Surveying Aviation Professionals on the Security of the Air Traffic Control System

Martin Strohmeier,[+] Anna K. Niedbala,[+] Matthias Schäfer,[*] Vincent Lenders,[#] Ivan Martinovic[+]

[+]University of Oxford, United Kingdom
[*]University of Kaiserslautern, Germany [#]armasuisse, Switzerland

Abstract. In this paper, we report findings from an exploratory study concerning the security of 15 different wireless technologies used in aviation. 242 aviation professionals and experts from 24 different countries completed an on-line questionnaire about their use and perceptions of each of these technologies. We examine the respondents' familiarity with and reliance on each technology, with particular regard to their security. Furthermore, we analyse respondents' perceptions of the possible impact of a wireless attack on the air traffic control system, from both a safety and a business point of view. We deepen these insights with statistical analysis comparing five different stakeholder groups: pilots, air traffic controllers, aviation authorities, aviation engineers, and private pilots.

Keywords: aviation security, air traffic control, survey, transportation systems

1 Introduction

Over the past decade, the (cyber) security of wireless aviation technologies has gained increasing attention. With both hackers [5] and academic researchers [3] detailing flaws in the fundamentally insecure protocols, awareness of the issue has risen, particularly with regards to the newest, 'next generation' technologies such as the Automatic Dependent Surveillance–Broadcast (ADS–B) protocol [9].

Attempting to fix these security problems requires broad awareness, agreement, and potentially also education across the different stakeholder groups found in aviation. To create the necessary momentum for implementing such changes in a system as slow-moving, safety-focused, and globalised as aviation, a sufficiently large number of people must be familiar with the security problems, their potential impact, and possible solutions. To assess the current level of such awareness, we conducted a survey across all aviation circles. This survey is the first to address these issues publicly, and we are thankful to all involved aviation authorities and air navigation service providers (ANSPs) for their help.

We focus on two specific areas within our research. First, we examine the survey respondents' familiarity and knowledge of 15 different wireless technologies, in particular with regards to their security. Second, we examine the respondents' views of the potential impact of wireless attacks on each technology from a safety

and business point of view, respectively. We deepen our analysis by comparing the perceptions of the different stakeholder groups.

It is important to note that our goal was not to survey those members of the aviation community with specialist knowledge of computer and systems security. Rather, we attempt to capture the realistic perceptions of typical aviation stakeholders, as we believe these views are more representative, and thus more crucial to influencing key decision making processes.

Some findings from this survey—concretely, an assessment of threat scenarios—have previously been reported in [9]. In the present paper, we focus instead on new quantitative and qualitative data from previously unreported questions and comments, providing novel results and insights through comprehensive statistical analysis. Further, we detail our experiences while conducting this survey and relate these to prevalent attitudes in aviation.

The concrete contributions we make in this work are the following:

- We report insights from an exploratory study with 242 aviation professionals regarding the security of the wireless technologies on which they rely.
- We present previously unreported data on the technological familiarity and dependency of different stakeholder groups found in aviation.
- We analyze the perceptions of flight safety and business impact through attacks on different key technologies and how they vary between stakeholders.

The remainder of this work is organized as follows: Section 2 provides the necessary background on the air traffic control technologies examined. Section 3 describes the design of the survey, Section 4 its results and Section 5 the possible limitations. The related work is outlined in Section 6. Section 7 discusses potential implications, and finally, Section 8 concludes this paper.

2 Air Traffic Surveillance Technologies

We provide a very brief overview of the type of technologies that we surveyed. For a full description of the specific aviation technologies and a review of the related technical work concerning their security, we refer the reader to [9].

Table 1 lists the full name of the technologies that were given to the aviation professionals in our survey. We systematize them into four different categories:

- **Air Traffic Control:** These technologies serve to establish the surveillance picture of the airspace. **VHF**, or voice communication, is the primary means of surveillance for most purposes. **Primary** and **Secondary Surveillance Radar** are the traditional means of locating aircraft's positions, altitude, and identities and providing them to the controller. **ADS-B** and **Multilateration**, on the other hand, are the 'next generation' approach, providing a more accurate surveillance picture with enhanced information.
- **General Purpose Data Links:** **ACARS** and **CPDLC** are data links that can be used to transmit arbitrary data, from clearances over weather reports and maintenance data to free text. Apart from direct line of sight communication, they also offer High Frequency (HF) and satellite options.

Table 1: Overview of the surveyed technologies.

Abb.	Technology
Air Traffic Control	
VHF	Voice (Very High Frequency)
PSR	Primary Surveillance Radar
SSR	Secondary Surveillance Radar (Modes A, C and S)
ADS-B	Automatic Dependent Surveillance-Broadcast
MLAT	Multilateration
General Purpose Data Links	
CPDLC	Controller-Pilot Data Link Communication
ACARS	Aircraft Communications Addressing and Reporting System
Special Information Services	
TCAS	Traffic Alert and Collision Avoidance System
FIS-B	Flight Information System-Broadcast
TIS-B	Traffic Information System-Broadcast
Navigation Aids	
GPS	Global Positioning System
VOR	VHF Omnidirectional Radio Range
ILS	Instrument Landing System
NDB	Non-directional Beacon
DME	Distance-measuring Equipment

– **Special Information Services:** Contrary to the last group, these technologies provide specialized information: **TCAS** uses SSR and ADS-B to deliver collision avoidance to pilots, **TIS-B** provides traffic information, and **FIS-B** delivers well-defined services such as weather and other flight information. Both TIS-B and FIS-B are ground-based, and are provided by the FAA for general aviation; thus, they are currently only available in the US.
– **Navigation Aids:** The remaining five technologies help pilots navigate. **GPS** provides satellite positioning, while **VOR**, **NDB**, and **DME** are ground-based systems, delivering directions and distances. Finally, **ILS** provides the pilot with an acoustic indication of the correct glide slope for landing.

3 Survey Design

We planned and conducted our survey with the help of private pilots and a full-time professional ATCO. They advised us on the appropriate question language with relation to aviation subject terms. Furthermore, they provided us with the necessary aviation expertise and background at every stage during the design, implementation, and execution of this survey. We report the questions and answer options in Appendix A, and the comments in Appendix B.

Our survey was conducted fully anonymously over the internet, in order to protect respondents from potential repercussions when speaking freely about

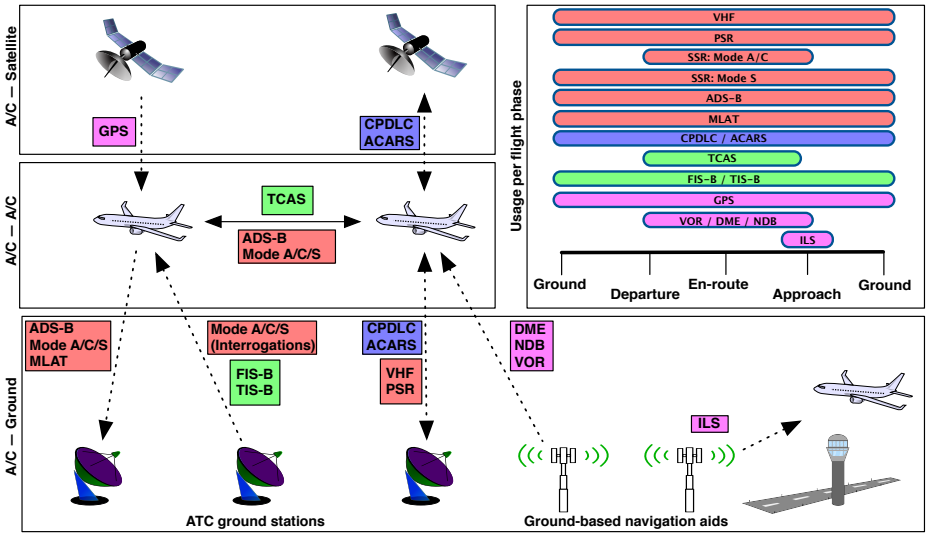

Fig. 1: Overview of wireless communication between ground stations, aircraft and satellites. Colours indicate groups, arrows the communication direction.

the security of ATC systems or disclosing potential safety problems. We designed and distributed the questionnaire using SurveyMonkey,[1] without storing participants' IP addresses or other metadata. Thus, no inferences about location or employer could be made from the responses. The study was approved by the University of Oxford Social Sciences & Humanities Inter-Divisional Research Ethics Committee (IDREC) under the reference SSD/CUREC1A/15-033.

3.1 Recruitment

We recruited participants through two channels: controlled dissemination (CD) and open dissemination (OD). In the CD phase, we sent our survey to about 20 air navigation service providers, airlines, and other aviation-related organisations across Europe and the United States. We asked these institutions to post our recruitment page on their mailing list and disseminate it further to other interested entities. This phase lasted from 27 March until 23 June 2015.

In the OD phase, we distributed the questionnaire link in eight large but closely-moderated aviation forums. Two of these forums, focussed mainly on private pilots, agreed to post our survey. This second phase was significantly shorter, owing to the limited time our dissemination link was seen widely in these forums. It lasted from until 21 April until 29 April 2015.

A total of 242 participants completed the survey: 110, or 45.5% in the CD phase, and 132, or 54.5%, in the OD phase. We analyse the responses as a whole. The average response time length was 31 minutes 10 seconds.

[1] https://www.surveymonkey.com

Table 2: Overview of occupations and self-assessed technical comms knowledge.

Occupation	Group	Number	Share [%]	Avg. Knowl.
Pilot	Private	79	32.6	3.51
	Commercial	64	26.4	3.92
	Military	5	2.1	3
Air Traffic Control (ATCO)	Civil	39	16.1	4.13
	Military	4	1.7	3.25
Aviation Engineer (AE)	-	19	7.9	4.11
Aviation Authority (AA)	-	11	4.5	4.18
Other	-	21	8.7	3.29

Recruitment Experiences Anecdotally, the attitudes of the aviation stakeholders contacted via email proved to be positive, interested, and encouraging (where informal feedback was provided). This may naturally be influenced by the fact that the contact persons knew someone in the recruiting team with one or two degrees of separation and were acting in their professional capacity.

The response in the pseudonymous aviation forums was very different. The two that posted the survey, only did so after thorough vetting of our 'bona fides'. Several negative questions about the intent of the research were posed, reflecting on aviation as a highly guarded community. This sentiment was multiplied in the other six forums, which were not willing to post our survey. Four did not give a reason for declining our request, *i.e.*, they did not allow publication of our recruitment page or deleted it shortly after posting. Two stated that they were explicitly concerned with potential negative publicity for the aviation sector as a whole, presumably because negative media headlines about the security of aviation systems are perceived to be either unfair, uninformed and/or unduly hurting the community, which is best poised to fix these problems without outside help.[2]

3.2 Demographics

Illustrated in Table 2 is the response to Question 1 about the respondents' occupation. A majority were private (33%) or commercial pilots (26%) followed by civil ATCOs (16%) and aviation engineers (8%). Among the respondents who chose 'Other', the professions ranged from software developers in aviation to Flight Information Service Officers. A slight majority (56%) of all OD respondents were private pilots, compared to less than 4% of CD respondents.

