Cyber vulnerabilities in the aviation ecosystem: reducing the attack surface through an international aviation trust framework

Saulo José da Silva

Thesis for obtaining the degree of Doctor of Philosophy in
Aeronautical Engineering
(3rd Cycle Studies)

Orientador: Prof. Doutor Jorge Miguel dos Reis Silva

Júri:
Prof. Doutor Abel João Padrão Gomes
Prof. Doutor Remzi Seker
Prof. Doutor Francisco Miguel Ribeiro Proença Brójo
Prof. Doutor Jorge Miguel dos Reis Silva
Prof. Doutor Paulo Fernando Vieira de Carvalho Cardoso do Amaral
Prof. Doutora Maria Emília da Silva Baltazar

10/10/2022

Dedicatory

All the work presented in this document has the origin in one professional and one personal motivation. In the professional field it is an effort to improve even more the services provided by the aviation industry, that was for my entire life my professional passion, to our society and allowed me to do what I always wanted to do that was to help others to have better education and well being. In the personal field it was the will to show to my parents that they did a good job in my education and if they were alive they could be proud of the education they provided to me. I dedicate this work also, and with tear in my eyes, to the memory of my sisters Gisele and Marília, that are not among us anymore, but were always proud of my work, supported me and always understood my initiatives. This work was also motivated by the will to show to my kids Saulo Filho, Matheus José and Marcella Maria that they are capable of anything as long as they can put their minds and hearts in the same place and looking forward to the same objectives. Therefore, to you my parents, brothers and sisters, sons and daughter, aviation professionals, I dedicate this work, because you were the ones who always motivated me and made me the professional I am today.

Dedicatória

Todo o trabalho apresentado nesse documento tem origem em uma motivação profissional e uma motivação pessoal. No plano profissional é uma tentativa de melhorar ainda mais os serviços prestados pela indústria da aviação à nossa sociedade que foi por toda vida minha paixão profissional e me proporcionou a oportunidade de ver e fazer o que sempre quis, que foi ajudar ao próximo a ter o que todos os seres humanos merecem que é educação e dignos níveis de vida. No plano pessoal a vontade de mostrar aos meus pais que eles acertaram sempre na minha educação e que se fossem vivos hoje poderiam se orgulhar da educação que me proporcionaram. Dedico esse trabalho também, com uma lágrima nos olhos, a memória de minhas irmãs Gisele e Marília que já nos deixaram, mas que sempre se orgulharam, apoiaram e entenderam todas as minhas iniciativas. Esse trabalho também foi motivado pela vontade de mostrar aos meus filhos, Saulo Filho, Matheus José e Marcella Maria, que eles são capazes de tudo, desde que possam colocar seus corações e mentes no mesmo lugar e visando o mesmo objetivo. Portanto a vocês, profissionais da aviação, meus pais, irmãos, irmãs e filhos, eu dedico esse trabalho, pois foram vocês que me motivaram sempre e me fizeram ser o profissional que hoje sou.

Acknowledgment

This work could not be done without the support and cooperation of many people and organizations. Therefore, I would like to thank the Brazilian Airspace Control Department (DECEA) to allow me to start and progress my career in air traffic management. Particularly I would like to thank Mr. Ricardo Nogueira who always believed in the professionalism of air traffic management specialists in the development of the Brazilian aviation system. To the International Civil Aviation Organization (ICAO) that allowed me the opportunity to be involved and develop international regulations related to different areas of the civil aviation system. Specially, I would like to thank Mr. Vincent Galotti, my first chief in the air traffic management section of ICAO for always believe, support and provide the guidance that any air traffic management expert need to evolve professionally. To the University of Beira Interior to believe in the potential of my work. To my friend and motivator Omar Daniel that convinced me to proceed in my researches and was always at my side helping and guiding when necessary. To my friend Elaine Cristina Arantes that in my moments of apprehension provided the enlightenment and guidance that was missing. To my supervisor Professor Doctor Jorge Miguel Reis Silva, that became a special person to my life and that without his positive guidance I would never have concluded this work. And more than a supervisor, Professor Jorge was always a good friend ready to understand the difficulties associated to this kind of research and always point to the right direction. To my parents Mario e Maria José da Silva (in memorian) to create the conditions to my studies that allowed me to become the professional I am today and for teaching me the importance of the persistence in the path towards personal ideals. To my sons Saulo Filho and Matheus José and my daughter Marcella Maria that always incentivized me to continue my studies. To my aviation professional friends and experts from all over the world that with their contributions and conversations that many times made me rethink and modify important concepts allowed me to learn and grow as a professional.

To all of you, my big thank you.

Agradecimentos

Esse trabalho não poderia ter sido realizado sem o suporte e cooperação de várias pessoas e organizações. Portanto, gostaria de agradecer ao Departamento de Controle do Espaço Aéreo Brasileiro (DECEA), por ter me proporcionado a oportunidade de começar e evoluir na carreira de gerenciamento de tráfego aéreo. Em particular ao Coronel Aviador Ricardo Nogueira que sempre acreditou no profissionalismo de especialistas em controle de tráfego aéreo no desenvolvimento do sistema de aviação civil brasileiro. A Organização de Aviação Civil Internacional (OACI) por ter me proporcionado a oportunidade de me envolver e desenvolver regulamentos internacionais relacionados a diversas áreas da aviação civil. Em particular ao senhor Vincent Galotti, eterno chefe da seção ATM, por sempre acreditar, apoiar e proporcionar a orientação profissional que qualquer especialista em gerenciamento de tráfego aéreo necessita para evoluir profissionalmente. A Universidade da Beira Interior por acreditar no potencial do meu trabalho. Ao amigo e incentivador Omar Daniel que me convenceu a prosseguir em minhas pesquisas e esteve sempre a meu lado orientando e ajudando. A minha amiga Elaine Cristina Arantes que em momentos de apreensão proporcionou a luz guia que faltava. Ao meu orientador Professor Doutor Jorge Miguel Reis Silva, que se tornou uma pessoa especial em minha vida e que sem a positiva orientação eu jamais teria concluído esse trabalho. E mais que um orientador, Professor Jorge foi sempre um grande amigo disposto a entender as dificuldades de uma pesquisa como essa e sempre apontar na direção correta. Aos meus pais Mario e Maria José da Silva (in memorian) por terem me proporcionado as condições para que eu pudesse estudar e me tornar o profissional que hoje sou e me ensinarem o quão importante é ter persistência na busca por ideais. Aos meus filhos Saulo Filho, Matheus José e Marcella Maria que sempre me incentivaram a continuar meus estudos. Aos meus amigos profissionais da aviação e especialistas de todo o mundo que com suas contribuições e conversas por muitas vezes me fizeram repensar e modificar conceitos importantes que me fizeram aprender e crescer como profissional.

A todos vocês, o meu muito obrigado.

List of publications

Published articles resulting from this doctoral thesis:

1. Cyber resilience

Saulo José da Silva (2018). Thirteenth Air Navigation Conference (09-19 October 2018), https://www.icao.int/meetings/anconf13/Pages/default.aspx

2. A comprehensive strategy for air navigation: Endorsement of the updated Global Air Navigation Plan

Saulo José da Silva (2019). Fortieth Session of the ICAO General Assembly. Agenda Item 28: Aviation safety and air navigation policy (24 September to 04 October 2019), Assembly 40th Session (icao.int)

3. Trust framework for a digital environment

Saulo José da Silva (2019). Fortieth Session of the ICAO General Assembly. Agenda Item 30: Other Issues to be considered by the Technical Commission (24 September to 04 October 2019), Assembly 40th Session (icao.int)

4. Cyber Risks In The Aviation Ecosystem: An Approach Through a Trust Framework

Saulo José da Silva (2021). Integrated Communications Navigation and Surveillance Conference (ICNS). https://ieeexplore.ieee.org/document/9441596

Resumo

Atualmente, no início do século vinte e um, a aviação está em uma situação similar ao início do século vinte, entretanto, desta vez, o sistema de aviação civil está bem consolidado, mas se transformando rapidamente motivado por uma onda de novas tecnologias que apresentam grandes promessas, mas que ao mesmo tempo podem expor a aviação a novas ameaças.

Certos aspectos da transformação digital do sistema de aviação civil, baseado em redes que permitem ampla conectividade, devem ser corretamente orientados para garantir níveis globais de segurança e interoperabilidade ainda mais elevados. Para enfrentar esse desafio, necessário se faz o estabelecimento de um sistema de identidades digitais e confiança que integre a sabedoria da Convenção de Chicago ao mundo digital que está invadindo a indústria da aviação.

Provedores de serviços, fabricantes de aeronaves e aviônicos estão todos colocando em prática seus próprios sistemas de identificação e confiança por necessidade. Isso significa que em um futuro próximo, uma aeronave poderá precisar de diferentes certificados para conectar-se com seus provedores de comunicações por satélite, receber dados de um centro de coordenação de uma compania aérea, atualizar programas em seus aviônicos, baixar dados para monitoramento do funcionamento de seus motores e outras funções. Esse conjunto de iniciativas isoladas para se reduzir a superfície de ataque cibernético para operações no solo e no ar adicionam complexidade ao sistema considerando que essas iniciativas isoladas tornam o sistema como um todo custoso para se manter e também oferecem uma série de vulnerabilidades a serem exploradas por atores mal intencionados.

Na ausência de uma direção global, diferentes fabricantes, provedores de serviços e Estados tomarão direções distintas. Entretanto, se um sistema global de identificação digital e confiança que possa ser usado indistintamente pela aviação tripulada e não tripulada, por provedores de serviços, fabricantes e usuários for posto em prática, é muito provável que o mesmo seja adotado por todos dentro do sistema de aviação civil.

Portanto, baseado nas novas vulnerabilidades que a evolução dos sistemas de navegação aérea estão trazendo com o uso intenso de tecnologias digitais e conectadas, o objeto desta tese está relacionado às vulnerabilidades do sistema de aviação civil a um ataque cibernético e o objetivo foi o de propor um conceito operacional que permitisse a

implementação de uma estrutura capaz de identificar todos os atores da comunidade de aviação civil através de procedimentos e processos específicos e uma rede virtual para preservar a confidencialidade, a integridade e a disponibilidade das informações e dados sendo intercambiados ao mesmo tempo em que a resiliência do sistema é melhorada através de uma arquitetura específica.

Palavras-chave

Ataque. Confiança. Digital. Identidade. Interoperabilidade. Segurança. Vulnerabilidades.

Resumo Alargado

Introdução

Este capítulo contém a descrição da motivação que levou ao desenvolvimento da investigação desenvolvida na tese de doutoramento na área de Engenharia Aeronáutica. Em particular este capítulo ressalta os passos associados à invenção do avião e os aspectos das novas demandas associadas à operação de aeronaves, incluindo a evolução da infraestrutura dos sistemas de comunicação, navegação e vigilância em suporte às operações aéreas, assim como aqueles desenvolvimentos que permitiram o gerenciamento de trafego aéreo como consequência do aumento da demanda por transporte aéreo desde a invenção do avião e passando pelos impulsos recebidos durante as guerras do início do século vinte. Ressalta-se também as necessidades relativas ao gerenciamento de informações críticas ao suporte das operações aéreas. Nesta secção descreve-se também o problema abordado e os objetivos da pesquisa, assim como a estrutura dos capítulos.

Enquadramento da Tese

Desde a invenção do avião foi identificado que para permitir o compartilhamento do mesmo espaço aéreo por diferentes tipos de aeronaves, sistemas de suporte ao gerenciamento de tráfego aéreo incluindo aqueles relacionados à provisão de informações em apoio às operações aéreas eram cruciais. O conceito de gerenciamento de informações evoluiu muito durante o século passado não somente no conteúdo das informações necessárias, mas nos meios utilizados ao intercâmbio de mensagens.

A indústria do transporte aéreo, pressionada por fatores econômicos e ambientais iniciou uma corrida por novas soluções que pudessem trazer os benefícios esperados pela sociedade sem, no entanto, afetar os níveis de segurança operacional praticados pela indústria aeronáutica.

Observou-se que o uso de novas tecnologias e conceitos operacionais poderiam trazer os benefícios esperados, no entanto, com a introdução dos novos conceitos e tecnologias, novos pontos deveriam também ser considerados visto que novas tecnologias também abriram as portas para novos eventos que podem afetar direta e negativamente a segurança e a eficiência das operações aéreas. Notadamente, as melhorias operacionais utilizando os conceitos de conectividade para disponibilização de informações a todos os usuários em qualquer lugar do planeta e a qualquer tempo.

A indústria aeronáutica tem uma grande influência na economia global e o equilíbrio entre o interesse público em geral, os provedores de serviços e os operadores de aeronaves devem ser conciliados.

A indústria da aviação civil é também reconhecida por ser complexa em termos de segurança operacional e baixas margens de lucro financeiro. O Plano Global de Navegação Aérea publicado pela Organização de Aviação Civil Internacional ressalta que o sistema de navegação aérea está se tornando cada vez mais complexo não somente devido ao aumento do tráfego aéreo que é esperado duplicar nos próximos vinte anos, mas também pelo aparecimento de novas plataformas de vôo dedicadas a novos usuários do espaço aéreo. Esses novos usuários vêm com novas demandas ao sistema considerando suas distintas necessidades, missões e características operacionais.

A transformação do sistema de navegação aérea para apoiar essa nova demanda é, portanto, necessária se o sistema de aviação civil quiser manter ou melhorar os níveis de segurança operacional e a eficiência até então praticados e apreciados pela sociedade e que são refletidos no sucesso financeiro global proporcionado pela indústria da aviação. Essa transformação do sistema de aviação civil depende necessariamente do uso de novas tecnologias e conceitos operacionais, alguns deles desenvolvidos para atender outras indústrias e sem atenção aos requisitos operacionais da indústria da aviação.

A necessidade de um sistema de intercâmbio de informações a nível global torna-se, portanto essencial para a transformação do sistema de aviação civil. Esse sistema global para intercâmbio de informações não pode ser bem sucedido se os diferentes participantes do sistema não puderem confiar em seus diferentes componentes. Dessa forma, uma rede resiliente para intercâmbio de informações baseado em uma estrutura de confiança surge como o único meio capaz de permitir a transformação do sistema de aviação civil em um ambiente digital. Portanto, qualquer evolução passa necessariamente pela solução dos problemas associados às ameaças cibernéticas.

Ao longo desta pesquisa necessário se fez ressaltar que o termo segurança cibernética é entendido não somente como medidas de proteção de sistemas de suporte a navegação aérea, mas também medidas para garantir a resiliência do sistema em caso de eventos inesperados realizados por atores com a clara intenção de causar problemas aos serviços de navegação aérea essenciais à segurança operacional, eficiência e continuidade das operações aéreas.

E considerando o ambiente digitalmente conectado que se apresenta à sociedade atualmente, necessário se faz que a comunidade de aviação civil adote uma posição

harmonizada para garantir a confidencialidade, integridade e disponibilidade das informações em um ambiente que possa ser confiável. Iniciativas isoladas, apesar de ajudarem a proteger recursos locais, não contribuem muito para um comportamento global do sistema de aviação civil considerando os possíveis intervalos e/ou sobreposições que podem ameaçar a segurança e resiliência do sistema como um todo.

A necessidade de um sistema global projetado com defesas em camadas de forma a reagir aos ataques cibernéticos requer a existência de uma rede para intercâmbio de informações resiliente e segura que possa atender aos requisitos específicos da aviação civil além de processos que possam garantir a identidade digital de seus componentes.

Descrição do Problema e Objetivos da Investigação

O objeto da presente tese é a confiança entre os diferentes participantes do sistema de aviação civil e os procedimentos para assegurar a resiliência cibernética em um sistema que está evoluindo em direção a uma conexão digital cada vez mais presente nos processos de gerenciamento de tráfego aéreo.

No presente sistema conectado digitalmente, informações críticas e não críticas para a segurança das operações aéreas fluem de ponto a ponto sem ou com mínimo controle da integridade das informações sendo intercambiadas entre os diferentes participantes e com diferentes procedimentos associados à geração e preservação do conteúdo das informações. Ao mesmo tempo, a verificação da identidade dos participantes envolvidos no intercâmbio de mensagens se torna um desafio que necessita ser resolvido de forma a garantir que somente fontes confiáveis e autorizadas possam prover e consumir informações que serão utilizadas operacionalmente.

Esta pesquisa procura discutir como a evolução sendo feita por usuários do espaço aéreo, provedores dos serviços de navegação aérea e de comunicações, operadores aeroportuários e autoridades reguladoras através de conexões digitais visando um aumento da capacidade do espaço aéreo e a eficiência do sistema de navegação aérea podem ser realizados de uma forma gradual e sem afetar os níveis de segurança operacionais acordados pela comunidade de aviação civil. Essa evolução está diretamente associada à necessidade de informações confiáveis para uma melhor tomada de decisão pelos gerentes e pessoal técnico e operacional reconhecendo que as necessárias conexões digitais também geram novas vulnerabilidades relacionadas a uma operação com processos realizados usando o espaço cibernético.

Metodologia da Pesquisa

No desenvolvimento desta tese e considerando o problema a ser investigado, a metodologia para coleta de dados que apresentou melhores resultados, e seguindo um paradigma pragmático, foi o de entrevistas com profissionais de aviação de diferentes áreas e níveis, associada à análise de documentos publicados.

As entrevistas geraram uma fonte de dados muito rica considerando a liberdade que os entrevistados tiveram para expressar suas visões sem se preocupar com qualquer formalidade ou quebra de sigilo. A decisão por utilizar um método de entrevistas não estruturada foi feita depois de se considerar a complexidade do assunto e a falta de uma literatura especializada no tema relacionado aos desafios enfrentados pela comunidade de aviação civil usando conexões digitais para intercâmbio de mensagens críticas à segurança das operações aéreas.

Principais Contribuições

Esta tese tem como primeira contribuição o esclarecimento para a comunidade de aviação civil das consequências relativas à utilização do espaço cibernético para o intercâmbio de informações e os possíveis impactos na segurança, eficiência e continuidade das operações aéreas.

O estado da arte apresentado no capítulo 2, apresenta uma descrição detalhada das evoluções dos diferentes sistemas de suporte às operações aéreas e a introdução gradual de novos sistemas, alguns não originalmente projetados para uso pela aviação civil, mas que atualmente fazem parte da realidade operacional de operadores de aeronaves e provedores de serviços de navegação aérea, o que contribui para um melhor entendimento da comunidade aeronáutica dos benefícios e também dos riscos associados ao alto grau de conectividade no atual sistema de aviação civil.

A terceira contribuição é a proposta de um conceito operacional que pode ser utilizado por todos os membros da comunidade aeronáutica para melhorar a segurança e eficiência das operações aéreas através da digitalização de sistemas e processos sem reduzir os níveis de segurança acordados para a indústria do transporte aéreo. Este modelo está descrito de forma detalhada no capítulo 5 e culminou na submissão de um artigo para a Conferência Integrada de Comunicação, Navegação e Vigilância e publicação na revista internacional do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE).

Principais Conclusões

Algumas das premissas resultantes deste trabalho de investigação foram testadas através de uma prova de conceitos realizada entre provedores de serviços de navegação aérea de forma a produzirem evidências da possibilidade de implementação e eficiência dos conceitos e processos propostos.

O aumento da demanda por utilização do espaço aéreo por novas plataformas voadoras e tipos de usuários resultaram na implementação de sistemas automatizados e para suporte à tomada de decisões.

Com fortes requisitos por automação veio também a necessidade de conexão de sistemas antes isolados e o gerenciamento de informações se tornou crucial para a segurança e eficiência do transporte aéreo.

Com a gradual transformação das comunicações ponto-a-ponto para um sistema global de gerenciamento de informações utilizando a infraestrutura instalada da Internet, atenção se faz necessária ao fato de que a confidencialidade, a integridade e a disponibilidade das informações no espaço cibernético podem ser afetadas se medidas de segurança para gerenciar as informações sendo intercambiadas não forem tomadas de forma pró-ativa.

Para permitir uma transformação digital do sistema de aviação civil, processos e procedimentos associados a um intercâmbio de informações de forma global se tornam essenciais. O intercâmbio seguro de informações críticas às operações aéreas só pode ser realizado através do uso de uma rede resiliente construída através de uma estrutura de confiança. Isso ressalta a importância de informações seguras para um sistema de aviação civil resiliente e que atenda aos requisitos de segurança operacional.

Perspetivas de Investigações Futuras

Como consequência do trabalho desenvolvido e do conhecimento adquirido, as perspetivas de investigações futuras relacionadas a esta tese são as seguintes:

I. Aplicação da estrutura de confiança como parte de um estudo de caso envolvendo diferentes componentes da indústria da aviação e das indústrias de suporte.
II. Diferentes tecnologias existem para gerenciamento de identidades digitais. Uma nova investigação poderia ser feita para uma avaliação dessas tecnologias.
III. Implicações do uso de DNS públicos e privados com um DNSSEC como parte de uma estrutura de confiança.

IV. O impacto da blockchain na confidencialidade, integridade e disponibilidade de informações críticas à segurança operacional.

V. As possíveis arquiteturas de uma infraestrutura de chaves públicas para uma estrutura de confiança global.

VI. As melhores opções para o gerenciamento de uma estrutura de confiança global do alto de uma visão política, operacional e econômica.

VII. Um modelo de ameaças para identificação e análise de riscos cibernéticos.

VIII. Um sistema seguro de gerenciamento de informações adaptado às necessidades da indústria da aviação civil.

IX. Os riscos associados ao uso das comunicações por satélites em um ambiente de confiança.

X. Vulnerabilidades cibernéticas e soluções para o sistema dependente automático de vigilância (ADS) como tecnologia para vigilância aeronáutica.

XI. Vulnerabilidades cibernéticas e soluções para o uso das comunicações por dados entre piloto e controlador de tráfego aéreo (CPDLC).

Abstract

Now, at the beginning of the 21st century, the aviation system is well developed, however, the community is at similar juncture as the beginning of the 20th century, only this time the civil aviation system itself is being rapidly transformed by a wave of digital technologies that hold great promise but could also expose the aviation system to new threats.

Certain aspects of the digital transformation of the aviation system, based on network connectivity, must be guided to ensure that it generates ever higher-levels of global interoperability and safety. To address this challenge, it is necessary to go back to fundamental principles. It is necessary to establish a system of identity and trust that integrates the wisdom of the Chicago Convention into the digital world that is already overtaking the aviation industry.

Service providers, aircraft manufactures, and avionic producers, are all putting in place their own systems of identity and trust as a matter of necessity. That means, in the near future, an aircraft may need different digital certificates to connect with its satellite communications service provider, retrieve data from the airline operations centre, update its avionics software, download engines monitoring data and other functions. The potential number of proprietary secure links is nearly endless. This patchwork of disparate efforts to reduce the attack surface to air and ground operations will add complexity to the system that will be costly to maintain and will offer a myriad of gaps for adversaries to exploit.

In the absence of global direction, different manufactures and different States will take different approaches. However, if a globally acceptable system for identity and trust that can be used by manned and unmanned aircraft indistinctively as well as by different service providers and users is available it would likely be embraced by many or all.

As such, based on the new vulnerabilities brought by the evolution of the air navigation system through the intense use of digital and connected technologies, the object of this research relates to the vulnerabilities of the aviation system to a cyber-attack and the objective of this thesis is to propose a concept of operations that allows the implementation of a framework able to provide positive digital identification of all members of the aviation community through specific processes and procedures and a virtual network able to preserve the confidentiality, integrity and availability of the data and information being exchanged at the same time it increases the resilience of operations.

Keywords

Attack. Digital. Identity. Interoperability. Networks. Safety. Trust. Vulneralities.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACAS	Airborne Collision Avoidance System
ADF	Automatic Direction Finder
ADS-B	Automatic Dependent Surveillance-Broadcast
AI	Artificial Intelligence
AIP	Aeronautical Information Publication
AMQP	Advanced Message Queuing Protocol
ANSP	Air Navigation Service Provider
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASM	Airspace Management
ATC	Air Traffic Control
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATS	Air Traffic Services
BCA	Bridge Certificate Authority
BI	Business Interruption
CA	Certificate Authority
CAA	Civil Aviation Authority
COTS	Commercial Off-The–Shelf
DME	Distance Measuring Equipment
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
EBCDIC	Extended Binary Coded Decimal Interchange Code
FBI	Federal Bureau of Investigation
FCS	Frame Check Sequence
FTP	File Transfer Protocol
GBAS	Ground-Based Augmentation System
GCA	Ground-Controlled Approach
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HF	High Frequency
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation of Assigned Names and Numbers
ICAO	International Civil Aviation Organization
ICMP	Internet Control Message Protocol

IDC	International Data Corporation
IETF	Internet Engineering Task Force
IFF	Identification Friend or Foe
IFR	Instrument Flight Rules
IGMP	Internet Group Management Protocol
ILS	Instrument Landing System
IMAP	Internet Message Access Protocol
INS	Inertial Navigation System
IP	Internet Protocol
IPS	Internet Protocol Suite
IT	Information Technology
ISMS	Information Security Management System
JMS	Java Message Service
LAN	Local Area Network
LCD	Liquid Crystal Display
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MEDS	Multifunction Electronic Dis[lay Subsystem
MTBF	Mean Time Between Failures
NDB	Non-Directional Beacon
OCSP	Online Certificate Status Protocol
OSI	Open System Interconnection
PAN	Personal Area Network
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PSR	Primary Surveillance Radar
RA	Registration Authority
RAIN	Receiver Autonomous Integrity Monitoring
RAN	Regional Area Network
RIP	Routing Information Protocol
RPC	Remote Procedure Calls
SARPs	Standards and Recommended Practices
SBAS	Satellite-Based Augmentation System
SE	Security Environment

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoS	System of Systems
SSR	Secondary Surveillance Radar
TCP	Transmission Control Protocol
TELNET	Teletype Over Network Protocol
TLD	Top Level Domain
TLS	Transport Layer Security
UDP	User Datagram Protocols
UHF	Ultra-High Frequency
VFR	Visual Flight Rules
VHF	Very-High Frequency
VOR	VHF Omni-Directional Range
VPN	Virtual Private Network
WAN	Wide Area Network

Chapter 1

Introduction

1.1 Motivation

The invention of the airplane was a challenge for a series of researchers, scientists, engineers and entrepreneurs, some of them with a life dedicated to discover the secrets of birds to stay and navigate in the air in a controlled way. These challenges were associated, among other aspects, to discover the dynamic reactions of flying platform surfaces while in the air and development of reliable engines that could be able to sustain an airframe in the air after take-off. Moreover, if this was not sufficient, the initial pioneers had the challenge to develop a system capable of controlling a flying platform in three dimensions simultaneously and independently.

It was only at the beginning of the 20th century, after years of research and some frustrated trials, that the Wright brothers could finally solve the basic problems associated to a flying platform while in the air. Their discovery served as the start of the era of aviation that developed fast initially for military purposes but soon adapted for civilian use.

When airplanes started flying more, communication between pilots and people following or providing basic services to the crew became a need until the point where communication, besides solving some problems, started to create others when the communication moved from voice to data and used largely for safety critical messages through systems not originally designed for aviation purpose and application.

This evolution of the way data and information is exchanged using up to date technologies, open and off the shelf, however, bring new challenges to the confidentiality integrity and availability of the information being exchanged. These new challenges may impact at the end the agreed levels of safety being practiced by the aviation community and the continuity of operations with the associated economic impacts that stop in operations can bring in particular to all airspace users and the society at large.

The current work of the International Civil Aviation (ICAO) reporting that thirty-five acts of unlawful interference recorded in the ICAO Database of Acts of Unlawful Interference in 2018, as compared to 22 in 2017 demonstrates the importance of controlling the cyber threat and attack surfaces. These acts covered a range of geographical regions and

consisted of various attack types including 17 attacks on, or at, aviation facilities, 1 attempted attack using an aircraft as a weapon, 1 cyber-attack, 2 unlawful seizures and 14 attacks qualified as “others”, which include breaches of secure areas and systems [1].

Other occurrences or incidents, identified through media reports but not officially reported as acts of unlawful interference, continue to provide further evidence of planning by terrorists and sometimes just activists to commit acts of unlawful interference against aviation targets and infrastructure.

It is accepted the fact that we are living in a world of evolving technologies and driven by online transactions, artificial intelligence (AI) technologies and automated processes. With the increased use of digitally connected technologies in the aviation industry, the cybercrimes have amplified. Attackers are using well developed tools and techniques which allow access to more complex and well-managed systems, and most of the time remaining untraceable. The statistics about cybercrime provided by google, as of January 2021, has shown around 2 million phishing websites. In 2019 around 93.6% of observed malware was polymorphic, avoiding this way their detection through continuous changes in the code. According to the American Federal Bureau of Investigation (FBI) 2020 crime has doubled compared to 2019. The expenses on cybersecurity solutions will reach $133.7 billion by 2022 as cyber threats continue to increase, according to the International Data Corporation (IDC) [2].

A cyber threat or an effective cyber-attack carry a high possibility of bringing negative effects to the aviation industry. Due to the need to find a common global solution to reduce the cyber threat and attack surfaces, the focus of this work is the identification of processes and procedures that can minimize and/or avoid the damages that can be caused by a cyber-attack. It is also the intent of this work to propose a solution for protection against cyber-attacks to the aviation infrastructure and operations and guarantee the continuity of operations through a resilient and interoperable network.

A cyber-attack in this research refers to an attack against civil aviation perpetrated on or through the cyber space. These attacks involve actions to disrupt the air traffic management supporting infrastructure and applications, including networks, communication and information technology systems, computer and automated systems. In this context, the cyber space may be seen as a target for attack or as a vector or facilitator for other forms of disruptions.

1.2 Invention of the airplane

Until the first airplane took-off, all the researchers and inventors interested in aviation were trying to solve three basic issues related to flying [3].

1. How to lift and sustain the wings in the air.
2. How to generate and apply power to a flying platform in such a way that the platform would be able to drive through the air.
3. How to control the flying platform after it is in actual flight.

1.2.1 Problem of lift

The observation of birds flying in the sky were the initial motivation for dreamers that would like to cross the airspace onboard flying platforms. These observations, associated to the attempts to have a flying platform imitating the bird's movements were a good start. However, these observations and the associated trials did not add much to the invention of the airplane, or even to solve the problem of lift, except for the fact that they showed that the approach to birds' movements didn't work when trying to develop a machine for a flight heavier than the air.

It is considered that the real start of the invention of a flying platform started in the 16th century when important aerodynamics research can be found [3]. Among the pioneers, it can be mentioned researchers such as Leonard da Vinci, Galileo Galilei, Christian Huygens and Isaac Newton, that in different times and using different approaches, contributed some way to the understanding of the different forces acting over an object moving in a fluid with a specific density.

At the same time, other scientists and mathematicians, not specifically investigating possibilities for a future aviation, were investigating the relationship between pressure and velocity that contributed to the science in general as studies related to flying were progressing.

By the 18th century, Mr. George Cayley, in England, covered the gaps between the physical and mathematical theories and engineering research. Through studies of ballistics, Mr. Cayley could analyse data and create theories that would support the development of wings for a flying platform. As part of his research, Mr. Cayley ended up contributing to the development of aircraft design. He could anticipate that if one day a flying platform could successfully take off, it would need separate systems for lift, propulsion and control. This concept was further developed and became the basis for the aircraft development and are

used in current aircraft production. In his research, he also started to experiment fixed wings as the basis for providing lift.

In his studies, Mr. Cayley found that the arched shape for an airplane wing, similar to the bird's wings, would provide better lift to a flying platform than flat wings. These observations were due to the analysis of the difference in pressures between the bottom and the top of curved surfaces. He also observed that long and narrowed wings would provide more sustainability. Nowadays this relationship, known as the high-aspect ratio, is one of the factors that defines the sustainability of flying platform with fixed wings. To improve sustainability, in his designs, Mr. Cayley used then biplane or multiplane wings aiming to get as much sustainability as possible through maximization of the lifting surface area [3] (Figure 1).

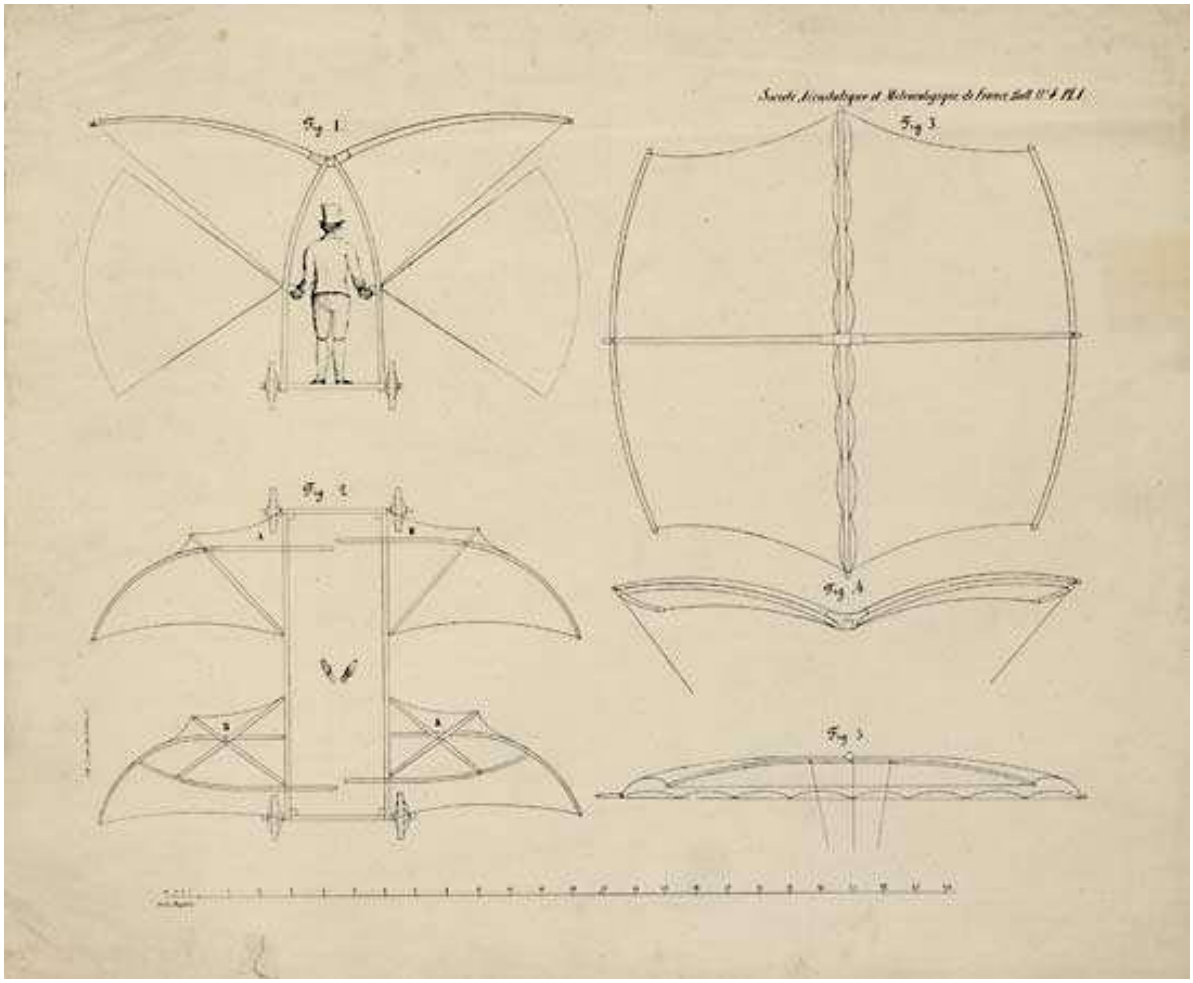

Figure 1 - Glider designed by George Cayley. Source: [3]

Following Mr. Cayley's studies, other engineers and researchers started in the 19th century to study wing designs that could produce the lift necessary for a heavier than the air

flight. Later research and experiments were made to calculate the performance of different wing formats and shapes while operating in different angles of attack.

Otto Lilienthal, a German engineer, as part of his research flew more than 2000 flights on a series of monoplane and biplane gliders, until his fatal glider crash in August 1896 [4]. These experimental flights were useful for his data collections that were used to design different types of wings to be tested aiming future production.

Studying the work of some of previous pioneers, the Wright brothers could evaluate and decide what would be the best design for wings of their, under development, airplane. They agreed that the efforts made by the earlier pioneers were sufficiently well based and explained and they should focus more on how to make the wings sustainable in the air and how to control when in flight. Some of their conclusions pointed to the condition that if they could drive the wings through the air with sufficient speed, they would sustain themselves and any other load put on the top of them.

However, after the practical experiments made by the Wright brothers with gliders, they realized that it was necessary a better wing design than the ones previously developed by their predecessors. For this purpose, they built a facility to serve as a wind tunnel where data was then collected and analyzed. This data collection served to calculate values associated to lift and drag for different types of airfoils and in different configurations in terms of angle of attack and different shapes and aspect ratios. After all trials, data collection and calculations, in 1902 they finally had a breakthrough that allowed them to progress the work towards the invention of the airplane and the realization of the first flight heavier than the air the year later.

1.2.2 Problem of propulsion

A mechanism to power a platform heavier than the air was not developed until the beginning of the 20th century due to not only the knowledge of all processes involved but also the poor technology expertise available at that time. The research and trials realized during the 19th century proved not suitable for lifting and keeping a flying platform in the air. Mechanisms such as clockwork or other spring-powered systems could not provide the power necessary for flying platforms carrying humans onboard. At the same time, electricity powered engines did not present a power to weight ratio that could be used for aviation.

Internal combustion engine, developed around the end of the 19th century, started to be seen as a promising technology to power airplanes by the researchers and would bring great benefits in the future.

Based on the developments being made by the automotive industry related to engines of internal combustion, the Wright brothers decided to concentrate their research and developments to gain more knowledge and experience using gliders. The decision was made to wait the automotive industry to progress the work on more powerful internal combustion engines that could be in the future adapted to power their flying platforms.

Their decision was paid-off when at the beginning of the 20th century, in 1903, they developed an engine that was able to provide the power required to move their flying platform, through the air. The Flyer became then the first airplane to demonstrate a sustainable flight (Figure 2).

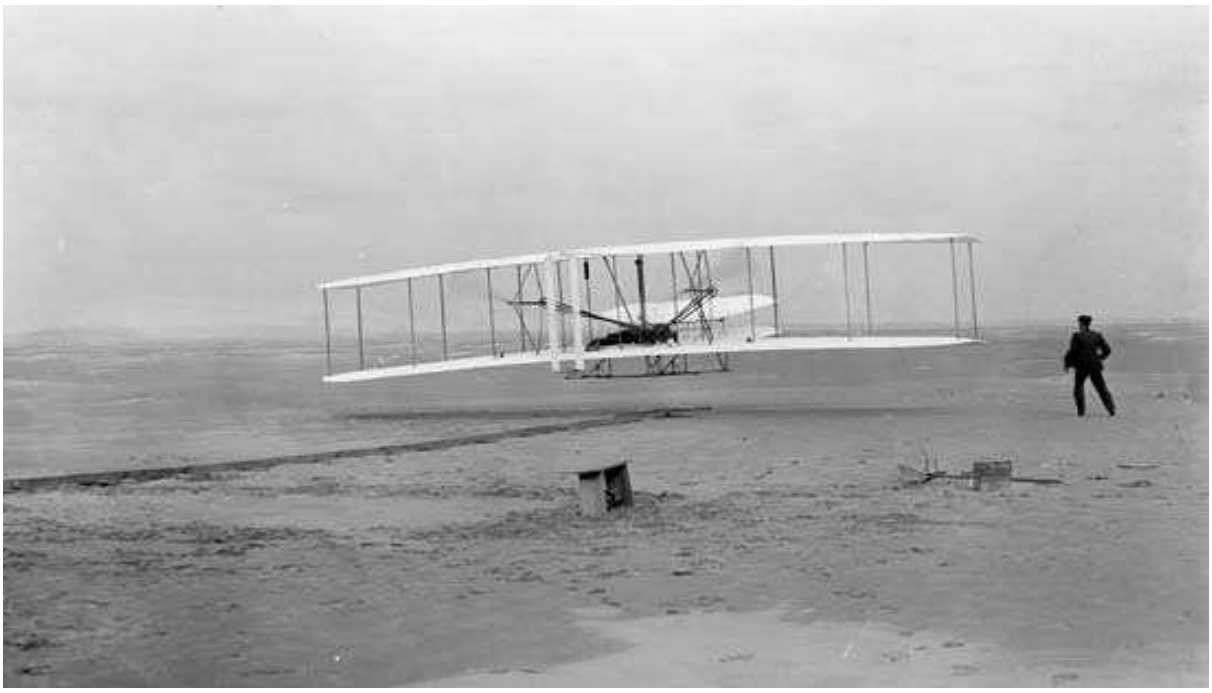

Figure 2 - First controlled flight in history. Source [3]

The development of propellers proved more difficult than imagined by the Wright brothers initially. The propellers development could be compared to the difficulties of developing an engine to power their flying platform considering all the factors involved in the propeller's operations in support of a flight heavier than the air. The relationship of the propeller and engine operation became a complex calculation considering the need to relate the amount of thrust provided by the propellers and the speed of the engine.

After the achievement of an engine able to power an airplane in the air, the focus became in the improvement to the efficiency of engines aiming flights to longer distances and with a better weight to consumption ratio.

1.2.3 Problem of control

When researchers, engineers and constructors arrived to the conclusion that the problems associated to lift and propulsion were well in hand, their attention moved to the control of the flying platform. Among the pioneers, Mr. Cayley was the first to develop and experiment an structure to control the nose of the platform in its movement up and down. His dedication to research ways to control the pitch of the flying platform was due the fact that since the second half of the 19th century engineers were using already rudders to control the movement of the nose to the right and left (yaw).

At that time, engineers were not convinced yet that it was possible to control the flying platform balancing the wings to give a bank angle that would control the flying platform in roll. This limitation was related to the fact that the experimenters were not convinced that a human would be able to control a flying platform that was free to move in three axes at the same time. Because of this limitation, the engineers and constructors tried to guarantee the stability of the flying platform instead of investing in control systems that would enable the flying platform to be fully managed by a single operator.

In the case of the Wright brothers, since the beginning of their developments, they decided to control the center of pressure of the wings instead of the center of gravity of the flying platform. This decision was made after the analysis of the risks involved in the control of the center of gravity. Their projected system allowed the operator of the flying platform to make a twist in the upper and lower wings up and down and as such achieving the necessary control. With this system in place, they solved the crucial problem of roll control.

To achieve the control in pitch, the Wright brothers installed an elevator in the frontal part of the aircraft. This construction could effectively control the movement of the nose up and down.

In 1905, based on their experiments of 1902 when they introduced the rudder to their flying platform, the Wright brothers decided to disconnect the rudders from the wing warping system. This disconnection resulted in the pilot being able to control independently the yaw of the flying platform for the first time. This new management structure of the flying platform allowed their flyer to be fully controlled and is considered the first fully controllable flying platform in the world (Figure 3).

Figure 3 - The first practical flying machine. Source: [3]

1.3 First airlines

After the Wright brothers and other pioneers' developments proving the possibility of sustainability of a flying platform and the control in three different axes independently, researchers and constructors started to invest in developing better flying platforms aiming a commercial use of the new invention.

Due to the impact in the infrastructure used for transportation, when normal rail travel lost the public confidence due to the risks associated to ground travels and the destruction of rail tracks and supporting equipment, all brought as a consequence of the First World War, entrepreneurs started to invest in aviation as a new form of civil transportation.

Based on the progress achieved by the new flying platforms emboldened by the wartime and the chaotic political conditions, mainly in Europe where schedules of ground transportation were constantly disrupted, the investments of the first entrepreneurs started to pay dividends very soon.

The poor infrastructure to support ground transportation and the associated risks created after the war called the attention of entrepreneurs to the possibility of creating airline routes.

There was no sufficient aerodrome infrastructure to support full aviation operations, however, the aircraft of the post war did not demand much for operations. The performance

of these aircraft was such that they could operate in short sod runways relatively safe. Besides, it was not hard to find a place near the cities where these aircraft could operate.

In addition, the first airline's investors could use the relatively inexpensive aircraft used for military purposes with few modifications to transport cargo and people, especially the bombers.

Several single engine aircraft were modified to enable space in the fuselage with space to transport passengers and light cargo. The Air Transport and Travel Ltd., a British group, can be considered one of the first airlines in the world using this type of modified military aircraft, which had its inaugural flight in 1919.

Other entrepreneurs soon followed the idea of modifying military aircraft for commercial purposes, started to populate the market of aviation with this type of aircraft and created a suitable mean of transportation. Some entrepreneurs modified wartime twin-engine bombers in such a way that it could transport comfortably 14 passengers [4].

To satisfy the needs and luxuries of part of the population that was able to first experiment and afford aviation to go from one place to the other faster and with comfort, airlines started to invest in quality for passengers. Modifications to military aircraft were done and sometimes the modifications changed important characteristics such as aerodynamic and speeds. These new airlines used slow but roomy military aircraft able to have ornately embellished interiors and spacious surroundings to attract the more privileged layers of the society emerging in the post war.

The problem of the early airlines was still the risk for safety of lives when flying due to the lack of ground aids to support navigation and the primitive instrumentation available onboard the airplanes, which made the aviation system prone to accidents that invariably occurred with the early airlines. Services to support pilots were rare and most of the time they depended on luck and quick thinking to solve problems such as when they were caught in adverse weather.

With the expansion of the aviation in the 1920s to Africa and the Middle East, aviation started to be considered an evolving industry, demanding more investments in infrastructure. The investments had a double objective of providing more support to flight crews at the same time to gain more the public confidence. Due to the need to fly most of the time over inhabited areas, some entrepreneurs started to create solutions. In areas such as over deserts, some creative entrepreneurs, in the intent to improve guidance to pilots and reduce the risks associate to flying, sent cars and trucks to create tracks on the ground.

These tracks, in the form of furrows on the ground could be visible from the air and reduce the probabilities of crews getting lost between origin and destination.

With France having several possessions in the African continent, the newly created French airlines entered in operation with flights crossing extremely remote areas where local population still had high prejudices. Airlines were covering distances from the coast of Spain as far as Dakar, Senegal.

If for any reason, an aircraft was forced to land in the desert, most invariably the crews were killed, and passengers taken as hostages in cages to latter be used for ransom request. To overcome some of the resistance of local population in Africa, a smart French aviator and author called Antoine de Saint-Exupéry, started putting on native clothes and negotiating peace with local tribal chiefs. With this attitude, Saint-Exupéry could manage the operations in Africa with reduced risks associated to reaction of the local population that started to see him as one of them.

Anthony Fokker started in the Netherlands to produce a new type of aircraft that carried his family name, and the government created a new airline called KLM. This newly created airline started to compete in the market operating weekly routes between London, Amsterdam and Batavia, which later was called Jakarta.

The communist regime that arose in the Soviet Union out of the chaos of the First World War saw in aviation an opportunity to create a new world to be shaped by the proletariat. With different purposes Aeroflot, a State airline, was formed. However, Aeroflot was not only a means of propaganda for the regime recently created. In the Soviet Union, due to its vast territory, aviation became a medium for rapid transportation and a tool for uniting divergent regions. Aviation was used as a means for integration of the vast land managed by the Soviet Union.

With the aim of isolate the influence of capitalism over the Soviet population, and despite the fact that the regime occasionally purchased some western technologies, the Soviet Union emphasized the development of national technologies. With this type of approach and incentives to local entrepreneurs, the Soviet Union, through their engine and aircraft design bureaus, produced a vast amount of airplanes to support the Aeroflot's internal airway system in the Soviet Union airspace.

In 1918, the United States Post Office launched an airmail operation as a wartime effort. Among the objectives of this effort was the idea of stimulating aircraft production and preparation of trained pilots that could be used later for different purposes. Despite

following some European trends, the American experience demonstrated clear differences that proved helpful in support the fast evolution of the aviation industry around North America.

A good impulse for the aviation industry development in North America was the acquisition of larger De Havilland DH-4, an American built aircraft, from surplus military stocks by the airmail industry. The characteristics of this type of aircraft such as its top speed of 130 km/h allowed the aviation industry supporting mail delivery to beat the railway competition when delivering long distance correspondence and small cargos.

With the use of light-beacons, the coast-to-coast airmail service quick developed considering that the beacons could serve as guide for airplanes flight at night reducing the time restrictions to the services provided. The speed and continuity of services allowed correspondences to go from the east coast of the US to the west coast in only two days. At the same time, the railway system could only deliver the same correspondences in five days. The economic impacts of the time savings could be seen in the reduced time used for clearance of check orders and other business papers what was very much appreciated by financial institutions and business people that saw these transactions as highly time-sensitive.

The use of aviation for mail and financial purposes provided the incentives that the North American aviation industry needed to rapidly progress.

The different approaches between Europe and US were in the way the aviation industry operations were financed. While in Europe national flag airlines were subsidized, discouraging as such innovation and competition in the airline industry, in the United States, civil aviation was turned over to commercial operators. The aggressive competition between commercial competitors significantly accelerated the developments in aviation technology that also influenced the aircraft performance. This different type of approach is still felt today with the level of development of the aviation industry when seen from a global perspective.

The Boeing's Stratoliner can be considered a pioneer airplane that brought pressurization capability in 1940. This new capability, besides comfort to passengers, allowed airplanes to fly above clouds, avoiding as such adverse weather and permitting air transportation to maintain dependable schedules. In addition, flights at higher altitudes enabled aircraft to reduce atmospheric drag, reduce flying time and improve fuel efficiency, with the consequent reduction in the costs associated to the aircraft operations.

1.4 Aeronautical infrastructure

It would not be possible for the aviation industry to evolve with the precarious supporting infrastructure of the beginning of the 20th century. The hazards and risks associated to air navigation were too high to convince a number of people sufficient to provide sustainability to the industry. When the commercial and safety aspects in the aviation industry were recognized as impediments to its progress and evolution, the aviation community saw the need to create specialized organizations to collect data regarding accidents to allow determination of their probable causes and generate lessons and practices that could reduce the probability of the same accident happening again. This approach allowed the evolution of the industry through the improvement of safety in operations that also improved the reputation of the airlines.

Experiments that analyzed the response of pilots to electronic signals coming from the ground and received by instruments on board the aircraft, proved successful in 1928 and allowed aircraft to fly without reference to geographical points on the ground. These blind flights, realized on top of clouds, allowed the start of the flights using instrument, which today is the common way to fly commercial airplanes to cross different airspaces all over the world.

Flights using instruments instead of geographic references on the ground represented a huge step forward for aviation. Night flights and flights under adverse weather that did not allow references on the ground to be seen were now possible and allowed airlines to sustain schedules without the need for pilots to land before the planned destination or stay grounded until perfect weather conditions were present.

In addition, investments in the science of meteorology accelerated the knowledge of the behavior of the atmosphere allowing the anticipation of weather phenomena that would affect the flight in the planned route. This anticipation promoted substantial improvement in the safety of air operations with consequent improvement in the reputation of the aviation industry with the general public.

The establishment of engineering schools dedicated to the study of the sciences associated to the flight and the development of rules for air operations and laws to protect people on the ground and onboard the aircraft helped to promote the benefits of the aviation industry and its safety aspects.

The development of the infrastructure was such in North America that by the decade that followed the end of the First World War, major cities established municipal airports to serve the local population in the United States. As a vector to help solving the economic crisis that followed, several governments created programs to construct new aerodromes with paved runways in recognition to the contribution that aviation could give to stop the economic depression.

At the same time, the provision of aerodrome services, through the implementation of control towers in aerodromes experiencing substantial increase in demand for air travel served to promote safety of operations within an increasingly busy airspace. In these airspaces and aerodromes, the use of radio equipment for bilateral communication represented a major improvement in knowing the real location of the aircraft and providing information that would promote a safer flight.

With the investments made to develop new technologies to support aircraft operations and the improvements realized in the infrastructure, it was also necessary to develop regulations to harmonize its use. The investments that followed in the deployment of improved infrastructure set the environment for the introduction of modern aircraft that affect passenger perception and improved demand for air travel.

1.5 Second World War legacies

At the end of 1930s, the world political situation between Japan and China and within Europe was already pointing to a global crisis that would have direct impact in the aviation industry developments for good and bad.

In the United States, the US Army Air Force Transport Command missions in the Himalayan Mountains helped to motivate the development of technologies and concept of operations that would influence commercial operations in the future.

In addition, to support their operations, the Air Transport Command had to establish an infrastructure of aerodromes, communication centers and weather forecast facilities that would later serve to commercial operations as well. The test of new concept of operations for air transportation on an intercontinental basis also served for development of procedures to better support the commercial aviation industry.

The experiments made during the different campaigns at the wartime helped to reduce the time spent to fly between distant destinations. Journeys that would normally take weeks were reduced to just a few days and sometimes to just a few hours. Flights over

the ocean became a routine. At its peak of operations, the Air Transport Command aircraft operated at an average rate of one aircraft every 13 minutes over the Atlantic Ocean [4].

Based on what was happening during the war and anticipating possible future consequences, authorities from all over the world started to advocate worldwide applicable regulations to normalize and harmonize procedures applied to aircraft operations and air navigation services. It was also necessary to foresee issues and define legal processes to promote the orderly development and deployment of international routes.

In 1944, in the city of Chicago, United States, international representatives met and came to an agreement to create a provisional administrative entity for the aviation industry and signed the Convention that until today drives the operations of aviation worldwide, the Convention on International Civil Aviation. By 1947, the International Civil Aviation Organization (ICAO) was established with headquarters located in Montreal, Canada, as a specialized agency of the new United Nations. ICAO was created to deal specifically with aviation matters.

ICAO's work follows the convention signed in 1944. The convention on international civil aviation considered that "the future development of international civil aviation could greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse could become a threat to the general security" [5, p. 1].

The convention recognized that peace was dependent on cooperation between the different nations and aviation should serve as a vector to achieve that objective. With this vision in mind the pioneers of the convention agreed on certain principles and arrangements in order that "international civil aviation could be developed in a safe and orderly manner and that international air transport services should be established on the basis of equality of opportunity and operated soundly and economically" [5, p. 1].

In cooperation with and the agreement of the international community, ICAO established English as the universal language for pilots and air traffic controllers engaged in international operations [6]. Despite the agreements about the use of the English language, this is still a point of discussions when in the same airspace one have domestic and international flights operating at the same time. Additional standards and recommended practices (SARPs) and procedures for air navigation services (PANS) specified more precise requirements and best practices. These provisions relate to terminology, use of navigational aids, emergency procedures, search and rescue, airport markings and lighting and more recently how information should flow from the provider to

the consumer and which requirements should be observed to guarantee seamless operations and resilience on the ground and in the air operations. Without these regulations, it is recognized that global air travel would experience a chaotic and unacceptable dangerous evolution.

The ICAO provisions are considered live documents that are amended as necessary to consider the evolution of technologies and practices by States and international organizations. Most recently, these provisions are under severe review to account for new flying platforms such as unmanned aircraft systems and, as a consequence of the use of digital connectivity between ground and air systems, new threats brought by the use of the cyber space for message exchanges between different stakeholders.

As the Second World War ended, there was an increase in the demand for personal and utility aircraft. This new emerging sub-set of the aviation industry, described as general aviation, encompasses all the aircraft and aviation operations that cannot be qualified as military or commercial scheduled air transport operations according to the regulations.

General aircraft manufactures started to invest in the research and development of light aircraft to attend specific missions, but at the same time, the general aviation industry also started to use modified military aircraft already used during the war. Among these aircraft it can be highlighted the use of former bombers rebuilt with luxury passenger cabins and also aircraft used for transport of personnel that were reequipped with big internal fuselage water thanks to extinguish forest fires.

Considering the size of the general aircraft, manufacturers had also to develop compatible lightweight communication and navigation equipment to support operations under adverse weather.

Due to the increase in demand experienced by air transport after the war, and the appearance of a new emerging middle class, manufacturers invested in the production of aircraft that would be able to carry four to six passengers with more comfort and at faster speeds.

The new aircraft designs provided new commercial airplanes equipped with engines that were more efficient. To improve safety of operations and, provided the higher complexity of the instruments to be managed onboard associated to the need for compliance with new regulations, airplanes started to be flown by a crew made of pilot and copilot. These newly developed airplanes were equipped with luxury accommodations for four to eight passengers in a pressurized cabin.

1.6 Avionics, communication, navigation, surveillance and air traffic management

The term avionics, meaning aviation electronics, was coined during the jet age when aviation saw a rapid growth in all aspects, including technologies to support better communication, navigation and surveillance. All these developments contributed to the achievement of several operational improvements influencing the levels of safety and efficiency practiced by aircraft operators and air navigation and communication service providers.

At the same time, these evolutions brought new challenges to the aviation community in terms of the performance of the new systems to cope with the society expectations regarding the air transportation. These challenges could be observed in all technological areas supporting infrastructure for air traffic management as well as challenges associated to the role of human in the loop that could jeopardize safety and continuity of operations in a similar fashion as a failure in technological systems.

1.6.1 Communications

Telecommunication can be defined as the science of communicating over long-distances. This involves the use of telephone or radio technology, computers, and more recently network technologies to transmit, and switch voice, data, and video communications over different transmission media, including, but not limited to copper cables and fiber cables.

Radios operating in high frequency (HF) and very-high frequency (VHF) to support aeronautical communication processes to civil aviation operations were used after the Second World War. At the same time, to support military operations, ultra-high frequency (UHF) radios were most common.

Due to the different missions to be accomplished and prevalent relief in the area of operations, different types of radios are used. Through a combination of parameters, each mode of radio wave propagation can be defined as the most suitable for different areas or portions of airspace. HF for example is useful and necessary when operating in areas where the distance between transmitters and receivers are vast like the oceans.

VHF/UHF radio waves are better used for communications between numerous locations or stations where line of sigh can be achieved. As long as obstacles do not block

the signal path, these radio waves improve the accuracy of the communications compared to HF.

In the 1960s, the introduction of satellite communication, despite the costs associated to this new technology, offered the potential for real-time communication with aircraft and surveillance of every airborne aircraft anywhere in the world.

Around the 1970s and 1980s, the telecommunication technologies were developed focusing on voice communications. Later it was necessary also to develop technologies to allow transmission of data and images.

With the development of digital technologies offering the capability of internetworking, communication means to support voice dialogues, or data and image exchanges became available for any type of application. The use of the Internet is serving as a focal point for delivering communication services to all sort of consumers in most places of the globe.

1.6.2 Navigation

Air navigation is the process by which an aircraft can plan and control its movement from one place to another without endangering the safety of crew and passengers or people on the ground.

The procedures associated to air navigation are dependent on the rules being followed to fly that can be visual flight rules (VFR) or instrument flight rules (IFR). In the latter case, the navigation is made almost exclusively using instruments on board the aircraft and radio navigation aids on the ground such as beacons, or as directed by air traffic controllers when under radar surveillance. In the case of VFR procedures, navigation is made through calculations of the current position of the aircraft by using a previously determined or known position and advancing that position based upon estimated speeds they flown, time and course. To improve knowledge of location of an aircraft the calculations can be combined with visual observations with reference to appropriate maps or references on the ground.

Due to the normally long distances involved in a commercial flight, as well as the areas where these flights are conducted, many times without any sort of reference on the ground or existing charts to guide the flight, it was necessary to evolve the means for air navigation. The navigation aids developed are normally in the form of beacons located on the ground that allow pilots to know the position of the aircraft at all times.

The current aircraft fleet is equipped with a variety of navigation aids. Some of these aids are referenced in the ground and others based on satellites and others very independent. Examples are the Automatic Direction Finder (ADF), Inertial Navigation Systems (INS), compasses, VHF-Omni-directional Range (VOR), Distance Measuring Equipment (DME) and Global Navigation Satellite System (GNSS).

ADF uses non-directional beacons (NDBs) installed on the ground and through a display on board shows the bearing for the beacon considering the aircraft present position. The pilot may use this bearing to draw a line on the map to show how to achieve the beacon location. By using a second beacon, two lines can be drawn to locate the aircraft in the airspace at the intersection of the lines. Alternatively, if the track takes the flight directly overhead a beacon, the pilot can use the ADF instrument to maintain heading relative to the beacon if this is his flight plan. Despite the fact that this type of instrument is very sensitive to atmospheric condition interferences resulting in non-precise navigation, these instruments are still available and in use in several areas around the world where other aids to navigation are non-existent. Due to the use of very long wavelengths, and in the presence of obstacles on the ground or adverse weather, NDBs can give erroneous readings reducing as such the accuracy of navigation when they are the source of location information. Although NDBs continue to be used as a common form of navigation in some countries, the modern aviation is eliminating this type of navigation due to the lack of accuracy it can bring to the position of the aircraft and the risks it can induce to air navigation.

VHF Omni-Directional Range (VOR) is a more sophisticated system, and associated to distance measuring equipment (DME), is, together with satellite navigation, the primary system for air navigation for aircraft flying under IFR in those countries where a sufficient number of these navigational aids are available. In this system, a beacon emits a specially modulated signal, which consists of two sine waves that are out of phase. The phase difference corresponds to the actual bearing relative to the magnetic north that the receiver is from the station. In some areas, the bearing can also be relative to the true north and this is normally done close to the earth poles. The important characteristic is that the receiver can determine with certainty the bearing to or from the station. A cross reference to more than one station can be used to locate the aircraft in the airspace. Many VOR stations also have additional equipment called DME, which allows a suitable receiver to determine the exact distance from the station. Together with the bearing, this allows an exact position to be determined from a single beacon alone.

Prior to the advent of ground-based and satellite-based navigation, trained navigators, mainly on military bombers and military transport aircraft used celestial

navigation in the event of a complete failure of electronic navigational aids during time of war. Starting in the 1970s airspace users started to use inertial navigation systems (INS), especially on inter-continental and oceanic routes due to the lack of ground-based aids.

The inertial navigation system is a navigation equipment that uses accelerometers and gyroscopes to calculate continuously, by dead reckoning, the position, orientation, and the direction and speed of an aircraft without the need of external references. The INS came to facilitate and made more precise the navigation over oceanic and remote areas where no ground aids were available.

Ground surveillance systems may also help to determine the position of an aircraft in the airspace or on the ground using surveillance information from a radar or multilateration systems. The air traffic management (ATM) system can then feedback information to the pilot to help establish position or can actually tell the pilot the position of the aircraft, depending on the level of service the pilot is receiving.

Since the declaration in 1994 of the availability of the Global Positioning System (GPS) constellation for civilian use, the use of satellite navigation by the aviation industry became increasingly common. Global Navigation Satellite Systems (GNSS) provide very precise aircraft position, altitude, orientation and ground speed information. GNSS makes navigation more precise to equipped aircraft at almost any time anywhere if the interferences to the signal are not significant. The signal low power though makes satellite navigation an easy target for interferences and denial of services.

Considering the vulnerabilities of the satellite signal, some integrity and availability issues need to be considered. As such, systems to improve its integrity and accuracy and to alert the pilot when the GNSS signal is not to be used for air navigation were developed. These systems, called augmentation systems, can be based in satellite information – Satellite-based Augmentation System (SBAS) or even in ground stations - Ground-based Augmentation System (GBAS). The later more used to support approach and landing procedures for specific airports [7].

A more simplified system to verify the integrity of the signal before and during the realization of the flight is also available on board in the GPS equipment, the receiver autonomous integrity monitoring system (RAIM). This system alerts the crew when the signal of the GPS is not good for navigation due to lack of integrity of the signal being received by the aircraft.

Another avionic system, the instrument landing system (ILS), uses onboard instruments to interpret signals sent from ground stations and provide more precise lateral and vertical guidance during the approach and landing phases of flight. A rather primitive ILS was introduced in 1929 but became truly useful only after 1945.

1.6.3 Surveillance

Soon after its initial use dedicated to military purposes in detecting the approach of enemies, the benefits of cathode-ray oscilloscopes migrated to civil aviation. Its main purpose was for improving the awareness of air traffic controllers on the position of an aircraft. In terminal control areas, applications using cathode-ray oscilloscopes helped to support landing operations through reduction of separation. For a more advanced use, ground-controlled approach enabled pilots to land under extremely adverse weather. This type of operation required though specific training and qualification of air traffic controllers and crew receiving the service.

After the invention of the cathode-ray oscilloscope, applications with its use onboard aircraft produced a revolution in avionics. The use of cathode-ray display into the cockpit helped manufacturers to replaced standard analogic information presentations and made far more information instantly available to pilots. It is recognized that this information available at the cockpit enhances considerably the flight safety and efficiency when they are integrated into automatic pilots.

From the mid-1970s, there were almost-continuous experiments with the cathode-ray tube but it was supplanted by the computer-based electronic display in the 1980s.

Since the first true glass cockpit was implemented in the Boeing 767 in the year of 1981, electronic displays have progressed throughout aviation and may now be found even in very light aircraft.

The evolution in cockpit management brought the Multifunction Electronic Display Subsystem (MEDS), which allowed pilots to call up desired and different types of information on a liquid crystal display (LCD).

Aircraft localization has been relying on radar systems, which had been developed initially for military applications, namely identification friend or foe (IFF). Sooner, radars started to support also air traffic management of civil operations. In the current status of the technology, there are two different types of radars: primary surveillance radars (PSRs) and secondary surveillance radars (SSRs).

PSRs have an independent way to detect the aircraft position. They work without the need of any participation of the aircraft considering that stations on the ground transmit high-frequency signals, which are reflected by the fuselage of the aircraft. The echo reflected allows the identification of distance, direction and estimated speed of the aircraft.

Secondary radars or SSRs, use a more advanced method of location and identification of the aircraft. Interrogations from ground stations are responded to by onboard systems called transponders. Besides the location, information similar to the one provided by primary radars, the response from the transponders includes information related to the aircraft altitude and identification codes. The transponder can also be used to transmit information regarding specific situations being experienced by the flight crew, such as emergency, communications failures or even hijacking. Secondary radars are also recognized as being more accurate in terms of localization and identification of the aircraft than primary radars. Secondary radars are a dependent way of surveillance considering that all information is provided by onboard equipment and depends on the collaboration of the aircraft crew that in some circumstances can turn-off the transponder and stop the transmission of information to the ground.

Secondary radars use different modes to interrogate the altitude and identification of the aircraft allowing its use for air traffic management. In civil aviation 3 different modes are used to interrogate the aircraft. Mode A when used, requests the aircraft to inform the code set in the transponder that is a sequence of 4 numbers. Mode A also allow a more precise identification of the aircraft through a function that makes the code of the transponder to be highlighted in the scope of the radar used by air traffic controllers.

Mode C is an improvement to the information provided by Mode A transponders response. Besides location of the aircraft, Mode C allows the information of the altitude of the aircraft also to be transmitted to the ground stations and be presented in the screen used by controllers for service provisions.

The combination of Modes A and C responses from the transponders allow the provision of services by air traffic controllers that can guide the aircraft to routes that are not published in the specific en route aeronautical charts. With this procedure, that allows the simultaneous identification of the aircraft position, speed and altitude, flight and flow can be expedited with consequential efficiency and environmental benefits.

Due to the issues that can arise from over interrogation of transponders when flying in high density areas in terms of air traffic, another transponder mode was developed, Mode S (Select). Being compatible with Mode A and Mode C, Mode S is used for Airborne Collision

Avoidance System (ACAS) functions. The ACAS is a safety net included in the aircraft as the last resource to avoid mid-air collisions in case the separation between two aircraft is violated and reaches critical distance. The system would command the aircraft automatically without the need of the intervention of the crew to avoid a collision.

With the use of onboard systems being used to collect and transmit, directly from the aircraft, information such as position, altitude, heading, and speed of the aircraft to be used by air traffic management, and combined with satellite capabilities, the provision of surveillance services had a significant change and became dependent on the cooperation by aircraft systems and crew.

Satellite surveillance systems are growing in use with its associated benefits of allowing aircraft to see and be seen in any part of the globe.

The change in the surveillance services that moved from independent and uncooperative to dependent and cooperative systems and services provoked also a change in the paradigm associated to air traffic management. This change, which allows more accurate aircraft position determination, as well as other parameters associated to the flight and flow of aircraft, is now available for use worldwide due to the reduced costs of the technology involved. On the other hand, the aviation community recognizes that the most prominent means for surveillance, represented by Automatic Dependent Surveillance-Broadcast (ADS-B), when developed, did not consider the possibility of intentional adversaries to interfere with the signals and was not developed with possible cyber-attacks aiming to stop the system in mind. This lack of cyber protection may jeopardize the capability of this mode of surveillance to support air traffic operations.

1.6.4 Air traffic management

According to the International Civil Aviation Organization [8, pp. 1-4], “Air traffic management (ATM) is the dynamic, integrated management of air traffic and airspace including air traffic services, airspace management (ASM) and air traffic flow management (ATFM) safely, economically and efficiently through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions.”

Air traffic services, as a sub-set of ATM is a generic term meaning variously, flight information service, alerting service, air traffic advisory service and air traffic control service (area control service, approach control service or aerodrome control service). It is implemented when necessary to guarantee the separation between two or more aircraft

operating in the same airspace simultaneously or to provide information necessary to support safe and efficient operations by aircraft and other forms of flying platforms. The services are deployed and the infrastructure implemented to guarantee that air traffic controllers are able to intervene in due time to avoid mid-air collisions or improve the flight experience. This capability contributes to the maintenance of the agreed levels of safety under the values accepted by the aviation community.

Having started with simple procedures, air traffic control is evolving towards complex services and becoming technology dependant. With air traffic control there was no big bang; it wasn't discovered or invented, but it has evolved gradually by need.

Once man became airborne in a flight heavier-than-air, his ingenuity and parallel-developed technologies have permitted him to fly higher and faster. Then, to safeguard air operations, air traffic control was born and evolved gradually, employing new technologies to manage the traffic.

Within two decades of the Wright brothers changing the concept of travel, rudimentary oversight of flights followed, but little progress was made until the Second World War. The modern aircraft were then pushing the boundaries and testing hitherto notions of absolute sovereignty of airspace and governments were forced to act to ensure safety and efficiency whilst guaranteeing the freedom of the skies. Better route structures were initiated, more efficient radio navigation aids were introduced progressively, and international agreement struck. In years that are more recent the use of satellite technologies and the Internet are allowing the development of an air traffic management environment that could have scarcely been imagined not long ago.

It is possible to theorise that Wilbur Wright was the world's first air traffic control provider with Orville a close second. Whilst Orville did not need to file a flight plan nor seek authorization to take off or land, Wilbur maintained what could be taken as an operational watch over the safety of the Flyer during Orville's momentous twelve seconds flight on the 17th December 1903 at Kitty Hawk, North Carolina.

The same kind of need for operational watch over an aircraft in flight prompted the institution of air traffic control. Firstly, it was the need to know where an individual aircraft was that led airline companies and, later, national institutions to maintain such a watch in the event of something going wrong so that action could be speedily taken. To do this efficiently, the new invention wireless was to be utilised. Since there were few of those about, much cooperation was also needed. In Europe, national military and post and telecommunication authorities, who employed professional radio operators, made available

their ground stations for the relay and exchange of information soon after the First World War ended. Then, as more and more aircraft took the skies, the need to keep these aircraft apart, initially when they were manoeuvring on the ground and, later in the air, became paramount.

Air traffic controll expanded after the Second World War with new airlines crossing the skies and being managed by a well established route and airspace structure now with air traffic control better supported by communication and navigation means.

After the fast evolution of its use after the Second World War, the aviation system focused on improving levels of safety to guarantee the trust of the public and this rapidly expanded the aviation industry. And this expansion doesn't stop. Even during wars or global crisis, the demand for air transportation continues to grow and it is expected that in 20 years, the already high movement of aircraft and passengers will double and new forms of flights, some of them unmanned or remotelly piloted start to populate the skies and putting even more pressure on the aviation system to allow safe and secure access to the airspace and also guranteeing the equity in the use of scarce airspace [9]. This forecast already considers the effect of the Covid-19 pandemic which brought the aviation industry to an almost satndstill in 2020.

To allow this expansion, new technolgies and concept of operations were necessary and in 2005 the International Civil Aviation Organization developed a Global Air Trafffic Management Operational Concept, presenting a vision of an integrated, harmonized and globally interoperable system. The baseline against which the significance of the changes proposed in the operational concept could be measured was the global environment in 2000 [10].

The vision outlined by the concept was "to achieve an interoperable global air traffic management system, for all users during all phases of flight that meets agreed levels of safety, provides for optimum economic operations, is environmentally sustainable and meets national security requirements" [10, pp. 1-1].

As part of this concept a set of principles were established and great enphasis was put into the role of information exchange and the integrity and availability of the same information. It is recognized that information provided with high level of quality and integrity became crucial to the safe and efficient operation of any air navigation system and, as a consequnce, also for any aircraft operation. The legacy method of exchanging information only point-to-point does not provide for the efficiency required by the aviation

community to take informed decisions and as such, a mechanism to provide information on a system-wide basis is now required.

In addition, the global operational concept highlighted the benefits from different stakeholder's perspective of moving towards new concept of operations.

Access to timely and meaningful information allowing more autonomy in decision-making, provide the opportunity to meet better business and individual expectations of airspace users.

The possibility to access real-time, as well as predictive data besides all relevant and necessary information in an information-rich environment enable the optimization of the services provided to airspace users by different service providers.

Through the same information-rich environment, regulators can have the opportunity to measure the level of safety occurrences, monitor the health of the system, and compare to a global system for performance improvement.

1.7 Information management

Information management can be seen as the element that connects all components of the aviation system, allows all services to be shared seamlessly at global level, and provides the necessary and relevant information to support operations and monitor and control the quality of the services being provided to support the aviation community activities.

In a highly connected environment, and to improve the capabilities associated to decision-making, highly accurate and timely information becomes crucial. The information availability would allow the aviation community to develop not only the real time picture of the situation but forecast future situations that can jeopardize safety and efficiency of operations.

Key to the vision of an integrated system is the management of an information-rich environment that would support the expectations of the community through all operational services.

Several different benefits can be brought to the aviation community if an information management system is in place to guarantee availability and accuracy of information to be used for services provision and aircraft operations. When airspace users have access to high quality and standardized data and information to support their

operations this availability brings direct impact to safety and continuity of operations even under circumstances that deny the capability of primary sources to provide the users with the expected information to manage air operations.

In an information-rich environment, what is more important is the quality and availability of the information itself and not the technology used to support it. However, with the high level of dependence by the aviation community on information, a system for information availability worldwide is necessary to be established to allow collaboration and more effective business and operational decisions.

The timely availability of accurate information is crucial for the aviation system to operate at its full capacity. The systems used for information management needs to be flexible and scalable considering the needs for constant evolution according to the different scenarios and evolution the aviation system is going through, mainly with the introduction of new entrants and the surge of cyber threats.

Domains of information such as aeronautical information, meteorological information and flight and flow information need special attention considering their direct impact in the operations of the aviation system. These domains need to be managed in such a way that the confidentiality, integrity and availability of the information is always pursued if safety and continuity of operations are to be guaranteed.

With the increasing use of system-wide exchange of information using the well-established Internet infrastructure, careful attention is necessary to the fact that the confidentiality, integrity and availability of the information may be compromised if measures to protect the exchange of information are not taken in a proactive manner.

Currently the COVID pandemic may be decreasing; but as 2022 progresses, bad actors will continue to exploit excessive connectivity. According to the Mimecast Threat Center Report [11, p. 14], which analyses over one billion emails globally each working day, “statistically speaking, the likelihood of them doing so is greater than 95%”.

At the same time, measures to guarantee that the aviation network of services provision is resilient to failures in the protection measures are also necessary. Distributed denial of services (DDoS) is increasing as a threat in the highly connected environment and, for the aviation business, where safety of lives and continuity of services are paramount, challenges on the operational use of information exchange system-wide arises as a top priority to the aviation community.

1.8 Object and Objectives

The object of the current thesis is the trust among all aviation stakeholders and the procedures to assure cyber resilience in a growing and digitally connected aviation ecosystem.

In this digitally connected ecosystem safety and non-safety critical information digitally flows with no or minimum control on the integrity of the information being exchanged among different stakeholders with different procedures to generation and preservation of the content of the information. At the same time, the verification of the identity of these stakeholders become a challenge that needs to be overcome to guarantee that only authorized and trusted sources are providing information that would be used for operational purposes.

This research aims to discuss how the evolution being made by airlines, air navigation and communication service providers, airport operators and regulators to improve the capacity and efficiency of the aviation system can be done in an evolutionary basis and without jeopardizing agreed levels of safety. This evolution is directly associated to the need of more and more trusted information for better decision making among managers, technical and operational personnel recognizing that the necessary digital connection brings new vulnerabilities related to operations in a cyber space.

The main objective may be divided into three sub-objectives. The first is to analyse the evolution of the air traffic that despite facing local, regional or global economic crises and/or wars continue to grow at an accelerated pace demanding a more information-rich environment to support decision making processes.

The second sub-objective is to describe the transformational evolution and challenges being experienced by the aviation community with the availability of real time information system-wide made available by a global Internet that is crucial for the management of the growing traffic and the inclusion of new airspace users with differing expectations, requirements, physiological and flight parameters.

The last sub-objective is a consequence of its predecessors and implies a set of founded recommendations related to an international aviation trust framework for exchange of information in a trusted environment and using the Internet infrastructure without exposing the aviation system to all threats brought by operations in a cyber space.

1.9 Structure

The development of this thesis starts with a literature review of the evolution of the art of flying and the invention of the airplane, highlighting how hard it was to break the challenges of a flight heavier than the air. This includes the analysis of the problems related to lift, power and control of the aircraft that demanded the work of scientists, engineers, researchers, inventors and entrepreneurs who believed that controlled flight was possible.

Then, an evolution of the processes and infrastructure associated to air traffic management is analyzed and the role of information in supporting the management of operations in a complex environment is highlighted.

At the end, a proposal is made to an international aviation trust framework, which could be the approach by the international civil aviation community, to address the issues associated to cyber threats in a digitally connected aviation ecosystem for the exchange of information.

The first chapter is the study introduction, which is divided into nine sections, including the evolution of the aviation infrastructure, the object and objectives of the research, and the structure of the thesis.

The second chapter corresponds to the state of art and contains information that justifies why this study is important for the management of air operations in a digitally connected environment.

In the third chapter, the way followed to find the best methodology to develop the subject of the thesis is described.

The fourth chapter brings the results of the data collection made trough interviews with different professionals involved in the aviation system and developing practices and procedures to guarantee protection and resilience in the exchange of information in a digitally connected environment.

In the fifth chapter, a description of a proposed international aviation trust framework is made aiming the reduction of the attack surface for the aviation system with the use of the Internet infrastructure and a proposed network architecture to support the trust framework.

The sixth (and last) chapter contemplates the thesis synthesis, the final considerations and the prospects for future work in this matter.

1.10 Methodology

The methodology chosen as the best approach to develop the proposal in this thesis used a qualitative approach to data collection and analysis considering the relatively new nature of the discussion on digital trust, resilience and its impact in safety and continuity of air operations.

To collect the data, open interviews were conducted with members of the aviation community and the new entrants that although not directly working with the aviation industry operations are providing services in support of it. It was observed that there is a lack of profound literature on the subject due to the wrong impression on the small size and significance of the industry. In addition, it can be mentioned the lack of knowledge on how the aviation ecosystem would behave in a digitally connected environment when sharing safety critical information through a system where digital identity could not be physically verified.

Despite some criticism to the method of individual interviews due to the possibility of the interviewer influence the response of some interviewees due to their possible relationships, the decision to use a qualitative approach to data collection was supported by the interviewees.

Unstructured interviews, in support of the development of a concept of operations to be pursued by the aviation community, allowing the introduction and connection of digital technologies without jeopardizing safety of operations was mentioned by all interviewees as the correct approach. This approach was fully supported considering that the interviews would also subsequently open the possibility for development of use cases. Use cases would then demonstrate how the different stakeholders would be impacted by a common and global trust framework in support of automation and virtual connection of different systems for exchange of safety and non-safety critical data and information in and between ground-ground, air-ground and air-air systems.

The steps followed in the development of this thesis started with the reading of a series of cyber incidents published by the conventional and specialized media to verify the amplitude of the subject. It was also necessary to review the current and future air navigation systems including the ones dedicated to information exchange before the data collection could start. This step was followed by the review of related theories and studies on different methodologies for data collection and analysis. Unstructured interviews were then conducted for data collection as described in chapter 3. Based on the results of the

interviews a proposal to address the cyber issues in the civil aviation system was developed and is described in chapter 5.

Chapter 2

Literature review

2.1 Introduction

Aviation is recognized as a safety and continuity critical business. The ICAO Global Air Navigation Plan [12] highlights that the air navigation system is becoming more complex due not only to the traffic growth, which is expected to double in the next 20 years, but also due to the start of operations of new flying platforms supporting the mission of new airspace users [13]. These new airspace users come with new demands on the system considering its different needs, missions and operational characteristics.

The transformation of the air navigation system to support the new demands is necessary if the aviation system wants to maintain or improve the agreed levels of safety and operational efficiency that at the end reflect in the financial achievement of the industry. The transformation of the aviation system depends necessarily on the use of new technologies and sometimes the available technology has not been developed having the aviation requirements as motivation.

The need for a secure exchange of information on a global basis is essential to allow this transformation. This global system for exchange of information cannot be successful if different participants of the system do not trust its components. Then, a resilient network build on a trust framework appears as the only way to allow transformation in a digital environment [14] [15]. Therefore, the community needs to address the issues related to cyber security.

In this research, cyber security must be understood as not only measures to protect the air navigation system, but also measures to guarantee resilience of the system that are under attack and is eventually penetrated by agents willing to disrupt or interrupt the provision of air navigation services essential to the safety, efficiency and continuity of air operations.

In a digitally connected environment, it is necessary that the aviation community take a globally agreed and harmonized approach to guarantee the exchange of information in a secure environment that can be trusted. Isolated initiatives, despite helping to protect local assets, do not contribute much to the global behavior of the aviation system

considering the possible gaps and overlaps that can exist putting in jeopardy the safety and resilience of the system as a whole.

What is known today is that despite the risks associated to digitally connected technologies, digitalization continues to be more present in our daily lives with an ever-increasing attack surface and attackers are combining creativity with pragmatism to break into information technology (IT) systems [16]. It is also known that hackers will seek out the weakest link, whether that's third parties and supply chain partners, unpatched systems, weak passwords, unprotected privileged accounts or humans who are susceptible to errors, phishing, social engineering, and insider threats.

The need of a global system with multilayer defenses to cyber-attacks requires the community to develop a global resilient and secure network with specific characteristics to meet the aviation requirements.

2.2 Networks

Networks are not only to serve aviation purposes. We are now living an era when all is connected to allow people and goods to move or just to exchange information without the need of physical movement. The society makes use of email exchanges, place phone or, more recently, computer conference calls; use the aviation system for travels and the banking system for financial transactions. In all these applications, networks are being used.

Networks and their properties influence even global phenomena. Due to the connections between different systems and communities, financial crisis, or help to solve the same crisis, can propagate quickly. Through the web of connections even pandemics like the Corona virus, more recently, can use the aviation network to spread.

Networks can be used to perpetrate terrorist attacks to critical infrastructure supporting basic services in a community or in a country. The network represented by the Internet can be used to diffuse computer viruses that can cause large failures to electric energy distribution that can bring a community to a halt.

Networks can also be used for intelligence data collection. Through this data collection governments can monitor social networks that can be used for identity tracking and serve as inputs for defense or investigation activities.

As mentioned above, on a daily basis the society is connected through networks performing different interactions, sometimes with a disordered pattern, to perform different activities.

In 1969, when computers were connected for the first time, messages were able to travel between computers using a telephone line as the medium. Despite the issues related to the poor connection, at that time, this connection event could be considered the moment when the Internet as we know it today was born [17].

The United States Advanced Research Project Agency (Arpanet) starting with connection between the University of California and the Stanford Research Institute, could, after the connection of two computers, expand the number of them that at this time was used to connect other universities and private companies.

With the consolidation of the success of connecting computers, other entities started to develop new networks and the challenges shift from connecting computers to connecting networks. This represented a motivation to experts from all over the world to investigate and define the best ways to connect distant networks and internetworking became the challenge to be solved.

The development of the Transmission Control Protocol/Internet Protocol (TCP/IP) was the breakthrough that allowed networks to connect to each other independently of the internal structure of the networks. This created the possibility for the deployment of a network of networks and it is how the global Internet works today.

The Internet is the best example of a network considering that for messages to fly from one computer to the other, the two computers do not need to have a direct medium connecting them. As long as they are connected to the Internet, they serve as hosts that allow messages to be exchanged from different origins and destinations.

In the Internet, for a message to travel from one origin to the target destination, the message travels along routers, which are devices responsible for transmitting packets of data.

The physical infrastructure that allows the connections in the Internet is made of cables, satellite connections and other means that creates an environment where everything and everybody can be discovered. In this environment and considering that hosts and connections can be added at any time or location, it is almost impossible to define the actual structure of the Internet.

It is recognized that the differences between the ways information are transmitted through the Internet can vary from country to country. This is dependent on the infrastructure available and the access to up to date technology. This makes the mapping of

the Internet at a host level almost impossible considering that any connected device can connect another connected device independently from their geographic location.

To better classify and manage the specific requirements for the networks, they can be categorized by different aspects including, but not limited, to its size or geographical range. As such, Personal Area Network (PAN) for example can be considered the interconnection between devices within the range of a person's private space, typically within a range of 10 metres (Figure 4). Examples of use of this type of network are transfers of any kind of data from different connected devices through Bluetooth.

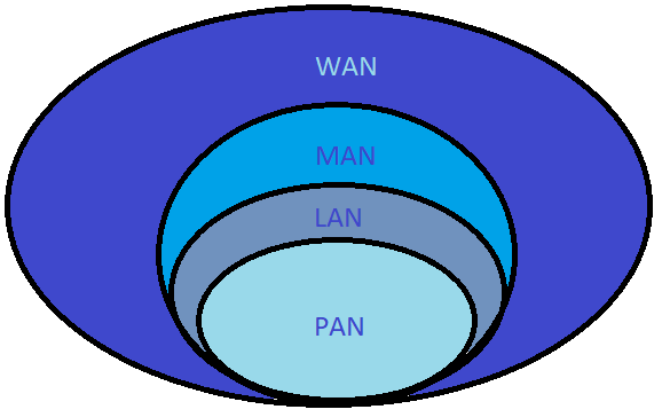

Figure 4 - The classification of data networks by spatial scope. Source: Own development.

When the need is to interconnect devices within a limited area, a local area network (LAN) is preferred. LANs are normally used to connect office buildings such as private companies or schools where the need for an efficient and secure connection is necessary [18]. In opposition to the LANs, a wide area network (WAN) is developed to connect larger geographic areas. WANs generally requests a more robust telecommunication infrastructure.

A specific connection infrastructure made sometimes of leased circuits needs to be in place for the interconnections of different LANs. Across the Internet, the use of virtual private network (VPN) technologies is common for the LAN interconnections. When a series of LANs are connected, they can give origin to a metropolitan area network (MAN) or even to a wide area network (WAN).

Being aviation a global business and connected worldwide, the interest of this research is on the architecture and behavior of WANs that are supporting the aviation industry considering its security and safety aspects involved. However, this WAN to support aviation operations is quite often made of connection of several LANs or even MANs.

The justification for the establishment of a WAN is the need to connect devices located in large geographical areas. As the services provided using networks can go beyond the areas where a certain company has its own infrastructure in place, WANs are normally connected using leased telecommunication circuits.

In the virtual era we are living these days, where services and even education can be provided remotely, students, buyers and services and goods providers exchange data and perform business normally using WANs. The use of WANs allows companies and/or public institutions to carry out their activities regardless of their geographic location using the Internet, which is considered the biggest WAN implemented worldwide [19].

According to Forouzan (2013) [20], the definition of a WAN is a computer network spanning regions, countries, or even the world.

For this research, that relates more to the use of computer applications to support aviation operations harmonized at a global level, a WAN is considered a network to allow safe and secure transmission of data and information between distant located computers and systems through the interconnection of LANs. This interconnection is enabled by using circuits that connect networks to generate a global resilient network for aviation. This simplified architecture can be visualized in (Figure 5) below.

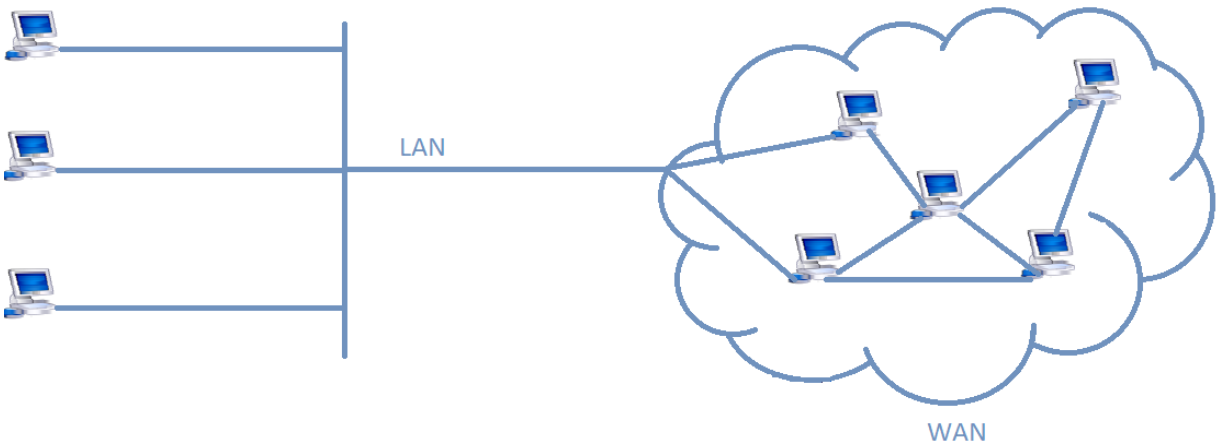

Figure 5 - Relationship between LANs and WANs. Source: Own development.

The characterization of the aviation global WAN is necessary to make the distinction between the different aspects and architecture of the different LANs designed for and operating with physically close networks that cannot support by itself the exchanges of complex data and information between systems located in distant geographic areas as covered by the aviation industry.

In this case, the aviation industry is making use of WANs to connect LANs and doing that be able to provide the services requested by the aviation community to support aircraft operations through the connections between systems and computers located all over the world.

Like the LANs, WANs can also be built by particular public or private entities and remain private. However, the most common architecture is to have a LAN that through services provided by specialized Internet service providers, connect the LANs to the global public Internet. In this scenario, using leased telecommunication circuits, routers connect different LANs established at the end of the linking circuit.

Connection between different networks are necessary to provide global or regional services, however, this connection cannot be successful without common rules being followed by the participants in the internetworking connections. Known as protocols, these rules allow the transmission and reception of data packets between different networks. The Transmission Control Protocol (TCP)/Internet Protocol (IP) is the widely used model and protocol for supporting the mentioned connections. An open system interconnection (OSI) model also exists and, despite different in nature from the TCP/IP, it has similar description and objective as the TCP/IP.

As the TCP/IP, the OSI model is conceptual and aims to describe and standardize the communication functions of a computing system despite its architecture and supporting technology. The idea behind the characterization of the OSI model, similar to the TCP/IP model, is to guarantee the interoperability of different communication systems through the division of the communication process in layers.

The OSI model is considered the first effort of the virtual telecommunication industry to harmonize and standardize the process associated to data communication through interconnected systems and as such achieve interoperability between the different service providers and vendors.

At the beginning of data communication, networks were supporting different protocols, what made impossible to interconnect them or when connected they did not provide interoperability between devices due to the lack of a common and standardized protocol. The OSI model associated developments were aiming to provide the necessary harmonization and standardization of protocols, however, as the consensus among the developers took too much time, the industry took a pragmatic approach, agreed on the TCP/IP protocol and associated standards and it became widespread used for internetworking by producers of network systems [21].

The discussions associated to the development of the OSI model allowed great evolution in the network concepts understanding and served as the basis for educational programs on network protocols. The OSI model also promoted the idea of consistency between protocol layers and was the precursor for interoperability between network devices and software.

According to Russel (2019) [21], if everything had gone according to plan, the Internet as we know it would never have sprung up.

It is recognized that the plans associated to the OSI model were to create a set of standards for network connections. With the participation of government and industry representatives from Europe and North America, the group of developers aimed at achieving an open system that through multilayers would allow users all over the world to connect seamlessly and exchange data and information that would boost collaboration and business results.

At the beginning, the vision of the pioneers on this study for OSI was seen as the only way possible to achieve the interconnection standardization objectives. These experts from all over the world got the necessary support from the different segments of the telecommunication industry and regulators from States and by the 1980s it was almost decided that the adoption of the OSI model, as the only guide for interconnectivity, was the way to follow.

By the 1990s, however, another model was developed by the industry that considered the model cheaper and easier to implement, despite not being as comprehensive as the OSI model. This new model was the Transmission Control Protocol and Internet Protocol (TCP/IP). As the OSI model was left behind, one of the Internet's chief advocates, Einar Stefferud, pronounced with a great delight that OSI was a dream, and TCP/IP was living it [21].

For sake of clarification, reference, and understanding why TCP/IP is the protocol to be used in this research proposal for exchange of data and information, it is necessary to understand the differences between the two models.

2.2.1 OSI model

The OSI model shown in Figure 6 below with its seven layers, was developed to explain and standardize the different functions realized during any process of communication that involves network by its different software and hardware. The model

also defines the different work done in each layer and how they interact among themselves [22].

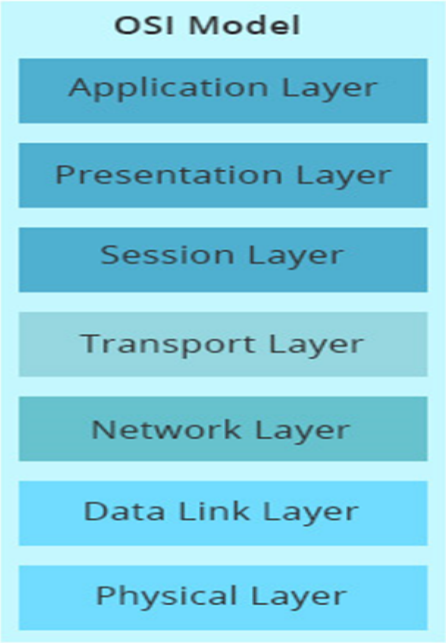

Figure 6 - Seven layers of the OSI model. Source: [22]

Layer 7: Application Layer

This layer serves for the direct interaction between the applications and end users through the necessary communication capabilities or functions. This layer has the main function to verify the availability of the communication partners and the respective resources necessary for the exchange of data. It is at layer 7 that the protocols for end applications are defined. Some of the protocols used at this layer are the hypertext transfer protocol (HTTP), the file transfer protocol (FTP), the simple network management protocol (SNMP), the post office protocol (POP), the simple mail transfer protocol (SMTP), the internet message access protocol (IMAP) as well as the teletype over network (Telnet) protocol.

Layer 6: Presentation Layer

Layer 6 is where the verification of the resources available for communication are done to guarantee compatibility with the data to be exchanged. Its main function is to adapt or translate the data into a format that lower layers will understand and accept. In the process of formatting for lower layers acceptance, layer 6 also make a code conversion. Code conversion can be for example converting an Extended Binary Coded Decimal Interchange Code (EBCDIC) coded text file to an American Standard Code for Information Interchange (ASCII) coded text file, besides executing, when necessary, data compression and

encryption. This function expedites the transmission of big files such as video that will be compressed and recovered at the destination. For sensitive data, is at layer 6 that the data is encrypted before transmission.

Layer 5: Session Layer

Layer 5 main function is to manage the connections between different hardware. Layer 5 has the authority to establish, maintain and terminate a connection between a local and a remote application. Through its management functions, layer 5 handles the tasks of authorization and authentication besides verifying if the data to be exchanged is in fact delivered to the destination. If a program needs to use another program located in a different network, it is in layer 5, using a remote procedure call (RPC), that the request is made without the need to know the other network details.

Layer 4: Transport Layer

It is in layer 4 of the OSI model that the means for transferring data from a source or origin to a defined destination host are located. The functions of the transport layer are to manage the movement of data until a complete delivery of the data through one or more networks without losing the quality and integrity of them. To guarantee the integrity, the layer can apply a flow control to the data being exchanged.

Layer 3: Network Layer

The main function of layer 3 is to handle the routing of the packets of information. Switching functions and logical addressing are used for routing. The network layer executes the routing transferring the packet from origin to destination most of the times through several different nodes. The sending application only needs to provide the message to be exchanged and the desired destination and the network layer will find a way to deliver the message. Sometimes, due to the size of the packet to be exchanged, the message can be split in separate segments by the network layer that will also be in charge of reassembling the different segments in a node before the final delivery address.

Layer 2: Data Link Layer

Layer 2 is the layer that provides the connection between two nodes directly. Its main functions are to pack and unpack data in frames and to define the protocol that will be used to establish and terminate a connection between devices. To perform correctly its functions, the data link layer is normally subdivided in two sublayers named the media access control (MAC) layer and logical link control (LLC) layer. While the MAC sublayer

controls how devices get access to a media in a network as well as gets permission to data transmission, the LLC sublayer identifies and encapsulates network layer protocols at the same time it synchronizes frames and check possible errors that can stop the message exchange.

Layer 1: Physical Layer

Layer 1 represents the lower-level equipment in networking and sees protocols or any other higher layer elements in a transparent way. The physical layer is responsible for the transport of raw data through a physical medium. To guarantee the transport the physical layer is the layer that defines the physical specifications for the connections including cable voltages for electrical cables and frequencies to be used in case of wireless devices.

2.2.2 TCP/IP Model

Similar to the OSI model, the TCP/IP is a layered model as shown in Figure 7 below. However, it is simplified to four layers instead of seven as in the OSI. The denomination of the TCP/IP model comes from the fact that it is constituted by two main protocols, TCP and IP, despite the fact that in this model other protocols are also used. To avoid interpretations on the limitation of protocols, the TCP/IP model is also called Internet Protocol Suite (IPS).

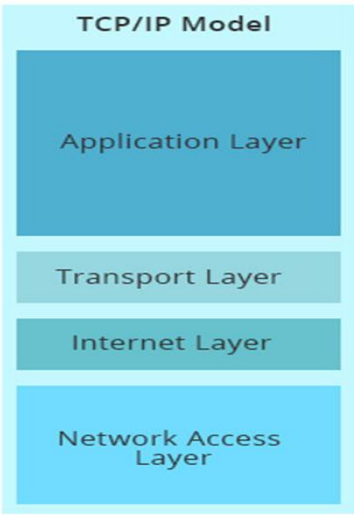

Figure 7 - Four layers of the TCP/IP model. Source: [22]

Layer 4: Application Layer

In the TCP/IP model, layer 4 is the layer that serves as the door for the access to the lower layers. This layer defines the protocols to be used by the applications to exchange data. Among these protocols it can be mentioned hypertext transfer protocol (HTTP), file

transfer protocol (FTP), simple mail transfer protocol (SMTP), simple network management protocol (SNMP), teletype over network protocol (Telnet) and routing information protocol (RIP).

Layer 3: Transport Layer

Directly interacting with the application layer, the transport layer, that can be also called the host-to-host layer, provides the application layer with session and datagram communication services. To perform its functions the transport layer makes use of transmission control protocol (TCP) and user datagram protocol (UDP). While the TCP is in charge of the communication services through sequencing and acknowledgement of the packets that were sent, it also has the extra function to recover packets lost in the exchanges. If the amount of data to be transmitted is sufficiently small that can be accommodated in only one packet, the UDP is used. Despite not being reliable, it can provide one-to-one or one-to-many connections.

Layer 2: Internet Layer

In the TCP/IP model, the layer responsible for the packaging and routing functions is the internet layer. To perform its function the internet layer makes use primarily of the following protocols: internet protocol (IP), address resolution protocol (ARP), internet control message protocol (ICMP) and internet group management protocol (IGMP).

The different protocols used in this layer are responsible for specific functions. Among them it can be mentioned the routing and reassembly of packets done through the IP, the discovery of network access layer which is performed by the ARP. The diagnostic functions that serves to detect and report errors in the packet of data transmission is performed through the ICMP.

When there is a need to distribute the data packet to various computers simultaneously, this is performed through the IGMP.

It is in this layer that the IP address of the destination of the data packet is added to the head of the message. Nowadays, there are two different set of IP used for address definition. Initially, only 32 bits were used for address definition and it is known as the IP version 4, or IPv4. With the exhaustion of the available number of IPv4 addresses to take care of the needs of the digital community, a new version of IP addresses, carrying 128 bits were developed and is being deployed worldwide. This new version is the IP version 6, or IPv6. The differences can be seen in Figure 8 below.

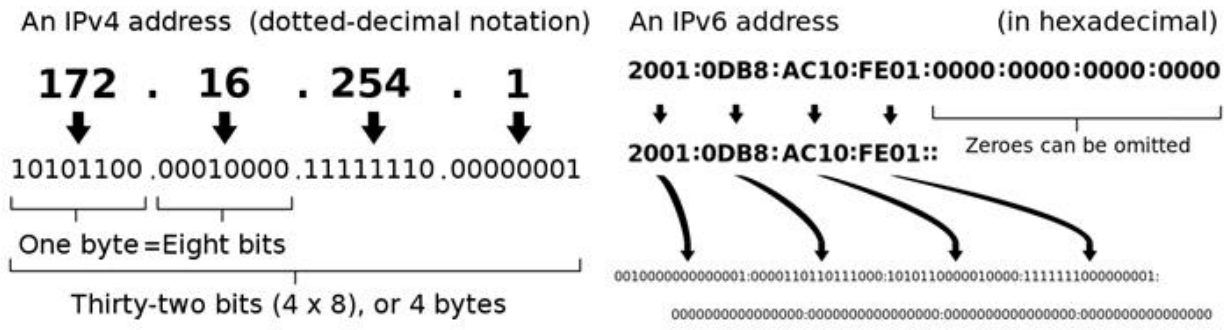

Figure 8 - IPv4 address and IPv6 address examples. Source: [22]

Layer 1: Network Access Layer

This is the last layer of the TCP/IP model. Its main function is to deliver and recover packets to and from the network medium.

When TCP/IP was developed, developers had in mind to achieve a model that could be technology agnostic when it comes to which network technology is used by the different users and providers. This allowed the TCP/IP independency from any medium, frame format or network type or architecture.

2.3 Data processing during transmission

To complete a digital communication process using a layered system, different devices in a layer use different data format. Both the OSI model and the TCP/IP model use the format of protocol data unit (PDU) that varies depending on the layer it is used. Table 1 below shows the formats in different layers for the different models.

Table 1 - Protocol data unit (PDU) being processed in different layers. Source: [16]

Model type	OSI layers	Protocol data unit (PDU)	TCP/IP layers
Host layers	Application	Data	Application
	Presentation		
	Session		

	Transport	Segment (TCP) / Datagram (UDP)	Transport
Media layers	Network	Packet	Internet
	Datalink	Frame	Network access
	Physical	Bit	

The process of digital data communication can be simply described as a sequence of events that brings data back and forth from a requesting computer to a responding computer through networks and using the layered approach of the models. Starting with the application layer data is processed from layer to layer, each of them performing crucial functions to complete the digital data communication process. After all processing the data is transported through the physical layer until the desired destination that can be a server or any other device. Figure 9 below shows the steps and paths followed for data flowing from a transmitting device to a receiving device.

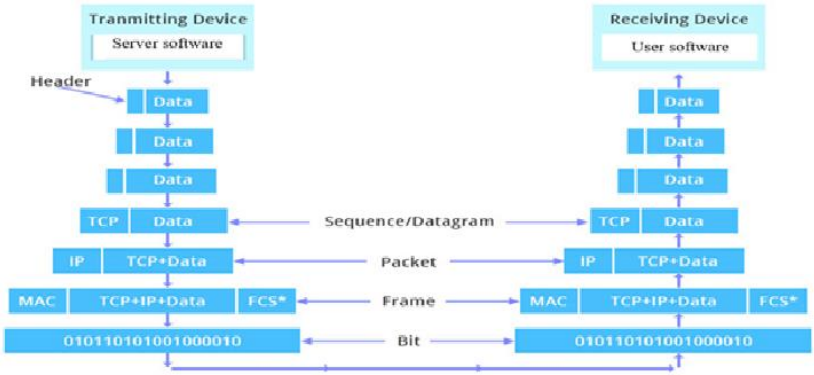

Figure 9 - Data flows from upper layers to lower layers. Source: [22]

To correctly support and complete the data communication, the distinct layers add headers or footers and sometimes both to identify directly the packets. Through this encapsulation process, the PDU is formed for the next layer. Going from layer to layer, the process is completed until reaching the last layer that can be the physical layer, in the case of the OSI model or the network access layer in the case of the TCP/IP model. From this point, the next step is the data being transmitted to the receiving unit that can be a server or another device. When the data reaches the receiving device, the whole process is

performed again in reverse order from the lower layers to the upper layers until all the data is transmitted and can be used by the application.

2.4 OSI Model compared to TCP/IP Model

Despite being developed in different times and having different structures, the OSI and the TCP/IP model aim to support the same functions and as such can be compared for educational purposes. Figure 10 below shows the corresponding relationship of their different but corresponding layers.

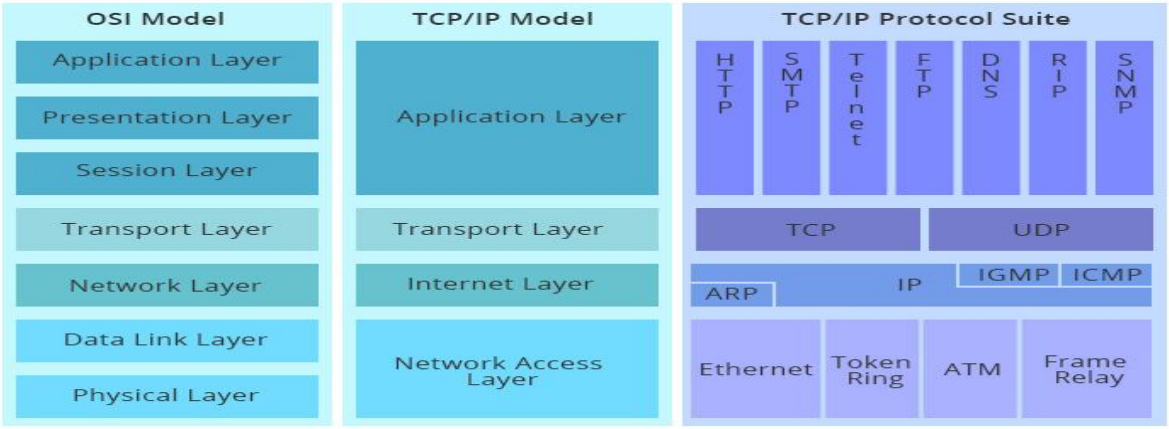

Figure 10 - OSI model vs. TCP/IP model, and TCP/IP protocol suite. Source: [22]

As can be seen in Figure 10 above, instead of having three layers, the TCP/IP model replaced the application layer, the presentation layer and the session layer of the OSI model in only one layer that is the application layer. The functions performed are similar and necessary for the completion of the digital data communication process.

Not having a session layer, in the TCP/IP model some of the session layer functions in the OSI model are performed by the transport layer, which accumulates the session layer and the transport layer functions of the OSI model.

As a more simplified model, TCP/IP does not have a data link layer and as such do not take advantage of the functions performed by this layer. In the TCP/IP model, the transport layer also does the functions related to sequencing and acknowledgment services, which in the OSI model is performed by the data link layer. In the TCP/IP model, the network access layer aggregates the functions performed by the data link and the physical layers of the OSI model.

If it is necessary to define the differences between the OSI and the TCP/IP model, it can be said that the OSI is an academic and conceptual model. On the other hand, the TCP/IP model is the practical model used by vendors to produce systems.

The OSI model can be seen as an easy way to explain and understand the different functions of the layers in the model. In opposition, the TCP/IP is problem solving oriented and not for generic descriptions of network communications.

Despite most protocols adhere to the OSI model; the model can be considered generic and protocol agnostic. On the other hand, the TCP/IP model works with specific protocols designed to perform the function specified for its different layers.

One important characteristic of the OSI model is that despite having 7 layers, not all layers are used by application with low level of complexity. While the low layers (1, 2 and 3) are mandatory for any data communication the upper layers are not and the application can use specific interfaces that would bypass the upper layers without any adverse impact in the communication services.

In a system of systems (SoS), networks and systems are connected to perform functions that a single system otherwise could not perform by itself. These connections are made using the models and protocols described above.

In this research, a definition of a system is not limited to technical equipment, but it must be seen as encompassing also people and processes with each of its components keeping its own functions, resources and goals, and adapting themselves to the end objectives of the SoS [23].

For better understanding of its functions and performance and despite the fact that the definition of a SoS is quite close to the one of a system, it is still important to differentiate a system from a system of systems in the context of civil aviation.

Maier (1998) [24], describes that there are a few characteristics, which allow for a distinction between a system alone and a system of systems. Among them, it can be mentioned at least the following:

Operational independence of elements: With independent operation and use, the SoS is made of systems that are self-sufficient.

Managerial independence of elements: Not only operational aspects differentiate a system from a SoS. Administrative aspects such as development and procurement of the elements of a SoS are also done separately. From a security perspective, however, a SoS will only be protected if all its components follow similar security rules and share the risks associated to their composability.

Evolutionary Development: A SoS is considered in constant evolution. Throughout its lifecycle, systems are included or excluded from the SoS, or simply modified, creating new responses and characteristics not present in the original configuration. This constant evolution brings the challenges associate to its composability that can directly affect the security of the SoS as a whole, considering that new compositions can bring degradations to its performance non-existent by the time it was formed.

Emergent behaviour: The interaction of its different components generates, sometimes quite spontaneously, new functions and/or qualities not present in an isolated system. This behaviour can be seen in natural systems presented in the nature as swarms of birds and fishes [24]. In these types of manifestations, the position and movement of its independent elements can only be seen and understood by the immediate close located elements. However, for an external observer, it seems that the movement of the whole system is done in an orchestrated manner. In a SoS this one-to-one interaction is able to create new capabilities that cannot be assigned to one single system in isolation.

Geographical distribution of elements: SoS are in general established through large geographical areas considering that SoS are normally created to satisfy the needs of users spread through long distances. Due to its geographical distribution, the aviation SoS are not capable of transporting significant amounts of matter or energy but only digital data and information.

Other authors, such as Dahmann and Baldwin (2011) [25] classify SoS using different criteria and considering different characteristics such as the following:

Virtual: The most important aspect that characterizes this type of SoS is its lack of an authority that can centralize the management of its components but instead it relies on mechanisms that are not apparent allowing different behaviours to emerge as the system operates.

Collaborative: This type of SoS is characterized by the collaboration between its components to achieve an agreed purpose. With this approach, collectively the SoS components have the authority to decide which service would be provided and which would not, always aligned with its main purpose.

Acknowledged: This type of SoS is considered more structured having specific resources, objectives and a defined manager. However, from an operational perspective, the independence of its components is maintained in terms of development, funding and

sometimes even objectives. All its component systems agree to collaborate when changes to the SoS is identified as necessary to maintain its pre-defined core objectives.

Directed: This type of SoS is characterized by its creation, constitution and management style to meet a specific objective. A central management is established to guarantee alignment with its original objectives and new ones that may appear as the SoS starts to operate. Despite the independence of its components, in this SoS the components follow a central guidance to meet the SoS objectives.

According to the previous classification and analyzing how the aviation system is organized and managed, with the community establishing multiple and independent but related types of sub-SoS, with pre-defined objectives and indicators to measure its performance, aviation can be then considered a SoS of the Acknowledged category.

As mentioned before, the composability of a SoS is a characteristic that needs to be considered if one needs to analyse it from an information security perspective due to the challenges associated to the integration of different elements to form the SoS that is designed to meet specific expectations. The integration of its different components is important considering the specific properties and objectives of these individual components as well as how they perform when connected to others. Among the characteristics to be observed are how the interfaces would be established to guarantee integration and interoperability, which are crucial characteristics to a global system such as aviation.

Requirements such as physical and logical performance establishes conditions under which different elements can be connected to achieve strategic objectives. If the requirements established by agreements are satisfied and the individual elements can maintain its relative independence, then integration can be realized without jeopardizing the final goals established for the SoS. The example shown in Figure 11 below demonstrates the integration of System A and System B to form the resulting System AB. Unless the combined characteristics of the two systems become internal to the new system, through well defined interfaces their combined aspects are exposed to the environment where they live.

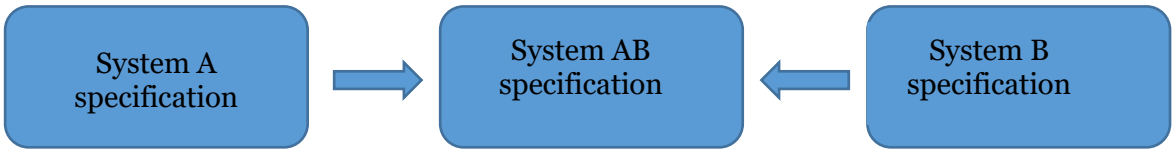

Figure 11 - Integration of two systems. Source: Own development.

If considered from an information security perspective, it is necessary to evaluate if limitations imposed to certain functionalities and required performance results are sufficient. In the information security context, it is also necessary to analyse the different security environments present in each of the different elements. The results of the integration of elements with different security environments will generate a system, which the resulting security environment will also be unknown, what will make impossible to predict the results of the integration from a security perspective. In these cases, the process of refutation becomes a requirement to guarantee a performance that can satisfy the final objectives of the newly formed system of systems.

In this case, the process of refutation aims to verify if the expected behaviours of different elements will not jeopardize the operations of the SoS refuting possible vulnerabilities. Using the refutation process to an information security environment will allow the demonstration of the absence of information security issues that could affect the system as a whole.

In Figure 12 below, it is shown a System A and a System B, each of them with its own information security environment being integrated to originate a new System AB that through composability generates a new information security environment. As shown in the previous combination of independent System A and System B, through interfaces and operational functions, System A and System B combined characteristics, unless internal to the new system, can be exposed to their environment. Considering then that no statement can be made regarding the information security environment of the newly formed system, the refutation process needs to be applied.

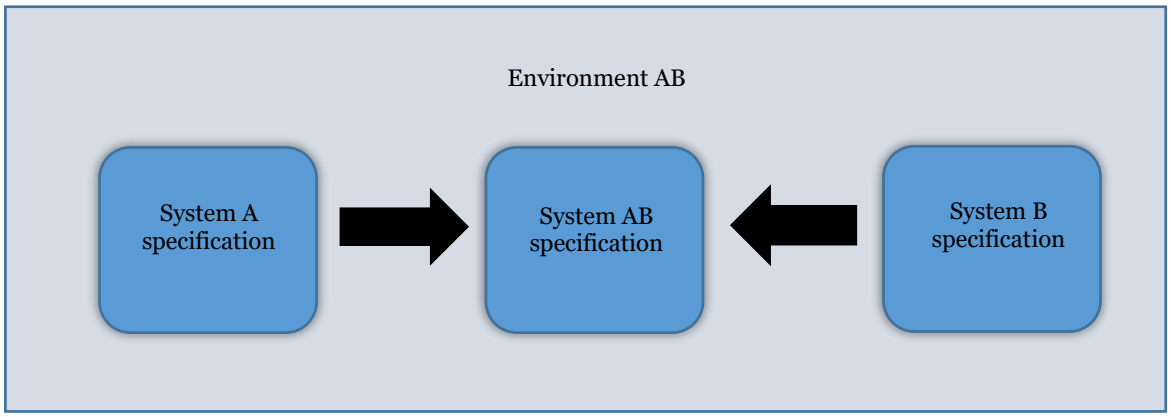

Figure 12 - Combined information security environment. Source: Own development.

According to the process used on a global basis to define system requirements, a set of requirements can be generated to specify the need of the absence of specific behaviours. However, despite developing requirements that can be considered aligned with the

objectives and complete, the assurance actions put in place cannot have the confidence of the community if the undesired behaviours are not present [26] [27].

In this scenario, to assure the expected behaviour of a combined system, refutation actions are put in place. These actions go beyond the established requirements and operational standards. Refutation can be used when the complexity of the system integration does not allow conclusive tests to guarantee unwanted behaviours to occur. The final goal is to assure that the unwanted behaviours have been considered and lies under acceptable levels of confidence [26] [27].

If we consider only simple systems like the one shown in Figure 12 above, the application of the refutation process becomes easy to apply. However, if we consider a complex SoS such as the one present in the aviation ecosystem nowadays, the application of the refutation process becomes a very demanding activity as the complexity of integrated systems increases. In this case, sampling subsystems and verifying how their behaviours can be transferred to other similar systems in the SoS becomes necessary for efficiency purposes of the analysis.

Through ongoing research, dedicated to this integration subject, different approaches for analysis of the components of SoS are being developed. The goal of these researches is to assure that the refutation results achieved with the analysis of one component of the SoS can be considered acceptable and transferred to the whole system without the need of exhaustive refutation processes applied to all of its individual components [28].

In the aviation ecosystem where the development of larger subsystems are under consideration, the analysis of the cyber security environment since the conceptual stages of development can serve to reduce the need of the application of refutation process to all of its elements. With processes applied to guarantee security requirements by design, the evolution of the aviation system can occur with higher levels of resilience against any event that can stop or disrupt normal operations. This also recognizes the fact that these events will invariably occur due the will of bad actors motivated by different causes.

There is a global but individualized movement by organizations to develop systems and measures to protect them against cyber-attacks. It is though globally accepted the fact that these measures have limited effectiveness due to the non-standardized and harmonized integration process being used for individual systems. The Internet can be mentioned as of one of these SoS that are under constant attack and this vulnerability was demonstrated by a famous case widely analysed by the global media when it happened in 2012.

In 2012, an editor of a magazine explained how his digital life was invaded by hackers that took control of his Twitter account in the article titled: How Apple and Amazon security flaws led to my epic hacking [29].

In the mentioned article, the aspects of an uncoordinated approach to information security by service providers such as Google, Apple or Amazon highlighted how the lack of harmonization and standardization between information security environments of different SoS components can affect the users of the system as a whole.

In addition, and as part of the lessons learned by this event, it was highlighted that not only gaps in security requirements can create loopholes. The protection and performance of a SoS can also be jeopardized by overlaps not coordinated among its different elements.

Some of the issues faced by all SoS and the aviation included, comes from the fact that its current technical and operational components, have been designed and deployed a long time ago when cyber threats were not considered part of the hazard's identification and risk analysis. The threat model used when these systems were deployed had assumptions not valid anymore. Some of these assumptions were the fact that bad actors had inferior financial or technological capabilities and knowledge that would not allow them to perpetrate an attack to such a sophisticated and private system such as aviation.

These assumptions led the aviation community to not recognize potential threats at that time and only a decade ago the participants of the aviation system made a decision that an insider threat should also be considered and a holistic approach to information security was necessary.

The general evolution of the societies towards the use of information management technologies, which brought important operational benefits, to not only the aviation system but also to the society in general, opened new possibilities for attackers. These attackers' goal is to access systems and perpetrate actions that jeopardize the confidentiality, the integrity and the availability of the different types on data and information being produced, stored and exchanged in support of operational activities. Because the uncoordinated evolution of the aviation technological supporting systems, the efforts now necessary by bad actors are reduced and they are able to take action that can deny services that are essential for the safety, security and continuity of aircraft operations and air traffic management.

In addition, due to its direct relationship with safety of lives and the vulnerabilities to passengers and properties on the ground when aircraft operations are under way, it is

crucial that the aviation system and its supporting infrastructure are immune to interferences. Reason being the fact that interferences can stop operations or change the intended behaviour or performance of component systems of the SoS that is aviation to the point where it can jeopardize safety of operations and lose public confidence.

Moreover, in a SoS with multiple stakeholders interacting for the provision of services necessary to conduct safe and interoperable air operations, it is worthy to highlight some characteristics that are inherent to a safe and resilient aviation system that is able to guarantee continuity of services under any circumstances. These characteristics are reflected by its dependability, the need for trust and confidence.

According to Avizienis (2004) [30] the dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable.

From an aviation perspective, the ability to avoid service failures or mistakes would be sufficient for other systems that are dependent on it to trust this system. An example can be given as a pilot responsible for the safe conduct of the aircraft operations while airborne (System A) and who is dependent on the clearances and information provided to him by air traffic controllers (System B).

In this scenario, trust can be defined as the anticipation of one system in the expected behaviour of another system that should not provide false data or information that can be anticipated as affecting safety of operations.

Related to trust there is also the concept of confidence that is connected to the degree of control that one entity can put into the expected behaviour of another entity. In the aviation context, one example is the process used for certification of a new aircraft. For the initial certification, there are assurance procedures that are put in place that guarantee a high-level degree of scrutiny of the development and integration processes aligned with the airworthiness mandatory standards. These procedures and processes together allow the certification authority to have the necessary confidence that a type certificate can be issued to the corresponding aircraft type.

In the information security environment, there is a similar situation where to trust the information being exchanged three levels of confidence can be verified by the involved transmitting and receiving systems [30]:

a) First, it is the confidence that participants in the communication process are positively identified and that the data and information they are exchanging were not modified when at rest or while in transit between origin and destination. This is considered

digital trust or technical trust as some authors use to call and is completely reliant on the technical infrastructure and procedures in place to guarantee the confidence in the communication process. One important aspect of digital trust is that it can be audited against the requirements or standards that are established to harmonize the communication processes.

b) Second is the confidence by the different components of a system that the infrastructure put in place by the different participants is resilient to electronic interference in accordance with the services expected to be delivered by each participant. This is known as organizational trust considering that it must rely on each organization's technical measures. This creates the dependability between organizations that can be used as an incentive for cooperation and collaboration between different entities. As the technical trust, organizational trust can also be audited through the verification of compliance with standards and procedures.

c) The third and final level of confidence is the necessary uncompromised information provision. This relates to an expectation on the behaviour of the originator of any type of information. This is considered from a social point of view and is called societal trust and is an aspect that cannot be audited.

In the case of digital trust, the main challenge associated to the assurance of the right originator providing information with the expected level of integrity relates to the system or processes and procedures in place to guarantee the digital identity of the participants in the process. This passes through the existence of a system to verify and validate the identity of the originator of the message that can be done through a recognition of an electronic signature.

The challenge associated to the assurance of organizational trust relates to the system or processes and procedures in place to oversee and approve the operations of another organization, which includes the infrastructure available in the organization to be overseen. The processes in place need to be sufficiently robust to guarantee that an organization involved in the provision of a certain service to the benefit of the community operates under a certain level of trustworthiness. This trustworthiness is achieved when the organizations have in place, and can demonstrate to all members of the community, a system to avoid unauthorized electronic interferences that can jeopardize the levels of service being provided.

The scenario is a bit more complicate when it relates to societal trust considering that there are no possible controls that can be used by the aviation community. In this case,

there is a need of blind trust. However, despite the lack of possibilities of collecting evidences that could generate societal trust, the past experience in some areas can contribute to a high level evaluation of the trust that can be assigned to a system or organization.

The need to fulfill the expectation that an organization or system is who it claims to be and that the same organization or system presents the behaviour as expected by other organizations participating in the same SoS, was highlighted by Gartner [31] in a study about digital trust. In this study, it was highlighted that any system engaged in the exchange of digital data and/or information need to follow some basic requirements related to:

a) The need of every system or organization involved in a process of exchanges of trusted digital information to have a digital identity.
b) The process for the scrutiny of the digital identity that needs to be in place to assure the validity of this digital identity and guarantee that the identity can be trusted.
c) The technology used for any participant organization or system to the generation and maintenance of the digital identity.
d) The trustworthiness on the exchange of digital information that will only be achieved if the participants in the exchange of digital data have a digital identity.
e) The necessary authentication of the validity of the digital identity before the exchange of digital data can be performed; and
f) The authorization of the participants in the process of exchange of digital data for the establishment of the communication.

In the process of exchange of data and information in a virtual environment, where physical verification of identity cannot be performed, the scrutiny process used for the verification of the real digital identity of the organizations and systems participating in the digital data exchanges becomes necessary. This aspect is crucial and it serves as the link between the technical, organizational and societal trust.

Similar to the processes in place to maintain the identities of citizens living in an organized society that start with a birth certificate and ends with a death certificate, equivalent processes, which differ sometimes between States and types of organizations, do exist.

The verification of the validity of the identity of individuals and organizations are normally on the hands of States to guarantee a certain level of scrutiny when the

communications are between individuals and/or organizations. Sometimes this verification is delegated to specialized entities. In both cases, it requests a high-level degree of societal trust.

When it comes to communications between technical systems used for operational purposes that may impact safety of lives or important business and operational decisions, such as uploading software to onboard navigation systems, it is necessary the establishment of procedures and processes that provide similar guarantees on the level of validity of the digital identities being used.

In the process of digital data exchanges, where the establishment of digital identities is a requirement, different organizations use different information management systems. These systems, to be trustworthy, are dependent on how they are designed, deployed, integrated and operated by their developers and users. A crucial aspect of this trustworthiness is how secure the processes associated to the phases from design to operations are. This highlights the need of not only verification of the system in use, but the supply chain associated to the production.

As in the case of citizens, which have their identities verified by two main processes, the birth certificates and death certificate, the processes in place to generate and also to decommission digital identities carry similar importance. The more the system for identity management can be trustworthy, the more trust will be put into the identities managed by the respective system. On the other hand, if a system loses trustworthiness, the digital identities being managed by them will also be considered not trustworthy, independently of the level of scrutiny that was put into their creation.

For the aviation system, de development and deployment of an international aviation trust framework becomes then necessary in enabling digital data and information exchanges among the different members of the aviation community and supporting systems. The trust framework to be put in place must cover the requirements for digital and organizational trust. These processes to be put in place are necessary in recognition of the different aspects related to societal trust at a global level.

2.5 Conclusion

The transformation of the current air navigation system is essential to guarantee safety, efficiency and continuity of air operations that are, among others, key requirements of the aviation community.

The current use of private networks for ground-ground communications is attending partially the needs of an evolving aviation system-of-systems.

To allow a more collaborative and informed decision-making and transformation of the aviation system as it grows in participants and number of messages being exchanged, a global resilient and interoperable network becomes essential. This network should provide access to all airspace users and equity in the use of the airspace and services available at the same time it guarantees continuity of operations under normal and sometimes specific constraining circumstances. The secure exchange of information on a global basis, enabled by a global resilient aviation network built upon a trust framework, is crucial to allow this transformation.

Personal, local, and regional area networks can help in the exchange of information for a limited number of members and in limited distances. However, being aviation international by default, wide area networks such as the Internet become crucial to interconnect stakeholders not sharing borders but in need of flight an flow information to attend the requirements established in terms of safety, efficiency and resilience of operations.

Being the wide area network a group of local or regional area networks connected, the data communications between different networks are not possible if there are no common protocols for transmitting and receiving the packets of data. The origin and integrity of these packets need also to be considered to guarantee trust between different participants with different requirements and expectations. The Internet protocol suite (IPS), composed of transmission control protocol (TCP) and internet protocol (IP) is one of the most widely used protocols and is the one chosen by the aviation community to support a global aviation interoperable network that can exist only if it can be trusted.

For aviation, trust can be seen as the anticipation of one stakeholder in the expected behaviour of another one expecting that an originating system does not deliberately provide false information.

Related to trust there is also the concept of confidence that is connected to the degree of control that one entity can put into the expected behaviour of another entity. In the aviation context, one example is the process used for certification of a new aircraft. For the initial certification, there are assurance procedures that are put in place that guarantee a high-level degree of scrutiny of the development and integration processes aligned with the airworthiness mandatory standards. These procedures and processes together allow the

certification authorities to have the necessary confidence to issue a type certificate to the corresponding aircraft.

It is recognized that a robust system to guarantee the digital identity of all participants in the exchange of digital data is crucial for the trustworthiness of the aviation system as a whole. The challenges associated to trust in the digital identity of systems and organizations is crucial to guarantee the integrity of the communications between different members of the aviation community and its supporting systems.

Chapter 3

Methodology

3.1 Introduction

The present chapter intends to describe the path taken to find the best applicable methodology necessary to the development of a practical and pragmatic approach on the subject being studied aiming a set of procedures to establish a process to guarantee the confidentiality integrity and availability of exchange of data and information in a digitally connected aviation ecosystem.

Several options are available in the literature including qualitative, quantitative and methodologies that mix both options. The choice made relates to the positioning and background of the researcher and the subject under investigation.

An analysis of the quantitative methodology shows that the positivism is the predominant paradigm in this approach. Meanwhile, in a qualitative approach the trend is towards an interpretative approach [32].

According to the research made and the readings of different sources, it is agreed among several researchers that quantitative methodologies are more used in exact sciences and are largely used in social sciences. This shows that quantitative methodologies are an option of the scientific community. Punch (1994) [33] remarks that the use of the qualitative methodology is highly contested by the scientific community.

During the decision making process regarding the methodology to be followed, it is worth to highlight that the background of this researcher is in air transport engineering with several years of experience in air traffic management, communication air-ground and ground-ground systems and protection of air navigation systems against physical or cyber threats. This would naturally motivate the researcher to adopt a quantitative methodology.

However, the subject to be studied relates to the aviation ecosystem which is formed by several complex systems where the causality principle is not always guaranteed, meaning that the same cause not always will produce the same effect.

Being the researcher actually working on the subject aiming the development of an operational system that is expected to be implemented by 193 member States of the International Civil Aviation Organization, and all the members of the aviation industry, care

was necessary to avoid biased influences. These influences could come due to the environment where the research is being developed and the limitations of the subjectivism of the research considering that the environment can influence its results.

3.2 Scope

It is important to define the scope of this research to guarantee that the readers are aware of the area covered by the study as well as the limitations applied to the research.

Being a research focused on finding a practical and pragmatic solution to the evolution, through digital transformation, of the air navigation system in support of the international civil aviation, the research does not cover the processes and procedures applied specifically by State aircraft operators to guarantee resilience of military air operations.

According to the Convention on International Civil Aviation, State aircraft are aircraft used in military, custom and police services and follow specific rules defined by the State where they are registered and operated. In this case, the procedures to be applied by State aircraft are sometimes unknown by the entire aviation community due to aspects related to national security and defence considering that they are not published through the regular national aeronautical information publication (AIP).

This research is focused on specific two key performance areas, namely safety and security and the impact of security or lack of in the paramount area that is considered safety for the aviation community and from a business perspective also the impact on the continuity or resilience of operations. The research also recognizes the complexity of the aviation system that to work harmoniously should find the balance among different key performance areas.

Safety is the highest priority in aviation and protecting and keep resilience of the aviation system plays a major role in ensuring overall aviation safety and continuity of operations. To guarantee the agreed levels of safety, the aviation community applies specific standards, procedures and processes for hazard identification and risk management to keep all risks under the limit that can be accepted by the society.

For these standards, processes and procedures to be accepted by the aviation community and the society in general, they need to follow a globally harmonized approach that is translated in terms of practices associated to safety management.

Besides safety events, which can jeopardize life of people onboard and on the ground, security is also another area to be managed. Security in the context of aviation is the capability to protect the aviation system against threats that can come from different sources, but most commonly, coming from terrorism. With the evolution of the industrialization and the impacts it brings to the environment, and the life of communities, reasons for security attacks, impersonated nowadays most commonly through cyber-attacks, can come though from actors not aiming terrorism, but that can cause similar negative effects in the aviation ecosystem as a well planned terrorist attack.

The challenge remains on the balance between the security measures to be put in place and the needs of the different members of the aviation community to access the different resources available to support air and ground operations.

The existence of threats to an isolated aircraft or threats that can simply use the aircraft as a weapon, as well as threats to installations on the ground providing air traffic management services are a constant concern of the aviation authorities. In this case, the aviation system needs to be able to support the authorities providing the necessary information that will serve for the decisions on the best action to solve efficiently an ongoing event. This information would enable investigation and practical measures to reduce the threat and attack surfaces and stop them, avoiding them to become an event that could affect safety of lives.

3.3 Methods and paradigms

The analysis of data and information for the development of a research can be performed initially using quantitative and/or qualitative approaches. These two terms can often be related to the methods associated to the research or to the research paradigm itself. According to McMillan and Schumacher (2006) [34], the quantitative and qualitative approaches refer, from one side to the understanding of the world and the objectives of the research, the nature of knowledge. From another side they refer to the processes associated to data collection, processing and analysis, the research methods.

Regarding the qualitative research, Bluhm, Harman, Lee and Mitchell (2011) [35] identified four characteristics that can be used in its definition.

Starting with the environment where they are realized, a qualitative research normally takes place in the normal and regular s etting of the organization.

In addition, in the qualitative research the sources of the data are the perceptions of the people participating in the research according to their personal experiences. It means that in a qualitative research, all the members of the organization are heard. The research can also approach only the individuals that are thought to have a better knowledge of the main subject of the research as representative of the whole organization population.

The data gathering and its corresponding analysis is not static. As the qualitative research progresses, the processes associated to data gathering and analysis may change. This can be considered a reflexive characteristic of the qualitative research. This characteristic is important to guarantee the right direction and outcome of the research considering that at the beginning of it, research have biases considering their knowledge and experience. Through the development of the research and the data collections, their bias may change and the process for data gathering and analysis is adapted to the new reality.

Lastly, but not less important is the fact that a qualitative data collection is not standardized. The questions used in a qualitative research influence the procedures for data collection and may also influence the instruments used for further data collection.

Baltazar (2018) [36] highlights that the important aspect is not to deduct nor test any type of model that exist in the literature. What is necessary is to elect, for the conduction of the research, a qualitative strategy where from data a theory can be inferred. This theory, when applied to the aviation ecosystem could then support the development of proposals for standards and recommended practices and procedures for air navigation services to support safety, efficiency and continuity of operations. In this case, as explained at the beginning of this chapter, the result of this study should be a proposal to reduce the attack surface of the aviation system against cyber-attacks. This reduction will contribute to the resilience of the system, which, at the end, will affect the safety and continuity of operations.

The table 2 below summarizes some important characteristics of the qualitative and quantitative methods.

Table 2 - Characteristics of qualitative and quantitative methods. Source: Adapted from [31]

Characteristics	**Qualitative**	**Quantitative**
Approach	Inductive	Deductive

Goal	Depth, generate hypotheses	Breadth, test hypotheses
Setting	Natural	Experimental/quasi
Sampling	Purposeful	Random
Data collection	Interview guides, observation tools	Surveys, administrative data
Data analysis	Iterative interpretation	Statistical testes, modeling

This research should be seen as an attempt to perform a pragmatic and systematic approach to collect, analyse and interpret data and information. This data processing is made towards the understanding and prediction of events that can affect safety and continuity of operations and an attempt to relate these events to others of similar nature and based on the knowledge acquired; develop solutions that can protect the aviation system from significant degradations.

The choice to use a pragmatic paradigm is important considering that this approach was the one who set down what can be expected as an outcome of this research. At the same time, the pragmatic paradigm was used as the framework for the theoretical analysis of the subject present in scattered literature.

According to Mackenzie and Knipe (2006) [37], without nominating a paradigm as the first step, there is no basis for subsequent choices regarding methodology, methods, literature or research design.

The development of this research was made following Mackenzie and Snipe (2006) that oriented the way of thinking of the researcher at the same time it motivated the progress of this research through the development of assumptions, concepts and proposals logically but loosely related.

Besides the pragmatic paradigm, there are several other theoretical paradigms described in the available literature. Among them it can be highlighted the positivist, the interpretivist, the constructivist, the deconstructivist, the critical and the transformative paradigms.

It is worth to highlight at that point that, one aspect that initially generated some confusion in this research, was the existence in the literature of different texts with different claims regarding the paradigms including the number of existing research paradigms.

The lack of commitment to any sort of philosophical or reality system was crucial to the choice of the pragmatic paradigm to be used in this research considering that pragmatists are often focused only on the what and the how of the problem subject to the research [38]. This approach gave the freedom to the researcher to mix the methods of data collection and interpretation. Placing the research problem as central to the research, the pragmatic paradigm allows the application of different approaches to understand the problem and develop possible solutions. This does not mean that the other paradigms cannot use mixed methods as well.

The main goal of this research is the investigation of a current and real problem affecting the aviation industry. As such, the approach taken in this research was to first identify the problem with the different technical and high-level political aspects involved before the development of a proposed solution that can be accepted by the entire aviation community and supporting industry responsible for the supply chain.

The implementation of the plan and observation of the changes are to be developed as part of a use case scenario for the proposal that can be performed as part of future work.

According to Creswell [38], the application of a mixed method to the research, following a pragmatic paradigm, allows the possibility to take different approaches and use different assumptions that would enhance the worldviews about the issues under study.

The previous paragraphs do not intend to simplify or mean that the analysis of the paradigms is not important, however, a detailed description of each paradigm can be found in different literatures, and it is not the goal of this research the discussion on any of them.

However, to contextualize the choice of the pragmatic paradigm for the subject of the research, the following table 3 could serve as a clarification of the differences and similarities between different paradigms and why the pragmatic paradigm was chosen as the basis for this research.

Table 3 - Paradigms: Language commonly associated with major research paradigms. Source: [38]

Positivist/ Postpositivist	**Interpretivist/ Constructivist**	**Transformative**	**Pragmatic**

Experimental Quasi-experimental Correlational Reductionism Theory verification Causal comparative Determination Normative	Naturalistic Phenomenological Hermeneutic Interpretivist Ethnographic Multiple participant meanings Social and historical construction Theory generation Symbolic interaction	Critical theory Neo-marxist Feminist Critical Race Theory Freirean Participatory Emancipatory Advocacy Grand Narrative Empowerment issue oriented Change-oriented Interventionist Queer theory Race specific Political	Consequences of actions Problem-centred Pluralistic Real-world practice oriented Mixed models

3.4 Incentives

The beginning of this research was motivated by the increasing need of the aviation community to expand the capacity and efficiency of the current aviation system. In 2005, the International Civil Aviation Organization published the Global Air Traffic Management Operational Concept that highlighted the importance of the evolution of processes and procedures associated to information exchange in support of the global management of air operations.

As part of the mentioned evolution, one of the principles was that the aviation community would rely more and more on different types of information to support efficient decision-making processes. For decisions to be made with low margin of errors compatible with the risks agreed by the community, the information to be provided should meet agreed levels of quality, including its integrity and be provided when and where required. For this process to be efficient, the community would need to share information on a global or system-wide basis to support the evolution of the aviation system in all key performance areas affecting aircraft and air navigation system operations.

Despite being an acknowledged type of system from a SoS perspective as described in the previous chapter, for the aviation system to operate with the high kevels of safety and efficiency requested by the aviation community, collaboration between different components and participants becomes a crucial characteristic. Cooperation will result in

better decision-making considering that it allows the sharing of timely information to all participants involved in the complex system providing a better integrated picture of the system as a whole.

From a service provider perspective, the optimization on the provision of the necessary services to support air traffic and aircraft operations can only be achieved if actual data or predictive data with the level of accuracy that can support efficient and effective decisions are available when and where necessary without unacceptable delay.

The effective management of the information in the aviation system would also allow the monitoring and control of the quality of the shared information. Only with a reliable system for information exchange, the aviation community will be able to take decisions based on the best possible current and future operational scenario. These decisions, to preserve safety of operations must consider that the traffic situation changes with time and sometimes the factors provoking the changes are not controllable using any tools available. This requires that information on events that could endanger aircraft operations, such as adverse weather, or the presence of volcanic ashes in the air, just to mention some, needs to be available as prompt and accurately as possible. This puts a serious concern on the capability of the current system to avoid unforeseen events such as denial of services due to cyber-attacks aiming the disruption of the aviation system.

The aviation system is highly dependent on accurate and timely information to support the evolution of operations by all airspace users and air navigation service providers. Only with the necessary information available to authorized users, the system can evolve from current level and achieve the proposed efficiency compatible with the levels required by the society.

To allow this evolution, the aviation community embarked in the development of a series of operational improvements using digital technologies and more digital exchange of data and information. Most of the time these exchanges are performed without worries regarding the confidentiality, integrity or even the availability of the information being compromised by external sources.

The confidence in the message exchanging processes in place rely on the fact that air operations have been supported by dedicated communication systems. These systems were specifically designed to meet the aviation community requirements and isolated from public access and for the fact that the threat vector was not identified by the time of the systems development, due to the low probability seen by the aviation community of a cyber-attack against the aviation system.

However, with the start of the use of the Internet, this confidence was affected based on the situation brought about by an increased reliance of avionics and ground systems on a small number of well-known technologies from the information technology world [39]. This includes Linux, Windows, Internet Protocol version 6 (IPv6), Ethernet, and others.

To speed up the development time, manufacturers also use commercial off-the-shelf (COTS) software and hardware in the development of onboard and ground systems, again adding to the potential risk as these technologies are not always developed following the aviation requirements and present unknown vulnerabilities.

As described in the last chapter on state of the art, the aviation system is going through an unprecedented change with the evolution of the communication means and the appearance of new flying platforms with different requirements from the legacy manned aviation. These communication means and the support they provide to new flying platforms are essential to achievement of the business continuity, security and safety requirements, however, because it was developed using open systems, it brought vulnerabilities and allowed occurrence of incidents that the aviation industry was not used to face before the advent of digitalization of the communication systems.

Some examples of these events have been explored by different researchers to find reasons and/or causes and means of protections and the conclusion has been unanimous saying that it is impossible to have a system one hundred percent secure [40].

Civil aviation has historically raised the appetite as a target for disruptions. With the evolution of the system towards more automation and digital connectivity, the possibilities of such disruptions increased to the point that cyber-attacks pose a threat to global aviation safety. Some examples, already published by the traditional media, are listed below in a chronological order for reference [41]:

2006: in this year, the American Federal Aviation Administration (FAA) was forced to stop several air traffic services in Alaska due to cyber-attacks.

2008: a Trojan in the computer system of the Spanair airlines can be considered as one of the contributing factors for the collision with the ground of flight JK5022 after taking off from the Madrid International Airport that caused 154 fatalities among passengers and flight crews. It needs to be highlighted though that the determination of the contamination of the system through Trojan is still inconclusive.

Spanish daily El País reported though, at that time, that according to an internal report issued by Spanair, a malware could have infected the airline's central computer

system. The computer system was used to monitor technical problems with its aircraft and may have resulted in a failure to raise an alarm over multiple problems with the aircraft before taking off.

2009: personal files of more than 48,000 employees of FAA were accessed through a cyber-attack.

2013: a cyber-attack on the passport control systems of the Istanbul Atatürk and Sabiha Gökçen airports resulted in a temporary denial of the respective services and passengers had to wait for hours until the reestablishment of the system with consequential effects in the operations of the airports.

2013: an intrusion aiming at spying who could be in certain flights or the cargo they were transporting was discovered affecting 75 airports under the FAA responsibility. Investigations raised the possibility of the attack being perpetrated by groups funded by a State due to the level of sophistication of the attack.

2014: inoperability of a system and loss of personal data files were reported by the Airports Authority of India's enterprise resource planning system. The cause is reported as being a cyber-attack.

2014: cyber-attacks on airport and airlines from, among other countries, Pakistan, Saudi Arabia, South Korea and the United States were reported, allegedly perpetrated by Iranian hackers. This attack was reported as affecting 16 different countries.

2015: malware was found in personnel emails accounts from FAA employees.

2015: a cyber-attack on the bank accounts of the Ryanair airline caused financial damages that could have reached 3 million pounds.

2015: a cyber-attack to the network infrastructure of the Polish National Airline (LOT) affected the system responsible for generating flight plans and caused the delay of several domestic flights as well as flights to Denmark and Germany.

2016: the Hanoi and Ho Chi Minh City airports information screens and the website of the Vietnam airlines were attacked. At the airports, all operations had to be performed manually for a significant amount of time. Besides, it was reported that more 400,000 passenger's data were vulnerable.

2017: this year can be considered to be subjected to an outbreak of cyber-attacks most of them in the form of ransomware aiming financial gains. Ransomware were used to

encrypt data from LATAM airlines and Ukraine's Boryspil International Airport. Despite not being directed to aviation safety critical systems, the cyber-attacks resulted in disruptions to airports and loss of money by the involved in the attacks.

The list above was just to exemplify some of the cyber-attacks that contributed to move the subject to the list of priority by many international organizations and become central for the aviation community considering the possible impacts a cyber-attack, perpetrated to safety critical systems, can bring to the aviation industry and the users of the aviation services as a whole.

At a global level there is no framework that can guarantee protection of exchange and storage of data and information related to civil aviation planning and operations. This is simply understood by the fact that only recently aviation became a target of bad actors. Being a system of systems built to meet specific needs of community of interests, the systems were developed in isolation and exchange messages according to their needs and using networks that meet their own requirements without attention to confidentiality, integrity or availability considering its presumed isolation from the public digital world represented by the Internet.

Nowak, Ogonowski and Kustra (2019) [42] highlighted that the levels of connectivity being practiced by the aviation industry brings with it new vulnerabilities that need to be addressed immediately if the industry wants to avoid serious safety operational and reputational damages. A proactive approach is highlighted as the only way to reduce the cyber-attack possibilities and to avoid serious incidents and possible accidents that can affect the perception of the society on the levels of safety of the aviation industry and represent a serious setback to the industry.

The hyper connectivity brings with it many cyber threats that can evolve to cyber-attacks to civil aviation. It is worth to highlight that cyber events are not always intentional. In a digitally connected environment, even an unintentional event can stop or harm essential systems and services.

Among the actions that can jeopardize safety and efficiency of any type of operations, some of the intentional actions are highlighted below:

- Malware: a virus, a network worm, a Trojan horse, a dialler, a botnet.
- Breaking security: unauthorized logs, account hacking, hacking into an application.
- Internet publications: offensive content, copyright breaching, misinformation.

- