

Received September 4, 2021, accepted October 8, 2021, date of publication October 18, 2021, date of current version October 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3121230

# Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment

AHMED ABDELWAHAB ELMARADY<sup>1</sup> AND KAMEL RAHOUMA<sup>1,2</sup>

<sup>1</sup>Faculty of Engineering, Minia University, Minya 61519, Egypt

<sup>2</sup>Department of Computer Science, Nahda University in Beni Suef, Beni Suef 62511, Egypt

Corresponding author: Ahmed Abdelwahab Elmarady (ahmedabdelwahab02@yahoo.com)


**ABSTRACT** In addition to the importance of safety in civil aviation, the significance of cybersecurity in the aviation sector cannot be ignored, and this fact has often been highlighted owing to frequent cyber-attacks that denigrate victim(s) and also lead to political and economic controversies. Cybersecurity has recently received a major boost, with the shift of air navigation facilities from analog ground-based systems to digital space-based systems to accommodate the tremendous growth in air traffic density. Furthermore, most air navigation facilities have open designs that tend to overlook security concerns. In this regard, identifying a systematic methodology for aviation cybersecurity risk assessment is a key element in the identification of potential threats, and assessment of their likelihood and risk levels, whereby risks can be reduced to tolerable levels through appropriate mitigation measures. Existing review articles have not addressed cybersecurity in all the various aviation systems, and have not considered a systematic methodology for aviation cybersecurity risk assessment. This paper therefore presents a systematic qualitative and quantitative cybersecurity risk assessment methodology for legacy and next-generation critical infrastructure in aviation systems, such as air-ground communication, radio navigation aids, aeronautical surveillance, and system-wide information management (SWIM). Our analysis shows that the communication, navigation, and surveillance systems with the highest risk levels are very-high frequency voice communication, satellite-based navigation, and automatic dependent surveillance-broadcast, respectively, while those with the lowest risk levels are controller-pilot data link communication, ground-based radio navigation aids, and secondary surveillance radar, respectively. Furthermore, the risk level of potential cyber-attacks in SWIM is medium.

**INDEX TERMS** Aeronautical communication systems, aeronautical surveillance systems, air navigation systems, cybersecurity, cybersecurity risk assessment, cyber resilience, radio navigation aids, system-wide information management (SWIM).

## I. INTRODUCTION

The aviation sector is one of the fast growing sectors in the world, with an annual passenger growth of approximately 4.2 % in 2019 [1]. Owing to the rapid growth of airspace users worldwide, the management of air traffic has become increasingly important. Such a significant increase in air traffic density necessitates enhancement in the capabilities of critical infrastructure in communication, navigation aids, aeronautical surveillance, and networking. A typical challenge in facilitating such tremendous growth in air-ground

communication involves increased workloads on the air traffic controller (ATC) in terms of handling more flights on the same frequency channel, which necessitates using data link communication as opposed to legacy analog voice communication. This decreases the workload on the ATC in that more information is sent at once, and repeated requests are avoided. Another challenge is to decrease the minimum separation between aircraft, which requires precise positioning. Therefore, aeronautical surveillance systems and navigation aids need to be more precise [2], [3]. Furthermore, to address the increase in air traffic density, the dissemination and exchange of information among various air navigation facilities need to be globally transparent, reliable, and timely [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Christian Esposito .



**TABLE 1.** Comparison of our study with existing surveys regarding the discussion of cybersecurity in civil aviation.

Review paper	Addressing cybersecurity in communication systems	Addressing cybersecurity in navigation systems	Addressing cybersecurity in surveillance systems	Addressing cybersecurity in SWIM	Consideration of cybersecurity risk assessment methodology
[16]	No	No	ADS-B only	Yes	No
[21]	CPDLC and ACARS only	GPS navigation only	ADS-B only	No	No
[10]	VDL2 only	GBAS only	SSR only	No	No
[20]	VHF, CPDLC, and ACARS	No	SSR, MLAT, ADS-B	No	No
[19]	Yes	Yes	Yes	No	No; however, it collects experience from international aviation experts to assess the overall likelihood and impacts of potential threats
Our review paper	Yes	Yes	Yes	Yes	Yes

potential cyber-attacks of ADS-B and SWIM. Unfortunately, that study did not provide a mean for cybersecurity risk assessment for those systems, including assessments of the likelihood of threats, their impacts, and risk levels. Furthermore, it did not identify potential threats related to other communication, navigation, and surveillance systems. The authors of [21] addressed cybersecurity in CPDLC, the Aircraft Communication Addressing and Reporting System (ACARS), GPS, and ADS-B, but did not address cybersecurity in other air navigation systems, such as VHF voice communication, the ground-based augmentation systems (GBAS), satellite-based augmentation system (SBAS), SSR, and SWIM. Similar to [16], the aforementioned review article did not provide a cybersecurity risk assessment for the systems presented. On the other hand, the authors of [10] addressed radio frequency interference, such as jamming and spoofing threats, in SSR, GBAS, and VHF data link mode 2 (VDL2). Unfortunately, that review article did not cover cybersecurity in other communication, navigation, surveillance, and networking systems, and it also did not provide a cybersecurity risk assessment. Likewise, the authors of [20] addressed potential cyber-attacks in various communication and surveillance systems; however, they did not address cybersecurity in SWIM and radio navigation aids, and they also did not address cybersecurity risk assessment for the presented systems. To provide cybersecurity risk assessment, the authors of [19] conducted a survey of aviation experts regarding air navigation technologies that have the largest impact on aviation safety and awareness of aviation stakeholders of security issues in systems that utilize wireless radio signals. In that study, the authors surveyed experts from air navigation service providers, ATC, air traffic safety electronics personnel, pilots, and airlines. Unfortunately, as in the case of the previously mentioned review studies, the aforementioned review study also did not consider threats related to the SWIM. Furthermore, it did not involve assessment of cybersecurity risk through a systematic methodology that

can be continuously applied with the ongoing technology upgrades in aviation systems. Additionally, it addresses the overall likelihood and impact of potential cyber-attacks for various air navigation systems, rather than assessing the likelihood and impact of each individual threat. Although these are dependent on the attack scenarios, assessing the general likelihood, impact, and risk levels for aviation systems is not reasonable. For example, the likelihood and impact of jamming attacks in VHF voice communication differ greatly depending on whether the attacker jams one frequency channel or all operating aviation frequencies in the airport, on the type of services attacked (tower, approach, or en-route), and on the availability of backup frequencies. The aforementioned review articles did not address all air navigation systems and did not provide a continuous systematic and analytical methodology for cybersecurity risk assessment. Therefore, in our paper, we propose to mitigate these challenges and provide a qualitative and quantitative methodology of cybersecurity risk assessment of various critical air navigation systems, including communication, navigation, surveillance, and networking systems. In our proposed methodology, we evaluate risk levels by identifying potential cyber-threats that could have a negative impact on aviation systems, their likelihood, and the possible impact on aviation operations, infrastructure, and other areas. Furthermore, we analyze the operational concept of various air navigation systems, and thereby identify potential cyber-attacks. Additionally, we describe general and specific mitigation measures for these threats. Table 1 summarizes a comparison between our study and those documented in other related review articles [10], [16], [19]–[21]. On application of our proposed cybersecurity risk assessment methodology, the communication system with the threat of highest risk level is determined to be VHF voice communication, while that with the lowest risk level is CPDLC. In the navigation domain, the radio navigation aid with the threat of highest risk level is satellite-based navigation, while that with the

lowest is the traditional ground-based navigation aid, ILS. The surveillance, the surveillance system with the threat of highest risk level is ADS-B, while that with the lowest is SSR. Moreover, the risk level of potential cyber-attacks in SWIM is medium. The results of our study agree with results of the survey mentioned in ref. [19] that the communication, navigation, and surveillance systems with the lowest trustworthiness levels are VHF, satellite-based navigation, and ADS-B, respectively, while those with the highest trustworthiness levels are CPDLC, ground-based radio navigation aids, and SSR, respectively, while they differ in the values of the risk levels. In general, the mitigation of cyber-attacks on civil aviation ecosystems and the employment of cyber-resilient aviation systems are based on three main pillars: capacity building, procedures, and systems [18]. Capacity building and training are crucial elements for mitigating cyber-attacks through raising of awareness and publishing of print materials as well as conduction of training courses, tabletop exercises, simulations, and workshops on cybersecurity issues. At the procedural level, effective international, regional, and national legislation and regulations on cybersecurity for civil aviation should be in place to protect civil aviation and provide the foundations of a cyber-resilient aviation system. Furthermore, guidance material on the urgency and concept of cybersecurity, potential cyber-attacks and their consequences, and possible mitigation techniques should be prepared and published. Additionally, existing contingency plans should include cyber-attack scenarios. At the system level, cybersecurity should not only be considered in the design of new aviation systems but also be implemented via periodic upgrades and maintenance of existing systems, to realize the concept of “security by design”. The main contributions of this study are as follows:

- Comparison between our study and those documented in other related review articles.
- Provision of a systematic cybersecurity risk assessment to identify potential threats in civil aviation systems, assess the likelihood of the threats and their impacts, and also assess the risk levels.
- Description of the operational concept and vulnerabilities of various critical aviation systems, including communication, navigation, surveillance, and networking, and subsequent identification of potential threats on this basis.
- Assessment of the likelihood of individual threats and their impacts followed by assessment of the risk levels.
- Identification of general and specific mitigation measures for potential cyber-attacks in various communication, navigation, surveillance, and networking systems.

The remainder of the paper is organized as follows: in Section II, we present our proposed methodology for aviation cybersecurity risk assessment, and in Section III, we describe our examination of various air-ground communication systems. In Section IV, we present our examination of navigation aids, and in Section V, we describe our examination of aeronautical surveillance systems. In Section VI, we discuss

SWIM and the relevant cybersecurity issues of each aviation system, as well as the application of our proposed cybersecurity risk assessment methodology. Finally, we conclude the paper in Section VII.

## II. CYBERSECURITY RISK ASSESSMENT METHODOLOGY

Cybersecurity risk management is an ongoing process of risk assessment and risk mitigation [22]–[26] to be planned and implemented in the aviation system to mitigate the negative impacts of cyber risks on aviation safety and other impacts on the economy and efficiency of aviation systems. In this section, we propose a qualitative and quantitative methodology for cybersecurity risk assessment, which is a key component of cybersecurity risk management. Cybersecurity risk assessment is a continuous analytical and systematic process to evaluate risk levels via the identification of potential cyber threats that have a negative impact on aviation systems, their likelihood, and their possible impacts on aviation operations, infrastructure, and other impacts. The entire process of risk assessment can be summarized as follows:

- Identification of the scope of systems that need to be protected. In this step, potential threats are identified by understanding the various air navigation systems (communication, navigation, surveillance, and networking), defining the boundary of the aviation systems to be assessed (system components, operating environment, interrelations to third parties), and developing a description of the various air navigation systems.
- Identification of potential cyber-attack scenarios that could cause harm to the aviation system either directly or indirectly. Such threats can affect the integrity, confidentiality, and availability of various air navigation services.
- Determination of the likelihood or probability of attacks being attempted, based on various factors including the capability and intentions of attackers, without considering current security measures. We defined a certain factors to estimate the likelihood of threats, such as required knowledge or expertise, historical data of occurrence of such threats, cost and accessibility of the tools used to conduct such attacks.
- Determination of the worst-case scenario impact of threats in aviation safety, efficiency/effectiveness, economic/financial, political, and reputation/public confidence, which depends on the nature and scale of the consequences of these cyber-attacks.
- Assessment of the risk profile or risk level using the results of the likelihood, vulnerability assessments, and impact of threats. The purpose of assessing the risk is to develop a comprehensive risk picture for potential attacks on air navigation systems.

