4-2020

Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems

Dhafer Fayez Alqushayri

Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems

by

Dhafer Fayez Alqushayri

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science in Cybersecurity Engineering
at Embry-Riddle Aeronautical University

Department of Electrical Engineering and Computer Science
Embry-Riddle Aeronautical University
Daytona Beach, Florida
April 2020

Cybersecurity Vulnerability Analysis and Countermeasures of

Commercial Aircraft Avionic Systems

by Dhafer Fayez Alqushayri

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Houbing Song, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity Engineering.

Houbing Song
____
Houbing Song, Ph.D.
Committee Chair

____
Radu Babiceanu, Ph.D.
Committee Member

____
Yuan Jiawei, Ph.D.
Committee Member

____
Timothy A. Wilson, Sc.D.
Chair, Electrical Engineering and Computer Science

Maj Dean Mirmirani
____
Maj Mirmirani, Ph.D.
Dean, College of Engineering

Christopher Grant
__________________________ 4/30/2020
Christopher Grant, Ph.D. Date
Associate Provost of Academic Support

Acknowledgments

I would like to acknowledge the dedication of my professors and the administration in the Department of Electrical Engineering and Computer Science at Embry–Riddle Aeronautical University. These individuals have not only helped me in each course of the program but have also shared their wealth of knowledge from their respective fields. I would also like to thank Dr. Houbing Song, Assistant Professor of Electrical Engineering and Computer Science for his mentoring throughout this process.

I would also like to thank Embry–Riddle Aeronautical University for facilitating a positive and forward-looking environment for research. Finally, I want to thank my family and friends for their love, support, and encouragement throughout this program. I am fortunate to have such great people in my life to share in one of my biggest accomplishments in my life.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

IFE – In-Flight Entertainment

EFB – Electronic Flight Bag

FAA – Federal Aviation Administration

ICT – Information and Communications Technology

Abstract

Nowadays, most commercial aircraft use systems with innovative technologies and unprecedented infrastructure of avionics applications which include cyber technologies. Airplane passengers are now using aviation cyber technologies when purchasing tickets, checking in at the airline counter, passing through airport security, and connecting to Wi-Fi and the embedded in-flight entertainment system.

Cyber technologies and connectivity expose aviation to a dangerous and costly world of cyber threats that pose a major challenge of an attack which makes the risks difficult to understand or to define. In addition, the opportunities for attacks continually grow as new services and systems are developed. This thesis looks at understanding these cybersecurity threats and countermeasures of avionics network systems, and their associated defense safety mechanisms and risk analysis will help to pave a secure path toward the increase of protection of our future aviation.

Chapter 1: Introduction

Aviation industries have begun to increase connectivity and digitization in their applications. But this computer interconnectivity from the manufacturers to aircraft puts the aviation industry at risk, similar to the cyber threats that other industries have already experienced. In addition, some pilots and navigators started to replace their traditional flight bag with an electronic flight bag (EFB) tablet, while airlines have started offering more enjoyable services in the in-flight entertainment systems (IFE) through Wi-Fi. Aircraft maintenance operations have also begun to navigate electronic manuals.

Computer interconnectivity from the manufacturers to the aircraft puts the aviation industry at a greater security and privacy risk just like other industries such as technology and telecommunication that have already experienced cyber threats in the past. Each new technological advancement gives hackers a potential doorway. Similar to other industries, the commercial aviation industry is progressively increasing and developing more computers and networks in their applications. With the increased digital connectivity of the aviation system, and its transformation into a globally connected technical system, any small cybersecurity threats on the aviation operating system have the potential of causing rapid global spread, whether this be with security and safety of passengers or at the corporate reputation and economic loss level.

1.1. Problem Statement

With the technology expansion in aviation comes the problem of security and privacy risks that emerge from cyberattacks. There is a growing threat from the use of technologies that may hinder the efficiency of operations. Therefore, the protection of avionics systems from malicious, unauthorized access and destructive activity has become a top priority to guarantee safety and privacy. According to "AVIATION CYBERSECURITY Scoping the Challenge" Report [1], there is a negative impact on expanding the digitization network of aircraft data systems with the internet. It threatens the cybersecurity of the aircraft and it can make them more vulnerable to data corruption and increase the number of vulnerabilities that can occur which threaten the aviation safety system. As a result, commercial aviation cybersecurity threats may have a serious impact and can lead to a hacker gaining control of the aircraft and disrupting its movement while flying.

