Conference*, March 2012, pp. 1–11.

[6] D. S. M. Schnell, U. Epple and N. Schneckenburger, "LDACS: future aeronautical communications for air-traffic management," *IEEE Com. Magazine*, vol. 52, no. 5, pp. 104–110, May 2014.

[7] SESAR Joint Undertaking, "SESAR P15.2.4 Future Data Link System Definition - WA1.1: Deliverable D03 - FCI Operational Concept," 2015.

[8] "ISO/IEC 27005:2011 information technology - security techniques - information security risk management."

[9] "SESAR Joint Undertaking." [Online]. Available: http://www.sesarju.eu/

[10] M. S. et al. (eds), "P15.2.4 WA1.3 Security Risk Assessment Report, SESAR deliverable D05, edition 00.01.01," SESAR JU, Tech. Rep., 2014.

[11] "European Organization for the safety of air navigation (EUROCONTROL)." [Online]. Available: https://www.eurocontrol.int/

[12] "Federal Aviation Administration (FAA)." [Online]. Available: https://www.faa.gov/

[13] EUROCONTROL and FAA, "Communications Operating Concept and Requirements for the Future Radio System," EUROCONTROL, Tech. Rep., 2007.

[14] "Next Generation Air Transportation System (NextGen)." [Online]. Available: https://www.faa.gov/nextgen/

[15] "Iris Precursor." [Online]. Available: https://artes.esa.int/projects/iris-precursor

[16] I. P. T. CGI, "Iris Precursor: System Security Technical Note, Iris deliverable IrisPre-C-GS-TN-0019-INM, v.1.2," CGI, Tech. Rep., 2015.

[17] E. Casado, "Information security in future air traffic management systems," *Journal of Aerospace Information Systems*, vol. 13, no. 3, pp. 101–112, March 2016.

[18] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proceedings of the IEEE*, vol. 99, no. 11, pp. 2040–2055, 2011.

[19] A. Costin and A. Francillion, "Ghost is in the Air(Traffic)," 2012. [Online]. Available: http://tinyurl.com/y8398kuh

[20] H. Kelly, "Researcher: New air traffic control system is hackable," 2012. [Online]. Available: http://edition.cnn.com/2012/07/26/tech/web/air-traffic-control-security/index.html

[21] A. The International Federation of Air Line Pilots, "Cyber threats: who controls your aircraft?" IF APLPA, Tech. Rep., 2013/06/05 2013, nOT IN FILE.

[22] R. Santamarta, "A Wake-up Call for SATCOM Security," IOActive, Tech. Rep., 2014, nOT IN FILE.

[23] N. Collins, "Cyber terrorism is 'biggest threat to aircraft'," 2013/12/27 2013, nOT IN FILE.

[24] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE Transactions on Intelligent Transportation Systems*, 2016.

[25] C. W. Johnson, "Cyber security and the future of safety-critical air traffic management: Identifying the challenges under nextgen and sesar," in *10th IET System Safety and Cyber-Security Conference 2015*, Oct 2015, pp. 1–6.

[26] ICAO, "Aeronautical Telecommunication Network (ATN). Manual for the ATN using IPS Standards and Protocols (Doc 9896), Draft ICAO Manual, version 19," ICAO, Tech. Rep., 2011.

[27] I. S. E. Team, "Iris Service Evolution: Mission and System Requirements Document (MSRD), Iris deliverable IrisSE-B1-OS-REQ-0001-CUK, v.0.5," CGI, Tech. Rep., 2016.

[28] "RTCA SC-206 Aeronautical Information and Meteorological Data Link Services," 2016. [Online]. Available: http://tinyurl.com/ycx4hp5x

[29] M. Krempel and M. G. Jaatun, "Learn to swim," in *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*. IEEE, 2014, pp. 556–560.

[30] NIST, "Standards for Security Categorization of Federal Information and Information Systems, FIPS Publication 199," NIST, Tech. Rep., 2004.

[31] "Link2000+ security considerations," 2006.

[32] "Standard: ARINC 823P1 - DataLink Security Part 1 ACARS Message Security," 2007.

[33] SESAR, "AOC Datalink Dimensioning, edition 01.00.00," SESAR JU, Tech. Rep., 2010.

[34] W. Stallings, *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

[35] EUROCAE ED 78, "Guidelines for approval of the provision and use of air traffic services supported by data communications," 2000.

[36] "Technical note on security analysis, iris deliverable: Irisse-b1-os-tno-0001-sin system security tn, v.0.4," 2016.

[37] ICAO, "Aeronautical Telecommunications, Volume III Communication Systems, Second Edition - Annex 10 to the Convention on International Civil Aviation," ICAO, Tech. Rep., 2007.

[38] ICAO, "Security: Annex 17 to the Convention on International Civil Aviation : Safeguarding International Civil Aviation Against Acts of Unlawful Interference," ICAO, Tech. Rep., 2011.

[39] The Commission Of The European Communities, "COMMISSION REGULATION (EC) No 29/2009 of 16 January 2009 laying down requirements on data link services for the single European sky," European Commission, Tech. Rep., 2009.

[40] ——, "COMMISSION IMPLEMENTING REGULATION (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010," European Commission, Tech. Rep., 2011.

[41] M. B. Line, O. Nordland, L. Røstad, and I. A. Tøndel, "Safety vs security?" in *PSAM conference, New Orleans, USA*, 2006.

[42] "ISO/IEC 27001:2013 information technology - security techniques - information security management systems - requirements."

[43] RTCA, "Do-356 airworthiness security methods and considerations," 2014.

[44] "Official journal of the europen union. regulation (ec) no 216/2008 of the european parliament and of the council of 20 february 2008 on common rules in the field of civil aviation and establishing a european aviation safety agency, and repealing council directive 91/670/eec, regulation (ec) no 1592/2002 and directive 2004/36/ec. 19.3.2008."