To obtain a numeric value of the risk level of various aviation systems against specific threats, we follow the ICAO methodology of security risk assessment [27], which rates likelihood and impact on a five-point scale from high to low. The descriptions of the ratings of likelihood and impact are presented in tables 2 and 3, respectively. The following

**TABLE 2.** Description of categories of likelihood.

Scale	Likelihood rating	Cost of tools used in attack	Accessibility of tools used in attack	Frequency of occurrence of past similar attacks	Required expertise to conduct attack
5	High	Less than \$1000	Easily accessible	At least once every two weeks	Basic knowledge
4	Medium- High	Less than \$5000	Available but not so easy	At least once every three months	Substantial basic information is required
3	Medium	Less than \$10000	Available with some conditions	Once every three months to a year	Advanced training and knowledge are required
2	Medium-low	Less than \$100000	Restricted access	Once every one to three years	Advanced knowledge and experience are required
1	Low	More than \$100000	Highly restricted access	Once every three years or more	Advanced and complex knowledge and experience are required

**TABLE 3.** Description of various categories of impact.

Scale	Impact rating	Impact on operations	Impact on finance	Impact on reputation
5	High	Serious impact where no operational services can be provided for an extended time period	Serious impact where recovery of such impact requires major support, e.g., governmental support	The reputation cannot be recovered with stakeholders and the organization/company may not continue in its current form
4	Medium- High	Major impact where a majority of operational services cannot be provided for some time	Major impact where recovery of such impact requires approval from the board level	The reputation can be affected on capability to provide function services by the majority of the stakeholders
3	Medium	Moderate impact where some operational services cannot be provided	Moderate impact where recovery of such impact requires upper management approval for response.	The reputation can be affected on organization/company services and activities by a key stakeholder.
2	Medium-low	Minor impact where some operational services are degraded	Moderate impact where recovery of such impact requires delegated approval for response	The reputation can be affected by the complaints of a key stakeholder on organization/company service and activities
1	Low	Insignificant impact where operational services can be provided as usual	Insignificant impact where recovery of such impact can be managed within business unit /section budget	The reputation can be affected by the isolated complaints of individual stakeholder

formula is used to obtain a numeric value of the risk for each asset to a specific threat:

$$r = L \times I \quad (1)$$

where  $r$  is the risk level of each specific threat, ranging from 1 to 25, and  $L$  and  $I$  are the 1-5 scale of the likelihood and the impact rating of the threat, respectively. Its necessary to covert the numeric value of risk level,  $r$ , calculated above into a qualitative term,  $R$ , to assess cybersecurity risk tolerability, and thereby apply mitigation and control measures when required. We therefore follow ICAO methodology of the safety and security risk assessment matrix [28], [29] which rates numeric values of risk level into three different categories: acceptable, tolerable, and intolerable. For an acceptable risk level, no further risk mitigation and control measures are required, while for a tolerable risk level, the risk level can be tolerated based on some risk mitigation measures. On the other hand, for an intolerable risk level, the cybersecurity risk index of the consequences is unacceptable, and immediate actions should be taken to mitigate the risk and reduce the cybersecurity risk index to a tolerable level.

The following formula is used to covert numeric value of risk level,  $r$ , into a qualitative risk index,  $R$ :

$$R = \begin{cases} \text{intolerable}, & r \geq 15 \\ \text{tolerable}, & 15 > r \geq 5 \\ \text{acceptable}, & r < 5 \end{cases} \quad (2)$$

Table 4 illustrates the cybersecurity risk matrix in which the risk index with acceptable levels is shown in light green, while that with tolerable levels is shown in orange and intolerable is shown in red. Table 5 shows the conversion of risk level,  $r$ , into an equivalent five-point scale. Fig. 2 shows the overall cybersecurity risk assessment. Algorithm 1 shows overview of the cybersecurity risk assessment.

### III. COMMUNICATION

Air-ground communication is one of the most crucial air navigation services that must be maintained to ensure the safety of flights. Such radio communication systems are used for communication between the pilot and ATC to ensure that the aircraft flies along the prescribed airways. These systems are also important for pilots as they are used as a medium to

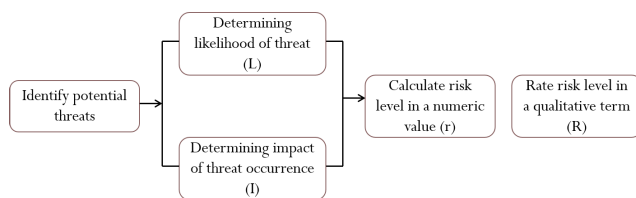


**TABLE 4.** Cybersecurity risk matrix.

Risk level ( $r$ )	Impact ( $I$ )				
Likelihood ( $L$ )	Low	Medium-Low	Medium	Medium-High	High
Low	1	2	3	4	5
Medium-Low	2	4	6	8	10
Medium	3	6	9	12	15
Medium-High	4	8	12	16	20
High	5	10	15	20	25

**TABLE 5.** Conversion of risk level into a five-point scale.

Risk level ( $r$ )	Tolerability of risk ( $R$ )	Five-point scale of risk level
$r \geq 20$	intolerable	5
$20 > r \geq 15$	intolerable	4
$15 > r \geq 10$	tolerable	3
$10 > r \geq 5$	tolerable	2
$r < 5$	acceptable	1

**FIGURE 2.** Proposed cybersecurity risk assessment process.

provide vital ATC information regarding aircraft clearance, adequate aircraft separation, weather bulletins, and the sharing of relevant flight-related data between the control tower and pilots [20], [30], [31]. In addition, other non-ATC-related information can also be transmitted for safe operations, such as flight planning, crew assignment, maintenance, airport ground handling, weather information, and communication between the aircraft and the airline operator. There are many communication protocols used, such as VHF voice [32], CPDLC [5], the ACARS [33], aeronautical mobile airport communication system (AeroMACS) [34], and L-band digital aeronautical communications system (L-DACS) [35]. Although AeroMACS and L-DACS are approved ICAO aeronautical communication protocols, they are not widely used worldwide and are not covered in this paper. Next, we briefly describe common communication protocols and their relevant cybersecurity issues.

## A. VERY-HIGH FREQUENCY VOICE COMMUNICATION

### 1) OVERVIEW OF VERY-HIGH FREQUENCY VOICE COMMUNICATION

VHF air-ground voice communication systems use amplitude-modulated (AM) carriers and operate in the frequency band

### Algorithm 1 Algorithm for Cybersecurity Risk Assessment

- Input:** descriptions of the ratings of  $L$  and  $I$  (tables 2 and 3), cybersecurity risk matrix (table 4), converting the risk level to a five point scale (table 5)
- identify the asset to be protected
- identify potential cyber-attack scenarios
- for**  $\forall$  scenario **do**
- determine the likelihood of occurrence of this cyber-attack using table 2
- determine the impact of occurrence of this cyber-attack scenario using table 3
- calculate the risk level in a numeric value ( $r$ ), given  $L$  and  $I$ , using eq. (1)
- categorize the risk level  $r$  into  $R$  (acceptable, tolerable, or intolerable) using eq. (2)
- convert the risk level from a numeric value to a five point scale using table 5
- end for**

of 117.975-137 MHz with a channel spacing of 25 or 8.33 kHz [32]. VHF ground stations transmit with an output power higher than that of relevant airborne systems to ensure sufficient radio coverage, depending on the operational functions [9]. Table 6 summarizes the characteristics of VHF voice communication along with other common aeronautical communication techniques.

### 2) CYBERSECURITY IN VERY-HIGH FREQUENCY VOICE COMMUNICATION

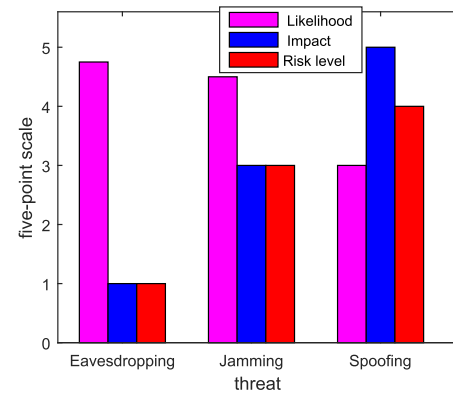
VHF frequencies used for aeronautical communication are standardized and known frequencies that are publicly available in Aeronautical Information Publications (AIP). Because VHF radio communication is not encrypted, conversations over VHF are vulnerable to eavesdropping [9]. The characteristics of analog radio transmission with known frequencies make them susceptible to external interference from other unlicensed intentional or unintentional (unauthorized) transmissions. In the case of an unintentional interference, the VHF voice originates from the use of VHF frequencies by unauthorized persons without prior approval from the national authorities, whereas in the case of intentional interference, the attacker intentionally jams the VHF voice communications. Furthermore, spoofing attacks are those in which unauthorized instructions are maliciously broadcast to aircraft, leading to untoward incidents or worse, devastating accidents. Therefore, interference in VHF voice communication can lead to a disruptions in air navigation services. Table 7 summarizes the various potential cyber-attacks on VHF voice communication as well as other common aeronautical communication techniques. Fig. 3 shows an assessment of the likelihood of eavesdropping, jamming, and spoofing attacks on VHF voice communication systems, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology

**TABLE 6. Comparison among various air-ground communication protocols.**

Communication protocol	Usage	Signal	Type	Frequency band	Link layer used	Standard references
VHF voice	Communication between ground and aircraft for ATC instructions and other information	Analog	Broadcast	117.975-137 MHz	VHF	Annex 10 vol. 3 [32], ICAO Doc. 9718 [6]
CPDLC	Communication between ground and aircraft for ATC and other information	Digital	Selective	VDL2: 136.975 common signaling channel	HFDL, VDL, SATCOM	Annex 10 vol. 3 [32], ICAO Doc. 10037 [5]
ACARS	Communication with aircraft for position, weather, fuel and engine information, delays, dispatch, operation, maintenance, and other information	Digital	Broadcast	VDL2: 136.975 common signaling channel	Plain old VHF, HFDL, VDL, SATCOM	ARINC 620 standard [33]

**TABLE 7. Potential cyber threats in various air-ground communication protocols.**

Communication protocol	Threat type / attack scenario
VHF voice	Eavesdropping
	Jamming (unintentional radio interference due to use of unlicensed frequencies)
	Jamming (unauthorized access to block the VHF frequencies)
CPDLC	Spoofing (unauthorized access to send fake instructions between ATC and pilot)
	Eavesdropping (listening to the data traffic messages)
	Jamming (Channel blocking)
	Flooding (transmitting multiple packets of CPDLC data to the same receiving entity)
	Injection (sending, possibly faulty, unauthorized messages)
	Alteration (modification of message content)
ACARS	Masquerading (attacker impersonates an authorized user whether ghost aircraft or ATC)
	ACARS weight/ balance update and the ACARS flight plan update events

**FIGURE 3. Illustration of cybersecurity risk assessment for VHF voice communication.**

described in Section II. As shown in Fig. 3, an eavesdropping attack is judged to be very likely owing to the capability of attackers and the lack of security algorithms; however the impact on aviation safety is low. Therefore, the risk level is acceptable. Furthermore, a jamming attack is likely to occur owing to the capability of attackers, in terms of accessibility and low costs of jamming devices, while its impact on aviation safety is of a medium level; therefore, the risk level is tolerable. A spoofing attack is less likely to occur but its impact is the highest on aviation safety; therefore, the risk level is intolerable. The impact of jamming and spoofing attacks depends on the attack scenarios assumed, such as whether the attack affects only one specific communication frequency or all operating frequencies in the airport. In the two scenarios assumed herein, we assume that the jamming and spoofing attacks affect only one specific operating communication frequency, while for other scenarios, the likelihood, the impact

and the risk level will greatly differ. Recall that for these three threats, attackers need to know the published operating frequencies, which differ from one airport to another. Furthermore, for an eavesdropping attack, the attacker only receives a wireless signal, while for jamming, the attacker transmits a wireless signal to block communication channels. Additionally, for a spoofing attack, the attacker transmits illegal instructions to the pilot. There are several procedures used to mitigate the vulnerabilities in VHF voice communication, such as issuing regulations/obligations regarding the use of VHF frequencies at the domestic and international levels, and proper frequency management for new and current frequency assignments. Furthermore, back-up frequencies can be used when interference is detected over the main assigned frequencies [6].