The participants' aviation (work) experience (Q2) was distributed fairly evenly, with 32% having 20 years or more, and about 22% offering an expertise of less than 5 years, 5-10 years, and 10-20 years, respectively.

The top working countries (Q3) were the UK (89 respondents) and the US (55). A further 86 worked in Continental Europe, with Germany (21), Estonia

[2] This was epitomized by the well-known 'It's a trap' meme among the forum replies, which aimed to deter other users from answering the survey.

(15), Switzerland (10), Spain (7), Norway (7) making up the majority. Six respondents work in countries around the world (Indonesia, Hong Kong, Canada, UAE, Greenland, Armenia), six did not answer this question.

3.3 Self-assessed General Knowledge and Work Environment

We asked the pilots which aircraft type(s) they were most familiar with (Q4). Among the commercial pilots, the most named model was the A320 (31 times), followed by the B737 (21). Airbus models overall were mentioned 41 times, Boeing 36 times, and Embraer 11 times. The most named single-engine piston was the Piper PA28 (35), followed by several Cessna models (22).

The respondents estimated their general knowledge about aviation comms (Q5) with a mean of 3.76 out of a symmetric, equidistant 5-point Likert-type scale, where 1 is 'very bad' and 5 is 'very good'. Table 2 illustrates small differences between the stakeholders on this general self-assessment.

4 Survey Results

In this section, we present the results of our survey. We report the answers to six questions: two regarding the familiarity of the respondents with the 15 technologies, two concerning trust and security issues, and two in which the respondents were asked to assess the impact of any potential attacks. The full details on these questions are included in Appendix A.

We group the respondents into six different stakeholder types: professional pilots (commercial and military), air traffic controllers (civil and military), employees of aviation authorities, aviation engineers, private pilots, and others not fitting into any of the previous groups (*e.g.*, software engineers and consultants).

Statistical analyses were completed using cumulative link mixed models, a type of ordinal logistic regression that estimates both fixed (predictors) and random (variance groups) effects for ordinal dependent variables. Unless otherwise noted, random intercepts for years of experience (Q2) and country (Q3) were included in each model to account for variance arising from these factors. Responses were coded as ordered factors with the same labels used in the survey (*e.g.* 'Very Unlikely'–'Very Likely'), and factor level contrasts were computed by re-parametrising the fitted model with different contrast codes and reference levels. All analyses were completed using the *ordinal* package in *R* [2, 6]. It is important to note that this study was exploratory, thus any effects reported here require further research and confirmatory analysis.

4.1 Self-assessment of Technical Familiarity and Dependence

First, we wanted to know which technologies were used by the respondents and how this varied across the different stakeholder groups. Respondents were asked to rate how familiar they were with the 15 technologies (Q6) and how much they relied on each one in their work (Q7). The answers were given on 5-point

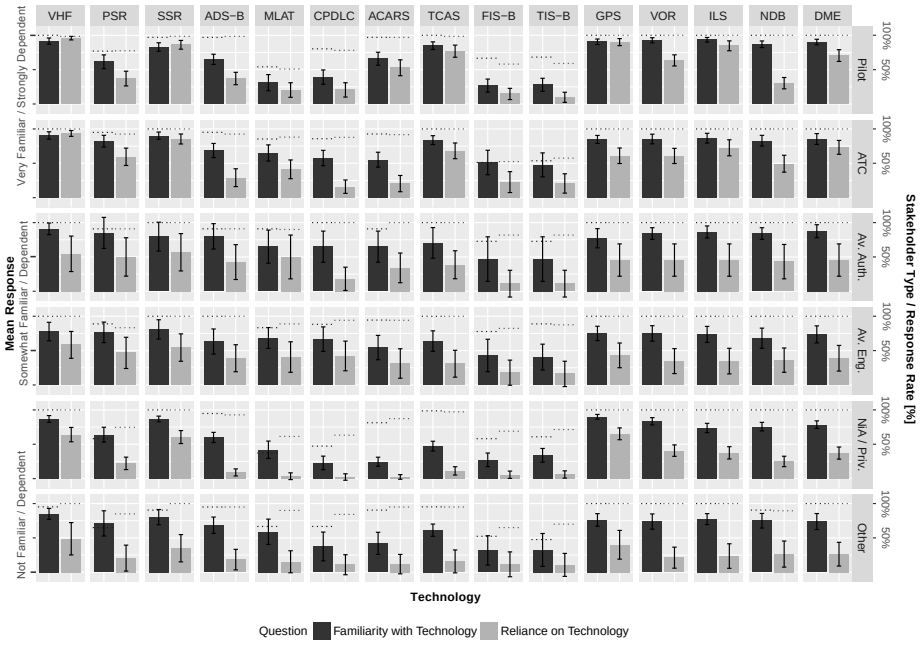

Fig. 2: Mean response values for familiarity with and reliance on all technologies by different stakeholders with 95% confidence intervals. The dotted lines illustrate the response rate for each stakeholder and technology.

Likert-type Scales with a separate 'Not heard of this technology' option for these and all following questions. Figure 2 shows the results.

The technologies that respondents across all groups considered themselves most familiar with are VHF and SSR, followed by navigation aids, in particular GPS. This is explained by the prevalence and importance of these technologies in current aviation processes: SSR and VHF are also the most relied upon technologies, followed by navigation aids. As is to be expected, there are differences between the different stakeholder groups. While commercial pilots and ATCOs are both familiar with and reliant on TCAS and ILS, this is not the case for private pilots, who do not usually have these technologies available to them. Respondents familiar with flying under instrument flight rules are unsurprisingly more likely to depend on all technologies, as they feed these instruments. This is in contrast to private pilots, who typically fly under visual flight rules.

At the end of the scale, we can find TIS-B and FIS-B, which are services that are currently only offered to general aviation in the United States; thus, a significant part of our sample would not be familiar with these technologies or use them in their work / aviation experience. Similarly, CPDLC is only being deployed slowly and for few IFR airspaces. Very interestingly, however, more than 50% of all respondents answered that they already rely on ADS-B to some extent, despite the protocol not being operational in most airspaces until 2020.

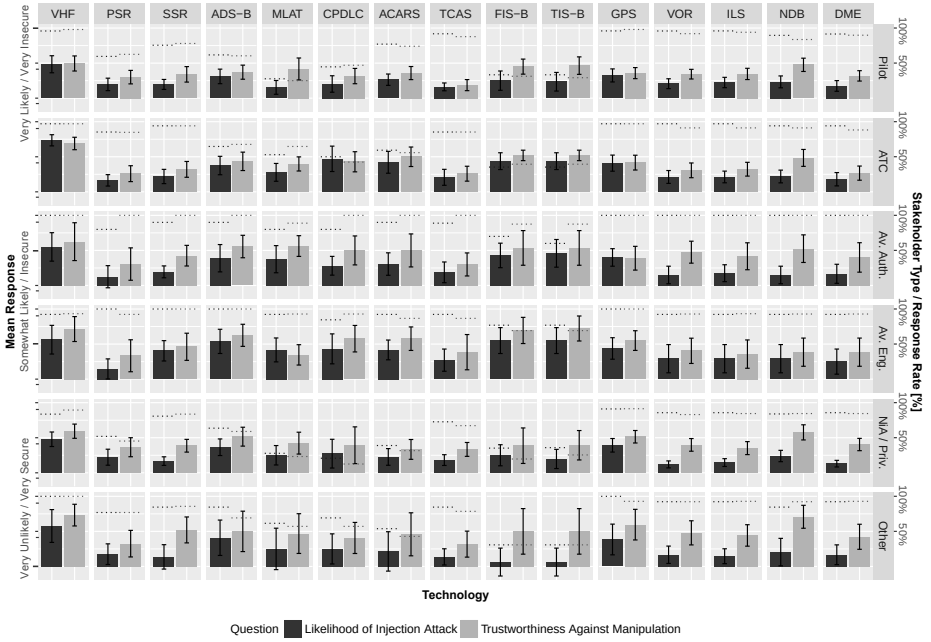

Fig. 3: Mean response values for attack likelihood (dark colour) and trustworthiness (light colour) of all technologies as seen by different stakeholders.

4.2 Assessment of Trust and Security Issues

Second, we examine the perceived attack likelihood and trustworthiness of each technology, again broken down by different stakeholder groups. Figure 3 shows the results for Q8 (*How would you rate the trustworthiness of information derived from these technologies against intentional manipulation by a malicious party?*) and Q9 (*How do you rate the likelihood that a malicious party injects false information into these technologies?*).

The most obvious result is the fact that the likelihood of injection attacks is considered relatively low across almost all technologies and stakeholders. With the (very notable) exception of VHF, which was rated as significantly less trustworthy (average $z = -5.39 \pm 1.9$, all ps < 0.001) and significantly more likely to be attacked (average $z = -3.43 \pm 2.25$, all ps < 0.01), than all other technologies when controlling for stakeholder type, the remaining technologies average a moderate or lower likelihood. As suggested by several comments (see Section 4.4), this is likely due to first- or second-hand experience with VHF interference. Such experiences may also explain the high likelihood rating of GPS. The technologies least likely to be attacked using wireless injection were also analog: DME and VOR, followed by PSR. We further note that while there is a correlation between attack likelihood and trust assessments (Spearman's $\rho = 0.324$), the values for the latter question were generally more similar across technologies, clustering around 'Moderately Secure'.

There were also differences in views between the different stakeholder groups. ATCOs found VHF by far the least trustworthy and most likely to be attacked compared to the other groups, in significant or marginally significant contrast to Pilots (commercial and military; trust $z = -1.95, p = 0.051$, attack likelihood $z = -3.76, p < 0.001$). Similarly to the previous set of questions, fewer pilots answered questions about MLAT (25%, compared to over 50% of ATCOs and over 90% of AEs), but those that did answer believed it to be significantly less likely to be attacked compared to the ATCOs ($z = -2.55, p = 0.011$) and engineers ($z = -2.76, p = 0.006$). Lastly, the private pilots judged a significantly lower attack likelihood across all technologies compared to ATCOs ($z = 3.79, p < 0.001$), AAs ($z = 2.01, p = 0.044$), and AEs ($z = 3.97, p < 0.001$), while their trust ratings across all technologies trended towards a significant difference compared to AEs and Others ($z = 1.75, p = 0.081$ and $z = 1.72, P = 0.085$, respectively).

4.3 Assessment of Attack Impact

Finally, we examine the perceived impact of attacks on flight safety as judged by the respondents, and how this contrasts with indirect impact on the business side (*i.e.*, not through effects on safety, but *e.g.*, through causing delays). Fig. 4 shows the full results for Q10 *(How would you rate the impact on flight safety by false information injected by a malicious party into each of these technologies?)* and Q11 (*How would you rate the business or monetary consequences of false information injected by a malicious party into each of these technologies? Assume no direct safety incidents.*)

First, it is notable that the flight safety impact is considered higher than the business impact across all technologies and stakeholders: a one-point increase in safety impact rating (*e.g.* from 'Mod. Severe' to 'Severe') predicted an approximately 56% increase in business impact ratings, controlling for technology type and the respondent's familiarity with it (Q6). It is difficult to estimate the reasons for this; the respondents may hold an overall bias towards safety. There are some exceptions, however: respondents working for AAs judged the business impact of some technologies (SSR, ADS-B, MLAT, CPDLC, ACARS) as equally severe or more severe than their safety impact, while ATCOs did the same for data links (CPDLC, ACARS) and special information services (FIS-B, TIS-B).

Across technologies, the highest safety impact values are found for ILS, TCAS, and VHF. This reflects their status as directly safety-critical technologies. TCAS features the largest difference between potential safety and business impact, indicating that other technologies may be more easily used to force *e.g.* unnecessary turnarounds or other flight-prolonging manoeuvres. In general, we find the highest impact ratings among the ATC and navigation aids and the lowest for general and specialized data links, with the notable exception of TCAS.

Stakeholders' judgements of safety impact depended strongly on the different groups' usage and familiarity. Responses to Question 6 (Familiarity) significantly predicted severity ratings of safety and business impact ($z = -2.67, p = 0.008$ and $z = -3.35, p < 0.001$, respectively), with a 13% likelihood of increasing

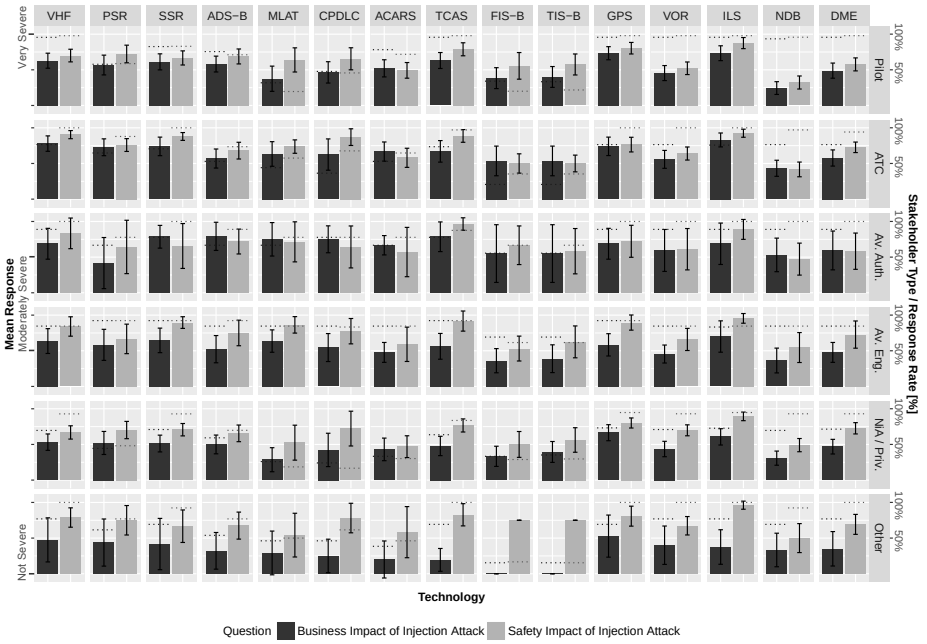

Fig. 4: Mean response values for business impact and safety impact of attacks on each technologies as considered by different stakeholders.

severity ratings for safety impact and 18% for business impact across all technologies and stakeholder groups. This varied significantly by stakeholder group, however. Controlling for familiarity, ATCOs were 40% more likely to judge the safety impact as higher and 63% more likely to judge the business impact as higher than were pilots across all technologies ($z = 3.16, p = 0.002$ and $z = 1$, respectively). We speculate that this is due to a different view on the aviation system in general, *i.e.*, the importance of the communication technologies as compared to the importance of the pilot. This is also illustrated by the differences in judging MLAT's impact in particular. MLAT is a passive localization technology that pilots do not normally come into direct contact with. Here, pilots' business impact ratings are as low as 2.1 ± 1.2) for private pilots (2.5 ± 1.2 for commercial pilots) but average around 3.7 ± 1 for ATCOs, AAs, and AEs. Overall, ATCOs and AAs were 61% more likely to rate an attack on MLAT as having a severe business impact ($z = 5.65$ and 3.75, both $ps < 0.001$; AEs were 24% more likely, but this contrast did not reach statistical significance, $p > 0.1$).

4.4 Qualitative Analysis

In addition to quantitatively-scaled questions, participants had the option to provide comments and additional thoughts in two free-response questions. All

of these responses are enumerated in Appendix B. While some participants conflated both questions, we received 33 comments overall, with three main themes:

- **Direct feedback on the survey:** The largest group consisted of feedback on the survey, both about its design and perceived impact. On the design, this included positive (12,14,31) and negative comments (4,8,15,16,21,24,28,29). Notably, none of the latter pointed out any concrete flaws but stayed very general. Several others pointed out that as private pilots they may not be able to answer all questions fully (7,30,32), which was the intended outcome.
- **Personal anecdotes about cybersecurity incidents:** Several comments (1,3,6,10,11,17,29) mentioned personal experiences of wireless interference, mostly on VHF but also SSR and GPS. Some of these were seen as malicious, in particular on VHF, where detection is straightforward. Two comments (25, 27) discussed potential countermeasures, suggesting the use of independent penetration testing or identity-based encryption for ADS-B.
- **Comments on the importance of security research:** Five respondents (3,5,13,14,19) emphasized the lack of current security research and hoped for increased activity in this area. One (22) hoped that legal threats will prevent any attacks, another suggested that digitalization may be the entirely wrong direction for aviation, in preventing future accidents. Finally, three comments (2,9,20) related to the fact that drones/Unmanned Aerial Vehicles (UAV) may be a bigger and more urgent problem to aviation than cyber security at this point in time.

5 Limitations

While we tried to carefully design our survey, limitations exist. Some of the more impactful ones are caused by characteristics inherent in the underlying aviation technology others by our design. We discuss all in the following:

- **Exploratory study design:** Participants are likely to have varying grasp of the technical security terms 'authentication' or 'integrity', which is difficult to mitigate without extensive briefing and instruction—something unlikely to be completed by most respondents. Thus, we had to focus on the *relative* differences, *i.e.*, between groups and technologies. Since this was an exploratory study, there were no *a-priori* hypotheses to examine, and thus some significant differences are possibly due to random chance, given the large number of comparisons. However, all significant reported p-values survive a Holm-Bonferroni correction for multiple comparisons.
- **Participant selection:** Our survey cannot necessarily be considered fully representative of the aviation community and its different subgroups. While the sample size is large, there are certainly concerns regarding distribution and potential self-selection. However, we have good reason to believe in the general validity of the results, as they fit in well not only with the existing literature but also with our own extensive experiences in this space as well as the reports of experts we have consulted during this and previous studies.

- **Design:** Because of the varying labels assigned to each survey question (*e.g.* 'Severe', 'Likely', 'Familiar'), the Likert-type scale items cannot be assumed to be equidistant, and thus, it is possible that some scales are slightly imbalanced. This was corrected for in the statistical models. Also, as only one question was posed for each construct we measured, the reliability and validity of the questions cannot be ascertained. Rather, this survey provides a snapshot of individuals' attitudes that can inform future research.
- **Proprietary technology:** Many of the surveyed technologies are implemented by different companies, following open standards that are comparably loose, or even non-existent, as in the case of MLAT. Even some of the very widely used protocols (*e.g.*, ACARS or CPDLC) have proprietary elements that are not freely available. Thus, we were more interested in the participants' general assessment and experiences with the abstract systems, no matter the exact implementation.
- **Fragmentation:** Likewise, there is a forest of different systems, regulations, and processes in aviation. Depending on the airspace, the availability, knowledge, and usage of the discussed protocols differs. However, we mitigated this problem by surveying experts from many countries, making sure their judgement of security in aviation technologies did not vary significantly.

6 Related Work

Survey-based analysis is an accepted tool in aviation research, in particular when it comes to examining opinions on and perceptions of safety. For example, a recent article [7] recently used it to analyse the safety of the ADS-B In technology (including the related FIS-B and TIS-B, also covered in our survey). The authors report that almost two thirds of the respondents who used ADS-B-based services felt that they have helped them to visually acquire traffic; more than 40% even believed the information provided aided in the prevention of mid-air collisions. The results clearly illustrate the safety-related benefits of these technologies.

Following recent headlines and increased awareness on security, at least in the academic community, there have been some attempts at extracting the opinions of aviation professionals on this matter. Besides our own survey, the authors in [10] complement our mostly quantitative approach on aviation security perceptions with a number of expert interviews specifically on ADS-B security. Their findings indicate which concrete cyber attack classes are more likely to seriously impact the work of pilots and controllers.

Finally, there have been similar attempts recently to capture the cyber security perceptions of professionals working in the maritime sector, an industry suffering from the same problems as aviation [8].

7 Discussion

Our overall results suggest that knowledge about security issues in ATC technology is limited, experience-dependent, and varies strongly across different stakeholder groups. However, while this indicates that the state of cybersecurity in

aviation leaves much to be desired—both in knowledge about and awareness of the problem among key stakeholders—there is a slow and steady change in the right direction. In recent years, many regulators and authorities have finally put security higher on the agenda. There are concrete new efforts with regards to information sharing, including the European Centre for Cyber Security in Aviation (ECCSA), which is currently being developed by the European Air Safety Agency (EASA). Along similar lines, a Cyber Air Act has been discussed in the US [1]. We hope that our survey can help to additionally inform these initiatives.

Related to the previous point, we further suggest a reassessment of the wider industry's approach to security and obscurity. The current state of defensiveness and secrecy encountered on security issues in aviation (not only during the implementation of this survey) is notably reminiscent of the behaviour of large software companies in the 1990s, which often preferred to take legal measures against independent security researchers instead of working closely with them as they do today. This has been reflected in our experiences during the recruitment phase of this survey. However, we also found many helpful individuals, typically aided by pre-existing relationships, in particular when established on the personal rather than the institutional level.