1.2. Objective

In the thesis, I examine the recent technological advancements that the aviation industry has undergone and the extent to which they have improved the operational efficiency in the industry. More importantly, I address the cyber risks to which the industry has been exposed as a result of the progressive implementation of new technologies. This thesis addresses specific threats such as attacking critical systems, malware infection, vulnerabilities in the flight electronic devices being used by pilots. In order to develop a better understanding of the problem, the thesis discusses the evolution of cyberattacks: That is, how the attacks have changed over the years with the new developments in technology. Understanding the risk exposure also requires an appreciation of the models that have been advanced to explain the concept of cyber-risks and the extent of damage they can have on systems. Although there have been expansive studies on cybersecurity and potential threats that new technologies present to organizations, little has been done to examine the exposure of the aviation industry to the threats. This thesis aims to improve the existing studies by narrowing down the aviation industry as one of the sectors that are at a greater risk of cyberattacks. The vulnerability of the industry to cyberattacks informs the study to explore the risk management framework and safety systems models that can be employed to improve the security and privacy of the aviation industry as it strives to connect people across the world.

1.3. Thesis Structure and Organization

The remainder of this thesis is structured as follows. In the next chapter, there is a review of previous literature on cyber-attacks from a broader perspective. The review highlights some of the fundamental advancements that have been achieved in response to the attacks. There is an assessment of attacks in the aviation industry. Chapter 3 presents the proposed security system for avionics applications. Specifically, it identifies the threats and explains how STRIDE and DREAD models can be used for classifying the threats and rating and analyzing the risks. In chapter 4, there is a discussion of the proposed system safety hazard and risk analysis. It presents an analysis of hazards in the industry and how they contribute to risks. Chapter 5 presents a conclusion of the study and recommendations for future research in the field.

Chapter 2: Literature Review

This chapter discusses previous cyber-attack literature from a broader perspective.

2.1. Evolution of Cyber Attacks

The advent of the internet and subsequent advancements in mobile and computer technology has seen a significant rise in cyber-risks that threaten the security and privacy of personal data. The growth in cyber-attacks on personal platforms, corporate databases, and government infrastructure is an indication of the extent of risk exposure to different forms of databases [2]. The concept of cyber-attack has attracted the attention of several scholars with most studies addressing the evolution in cyberattacks and the threats that the intrusions impose on organizations and governments [3]; [2]; [4]; [5]. These studies have made a significant contribution to the growing body of literature in the field. The current research is aimed at building the existing literature by reviewing the previous studies with a goal of identifying potential gaps that would inform further research to boost an understanding of the concepts.

Nagpal examined the evolution of cyber-attacks from the time earliest forms of computers were developed in around 3500 B.C [6]. The author argued that error of modern computers created an array of analytical engines with much exposure to cyber-threats such as hacking. The advancements in computers that have been characterized by the development of neural networks and Nano-computing technologies increase the exposure of corporate databases and governments' critical infrastructure to potential attacks. According to Nagpal [6], the recent cyber-attacks such as the targeted denial of service access in Estonia increases the fears over the extent to which cyberattacks could hamper the efficiency of service delivery in different sectors. As technologies advance, cybercriminals are also in the race to update their wares for targeted attacks. Nagpal called for a coordinated approach in developing systems that could prevent possible attacks in the future [6]. The involvement of intelligence agencies can be critical in detecting the potential attacks before their actual execution. This can help in reducing the adverse attacks on individuals, governments, and corporate organizations. Moreover, as cyber-crime evolves, the cost associated with the attacks also continues to rise. Nagpal asserted that the attacks often lead to loss of huge data that yield losses not only for governments but also for corporate entities [6]. For instance, in the Estonia attack, the denial of services resulted in an interruption of operations with massive losses of revenues. The popular "Operation Firewall" attack that occurred in 2004 in the U.S resulted in a loss of more than $.7 million from credit cards. It was also characterized by identity thefts and loss of personal and corporate documents [6]. The negative consequences associated with the attacks call for immediate and elaborate action that would prevent potential occurrences and reduce the costs associated with the attacks.

An RSA presentation discussed the evolution of cyber-attacks and recommended threat protection of the next generation. [5] The author recognized that today's attacks are not only complex, but also successful. As such, they present organizations with evolving threat scenarios with which they are less prepared to encounter. Arguably, these threats have bypassed the traditional security protection systems that organizations still use [5]. In the early 2000s, most of the cyberattacks were in the form of disruptions where attackers used worms and viruses to infect databases and computer systems. Although these attacks had a notable impact on organizations and individuals, they were less hazardous compared to the current threats. As technologies continued to advance, the attacks were developed into spyware or bots. They were largely classified as cybercrimes due to the magnitude of their impact on personal data for corporate organizations and government. The last decade has been characterized by aggressive advancements in the attacks. The current attacks are largely in the form of cyber-espionage and cybercrime. These are characterized by dynamic Trojans, stealth bots, advanced persistent threats, and zero-day targeted attacks. The attacks are not only complex but more costly for organizations compared to the earlier forms of attacks.