## B. CONTROLLER-PILOT DATA LINK COMMUNICATION

### 1) OVERVIEW OF CPDLC

One of the major difficulties faced in voice radio communications is that all pilots handled by a particular controller are tuned to the same frequency. A large number of flights communicating with the same ATC will lead to congestion of VHF voice channels, leading to a higher probability of misunderstanding and repeated messages [9], [36]. In other words, VHF voice communications cannot meet the communication

requirements of increased capacity. CPDLC is an air/ground data link communication protocol that achieves safer and more efficient ATM. Hence, it is capable of functioning with increased airspace capacity and reducing stress on busy VHF frequencies by transmitting clear messages that prevent any misunderstandings [5], [11]. Furthermore, CPDLC improves communication capabilities by reducing VHF voice channel congestion and enabling the use of CPDLC-related automation [5]. Depending on the specifications of the CPDLC system used, additional features of CPDLC are also available, such as supporting the possibility of printing messages from the flight crew and the capability to store messages and retrieve them when required. In addition, it can also reduce flight crew and ATC input errors (and subsequent workload) by transmitting automatic flight-related reports and supporting automatic updates of flight plans.

## 2) CYBERSECURITY IN CPDLC

However, CPDLCs, along with other open and unencrypted communication systems, are inherently insecure because they do not have built-in security protocols, and thus provide unauthenticated and unencrypted data links. Therefore, CPDLCs are prone to man-in-the-middle attacks, such as eavesdropping and active attacks [11], [14], [15]. The authors of [11] listed a number of possible attacks against CPDLC, such as eavesdropping (listening to the data traffic messages), jamming (channel blocking), flooding (transmitting multiple packets of CPDLC data to the same receiving entity), injection (sending possibly faulty, unauthorized messages), alteration (modification of message content), and masquerading (where the attacker impersonates an authorized user, which can be a ghost aircraft or the ATC). To enhance the security of CPDLC, the authors discussed some techniques to secure CPDLC, such as protected aircraft communications addressing and reporting systems that use Aeronautical Radio, Incorporated (ARINC) 823 [37], elliptical curve cryptography, and the host identify protocol. Fig. 4 shows an assessment of the likelihood of eavesdropping, jamming, and spoofing (flooding, injection alteration, masquerading) threats of the CPDLC communication system, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 4, eavesdropping, jamming, and spoofing threats are less likely to occur than in the case of analog VHF voice communication because of the specific equipment, complex knowledge, and complex experience required to conduct such attacks. Therefore, their impact is of a medium-to-high level on aviation safety owing to the availability of traditional VHF voice communication systems where CPDLC is not yet mandated by all regions or states; hence, the risk levels are less than those in VHF communication systems. In other words, risk levels range from acceptable to tolerable levels. Recall that, unlike in VHF voice communication, where analog communication signals are broadcasted, data link communication signals are sent selectively in CPDLC. Similar to that for VHF

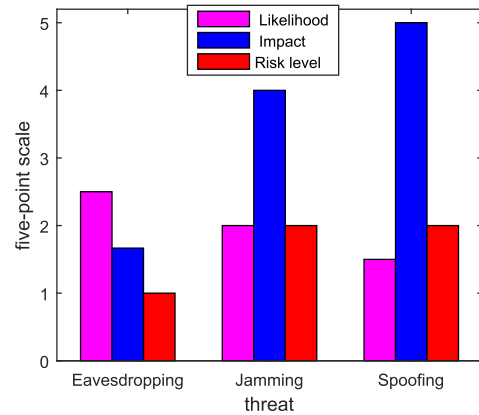


FIGURE 4. Illustration of cybersecurity risk assessment for CPDLC.

voice communication, the impact of jamming and spoofing attacks highly depends on the attack scenarios assumed. In the two scenarios presented herein, we assume that the jamming and spoofing attacks affect en-route communication services, while for other scenarios such as attacks on tower and approach communication services, the likelihood, impact, and risk levels will differ.

## C. AIRCRAFT COMMUNICATION ADDRESSING AND REPORTING SYSTEM

### 1) OVERVIEW OF ACARS

The ACARS is a character-based data link described in ARINC standard 618. It is used to provide data link communication between aircraft and aircraft operators via service providers subscribing to the aircraft operator. It uses the American Standard Code for Information Interchange (ASCII) character set and functions in a manner similar to that of the Short Message Service (SMS) [38]. Examples of data services provided by the ACARS include weather information, flight plans, and information on the performance of aircraft components such as engines [39]. Furthermore, the flight crew can use the ACARS for communication with the aircraft flight operation center and the ATC. The ACARS uses three different types of data links, depending on the aircraft equipment and required coverage: plain old VHF or VHF data link (VDL) [40], SATCOM (Inmarsat, Iridium), and a high-frequency data link (HFDL). Typically, VHF is used for populated land areas, SATCOM extends coverage to oceanic areas, and HF provides coverage worldwide. The ACARS message content is structured according to the ARINC 620-8 standard [33].

### 2) CYBERSECURITY IN ACARS

As the ACARS was not designed with in-built security protocols by default [40], the majority of ACARS traffic can be easily intercepted using inexpensive SDRs that can be obtained from the Internet (e.g., ACARS decoders [41]). In 2013, Hugo Teso, a security researcher and commercial



pilot, used second-hand hardware to illustrate the potential of remotely exploiting a flight management system [42] by attacking the ACARS. As shown by Teso, the attack code using an Android application can take full control of flight systems and the pilot's displays, including the modification of almost everything related to the navigation of the plane. Teso used the ADS-B system to update ground ATC with the aircraft's position, velocity, and other information. As illustrated in Section V, there are no security protocols in ADS-B; therefore, it can be used to passively eavesdrop on aircraft communications and actively interrupt broadcasts or feed in misleading information. Recently, [43] analyzed the injection of external ACARS messages into a flight management system, both theoretically and practically. Furthermore, the Impact Assessment of Cybersecurity Threats research project was developed by the European Union Aviation Safety Agency (EASA) to address security attacks on the safety of flight operations with a focus on several crucial aircraft systems, including ACARS [44]. In this research project, two scenarios related to ACARS were discussed: the ACARS weight and balance update, and the ACARS flight plan update events. In the first scenario, an attacker on the ground was assumed to have the ACARS addresses of multiple aircraft and send incorrect load sheet data via ACARS to the aircraft. On board the aircraft, the data are received either via a print-out or directly in the flight management system. In the worst-case scenario, the pilot loses the ability to pitch down the aircraft, which could result in uncontrollable aircraft behavior. Although the attack occurs during the preflight phase, the result manifests itself during the takeoff phase. In the second scenario, the ACARS flight plan update event, an attacker on the ground was assumed to have the ACARS addresses of multiple aircraft and proceeded to transmit incorrect flight plan data to aircraft. The attacker would need to know the departure and arrival airports and have an idea of the route used in order to tailor the attack to the actual flight path; however, this data can be easily obtained through observation. The pilots would accept the new flight plan and deviate laterally from their desired paths. Fig. 5 shows the assessment of the likelihood of the ACARS weight and balance update and the ACARS flight plan update threats, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 5, these two threats are less likely to occur than attacks on VHF voice communication are, because of the specific equipment, complex knowledge, and experience required to conduct such attacks, while their impact on aviation safety is high. Therefore, the risk level is acceptable. Recall that CPDLC and ACARS use data link communication. Furthermore, ACARS uses multi-link communication such as plain old VHF, VDL, HF DL, or SATCOM. Although the ACARS has no security system included in its original standard, add-on systems are available, such as the ARINC 823 standard and ACARS message security (AMS) [37], which offer enhanced security through a number of common cryptographic algorithms

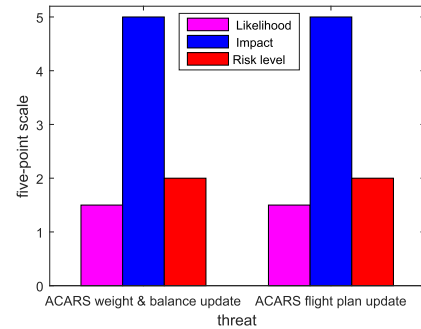


FIGURE 5. Illustration of cybersecurity risk assessment for ACARS.

and tools and provide message authentication, integrity, and confidentiality protection mechanisms, using modern cryptographic methods [45]. Despite the existence of ACARS security protocols, deployment is not implemented on a large scale. Furthermore, these systems typically require extra expenditure for aircraft operators [46].

#### IV. NAVIGATION

Radio navigation aids are needed for aircraft positioning and guidance in various phases of flights, such as landing, approach, and en-route, to ensure that the aircraft follows the prescribed dedicated airways. Therefore, radio navigation aids are the main components of air navigation facilities, along with communication and surveillance systems [47]. There are many radio navigation systems from legacy terrestrial navigation aids, such as the instrument landing system (ILS), distance measuring equipment (DME), VHF omnidirectional radio range (VOR), and satellite-based navigation aids, including the GNSS. Next, we briefly explain the operational concepts of various navigation aids and relevant cybersecurity issues.

##### A. GLOBAL NAVIGATION SATELLITE SYSTEM

The GNSS represents a new era of navigation that uses space-based navigation, rather than conventional terrestrial radio navigation aids. Ground-based navigation aids have many limitations, such as the cost of installation and periodic requirement for flight inspection [48]. Furthermore, the clearance area required around ground-based radio navigation aids restricts the heights of nearby buildings.

##### 1) OVERVIEW OF GLOBAL NAVIGATION SATELLITE SYSTEM

GNSS systems determine the position of aircraft and provide other information based on satellite broadcasting signals containing timing information and data messages [49], [50]. GNSS receivers deployed on board the aircraft receive the broadcast information and measure the signal propagation time from each satellite to estimate the range between the GNSS receiver and each satellite. The GNSS receiver can then estimate the 3D position of the aircraft on a globally standardized coordinate system (WGS-84), with signals

**TABLE 8. Comparison among various radio navigation aids.**

Navigation system	Usage	Type	Frequency band	Standard references
GNSS	Determine 3D position and timing	Satellites	L1: 1575.42 MHz L2: 1 227.6 MHz	Annex 10 vol.1 [48], Doc. 9849 [3]
ILS	Localizer: determine course guidance to the runway centerline Glide slope: provides the pilot with information about the aircraft's vertical deviation of the ideal approach to the runway	Ground	Localizer: 108 to 111.975 MHz Glide slope: 328.6 to 335.4 MHz	Annex 10 vol.1 [48], Doc. 8071 vol. 1 [7]
VOR	Determine bearing angle	Ground	108 to 117.975 MHz	Annex 10 vol.1 [48], Doc. 8071 vol. 1 [7]
DME	Determine slant range distance between aircraft and ground antenna	Ground	962-1213 MHz	Annex 10 vol.1 [48], Doc. 8071 vol. 1 [7]

received from a minimum of four satellites. Unlike in the case of ground-based radio navigation aids, by using GNSS, aircraft can continuously update their position and can fly on any desired flight path without any restrictions imposed by terrestrial legacy navigation aids, such as line-of-sight and radial interception restrictions. Currently, there are several satellite navigation systems that are operated and approved by the ICAO, such as the GPS, GLONASS (Russia), and GALILEO (Europe). The GNSS is therefore a common navigation infrastructure that can globally reap the full benefits of performance-based navigation, especially the required navigation performance owing to the enhanced accuracy level and the absence of limitations imposed by legacy radio navigation aids. Table 8 summarizes the characteristics of space-based navigation, along with other ground-based radio navigation aids. Unfortunately, the positioning accuracy of standard GPS is not high enough for the system to be used in the final approach with vertical guidance, precision approaches, and landing phases of flights, which necessitate more accurate positioning compared to the en-route phase of flights. To improve the navigation accuracy of the GNSS, augmentation of the GNSS signal has been proposed, such as the aircraft-based augmentation system (ABAS), ground-based augmentation system (GBAS), and satellite-based augmentation system (SBAS). The GBAS is a differential navigation system that uses GNSS receivers deployed at known and pre-surveyed locations to estimate and monitor the differential corrections in real time with the received GPS signals, such as satellite and ionospheric errors. Subsequently, the differential corrections are broadcast to the aircraft in the vicinity of an airport via a ground-based VHF data broadcast (VDB). The GBAS can be considered as an alternative to high-cost ILS systems with the additional advantage that it can replace multiple ILSs deployed on multiple runways at airports. Unlike the GBAS, which augments GPS in the vicinity of an airport and broadcasts augmentation signals via VDB, the SBAS is a regional system in which the user (e.g., aircraft or vehicles) receives augmentation information from a satellite. It uses a network of ground reference stations to monitor satellite signals; central stations to process data received from ground reference stations and generate SBAS augmentation signals, and uplink stations to send augmentation messages to geostationary satellites that can

be broadcasted to aircraft. There are four recognized ICAO operational SBAS systems: the Wide Area Augmentation System (WAAS) in North America, the European Geostationary Navigation Overlay Service (EGNOS) in Europe, the GPS-Aided GEO Augmented Navigation (GAGAN) in India, and the multi-functional satellite augmentation system (MSAS) in Japan. Another GNSS augmentation system is the ABAS, which augments and/or integrates the information obtained from GNSS receivers with other navigation information available on board the aircraft. There are two types of ABAS: RAIM, which uses GNSS information exclusively, and aircraft autonomous integrity monitoring (AAIM), which uses on-board sensors (e.g., barometric altimeter, clock or the inertial reference system, IRS) [3]. At least five satellites with good geometry are used to detect a faulty signal and alert the aircrew in RAIM [3]. The major advantage of ABAS is its cost effectiveness, as compared to that of SBAS and GBAS, in that it provides improved service without any expenditure on additional infrastructure being incurred [3].

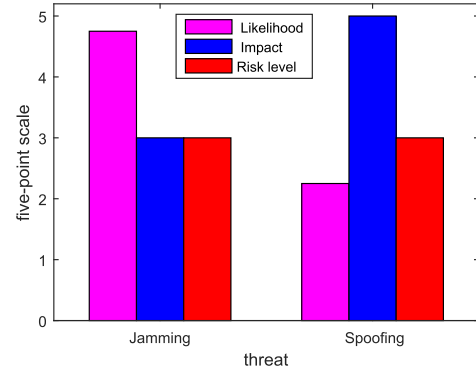
## 2) CYBERSECURITY ISSUES IN GNSS

The GNSS is vulnerable to interference that may affect wide geographic areas, owing to weak signals received from satellites by the GNSS receiver antenna. Furthermore, current GNSS approvals use a standardized single frequency band accompanied by GPS and GLONASS, which subsequently makes it easier to intentionally or unintentionally jam GNSS signals. Moreover, GNSS signals are prone to spoofing and ionospheric effects [49]. There are many sources of unintentional interference in GNSS from both in-band and out-of-band transmitters because of the various electrical devices operating at harmonic frequencies close to those of GNSS, such as harmonics of VHF communications, television stations, some types of radars and military systems, and mobile satellite communications. The GNSS is used in many applications other than those in aviation, such as weather, transportation, vehicle-tracking systems, and agriculture. Therefore, jamming directed at non-aviation users, known as intentional interference, could also affect flight operations. Another type of intentional interference occurs when a jamming device is intentionally used to disrupt air navigation facilities that are dependent on GNSS. These are either using personal privacy device (PPD) radio jammers or intentional aviation

**TABLE 9.** Potential cyber threats in various radio navigation aids.

Navigation Technique	Threat type
Satellite -based navigation	Unintentional interference
	Intentional interference
	Spoofing
ILS	Single-tone attack
	Overshadow attack
VOR	Jamming
	Spoofing

dedicated attacks [51]. The primary way to mitigate unintentional and intentional interference in GNSS is frequency management by establishing and enforcing regulations and laws that govern the use of the frequency spectrum, and carefully assessing assignments for new spectrum allocations. Additionally, next-generation GNSSs will be based on multiple frequencies. This will reduce the likelihood of unintentional interference. Another type of vulnerability in the GNSS is the susceptibility to spoofing, wherein the attacker broadcasts signals resembling GNSS signals, and causes the on-board aircraft avionics to malfunction via provision of erroneous information about the aircraft position as well as faulty guidance. GNSS spoofing is considered less likely to occur than jamming because it is technically much more complex. Table 9 summarizes the various potential cyber-attacks on GNSS and other ground-based radio navigation aids. Spoofing in GNSS can be detected by comparing the position received from the GNSS receiver with that obtained from other systems such as IRS or DME-DME positions, such that pilots can note deviations through normal monitoring of instruments and screens. Furthermore, the ATC can monitor variations between the reported aircraft positions and those illustrated on radar screens on the ground. As mentioned previously, the GBAS, SBAS, and ABAS are GPS-based augmentation systems. Therefore, vulnerabilities in the GNSS can lead to subsequent disruptions in GPS augmentation systems (SBAS, GBAS, and ABAS). The authors of [10] addressed additional weaknesses in the GBAS (rather than vulnerabilities in GNSS signals), such as vulnerabilities in VDB, whereby differential corrections are transmitted to aircraft. Through specific position corrections, aircraft navigation systems can thereby be misled. As an example of actual interference in airports, when the GBAS was first installed, GNSS signal interference was detected at Newark Airport in New Jersey in 2009. After two months of investigation by the Federal Aviation Administration (FAA), the interference was identified to be caused by a passing vehicle with a driver using a freely available PPD [51]. As mentioned before, there are two main types of ABAS: RAIM and AAIM. RAIM (where the attacker can spoof all five satellites used by the RAIM) is more susceptible to cyber-attacks than AAIM is. Thus, the vulnerabilities are the same as those observed in standalone GNSSs [19]. Fig. 6 shows an assessment of the likelihood of jamming (unintentional and intentional interference) and spoofing threats in GNSS, their impact, and risk

**FIGURE 6.** Illustration of cybersecurity risk assessment for GNSS.

levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 6, jamming attacks are very likely to occur owing to the accessibility and low cost of jamming devices, standardized frequencies used, and the reporting of thousands of GPS jamming attacks worldwide. Furthermore, GPS jamming will lead to denial of navigation service, and the relevant impact is medium on aviation safety where traditional ground-based radio navigation aids are still in place in most regions. Therefore, the risk level is tolerable. Additionally, a spoofing attack is less likely to occur owing to the high cost of devices used to conduct such attacks and the complex experience and information required, but the corresponding impact on aviation safety is high. Therefore, the risk level is tolerable. Recall that the impact of GNSS jamming and spoofing attacks highly depend on the attack scenarios assumed, such as the availability of other traditional ground-based radio navigation aids and the flight phase (en-route, approach, landing, etc.) of the affected aircraft. In the two scenarios herein, we assume the availability of traditional ground-based navigation and that jamming and spoofing attacks affect aircraft flying in the en-route phase of flight, while for other scenarios such as GPS jamming and spoofing attacks in the final approach and landing phases of flight, the likelihood, impact, and risk levels will greatly differ.

## B. TERRESTRIAL RADIO NAVIGATION AIDS

Ground-based radio navigation aids are legacy navigation aids, such as ILS, DME, and VOR, that have long been used. Next, we briefly discuss the ground-based radio navigation systems and the relevant potential cyber-attacks.

### 1) OVERVIEW OF GROUND-BASED RADIO NAVIGATION AIDS

ILS is a radio navigation aid that guides aircraft during the approach and landing phases of flight in a precise manner by a combination of horizontal and vertical guidance [7], [48]. The horizontal guidance signal is transmitted from a localizer while the vertical guidance signal is transmitted from a glide slope. ILS uses amplitude modulation: a 90-Hz

and a 150-Hz tone are sent with directional antennas in two lobes. For the localizer, one lobe is slightly directed to the left side of the runway centerline and the other is directed to the right side. Thus, an ILS receiver on board the aircraft not located on or very close to the front course line will receive one of the signals more strongly than the other. Similarly, a glide-slope antenna beside the runway is used to provide vertical guidance. DME is a ground-based radio navigation aid that uses interrogation to allow the aircraft to estimate its slant range distance from the DME ground station by measuring the propagation time delay in the radio signals transmitted between the DME ground station and the aircraft [7], [48]. In DME, an aircraft transmits a random sequence of pulse pairs and the ground DME transponder responds after a fixed delay (typically 50  $\mu$ s) with the same pulse sequence, while the interrogating aircraft searches for this pattern. The distance from the aircraft to the transponder can then be determined. VOR is another ground-based navigation aid that enables aircraft to determine their clockwise bearing from magnetic north, with reference to the VOR reference ground station, by transmitting VHF navigation signals 360° in radial angles, with the carrier radiated in the 108-118 MHz band, and modulation by two 30-Hz signals. Aircraft with a VOR receiver can determine their radial from the VOR ground station via signal phase differences [7], [48]. Owing to the high cost of ground-based radio navigation aids, installation, and periodic flight and ground checks, there is a compelling need to shift to satellite-based radio navigation.

## 2) CYBERSECURITY ISSUES IN GROUND-BASED RADIO NAVIGATION AIDS

Owing to the worldwide standardization of radio navigation aids and the use of wireless equipment, ground-based navigation aids are prone to jamming. Furthermore, owing to the lack of security considerations in the design of such systems, they are also prone to spoofing. The authors of [52] illustrated two possible types of wireless attacks in ILS: overshadow and single-tone attacks. In an overshadow attack, the attacker transmits pre-crafted ILS signals of higher signal strength, thus overpowering the legitimate ILS signals such that the receivers “lock” and process only the strongest received signal. In a single-tone attack, the attacker transmits a single frequency tone signal (either 90 Hz or 150 Hz) at a specific signal strength (lower than the legitimate ILS signal strength) to interfere with and control the deflections of the course deviation indicator needle. The authors assumed the attacker to process the technical details of the ILS, such as the frequencies and modulation index. Furthermore, the capability of an attacker to transmit radio signals in air was assumed. Additionally, in the case of a single tone, the knowledge of the flight’s approach path, aircraft’s manufacturer, and model would allow the attacker to significantly optimize their attack signal. On the other hand, owing to the wireless signal used in VOR, VOR signals in space are prone to potential cyber-attacks, such as jamming and spoofing. As mentioned in [52], there is a possibility of cyber-attacks in ground-based radio

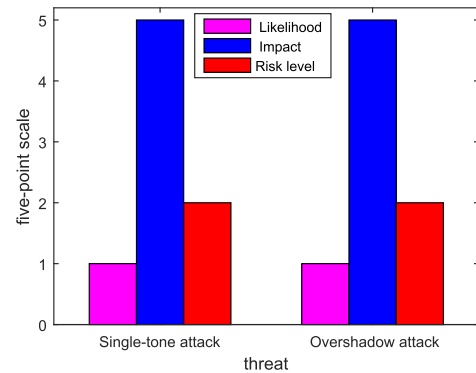


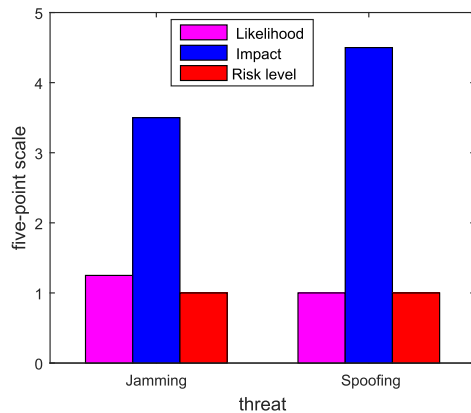
FIGURE 7. Illustration of cybersecurity risk assessment for ILS.

navigation aids; however, the likelihood of these attacks is very low when compared to that in the case of GNSSs, where complex knowledge is required and ground-based radio navigation aids are only dedicated to aviation applications, unlike satellite-based navigation systems. Fig. 7 shows an assessment of the likelihood of single-tone and overshadow attacks, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 7, the likelihood of these two attacks is low due to the complexity of such attacks, inaccessibility, and high cost of attacking devices used while the relevant impact is the highest on aviation safety. Therefore, the risk level is tolerable. Recall that, for these two attack scenarios, the attacker needs to know the published operating frequencies used which differ from one location to another. Fig. 8. shows an assessment of the likelihood of jamming and spoofing attacks of VOR, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 8, the likelihood of jamming and spoofing attacks is low due to the complexity of such attacks, inaccessibility, and high cost of attacking devices used, while the relevant impact on aviation safety is smaller than that in the case of ILS. Unlike ILS, which is considered to be a precision approach, VOR is considered for a non-precision approach and landing. Therefore, the risk level for jamming and spoofing attacks is acceptable. Recall that, for these two attack scenarios, the attacker needs to know the published operating frequencies used, which differ from one location to another.

## V. SURVEILLANCE

Air traffic surveillance plays a crucial role in the safety, efficiency, and demand capacity of airspace by determining the position of the aircraft in real time and periodically tracking it [8], [53], [54]. With accurate surveillance techniques and the ability to track aircraft, the workload on the ATC is reduced, thereby resulting in enhancement overall flight safety via alerts to ATC when the aircraft detects a deviation from its assigned airways or altitudes, or when the predicted future positions of two aircraft indicate an





**FIGURE 8.** Illustration of cybersecurity risk assessment for VOR.

imminent collision. Furthermore, this supports other alerts such as minimum safe altitude warnings, along with dangerous, prohibited, and restricted area warnings. In other words, accurate surveillance techniques enable the use of automated alerting systems called safety nets. Furthermore, accurate surveillance techniques enable a decrease in the minimum separation standard between two or more aircraft, and hence, safely accommodate the increasing demand for air traffic density. Therefore, air traffic surveillance is used in the management of airspace and standard separation distances required between aircraft. Various surveillance technologies have been developed for use in ATC services such as PSR [55], SSR [56], multilateration (MLAT) [57], and ADS [2], [8]. Next, we provide an overview of the various aeronautical surveillance systems and relevant cybersecurity issues.

### A. PRIMARY SURVEILLANCE RADAR

In this section, we briefly describe the operational concept of PSR and the relevant potential cyber-attacks.

#### 1) OVERVIEW OF PSR

PSR is an independent, non-cooperative surveillance, and the first automated surveillance technique, with a very long history [55]. PSR determines the azimuth and slant distance of an aircraft by transmitting a signal and processing the received echo signal. The slant distance between the aircraft and radar antenna is determined by measuring the time taken from the transmission of pulses to the reception of the reflected pulses, while the bearing angle of the aircraft is determined by noting the position of the rotating antenna when the echo pulses are received. Processing of moving targets is only displayed on ATC screens to eliminate the display of unwanted fixed objects on ATC screens, (known as clutter), such as buildings, terrain, and bird flocks. Special processing techniques are used to remove the clutter. The main advantage of PSR is its ability to provide aeronautical surveillance, (aircraft range and azimuth), without requiring a transponder to be equipped on the aircraft. There are many disadvantages of using PSR as the sole aeronautical surveillance, such as lack of target

identification, which requires other systems or procedures to correlate the received reflections with detected flights. Furthermore, PSR requires high transmitting power because signals must travel two-way. Additionally, the performance of PSR depends on the radar cross-section of the aircraft, requires very high cost, and has a low update rate owing to the use of a mechanically rotating antenna. Table 10 summarizes the characteristics of PSR, along with other aeronautical surveillance techniques.

#### 2) CYBERSECURITY ISSUES IN PRIMARY SURVEILLANCE RADAR

PSR determines the azimuth and slant range of the targets without involving data in the transmitted signal. Therefore, the commonly available SDR transmitters cannot be used to inject or modify the message content [19], [20]. Furthermore, the power of the transmitted signal is very high therefore, it is very complicated to jam the PSR signal [58]. Although PSR is still prone to jamming attacks using very high transmitted power, it requires more sophisticated equipment that is mostly available only to the military. Therefore, cybersecurity in PSR is not covered in detail in this study.

### B. SECONDARY SURVEILLANCE RADAR

In this section, we briefly describe the operational concept of SSR and the relevant cybersecurity issues.

#### 1) OVERVIEW OF SECONDARY SURVEILLANCE RADAR

One of the major disadvantages of PSR is the inability to identify aircraft due to the lack of communication between PSR and aircraft equipment. Unlike PSR systems, SSR systems consist of two main elements: radar sensor (ground-based interrogator/receiver) and aircraft transponder [2], [19], [20], [59]. SSR is a cooperative surveillance system in which the ground-based SSR sends interrogation codes to the aircraft at 1030 MHz, and the aircraft transponder replies to the SSR ground receiver at 1090 MHz. This communication link between the ground and transponder, in addition to measuring the distance and azimuth of aircraft, allows aircraft identification, aircraft altitude determination, and relaying of other relevant information depending on its chosen mode. There are three main modes of SSR, denoted as modes A (identification), C (pressure-altitude), and S (selective), whereby more information is provided than in the case of modes A and C, such as aircraft intent. The mode of the aircraft transponder determines the information sent in response to the interrogation. There are additional advantages of using SSR over PSR; for example, SSR requires lower transmitting power than PSR does because of the communication between the SSR ground station and the onboard transponder. Furthermore, the SSR system has a wider coverage range than PSR, which is typically 250 NM from the radar location. Although the cost of SSR is less than that of PSR, on a standalone basis, the cost of SSR is still high. Additionally, SSR has a lower update rate, owing to the use of a mechanically rotating antenna.



**TABLE 10. Comparison among various aeronautical surveillance techniques.**

Surveillance technique	Concept of operation	Information obtained	Signal	Type	frequency band	Classification	update rate	standard references
PSR	Uses echo of radiated electromagnetic waves from rotating antenna	Slant range and azimuth	Analogue	Broadcast	1-2, 2-4 GHz band	Non cooperative, Independent	Low	Document 9924 [8]
SSR	Uses interrogations/replies between SSR ground-sensor and on-board aircraft	Slant range, azimuth, ID, and barometric altitude	Digital	Interrogation	Uplink 1030 MHz Downlink 1090 MHz	Cooperative, Independent	Low	Annex 10 vol. 4 [2], ICAO Document 9684 [59]
MLAT	Aircraft position is mathematically calculated using TDoA from multiple ground sensors	Position in 3 D, identification, velocity, and other information	Digital	Passive WAM, systems do not interrogate the aircraft transponder; Active, in which the system itself interrogates aircraft in the coverage area	Uplink: 1030 MHz Downlink: 1090 MHz	Cooperative, Independent	High	Annex 10 vol. 4 [2], Document 9924 [8]
ADS-B	Aircraft determines its position, velocity and other information and broadcasts it to ground sensors	Position in 3 D, identification, velocity, and other information	Digital	Broadcast	978 , and 1090 MHz	Cooperative, Dependent	High	Annex 10 vol. 4 [2], Document 9924 [8]

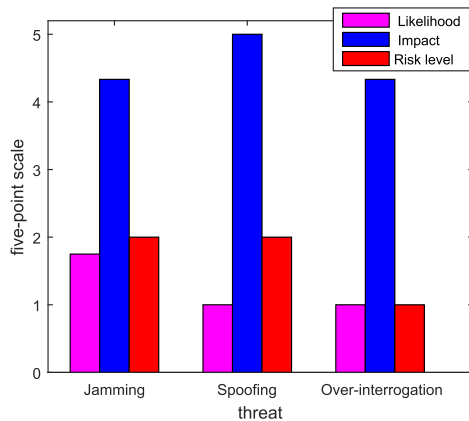
## 2) CYBERSECURITY ISSUES IN SECONDARY SURVEILLANCE RADAR

SSR systems are prone to potential cyber-attacks, such as jamming and spoofing (ghost targets) [10]. Another vulnerability in SSR is that the SSR transponders on board the aircraft can be over-interrogated [8], [10], [20], [60]. This occurs when the number of interrogations at 1030 MHz in their airspace coverage arriving from ground sensors, such as SSRs (civil/military), MLAT/wide-area MLAT (WAM), and test transmitters, exceed the acceptable standard rates pertaining to the minimum operational performance standards. In other words, transponders stop responding to interrogations when the interrogation rate exceeds their design limits. One common real-world example of such a vulnerability is the occurrence of radar loss from ATC area control center screens in central Europe on June 5 and June 10, 2014. This radar loss caused capacity reduction in some of the affected ATC sectors, and therefore delays in some flights. Owing to the impact of such occurrences on aviation safety, EASA was mandated by the Commission to execute a technical investigation and provide recommendations to mitigate and prevent such events from happening in the future. After a detailed investigation, EASA determined the source of the interference, which was due to the fact that some SSR ground installations over-interrogated the on-board aircraft transponders at 1030 MHz at rates beyond the design limits of such on-board aircraft transponders. The authors of [10]

discussed the possibility of a jamming attack in which the attacker transmits high-power signals at the same frequency band of SSR, leading to a DOS in SSR, so that targets disappear from ATC screens. Furthermore, the authors of [10] discussed the possibility of more sophisticated cyber-attacks in which ghost aircraft are inserted on ATC screens by an unauthorized user of SSR such that the attacker can spoof the interrogator with generated signals compliant with SSR standards. Table 11 summarizes the various potential cyber-attacks of SSR and other aeronautical surveillance techniques. Fig. 9 shows an assessment of the likelihood of jamming, spoofing, and over-interrogation attacks in SSR, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 9, the likelihood of these attacks is low owing to the complexity of such attacks, inaccessibility, and high cost of attacking devices used while the relevant impact on aviation safety is high owing to the use of SSR as the main surveillance system for most regions and states. Therefore, risk level ranges from tolerable to acceptable. Recall that SSR uses a mechanically rotating antenna to transmit directional interrogates to on-board aircraft transponder with high transmitting power. One of the possible techniques to mitigate potential spoofing attacks in SSR is the data fusion of SSR and PSR measurements [61]. In this data fusion technique, a consistency check between two different surveillance systems, SSR and

**TABLE 11. Potential cyber threats in various aeronautical surveillance techniques.**

Surveillance technique	Threat type
SSR	Jamming Spoofing Over-interrogation
MLAT	Miss synchronization due to vulnerabilities in GPS
ADS-B	Eavesdropping Jamming Spoofing



**FIGURE 9. Illustration of cybersecurity risk assessment for SSR.**

PSR, would detect SSR replies that are inconsistent with PSR measurements, thus overcoming the vulnerability to virtual ghost aircraft. Furthermore, it can be used to detect jamming attacks by detecting the presence of targets obtained from the PSR.

### C. MULTILATERATION

In this section, we briefly describe the multilateration (MLAT) concept and the relevant cybersecurity issues.

#### 1) OVERVIEW OF MULTILATERATION

MLAT is a cooperative independent surveillance technology that relies on the time difference of arrival (TDoA) principle [2], [19], [54], [57]. In MLAT, several ground sensors receive signals transmitted from an aircraft transponder, and the aircraft position is mathematically calculated using the TDoA principle. In the case of using MLAT, no additional avionics systems are required and an on-board transponder in place is utilized, while on the ground, the receiver sensors and central processing units must be deployed. Unlike PSR and SSR, MLAT does not use a mechanically rotating antenna; therefore, MLAT provides a high update rate. MLAT provides surveillance information, such as aircraft position, altitude and other information that is ultimately displayed on ATC screens. WAM is an MLAT system with a wider coverage that is used in the surveillance of en-route airspace. The positioning accuracy of MLAT is better than that of

traditional radar systems, PSR and SSR, and depends on the number of receivers and their deployment geometry. Furthermore, the installation and ongoing maintenance costs of MLAT/WAM systems are considerably lower than those of legacy radar systems. The MLAT system can be classified into two main types according to the interrogation process: passive and active. In the passive mode, MLAT using the transponder replies to other interrogations to estimate the location of the aircraft, while in the active mode, the system interrogates the aircraft in the coverage area itself [45].

#### 2) CYBERSECURITY IN MULTILATERATION

Unlike dependent surveillance techniques such as ADS-B, MLAT is an independent system that uses the solution of the TDoA set of equations to determine the location of the aircraft. Therefore, even if there is a modification in the message content in the MLAT system between an on-board aircraft transponder and ground sensors, the location of the aircraft is determined using the time taken to receive the messages and not the message content itself, which enhances security. However, MLAT ground receivers should be synchronized with methods such as GPS [3], [62]. Unfortunately, GPS is susceptible to jamming and spoofing attacks, which degrade the aircraft localization accuracy using MLAT, as discussed in Section IV. The authors of [62] introduced the issue of multi-device attacker models in which spoofing attacks on GPS were executed, which can successfully spoof locations within the OpenSky network with sufficient accuracy. The authors have shown that a distributed multi-device attacker model is a realistic threat scenario to MLAT systems using SDRs with GPS synchronization, such that the localization error of the MLAT becomes indistinguishable from the error of legitimate signals. To detect spoofing attacks in MLAT, the authors of [62] proposed using physical-layer features such as frequency-based, Doppler shift, and phase-based methods to detect the attacker locations. Fig. 10 shows an assessment of the likelihood of miss synchronization attack, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 10, the likelihood of this attack is of a medium level while the relevant impact on aviation safety is from medium to high. Therefore, the risk level is tolerable. The likelihood and impact of this attack highly depends on the attack scenarios assumed, e.g., whether the attack affects aircraft flying in the en-route, approach, or landing phases of flights (local area MLAT or wide area MLAT), and whether there are alternative surveillance systems or not. In the addressed scenario herein, we assume that the attack affects wide area MLAT and there are other surveillance systems in place, which is a reasonable scenario in many regions.

### D. AUTOMATIC DEPENDENT SURVEILLANCE

In this section, we briefly describe the operational concept of ADS and its relevant cybersecurity issues.

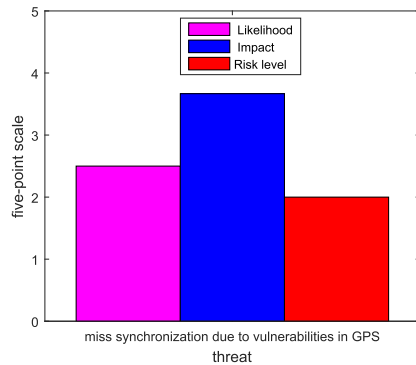


FIGURE 10. Illustration of cybersecurity risk assessment for MLAT.

### 1) OVERVIEW OF AUTOMATIC DEPENDENT SURVEILLANCE

ADS-B [2], [53], [63] is a dependent surveillance system used to periodically determine aircraft position via airborne navigation sensors, (integrated GNSS system and inertial navigation). The ADS-B broadcasted information is transmitted via extended squitter Mode S transponders on board the aircraft. The broadcasted aircraft information, such as identification, position, velocity, and other information is received by ground receivers at 1090 MHz, to be displayed on ATC screens. The update rate of surveillance data occurs twice a second for position and velocity, and once every 5 sec for identification. Therefore, the update surveillance rate for ADS-B is higher than that for legacy radars, PSR, and SSR. The accuracy in determining aircraft position using the ADS-B is much better than using legacy radar systems. Furthermore, ADS-B decreases the cost of surveillance systems by eliminating the high commissioning and ongoing maintenance costs of traditional radar systems. ADS-B broadcasted information can also be received and displayed by other neighboring aircraft that are equipped with ADS-B IN. ADS-B Out is mandated by many regions, such as the US, European, and Australian airspaces. There are two ADS-B data link standards: Universal Access Transceiver, (utilizing the 978 MHz frequency), and 1090 MHz Extended Squitter (1090ES). In this paper, we consider only the ADS-B over 1090 MHz. Recently, new ADS systems that have wider coverage than that of ground-based ADS-B, such as space-based ADS-B and Automatic Dependent Surveillance-Contract (ADS-C). Unlike ADS-B, which relies on ground-based infrastructure, space-based ADS-B utilizes satellite networks to receive ADS-B messages broadcasted from certified aircraft transponders [64]–[67]. Subsequently, the satellite network relays the ADS-B messages to the ground stations, which then forward the data to the ATC automation systems. Space-based ADS-B enables global coverage in areas where deploying ADS-B ground receivers is not applicable, such as in ocean areas, mountains, and conflict zones. On the other hand, ADS-C [68] enables aeronautical surveillance which is based on contracts established between airlines and ground-based air navigation units, which includes the specified reporting rate.

### 2) CYBERSECURITY ISSUES IN AUTOMATIC DEPENDENT SURVEILLANCE

ADS-B is prone to cyber-attacks, such as eavesdropping, jamming, and spoofing [12], [13], [69], [70] owing to the lack of security algorithms in ADS-B and the availability of SDR [53]. Therefore, attackers can modify ADS-B messages to virtually modify the aircraft trajectory, provide ghost targets on ATC screens, and delete ADS-B messages, leading to the disappearance of targets from ATC screens. Fig. 11 shows an assessment of the likelihood of eavesdropping, jamming, and spoofing threats in ADS-B, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 11, the likelihood of jamming and spoofing threats, as well as eavesdropping, is higher than that in SSR owing to the lack of security algorithms in ADS-B, and the low cost of ADS-B receivers. Furthermore, unlike SSR, which directionally interrogates on-board aircraft transponders with high transmitting power, the on-board aircraft ADS-B transponder periodically broadcasts surveillance information omnidirectionally to ground receivers. Additionally, unlike the complex mechanically rotating antenna used in SSR, the mechanism of ADS-B involves the use of simple receiving devices to receive ADS-B surveillance information. In more detail, as shown in Fig. 11, an eavesdropping attack is very likely to occur owing to the lack of security algorithms, low cost of ADS-B receiver, standardized ADS-B protocol, and frequencies used, while their impact on aviation safety is low. Therefore, the risk level is acceptable. Furthermore, jamming attacks are likely to occur because of the capability of attackers, in terms of accessibility and low cost of jamming devices used, low receiving power at ADS-B ground antennas, while their impact is medium on aviation safety, except for regions that use ADS-B as a sole surveillance system, where the relevant impact will be high. Therefore, the risk level is acceptable. Additionally, the likelihood of a spoofing attack is low, while its impact is high on aviation safety. Therefore, the risk level is tolerable, assuming that there is no correlation with other surveillance sensors to check the trustworthiness of received ADS-B information, and the impact will change for other attack scenarios. Recall that for an eavesdropping attack, the attacker only receives a wireless signal, whereas for jamming, the attacker transmits a wireless signal to block the ADS-B signal. Furthermore, for spoofing attacks, an attacker can inject, delete, or modify the content of ADS-B messages. Many studies have been proposed addressing ADS-B cyber-attack issues. Some techniques use cryptographic solutions [71]–[75], while others use location verification [63], [76]–[78], while novel techniques involving machine learning localization have been utilized more recently [53], [79]. Cryptographic techniques [71]–[75] use encryption protocols in the communication link between ground-based ADS-B receivers and ADS-B transponders on board the aircraft. Such techniques require the pre-sharing of a secret key between the transmitter and receiver. Cryptographic techniques

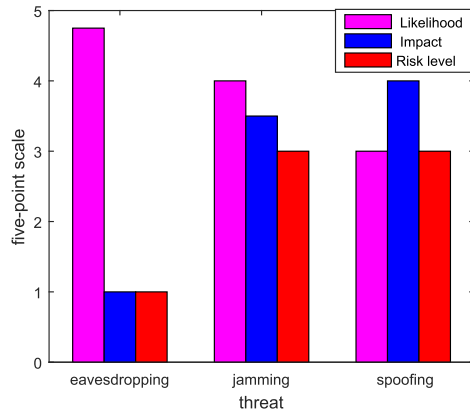


FIGURE 11. Illustration of cybersecurity risk assessment for ADS-B.

necessitate changing ADS-B standards and therefore major changes in the fleet. On the other hand, some location verification techniques detect spoofing in ADS-B by comparing the claimed aircraft position received from ADS-B receivers with those obtained from other techniques. The other techniques could be Doppler shift [63], Angle of Arrival (AoA) [77], [78], MLAT [80], and data fusion of ADS-B, flight model of aircraft, MLAT, and flight information [81]. Unfortunately, the proposed techniques involving Doppler shift rely on the participation of ground ADS-B receivers, while AoA techniques require using sector antennas, and the proposed techniques involving MLAT necessitate certain sensor deployment and accurate synchronization of the MLAT sensors. The authors of [53] proposed a novel machine-learning technique that establishes a theoretically calculated fingerprint map. Then, it uses historically recorded real data from the OpenSky network to augment the TDoA fingerprint map. For jamming attacks in ADS-B, the proposed technique can be used to independently determine the aircraft location regardless of whether it received from ADS-B messages. Furthermore, spoofing attacks in ADS-B can be detected via comparing the position received from the ADS-B with that obtained from the proposed framework.

## VI. SYSTEM-WIDE INFORMATION MANAGEMENT

### A. OVERVIEW OF SYSTEM-WIDE INFORMATION MANAGEMENT

With the increasing growth of air traffic density worldwide, the connectivity between various aviation sectors, including air navigation systems (ground/air and ground/ground), has received significant attention. To achieve cost-effective, reliable and accurate system wide-area connectivity between various air navigation facilities in a timely manner, the involved systems need to be globally interoperable [82]. Therefore, global information sharing systems, such as the SWIM concept, can dynamically manage air navigation facilities without isolation and avoid duplication of information. SWIM is a global concept consisting of standards, infrastructure, and governance designed to enable a harmonized global

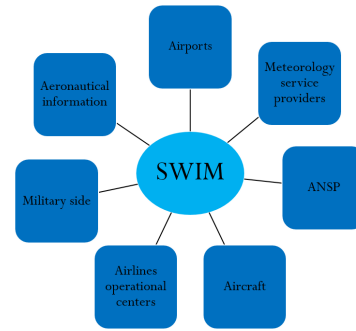


FIGURE 12. Overview of SWIM and its involved stakeholders.

exchange of air navigation information such as flight information and aeronautical, meteorological, and aeronautical surveillance for all airspace users and stakeholders [4], [82], [83], as shown in Fig. 12. The connectivity among various ATM systems will rely on the evolution of network-centric information sharing, in which the ground systems and the aircraft are considered as nodes that can be used for sharing information and relaying their intent through an integrated network. Additionally, SWIM is a crucial component of the Next Generation (NextGen) project (United States), Single European Sky ATM Research (SESAR) (Europe), collaborative actions for renovation of air traffic systems (CARATS) (Japan), and the ICAO Global Air Navigation Plan (GANP). In the GANP, SWIM can enable SWIM-B2/4 aviation system block upgrade (ASBU) modules [84], such as exchanging air/ground non-safety critical information with the aircraft to improve operational awareness and efficiency without the constraints imposed by voice communications between the on-ground ATC and the pilot. Additionally, SWIM can enable SWIM-B3/1 to exchange air/ground safety critical information with the aircraft to improve operational awareness and efficiency. Applying the SWIM concept will contribute to enhanced decision-making by all stakeholders during the various phases of flights through improved shared situational awareness. Furthermore, improvements in the availability of data and information, increased system performance, flexibility, and cost effectiveness were achieved by applying SWIM [4].

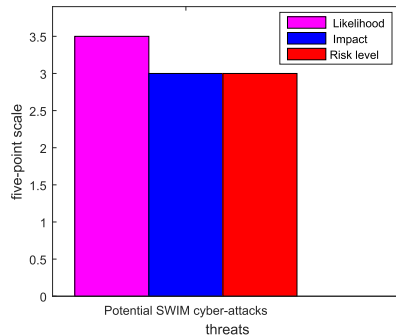
### B. CYBERSECURITY ISSUES IN SYSTEM-WIDE INFORMATION MANAGEMENT

As mentioned before, SWIM uses net-centric exchanges of aeronautical information, which exposes the system to potential interruption and damage. Such damage can also occur in other parts of the network, where the systems are connected using an IP network. The authors of [16] discussed a number of potential vulnerabilities in SWIM, such as a man-in-the-middle attack, where no end-to-end acknowledgment is provided about messages being sent or received on the network. Furthermore, because SWIM uses software with end users and through the network, such software is prone to a wide range of cyber-attacks that can increase instances of unauthorized access and malicious code.



**TABLE 12. Potential cyber threats in SWIM.**

Potential threats
Man-in-the middle attack
Unauthorized access/DOS attacks
IP-network attacks

**FIGURE 13. Illustration of cybersecurity risk assessment for SWIM.**

Other vulnerabilities of SWIM originate from the potential inherited vulnerabilities of the IP network connectivity used in SWIM. Table 12 summarizes the most common cyber-attacks relevant to SWIM. Fig. 13 shows an assessment of the likelihood of potential cyber-attacks in SWIM, their impact, and risk levels on a five-point scale based on application of the proposed cybersecurity risk assessment methodology described in Section II. As shown in Fig. 13, the likelihood of these attacks is of a medium level, as is the relevant impact on aviation safety. Therefore, the risk level is tolerable. The impact of these attacks highly depends on the attack assumed scenarios, such as the availability of alternative direct communication connections used to receive critical information. In the scenario addressed herein, we assume that there are alternative means of obtaining essential information, e.g., in case the SWIM network suffers a DOS attack, services such as meteorology, aeronautical, and flight information can be obtained manually from the sources of such information. In other words, information sharing changes from net-centric to isolated individual systems, which affects the timeliness of receiving the information. Recall that, unlike the wireless signal attacks associated with communication, navigation, and surveillance systems that allow attackers to jam or spoof wireless signals and without requiring attackers to be inside the targeted attacked systems, attacks in networks such as SWIM can be performed remotely, when systems have remote access, or from inside the organization. Furthermore, although SWIM uses an IP network, it uses a private IP network in which, attackers should have access to the systems to insert malicious programs, whether remotely or from inside the organization. To mitigate such cyber-attacks, the authors of [85] proposed the SWIM Common Public Key Infrastructure Project to establish a trust framework with the objective of enhancing the cybersecurity of exchanging aviation information in Europe. This project assumes the use of digital certificates with the users of SWIM, such as

ANSPs, airspace users, and airports, to increase the level of confidence and authentication of SWIM connections in an interoperable manner. This project will work in close cooperation with similar ICAO initiatives named INNOVA/ACORNS (Aviation Community Operational Resilience Network Services), which aims to have a global trusted, secured, and resilient framework to facilitate the global exchange of digital information. INNOVA/ACORNS will establish a trust framework based on a global interoperable private IP network for aviation stakeholders.

## VII. CONCLUSION AND FUTURE WORK

In this paper, we proposed a systematic qualitative and quantitative methodology of cybersecurity risk assessment for aviation, which includes identification of the potential threats in civil aviation systems, assessment of the likelihood of these threats and their impact, and assessment of the risk levels. Furthermore, we applied the proposed cybersecurity risk assessment on the legacy and next-generation critical infrastructure in aviation systems, including air-ground communication, radio navigation aids, aeronautical surveillance, and system-wide information management. Additionally, we addressed the specific and general mitigation measures used to reduce risks to acceptable levels. As seen from our study, the common potential cyber-attacks on systems that send signals to space, for example, in the case of air-ground communication, radio navigation aids, and aeronautical surveillance, are eavesdropping, jamming, and spoofing, whereas for networking systems including SWIM, the most common forms of cyber-attacks are unauthorized access, DOS attacks, man-in-the-middle attacks, and IP-network attacks. Our analysis showed that the communication, navigation, and surveillance systems with the threat of highest risk levels are VHF, satellite-based navigation, and ADS-B, respectively, while those with the lowest risk levels are CPDLC, ground-based radio navigation aids, and SSR, respectively. In future studies, we will address cybersecurity in the civil aviation sector with a focus on the period during the COVID-19 pandemic and beyond. With the outbreak of this pandemic, there has been significant growth in the use of online technologies, such as those that support remote work in airports and airlines, and therefore, increased levels of cyber-attacks related to COVID-19. Furthermore, we will address the cybersecurity in the next generation air navigation systems, such as AeroMACS, L-DACS, and space-based ADS-B.

## REFERENCES

- [1] *Air Transport Bureau, Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis*, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2020.
- [2] *Annex 10: Aeronautical Telecommunications: Surveillance and Collision Avoidance Systems*, vol. 4, 5th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2014.
- [3] *Document 9849: Global Navigation Satellite System (GNSS) Manual*, 3rd ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2017.



- [4] *Document 10039: Manual on System Wide Information Management (SWIM) Concept*, Unedited Version, Int. Civil Aviation Org., Montreal, QC, Canada, 2015. [Online]. Available: <https://www.icao.int/airnavigation/IMP/Documents/SWIM%20Concept%20V2%20Draft%20with%20DISCLAIMER.pdf>
- [5] *Document 10037: Global Operational Data Link (GOLD) Manual*, 5th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2017.
- [6] *Document 9718: Handbook on Radio Frequency Spectrum Requirements for Civil Aviation, ICAO Spectrum Strategy, Policy Statements and Related Information*, vol. 1, 2nd ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2018.
- [7] *Document 8071: Manual on Testing of Radio Navigation Aids Manual, Testing of Groundbased Radio Navigation Systems*, vol. 1, 5th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2018.
- [8] *Document 9924: Aeronautical Surveillance Manual*, 3rd ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2020.
- [9] T. H. Stelkens-Kobsch, "Towards a more secure ATC voice communications system," in *Proc. IEEE/AIAA 34th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2015, pp. 4C1-1–4C1-9.
- [10] O. Osechas, M. Mostafa, T. Graupl, and M. Meurer, "Addressing vulnerabilities of the CNS infrastructure to targeted radio interference," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 11, pp. 34–42, Nov. 2017.
- [11] A. Gurtov, T. Polishchuk, and M. Wernberg, "Controller-pilot data link communication security," *Sensors*, vol. 18, no. 5, p. 1636, May 2018.
- [12] M. Riahi Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system," *Int. J. Crit. Infrastruct. Protection*, vol. 19, pp. 16–31, Dec. 2017.
- [13] M. Strohmeier, M. Schafer, M. Smith, V. Lenders, and I. Martinovic, "Assessing the impact of aviation security on cyber power," in *Proc. 8th Int. Conf. Cyber Conflict (CyCon)*, May 2016, pp. 223–241.
- [14] D. D. Marco, A. Manzo, M. Ivaldi, and J. Hird, "Security testing with controller-pilot data link communications," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 526–531.
- [15] M. Wernberg, "Security and privacy of controller pilot data link communication," M.S. thesis, Fac. Sci. Eng., Dept. Sci. Technol., Linköping Univ., Commun. Transp. Syst., Norrköping, Sweden, 2018.
- [16] S. Sueki and Y. Kim, "Vulnerabilities and mitigation methods in the NextGen air traffic control system," in *Information Technology: New Generations*, S. Latifi, Ed. Cham, Switzerland: Springer, 2016, pp. 201–211.
- [17] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, Eds., *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*. Oxford, U.K.: Springer, ch. Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management, 2019, pp. 245–260.
- [18] *Civil Aviation Cybersecurity [Internet]*. Accessed: Sep. 1, 2021. [Online]. Available: [www.icao.int/cybersecurity](http://www.icao.int/cybersecurity)
- [19] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1338–1357, 2017.
- [20] M. Strohmeier, I. Martinovic, and V. Lenders, Eds., *The Security of Critical Infrastructures: Risk, Resilience and Defense*. Oxford, U.K.: Springer, ch. Securing the Air-Ground Link in Aviation, 2020, pp. 131–154.
- [21] F. Shaikh, M. Rahouti, N. Ghani, K. Xiong, E. Bou-Harb, and J. Haque, "A review of recent advances and security challenges in emerging E-enabled aircraft systems," *IEEE Access*, vol. 7, pp. 63164–63180, 2019.
- [22] G. Tamasi and M. Demichela, "Risk assessment techniques for civil aviation security," *Rel. Eng. Syst. Saf.*, vol. 96, no. 8, pp. 892–899, Aug. 2011.
- [23] C. Liu, C.-K. Tan, Y.-S. Fang, and T.-S. Lok, "The security risk assessment methodology," *Proc. Eng.*, vol. 43, pp. 600–609, Jan. 2012.
- [24] *Doc 9985: Air Traffic Management Security Manual*, 5th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2013.
- [25] K. Sampigethaya, P. Kopardekar, and J. Davis, "Cyber security of unmanned aircraft system traffic management (UTM)," in *Proc. Integr. Commun., Navigat., Surveill. Conf. (ICNS)*, Apr. 2018, pp. 1–21.
- [26] T. D. Tran, J.-M. Thiriet, N. Marchand, A. El Mrabti, and G. Lucilli, "Methodology for risk management related to cyber-security of unmanned aircraft systems," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2019, pp. 695–702.
- [27] *Doc 8973: Aviation Security Manual*, 12th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2020.
- [28] *Doc 10084: Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones*, 2nd ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2018.
- [29] *Document 9895: Safety Management Manual*, 4th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2018.
- [30] H. Dac Tu, Y. Tsuda, S. Shimamoto, J. Kitaori, and S. Kato, "The next generation air to ground communication system for air traffic control," in *Proc. IEEE/ACES Int. Conf. Wireless Commun. Appl. Comput. Electromagn.*, Apr. 2005, pp. 1010–1013.
- [31] M. Strohmeier, A. K. Niedbala, M. Schäfer, V. Lenders, and I. Martinovic, "Surveying aviation professionals on the security of the air traffic control system," in *Security and Safety Interplay of Intelligent Software Systems*. Cham, Switzerland: Springer, 2019, pp. 135–152.
- [32] *Annex 10: Aeronautical Telecommunications: Aeronautical Communications*, vol. 3, 2nd ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2007.
- [33] *Datalink Ground System Standard and Interface Specification*, Standard 620-8, 2014.
- [34] *Document 10044: ICAO AeroMACS Manual*, 1st ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2019.
- [35] A. G. Frequentis and C. Rihacek, "L-band digital aeronautical communications system (LDACS) activities in SESAR2020," in *Proc. Integr. Commun., Navigat., Surveill. Conf. (ICNS)*, Apr. 2018, pp. 4A1-1–4A1-8.
- [36] P. A. Massimini, J. E. Dieudonne, L. C. Monticone, D. F. Lamiano, and E. A. Brestle, "Insertion of controller-pilot data link communications into the national airspace system: Is it more efficient?" in *Proc. Gateway New Millennium. 18th Digit. Avionics Syst. Conf.*, vol. 1, Oct. 1999, pp. 5.A.3–5.A.3.
- [37] (ARINC): 823-P1: *Data Link Security, Part I—ACARS Message Security*, Aeronautical Radio Inc, Annapolis, MD, USA, Technical Standard, 2007.
- [38] T. F. Cary R. Spitzer, and U. Ferrell, *Digital Avionics Handbook*, 3rd ed. Boca Raton, FL, USA: CRC Press, 2017.
- [39] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Undermining privacy in the aircraft communications addressing and reporting system (ACARS)," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 3, pp. 105–122, Jun. 2018.
- [40] C. Risley, J. Mcmath, and B. Payne, "Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages," in *Proc. 20th DASC. 20th Digit. Avionics Syst. Conf.*, Oct. 2001, pp. 7D4/1–7D4/8.
- [41] T. Leconte. (2015). *ACARSDec ACARS Decoder*. Accessed: Aug. 1, 2021. [Online]. Available: <http://sourceforge.net/projects/acarsdec/>
- [42] H. Teso, "Aircraft hacking: Practical aero series," in *Proc. 4th Hack Box Secur. Conf.*, Amsterdam, The Netherlands, Apr. 2013.
- [43] R. Zhang, G. Liu, J. Liu, and J. P. Nees, "Analysis of message attacks in aviation data-link communication," *IEEE Access*, vol. 6, pp. 455–463, 2018.
- [44] *Impact Assessment of Cybersecurity Threats. Report no. EASA REP RESEA 2016 1*, Eur. Aviation Saf. Agency, Cologne, Germany, 2018.
- [45] A. Roy, "Secure aircraft communications addressing and reporting system (ACARS)," U.S. Patent 6 677 888, Jan. 13, 2004.
- [46] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Economy class crypto: Exploring weak cipher usage in avionic communications via ACARS," in *Int. Conf. Financial Cryptogr. Data Secur.* Cham, Switzerland: Springer, 2017, pp. 285–301.
- [47] *User Requirements for Air Traffic Services (URATS), Communications, Navigation, and Surveillance (CNS) Technologies*, International Air Transport Association (IATA), 2017. [Online]. Available: <https://www4.icao.int/ganportal/>
- [48] *Annex 10: Aeronautical Telecommunications: Radio Navigation Aids*, vol. 1, 7th ed, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2018.
- [49] J. S. Warner, R. Johnston, and C. L. Alamos, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *J. Secur. Admin.*, vol. 25, no. 2, pp. 19–28, 2002.
- [50] *Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Analysis Report*, Global Professional Services Partners Team, Guelph, ON, USA, 2014.
- [51] A. Novák, F. Jun, F. Škultéty, and A. N. Sedláčková, "Experiment demonstrating the possible impact of GNSS interference on instrument approach on RWY 06 LZL," *Transp. Res. Proc.*, vol. 43, pp. 74–83, Jan. 2019.
- [52] H. Sathaye, D. Schepers, A. Ranganathan, and G. Noubir, "Wireless attacks on aircraft instrument landing systems," in *Proc. 28th USENIX Secur. Symp. (USENIX Secur.)*, Santa Clara, CA, USA, 2019, pp. 357–372.
- [53] A. A. Elmarady and K. Rahouma, "Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B," *Chin. J. Aeronaut.*, vol. 34, no. 2, pp. 217–228, Feb. 2021.

- [54] *Guidance Material on Comparison of Surveillance Technologies (GMST)*, 5th ed. International Civil Aviation Organization Asia and Pacific, Bangkok, Thailand, Sep. 2014.
- [55] L. Du, H. Liu, Z. Bao, and J. Zhang, "Radar automatic target recognition using complex high-resolution range profiles," *IET Radar, Sonar Navigat.*, vol. 1, no. 1, pp. 18–26, Feb. 2007.
- [56] G. Galati, M. Leonardi, P. Magaro, and V. Paciucci, "Wide area surveillance using SSR mode S multilateration: Advantages and limitations," in *Proc. Eur. Radar Conf. (EURAD)*, Oct. 2005, pp. 225–229.
- [57] Andersen AC. (2011). *Comparative Analysis of Multilateration Methods for Signal Emitter Positioning*. [Online]. Available: <http://blog.andersen.im/2012/07/signalemitter-positioning-using-multilateration/>
- [58] D. L. Adamy, *EW 103: Tactical Battlefield Communications Electronic Warfare*, 1st Ed. Norwood, MA, USA: Artech House, 2009.
- [59] *Document 9684: Manual on the Secondary Surveillance Radar (SSR) Systems*, 3rd ed. International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2004.
- [60] "Results from EASA technical investigation on the radar detection losses in June 2014 in central Europe," Eur. Aviation Saf. Agency, Cologne, Germany, Tech. Rep. EDO.1-2014-ed04.00, 2014.
- [61] M. Andersson and M. Ilestrand, "Data fusion of secondary and primary surveillance radars for increased robustness in air-traffic monitoring," in *Proc. Eur. Microw. Conf.*, 2007, pp. 456–459.
- [62] D. Moser, P. Leu, V. Lenders, A. Ranganathan, F. Ricciato, and S. Capkun, "Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures," in *Proc. 22nd Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2016, pp. 375–386.
- [63] N. Ghose and L. Lazos, "Verifying ADS-B navigation information through Doppler shift measurements," in *Proc. IEEE/AIAA 34th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2015, pp. 4A2-1–4A2-11.
- [64] M. A. Garcia, J. Stafford, J. Minnick, and J. Dolan, "Aireon space based ADS-B performance model," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, Apr. 2015, pp. C2-1–C2-10.
- [65] Y. Zhang, W. Li, and Z. Dou, "Performance analysis of overlapping space-based ADS-B signal separation based on FastICA," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.
- [66] Y. Sunquan, C. Lihu, L. Songting, and L. Lanmin, "Separation of space-based ADS-B signals with single channel for small satellite," in *Proc. IEEE 3rd Int. Conf. Signal Image Process. (ICSIP)*, Jul. 2018, pp. 315–321.
- [67] S. Yu, L. Chen, S. Li, and X. Zhang, "Adaptive multi-beam forming for space-based ADS-B," *J. Navigat.*, vol. 72, no. 2, pp. 359–374, 2019.
- [68] R. Sosovicka, P. Vesely, and J. Svoboda, "Estimation of aircraft performance parameters from ADS-C EPP data," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, Apr. 2015, pp. N2-1–N2-7.
- [69] F. Shang, B. Wang, F. Yan, and T. Li, "Multidevice false data injection attack models of ADS-B multilateration systems," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Mar. 2019.
- [70] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Applied Cryptography and Network Security*. Berlin, Germany: Springer, 2013, pp. 253–271.
- [71] T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," *IEEE Trans. Comput.*, vol. 59, no. 8, pp. 1120–1133, Aug. 2010.
- [72] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *Proc. IEEE Aerosp. Conf.*, Oct. 2006, p. 7.
- [73] Z. Wu, A. Guo, M. Yue, and L. Liu, "An ADS-B message authentication method based on certificateless short signature," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, pp. 1742–1753, Jun. 2020.
- [74] Z.-L. F. Wei-Jun Pan and Y. Wang, "ADS-B data authentication based on ECC and X.509 certificate," *J. Electron. Sci. Technol.*, vol. 10, pp. 51–55, Mar. 2012.
- [75] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *Int. J. Crit. Infrastruct. Protection*, vol. 6, no. 1, pp. 3–11, Mar. 2013.
- [76] M. Schäfer, P. Leu, V. Lenders, and J. Schmitt, "Secure motion verification using the Doppler effect," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2016, pp. 135–145.
- [77] J. Naganawa, H. Tajima, H. Miyazaki, T. Koga, and C. Chomel, "ADS-B anti-spoofing performance of monopulse technique with sector antennas," in *Proc. IEEE Conf. Antenna Meas. Appl. (CAMA)*, Dec. 2017, pp. 87–90.
- [78] C. Reck, M. S. Reuther, A. Jasch, and L.-P. Schmidt, "Verification of ADS-B positioning by direction of arrival estimation," *Int. J. Microw. Wireless Technol.*, vol. 4, no. 2, pp. 181–186, Apr. 2012.
- [79] M. Strohmeier, V. Lenders, and I. Martinovic, "A k-NN-based localization approach for crowdsourced air traffic communication networks," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 3, pp. 1519–1529, Jun. 2018.
- [80] N. Xu, R. Cassell, C. Evers, S. Hauswald, and W. Langhans, "Performance assessment of multilateration systems—A solution to nextgen surveillance," in *Proc. Integr. Commun., Navigat., Surveill. Conf.*, May 2010, pp. D2-1–D2-8.
- [81] A. A. W. E. Marady, "Enhancing accuracy and security of ADS-B via MLAT assisted-flight information system," in *Proc. 12th Int. Conf. Comput. Eng. Syst. (ICCES)*, Dec. 2017, pp. 182–187.
- [82] Z. Wu, S. Zhou, L. Liu, and J. Lei, "Research on SWIM services dynamic migration method," *Future Internet*, vol. 11, no. 9, p. 187, Aug. 2019.
- [83] B. Stephens, "Security architecture for system wide information management," in *Proc. 24th Digit. Avionics Syst. Conf.*, vol. 2, Oct. 2005, p. 10.
- [84] *Global Air Navigation Plan (GANP)*, 6th ed. International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2019.
- [85] P. Mana and V. Friligkos, "Deployment: Swim common PKI and policies & procedures for establishing a trust framework," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, Apr. 2019, pp. 1–12.



**AHMED ABDELWAHAB ELMARADY** received the B.Sc. and M.Sc. degrees in communication and electronics engineering from the Faculty of Engineering, Cairo University, Egypt, in 2007 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Faculty of Engineering, Minia University, majoring in cybersecurity in aviation generally, and in air navigation systems in particular. He has been a Senior Communication, Navigation, and Surveillance (CNS) Safety Oversight Inspector—Air Navigation Engineer with the Egyptian Civil Aviation Authority, since 2012. He is a member of both the ICAO Secretariat Study Group on Cybersecurity (SSGC)—working group on air navigation systems, Montreal, Canada, and the ICAO MID—working group on cybersecurity in air navigation, Cairo, Egypt. He has published many journals and conference research papers. His research interests include the cybersecurity and cyber resilience frameworks in the various aviation systems (aerodromes, air navigation, flight operations, and airworthiness). Furthermore, his research interests also include new technologies in aeronautical communication, radio navigation aids, aeronautical surveillance, and system wide information management (SWIM).



**KAMEL RAHOUMA** received the B.Sc. and M.Sc. degrees in communications and electronic engineering from the Faculty of Engineering, Cairo University, in June 1984 and March 1988, respectively, the first doctoral degree in communications and electronics engineering jointly from the University of Kent, Canterbury, U.K., and Minia University, Egypt, in 1996, and the second doctoral degree in computer science from the University of Salzburg, Austria, in May 2001. He is currently supervising and guiding more than 40 postgraduate students who are working for their master's and doctoral degrees. He has taught and is teaching various undergraduate courses in Egypt and Saudi Arabia. This may include (but not limited to): analog and digital communications, electronics, electronic circuits, digital design, electric circuits, engineering mathematics, probability and statistics, control systems, artificial intelligence, image processing, embedded systems, computer programming (FORTRAN, Java, C, C++, Matlab, Basic, and Visual Basic), cryptography and network security, operating systems, information systems, optimization, computer networks, operational research, and distributed and parallel computer systems. He is also guiding many bachelor's graduation projects in different fields of computer science, communications and electronics engineering, and biomedical engineering. He has a strong ambition to work with teams in different areas of science. He is dreaming of a clean healthy society free of diseases. He has multidisciplinary research interests. This includes (but not limited to): cryptography and information security, artificial intelligence applications, biomedical application, bioinformatics, geolocation systems, LiFi communication systems, smart card systems, embedded systems, driverless vehicles, design and implementation of satellite systems, and educational applications.

...