It is clear that the fast pace of emerging cybersecurity threats clashes with the time that it takes for new aviation standards and technologies to be conceived, deployed, and finally used operationally on a global scale. This conservative approach has worked well to improve aviation's safety record by minimizing software bugs and hardware problems. However, with regards to wireless security vulnerabilities, aviation has moved at a pace much slower than seen in other, less safety-oriented industries, and it is quickly running out of time.[3]

We do not discuss any concrete security countermeasures, technical or procedural, as they are out of the scope of this paper. We argue that educating those stakeholders that use the affected systems regarding their security and and working closely with them may be one clear avenue to improve the current state of the art. Due to space limitations, we also do not analyze the accuracy of the perceptions individually; it is trivially obvious that all technologies are inherently insecure as security was never part of their design phase, despite some differences in the ease of exploitation. For an extensive overview of the technical possibilities, the reader is referred to [9].

8 Conclusion

In this paper, we reported from a survey about the security of wireless technologies used in aviation. We captured and analysed the knowledge and perceptions

[3] In Feb. 2018, the US Government Accountability Office stressed this point: "Given the amount of time that has transpired since DOD initially raised security concerns in 2008 and the amount of time it will take to formalize, operationalize, and train employees to implement any agreements prior to the January 1, 2020, deadline, it is critical that both DOD and FAA make this a high priority." [4]

of almost 250 aviation professionals and experts, from pilots over air traffic controllers to aviation engineers. As seen during the survey dissemination and the quantitative and qualitative analysis of our findings, there are very different attitudes concerning the topic of security, ranging from ignorance and complacency to hyper-awareness and anxiety.

In summary, we believe that increased awareness by *all* aviation stakeholders can provide the necessary basis for a change in the aviation community's approach to cybersecurity issues. Without all parties on board, crucial regulatory, educational and technical changes are unlikely to be implemented within reasonable time frames.

Acknowledgements

We thank Rui Pinheiro for his input on the survey design and all things air traffic control and Kasper B. Rasmussen for his point of view as a private pilot.

References

[1] P. Avionics. What Are the Biggest Threats to Airlines?, Jan. 2018. URL: `https://up.panasonic.aero/2018/01/18/cybersecurity-biggest-threats-airlines`.

[2] R. H. B. Christensen. Ordinal—regression models for ordinal data, 2018. R package version 2018.4-19. http://www.cran.r-project.org/package=ordinal/.

[3] A. Costin and A. Francillon. Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *Black Hat USA*, pages 1–12, July 2012.

[4] J. Kirschbaum. Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft. Technical report GAO-18-177, US Government Acocuntability Office, Jan. 2018.

[5] P. Polstra and C. Polly. Cyber-hijacking Airplanes: Truth or Fiction? Presented at DEFCON 22, Las Vegas, USA, Aug. 2014.

[6] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. Vienna, Austria, 2017. URL: `https://www.R-project.org/`.

[7] S. S. Silva, L. Jensen, and R. J. Hansman Jr. Safety Benefit of Automatic Dependent Surveillance-Broadcast Traffic and Weather Uplink Services. *Journal of Aerospace Information Systems*, 12(8):579–586, 2015.

[8] R. Skoglund. *Perceived Information Security in the Maritime Sector*. Master's thesis, Norwegian University of Science and Technology, 2017.

[9] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic. On perception and reality in wireless air traffic communication security. *IEEE Trans. on Intelligent Transportation Systems*, 18(6):1338–1357, 2017.

[10] C. A. P. Viveros. *Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts*. Master's thesis, University of Tartu, 2016.

Appendix

A Survey Questions

Question 1: What is your current line of work?
Answer options: Commercial Pilot, Civil Air Traffic Controller, Military Air Traffic Controller, Aviation Engineer, Military Pilot, Aviation Authority, Airline Operator, Not working in aviation; Private Pilot, Other (please specify)

Question 2: How long have you been in your current line of work?
Answer options: <5 years, 5-10 years, 10-20 years, >20 years

Question 3: In what country is your current work based?
Answer options: 249 global countries.

Question 4: What aircraft type(s) are you most familiar with?
Answer options: Free text.

Question 5: In general, how would you judge your knowledge of air traffic comm. technologies?
Answer options: 5-point Likert scale, 1=Very bad, 5=Very good.

Question 6: Which of these specific air traffic communication technologies are you familiar with?
Answer options: List of all 15 technologies, 5-point Likert scale, 1=Very familiar, 5=Not familiar (but heard of it). Separate option 'Not heard of this technology', also covering all following questions.

Question 7: Which of those technologies do you rely on in your work?
Answer options: 5-point Likert scale, 1=Very bad, 5=Very good.

Question 8: How would you rate the trustworthiness of information derived from these technologies against intentional manipulation by a malicious party?
Answer options: 5-point Likert scale, 1=Very insecure, 5=Very secure.

Question 9: How do you rate the likelihood that a malicious party injects false information into these technologies?
Answer options: 5-point Likert scale, 1=Very unlikely, 5=Very likely.

Question 10: How would you rate the impact on flight safety by false information injected by a malicious party into each of these technologies?
Answer options: 5-point Likert scale, 1=Not severe, 5=Very severe.

Question 11: How would you rate the business or monetary consequences of false information injected by a malicious party into each of these technologies? Assume no direct safety incidents.
Answer options: 5-point Likert scale, 1=Not severe, 5=Very severe.

B Survey Comments

Comment 1: Have experienced external parties checking in and disturbing on actual air traffic control frequencies, fortunately without any serious consequence.
Comment 2: New RPAS/UAV threat could ease both jamming ATC to pilots communication, and spoofing ATC instructions. Mechanisms to authentify (and encrypt) controllers-pilots communication will become necessary.
Comment 3: I do research in Mode S based systems. I think they are by far too easy to attack. Problem is that my company [an ANSP] is very closed-minded and not open for any help or suggestions to improve their systems. Existing problems are not recognized (missing Know-How) or are ignored intentionally. Actions are taken AFTER regulations are released by authorities (ex: Eurocontrol). I think, a lot of huge companies behave this way to save costs. EU is very strict in expecting air traffic service providers to reduce costs. So the main target of this research should be informing these authorities about the problems (not directly industry or air traffic service provider) to put them in a position being able to release necessary regulations to improve mentioned systems.
Comment 4: This survey is grossly misleading and the construction of the questions pay scant regard to the real world. There are many examples of these episodes occurring,and having been involved with some of them, this survey misses the mark totally.
Comment 5: Security is often considered as "just existing" investment is often stopped because management finds everything safe and above mentioned scenarios as too far fetched history states it different (9/11).

Comment 6: VHF is an increasingly common comms signal to be maliciously emulated by non involved parties. Particularly on tower frequencies. Anyone can buy a transceiver without licence.
Comment 7: I am a CPL working as a Flying Instructor on light aircraft. Consequently the impact of many of the technologies mentioned is limited for me.
Comment 8: You need to talk to Air Traffic Controllers face to face if you genuinely wish to formulate meaningful questions; you must also understand the if an aircraft does not carry a transponder, it will not show on TCAS hence your questions are irrelevant.
Comment 9: Commercially available drones are becoming more of a problem to general aviation. Those in control of the drones could deliberately endanger aircraft. Also the comms controlling the drones are susceptible to interference from terrorists. A potential development for airliners is the onboard systems overruling pilots thought to be deliberately trying to crash into mountains. If that is done by some remote override, the system needs to be robust against terrorists using that system and/or spoofing other navigation system information to remotely crash the airliner! I still prefer the pilot to be in ultimate control of where the plane is going.
Comment 10: There are plenty of known occurrences in Europe where things go wrong on 1030/1090 MHz. In most cases, it is not an intentional issue, but the effects are there.
Comment 11: I am not aware of any, other than spurious GPS during recent jamming exercises that were carried out, but this did not affect me directly.
Comment 12: Interesting survey which hopefully will contribute to form basis for future contingency policy on Aviation/ATM Security.
Comment 13: ADS-B has to be secured in case it becomes the primary means (and it will!).
Comment 14: In my point of view this study,is a very important area of research as a malicious attack on Aviation Technology can cause severe damage, and the entire aviation community should work together to enhance Security in aviation. Congratulations! Well done.
Comment 15: From the way you asked your questions and what you asked you should not expect to draw scientifically sound conclusions from the questionnaire.
Comment 16: As a human factors and system safety researcher, if a student of mine proposed a questionnaire such as this, there would be discussion about its limitations and council not to field as is. I can see not valid data being generated – it will lacks authority and credibility.
Comment 17: Updates on navigational aids e.g. running SkyDemon on an iPad using an external GPS. I recently carried out the iOS update on my iPad which had bugs which then did not allow SkyDemon to recognise location date being transmitted by the external GPS. All flights then were solely carried out using traditional charts!!!
Comment 18: That government which governs least, governs best. That ATC system that controls least, controls best. And is the most secure. More see and avoid, not more computerize and avoid, is not only safer, it is more secure. The enemy can outmaneuver us better if we are not looking. Patrol vigorously, less reliance on gadgets. I have been to many airports that lock pilots out of the ramp but don't even have a fence to keep a terrorist to set up on the end of the runway with a Stinger.
Comment 19: A general lack of appreciation, ignorance and complacency surrounds the vulnerability of civil aviation comms.
Comment 20: RC comms with mutlirotor RC aircraft seem a more likely route to attack than aviation specific comms.
Comment 21: Sorry, but the questions are phrased rather badly. Are you pilots?
Comment 22: I'm amazed that we still rely on the systems that we do. Even simple things like VHF. They're not secure, but they work and the cost to improve them is likely unmanageable. Hopefully laws will continue to work in preventing nasties.
Comment 23: Impact on automated operations is different - all the systems today are human mediated.
Comment 24: Well that survey isn't leading the answers in any way at all...
Comment 25: Need to make portable ADS-B out units assigned to a specific pilot with a encoded id an option for small private aircraft for a reasonable cost.
Comment 26: Silly survey questions. Adapted from a internet-like cyber security. Remember aviation is behind by 30 years!
Comment 27: Similar to pen testing in my industry (IT Security), can it be attempted to prove that hacking into the on-board system will not mean access to the primary flight controls (A/P). It would calm the travelling public, if that be undertaken by an independent / academic institute.
Comment 28: The writer needs to understand aviation technology a little better before embarking on a piece of work like this.
Comment 29: Some of the questions might have been worded better....perhaps should have run them past a pilot or controller first, or maybe even used some risk analysis from an aviation SMS. Just a thought. Quite interesting possible concepts though...the only time we really experience malicious interference is on VHF, and that, thankfully, is rare where we operate.
Comment 30: Many questions not comprehensible to simple private pilot.
Comment 31: Hope it's not too boring compiling this survey. Thank you for your good work. I'm sure the pub beckons soon...
Comment 32: Not so sure as a private pilot if I help in this survey, perhaps those with an IR and above [are] more helpful.
Comment 33: You are missing FPL comms.