The cybercrime landscape has significantly changed over the last two decades. From a persistent coordinated threat to dynamic and polymorphic malware, systems are being exposed to more advanced threats than ever before [5]. The attacks are in the form of multi-vector and multi-stage [5]. This scholar argues that multiple vector attacks target valuable assets of an entity, and they include spear phishing, web-based, and file-based attacks. In spear phishing, the target is often on financial information while web-based attacks target intellectual property of different entities [5]. By contrast, multi-stage attacks focus on the exploitation of systems and data exfiltration. Malware is spread vertically, where a download of executable malware is completed by an unsuspecting system user. Aziz recommended the need to adopt a new model to counter cyberattacks. Specifically, he recommended a legacy pattern-matching detection model [5]. The model is effective as it is signature-based and reactive [5]. However, it is limited by the fact that it can only combat known threats, and, considering the threats continue to evolve, it may be inefficient to guarantee full system or data protection. A virtual execution model can also be relevant in protecting private information [4].

2.2. Cyber Attacks in the Global Aviation Industry

The aviation industry is at greater risk of cyber-attacks owing to its unique operations and the extensive reliance on technologies to support operations such as air traffic control, airport control and coordination, and human resource management. The industry employs technologies such as artificial intelligence (AI), robotics, and the Internet of Things (IoT). The overreliance on these technologies exposes the industry to huge risks that could lead to significant damages in economic and technical terms. Additionally, the sensitivity of the industry to security also makes it at high risk for cyberattacks. The susceptibility of the industry to cyber risks has attracted the attention of different scholars. There is a growing body of literature that attempts to examine the reasons behind the industry's high exposure [7]; [8]; [9]; [10]; [11].

Lekota and Coetzee explored the incidence response to cybersecurity threats in the Sub-Saharan African aviation industry [12]. The study recognizes the growing threat that cyber-risks pose to the safety and security of the global aviation system. Some of the attacks identified by the researchers include malicious damage to ICT system, espionage, and theft of information [12]. According to the authors, the threats present huge losses to the aviation industry and are a potential threat to the reliability and safety of the air aviation industry. The growing interconnection of the aviation industry where there is an overreliance on computer-based information technology presents adverse challenges that hinder the efficient growth of the industry [12]. Between 2016 and 2018, there were several cases of cyberattacks in the industry [12]. The attacks varied from terrorism, spying, hackers exploiting loopholes and vulnerabilities of systems, and phishing for financial gains. Lekota and Coetzee recommended a collaborative approach where there is a sharing of responsibilities among different stakeholders in the industry [12]. They argued that the approach would help optimize the safety of the airspace. A coordinated approach to cybersecurity is also necessary for minimizing the risk exposure as each party would focus on their designated areas. It would also create room for innovation that leads to the development of more advanced systems for managing the threats.

According to Lykou, Anagnostopoulou, and Gritzalis, the growing number of air travel passengers per year has necessitated the adoption of technologies in the management and operations of most airports in the globe [13]. From inspection to surveillance of airports, technologies play an important role in enhancing the security of the global aviation industry.

However, the industry is not without risks that threaten the efficiency of operations. The IoT in airport facilities, for instance, present increasing challenges that affect the industry operations. The increased use of smartphones by employees and travelers increases the level of exposure to different threats such as phishing. Personal information such as credit card information is getting exposed to cyber-risks as most travelers prefer card transactions. Although the smart airport has presented notable contributions to the operations of airport facilities, the risk exposures call for action that would reduce the level of exposure and improve the safety and privacy of personal information of both travelers and employees.

Lykou, Anagnostopoulou, and Gritzalis also conducted research on the implementation of cybersecurity measures in airports as a way of improving resilience to cyber-attacks [11]. According to the authors, some of the potential threats include diversion of flights, interruption of system operations, and collapsing the operating systems. These forms of interruption can result in fatal crashes in airspaces. They can also result in the loss of airplanes in airspace. Lykou, Anagnostopoulou, and Gritzalis recommended the adoption of robust cybersecurity governance in smart airports [11]. The researchers also recommended a well-coordinated approach in the management of airport operations. Smart airports not only improve the efficiency of operations but also reduce the costs that airports incur in their daily operations. Nonetheless, without a proper cybersecurity system, the industry could suffer huge losses from the threats.

Rudner presented cybersecurity as an intelligence challenge for the aviation industry [8]. There have been attempts to develop systems that help in providing information on the possible cyberthreats that may hinder the efficiency of airport operations. Although some of the efforts have yielded positive outcomes in developing nations, there are different challenges in intelligence gathering in developing nations [8]. Rudner further recommended a comprehensive approach that involves the participation of different stakeholders in the development of security systems [8]. There is a need for governments to invest in intelligence as a way of collecting critical information that can help in the management of airport operations and eliminate the potential attacks that may affect performance [10]. The aviation industry is at a greater risk of cyber-attacks, particularly with the advancements in technologies.

According to Rudner, intensive investment in security systems will create internal structures that will minimize risk exposure [8]. At the governmental level, critical infrastructure is also at a greater risk of attack. Rudner asserted that airport facilities are part of critical infrastructure due to the important role that they play in the economic growth of countries. Various airlines across the globe are owned by the government, making them part of the critical infrastructure that can be used to improve efficiency [8]. Intelligence efforts should be focused towards creating effective security systems that will detect and prevent potential cyberattacks that may yield losses for the industry. The denial-of-service attack exposed a weakness in the system, the reliance on an infrastructure's unfailing availability. It was a result of the limitations of the current technologies utilized in the industry. Recent reports of remote hacking aimed at airlines, airports, and air traffic management systems suggest that there are only increasing cyber risks; airport passport control, airline flight crews, and baggage control systems are frequent targets.

According to Duchamp, Bayram, and Korhani [7], cybersecurity presents a major challenge for the aviation industry across the globe. The increasing threats of cybercrimes due to advancements in technologies present unprecedented challenges to the industry. The authors recommended a legislative approach towards the management of cyber threats in the industry [7]. They recommended that governments should formulate policies that will work towards enhancing the privacy and security of private data in the airport database systems. A legislative approach gives a less effective strategy in the management of cyber-risks. The increasing evolution of cyber-attacks is making it difficult for governments to develop legislation that will produce effective outcomes such as enhanced security in the aviation industry. Arguably, legislation often does not have a timely manner to be passed because of the technological advances before it is passed and/or implemented. Legislation is aimed to pursue cyber attackers, as general legislation, and it will not specifically address cyberattacks in commercial aviation.

The emergence of unmanned aerial vehicles (UAVs) that occupy the airspace also present notable challenges to the aviation industry. Previous studies have shown UAVs affect the efficient movement of airplanes as they may get into plane engines and could lead to a potential crash. According to Hartmann and Steup, UAVs are often used by terrorists to attack specific target locations [14]. Airports are some of the soft targets where drone technology is largely applied by terrorists to execute attacks. Although the technologies have had a positive impact on the delivery and logistics industry, they present a threat to the operational efficiency of the aviation industry [15]. UAVs are also used in the surveillance of airport facilities for targeted attacks, increasing the risk exposures.

Chapter 3: Security System for Avionics Applications

Security countermeasure is a critical component of the aviation industry. Securing both aircraft internal and external connectivity has become an operational requirement to avoid any cyber threats while also expanding digitization in avionics systems. Wherefore, an airplane's operations management and safety need a security system that can reduce potential threats that avionics applications may face, as well as, facilitate the achievement of security objectives of any organization. This thesis proposes a security system that identifies and classifies all sorts of risks. The said security system develops risk ratings and analysis which aim to reduce the dangerous cyber threats in commercial avionics. Figure 1 elaborates the process of the proposed system.

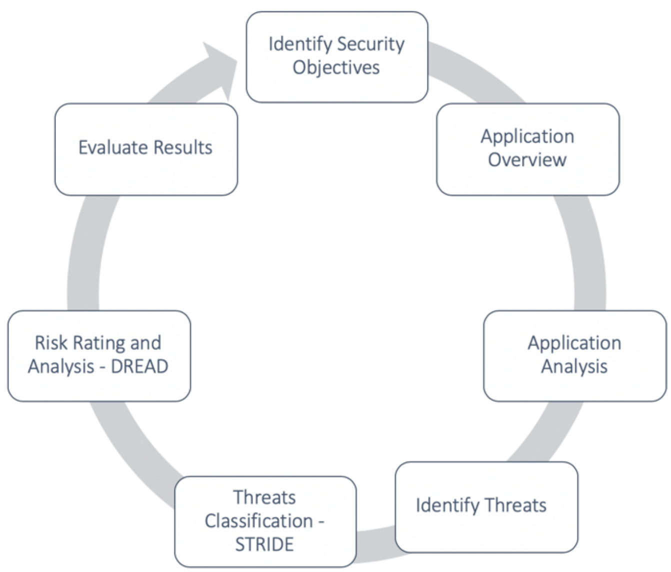

Figure (1): Proposed Security System Model for Avionics Applications

3.1. Identification of Threats

Threat identification is the first rule to adhere for the security process after the applications analysis step is complete. There are some application threats defined in this proposed system and different techniques and methods that are employed by attackers which can affect the avionics systems in commercial aviation as shown in figure (2).

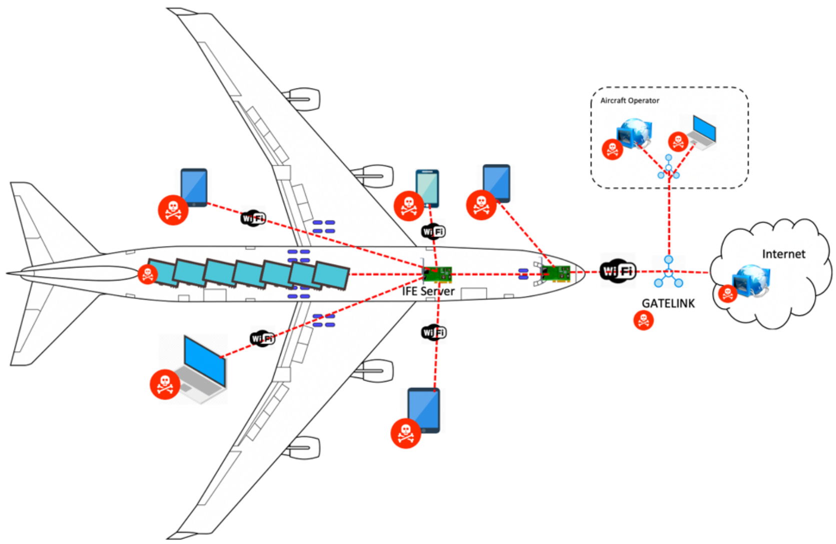

Figure (2): E-enabled Connected Aircraft Security Threats [17]

Threat 1: [16]

Threat ID	1
Threat Description	Attacking Critical Systems via In-Flight Entertainment Systems [16]
Threat Target	To gain control of the IFE system, or potentially crash an aircraft while in flight.
Attack Techniques	Search for security holes, install software before flight take off, and use established vulnerabilities.
Countermeasures	Secure memory, secure communication, and secure run-time environments between internal aircraft components.

Threat 2: [16]

Threat ID	2
Threat Description	Malware Infection over Wireless External Interfaces (2012) [16]
Threat Target	Potential Damage without much effort.
Attack Techniques	Automatic infection with malware from one aircraft to another using the external communication channels.
Countermeasures	Secure and updated firewalls.

Threat 3: [16]

Threat ID	3
Threat Description	Attacking Aircraft via Compromised Information Technology Infrastructures (2011) [16]
Threat Target	Damage connection network to the aircrafts
Attack Techniques	Use any point in the airport infrastructures which has system venerability to get connected to the aircrafts.
Countermeasures	Everything connected to the aircraft is secure, employee's awareness and training programs for potential cyber-attacks, update systems continuously

Threat 4: [16]

Threat ID	4
Threat Description	Vulnerabilities in Commercial-Off-the-Shelf-Based Electronic Flight Bags (EFB) [16]
Threat Target	Get access to electronic documentation of the airline's manuals.
Attack Techniques	Finding vulnerabilities in devices used by the pilot's devices, social engineering.
Countermeasures	Develop trustable protection measures for secure EFB integration that are completely specified, implemented, and approved, and update systems continuously

3.2 Using STRIDE Model for Classification of Threats

After the identification of potential threats, these types of vulnerabilities are classified by the method of STRIDE that was introduced by Microsoft. STRIDE is used as a solid system to characterize these vulnerabilities and security countermeasures. This characterization of vulnerabilities and security countermeasures can reduce potential risks during the engagements of security and privacy. Thus, the classification of potential threats using STRIDE methodology reduces the number of arguments about classification. It indicates that STRIDE comprehends the characteristics of any vulnerability which is caused by attackers.

Abbreviation of STRIDE:

- Spoofing: Impact related to Authentication
- Tampering: Impact related to Integrity
- Repudiation: Impact related to Non-Repudiation
- Information disclosure: Impact related to Confidentiality
- Denial of service: Impact related to Availability
- Elevation of Privilege: Impact related to Authorization

Threats ID	Spoofing Identity	Tampering with data	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
1					✓	✓
2			✓		✓	
3	✓	✓	✓	✓	✓	
4	✓	✓		✓		✓

Table (1): STRIDE threat classification for analysis

After the analysis for STRIDE threat classification Table 1, Threat 1 is classified as Denial of Service to break down the IFE systems or potentially crash an aircraft while in flight. Threat 1 is also classified as an Elevation of Privilege for an attacker who can be authorized using the stolen user seed. As we go through each Threat, this method will help to characterize each threat based on its measurement of the STRIDE threat model. It is very advantageous to know the kind of attack which is being posed by the attacker. It also enables us to know about the severity of the threat.

3.3 Using DREAD-Model for Rating Risk

It may be difficult to fully agree with co-workers on the chosen ratings by using a simplified rating framework. Therefore, to ease this difficulty, additional measurements are added to help figure out the effect of security threats. The DREAD model is used to help figure out the probability of risk, which is abbreviated as Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. By following the accompanying questions, each given threat can be rated:

- Damage potential – How great is the damage if the vulnerability is exploited?
    - 1 = Nothing will be affected.
    - 2 = Individual user data will be affected.
    - = Every user data will be affected.
- Reproducibility – How easy is it to reproduce the attack?
    - 1 = Very hard or impossible
    - 2 = One or more steps required, may need to be an authorized user.
    - 3 = Malicious app, No need of authentication.
- Exploitability – How easy is it to launch an attack?

- 1 = Complicated programming, deep knowledge, and advanced attack tools.
- 2 = Malware exists on the Internet, or an exploit can be easily completed using available attack tools.
- 3 = Easy malware or native application

- Affected users – As a rough rate, how many users are affected?
  - 1 = None
  - 2 = Some users, but not all
  - 3 = All users
- Discoverability – How easy is it to find the vulnerability?
  - 1 = Very difficult to impossible; requires additional source code or administrative authentication access.
  - 2 = Can be found by guessing or by analyzing the application data flow.
  - = Details of faults like this are already in the public domain and can be easily discovered using a search engine.

The previous scale is rating every threat risk by using a straightforward plan of risk rating, which include High (3), Medium (2), and Low (1). Characterizing risk rates in this model will make it easy to perform more clear risk analysis.

3.4 Using DREAD-Model for Risk Analysis

After defining the questions and qualities (1 to 3) for each given threat, the outcome can be in the scope of 5 to 15. At that point, threat dangers with general evaluations can be given as the following:

- (12 to 15) => High Risk.
- (8 to 11) => Medium Risk.

- (5 to 7) => Low Risk.

Priority is given for each threat in the following way to analyze the risk factor from first to last:

- First: High Risk
- Second: Medium Risk.
- Last: Low Risk.

Given threats: [16]

1. Attacking Critical Systems via In-Flight Entertainment Systems.
2. Malware Infection over Wireless External Interfaces.
3. Attacking Aircraft via Compromised Information Technology Infrastructures.
4. Vulnerabilities in Commercial EFB system.

Risk DREAD = D+R+E+A+D / 5

Threats ID	D	R	E	A	D	Total	Rating
Threat 1	3	3	1	2	1	10	Second: Medium Risk
Threat 2	3	3	2	3	1	12	First: High Risk
Threat 3	3	2	1	2	1	9	Second: Medium Risk
Threat 4	2	1	2	1	1	7	Last: Low Risk

Table 2: DREAD rating result for all threats

As Table 2 indicates, Threat 2 becomes the first high risk based on the calculation of D+R+E+A+D risk rating. Outcomes of Threat 1 and 3 are indicated as second high risk while Threat 4 is the last low risk. The method of DREAD model is implemented for comparing, rating, and prioritizing the severity of risk that is caused by given threats that are classified and narrated by using STRIDE model.

Chapter 4: System Safety Hazard and Risk Analysis:

Any current or possible condition which may cause injury or death, damage or failure of a device, structure or property, or environmental damage is a hazard. More often, the hazard is used to describe scenarios that may cause harm to the system. This chapter introduces a proposed system safety model for hazards and risk analysis in avionics applications. This system has two main stages which are hazard analysis and risk reduction management. The main objectives of this system are to make sure that we meet the system's safety requirements to avoid or respond to any potential hazard that may cause harm to the system.

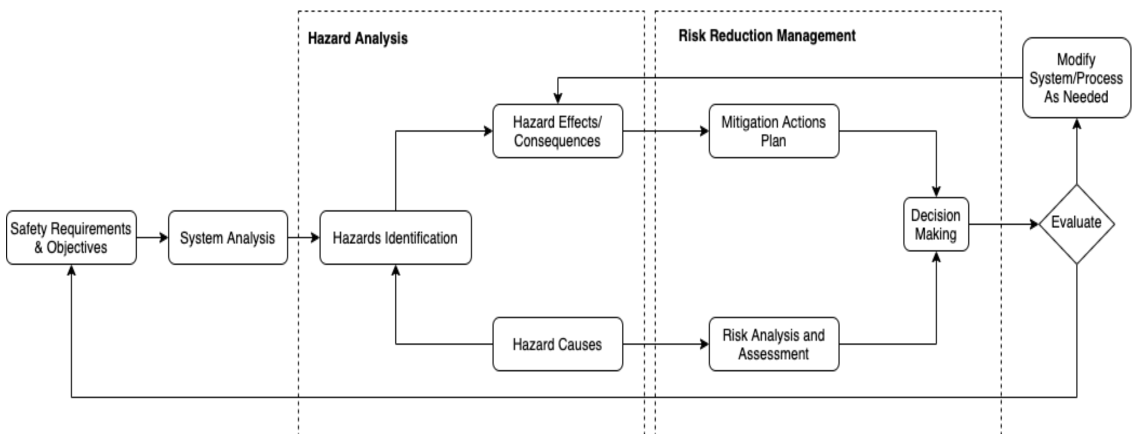

Figure 3: Proposed System Safety Process Model

4.1. Hazard Analysis

Recognizing the potential and severe threats and hazards from a large number of internal and external sources in avionics networks is an important matter. Therefore, by testing similar existing systems or by thinking of worst-case what-if scenarios, safety operators can avoid hazards that may occur due to the consideration of who, what, where, when, why, and how. These scenarios deliver the knowledge about the condition and the significances that will be used during risk analysis. Generally, threats and hazards are first described in the hazard classification list as described in Table 3, and, after that, they are merged in groups for further analysis.

Hazard ID	Hazard	Hazard Causes	Hazard Effects/ Consequences
1	Critical aircraft avionics systems crash	Cyber-attack in on non-isolated system connected to critical systems	Plane crash, civil disaster
2	Malfunction in the aircraft communication systems	Automatic infection with malware	Flight stops and delays, financial losses
3	Malfunction in boarding services	Cyber-attack in the infrastructure network at the airport	Air traffic breakdown
4	Malfunction in Airport Public Wi-Fi	Malware attack to breakdown the service	No public internet access

Table 3: Avionics Systems Hazards

4.2. Risk Analysis and Assessment

The likelihood of the avionics systems hazards shown in Table 3 are acquired using the rating likelihood occurrence levels described in Table 4. In the same way, the severity of the avionics network effects of Table 3 are acquired using the severity rating levels of Table 5. The measurement scale for quantitative evaluations for both tables are on a 1-10 scale. 1 is the least unlikely occurrence or no relevant effect, and 10 is the most frequent occurrence or catastrophic effect.

Rating	Qualitative Evaluation	Quantitative Evaluation
A	Unlikely occurrence	1-2
B	Remote occurrence	3-4
C	Occasional occurrence	5-6
D	Repeated occurrence	7-8
E	Frequent occurrence	9-10

Table 4: Hazard Causes Evaluation Model

Rating	Qualitative Evaluation	Quantitative Evaluation
I	No relevant effect on avionics network	1-2
II	Very minor effect on avionics network	3-4
III	Minor effect on avionics network	5-6
IV	Major effect on avionics network	7-8
V	Catastrophic effect on avionics network	9-10

Table 5: Hazard Effects Evaluation Model

In the process of risk analysis, it is crucial to comprehend the characteristics of threats and hazards on the basis of the severity of hazard effects and occurrence likelihood. The level and extent of risks can be obtained by using the matrix of Risk Assessment. The risk assessment is obtained by merging the severity of hazard with the likelihood of occurrence for each of the given hazards. The qualitative risk assessment is obtained by using the risk assessment matrix of Table 6, and the quantitative risk assessment is obtained by adjusting the quantitative results of risk, such that they can be determined on a 1-10 scale.

	A	B	C	D	E
I	Low	Low	Low	Moderate	High
II	Low	Low	Moderate	High	High
III	Low	Moderate	Moderate	High	Very high
IV	Low	Moderate	High	Very high	Very high
V	Moderate	High	Very high	Very high	Very high

Table 6: Hazard Risk Assessment Matrix

The low-risk cells in the Risk Assessment Matrix of Table 6 indicate a low risk to be affected by cyber threats in avionics systems. Consequently, the risk increases to moderate, high, and very high, which indicates that there is an increased risk of potential cyber threats in avionics systems. Thus, we can evaluate the hazard by using data from risk level. Either it meets the system safety requirements and objectives or it needs to be reprocessed again.

Chapter 5: Conclusion and Future Research Recommendations

In this chapter, I conclude this thesis, and then I discuss future research tasks.

5.1. Conclusion

Aviation is at the forefront of technological expansion, and that is because the number of air travel passengers is exponentially increasing every year. As a result, airline companies enhance their technology innovation plan and develop smart services to support growth and efficiency by offering an enjoyable travel experience. Additional challenges and risks are coming up, which aviation has to deal with and adjust to, such as integrating connectivity in airplanes and the increased use of smart devices from aviation industries and passengers.

In the thesis, I have proposed a security system to identify the threats in the aviation application. By applying the STRIDE and the DREAD models, we can mitigate the risks in cybersecurity. The proposed structure works by identifying the objectives of the application and then looks for the threats in the application. And, at the end, it applies different security measures like STRIDE to do the risk and hazard analysis and mitigates the threats.

Cybersecurity is becoming an important factor for safety, which is essential in the aviation field. By implementing cybersecurity standards and solutions in cybersecurity threats of avionics network systems, their associated defense mechanisms will help to pave a secure path toward the increase of protection of our future aviation.

5.2. Future Research Recommendations

There is a need for future research and work to identify areas that are accessible to cyber attackers when they are on aircrafts and define the vulnerability of NextGen in new and old aircrafts. Additional research is needed on how the aircraft manufacturers install the internal aircraft wiring, focusing on the aircraft's network, and how it will provide a better assessment of these areas of vulnerability. Future research should focus on how possible it is for a terrorist attacker to take control of the plane while in the air, as seen in Chris Robert’s YouTube video in which he illustrated taking control of the aircraft and moving it sideways. One of the largest questions there is regarding wireless access is, does a passenger have access to the aircraft network and access flight control?

REFERENCES

[1] Cooper, P. & Handler, S Shahwan, S(2019) *Aviation Cybersecurity: Scoping the Challenge.* Atlantic Council

[2] Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

[3] Tang, Y., Chen, Q., Li, M., Wang, Q., Ni, M., & Fu, X. (2016, October). Challenge and evolution of cyber-attacks in Cyber Physical Power System. In 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC) (pp. 857-862). IEEE.

[4] Minchev, Z., Dukov, G., Boyadzhiev, D., & Mateev, P. (2016). Future Cyber Attacks Modelling & Forecasting. ESGI, 120, 77-86.

[5] Aziz, A. (2013). The evolution of cyber-attacks and next generation threat protection. In RSA conference.

[6] Nagpal, R. (2008). Evolution of cyber Crimes. Asian School of Cyber laws, 2.

[7] Duchamp, H., Bayram, I., & Korhani, R. (2016). Cyber-security, a new challenge for the aviation and automotive industries. In Seminar in Information Systems: Applied Cybersecurity Strategy for Managers (pp. 1-4).

[8] Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and Counterintelligence, 26(3), 453-481.

[9] Holt, T. B., Moallemi, M., Weiland, L., Earnhardt, M., & McMullen, S. (2016). Aircraft Cyber Security and Information Exchange Safety Analysis for Department of Commerce.

[10] Shackelford, S. J., & Russell, S. (2014). Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector. FIU L. Rev., 10, 635.

[11] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018, June). Implementing cyber-security measures in airports to improve cyber-resilience. In 2018 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.

[12] Lekota, F., & Coetzee, M. (2019). Cybersecurity Incident Response for the Sub-Saharan African Aviation Industry. In International Conference on Cyber Warfare and Security (pp. 536-XII). Academic Conferences International Limited.

[13] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, 19(1), 19.

[14] Hartmann, K., & Steup, C. (2013, June). The vulnerability of UAVs to cyber-attacks-An approach to the risk assessment. In 2013 5th international conference on cyber conflict (CYCON 2013) (pp. 1-23). IEEE.

[15] Hu, Q., Chang, Y. H., & Tomlin, C. J. (2016). Secure estimation for unmanned aerial vehicles against adversarial cyber-attacks. ArXiv preprint arXiv: 1606.04176.

[16] Wolf, Minzlaff, & Moser. (2014). "Information Technology Security Threats to Modern e-Enabled Aircraft: A Cautionary Note". JOURNAL OF AEROSPACE INFORMATION SYSTEMS

[17] (2010), "*A Case For Aircraft Security.*" SpeedBired. Online: https://speedbird-ncl.com/2010/01/27/a-case-for-aircraft-security/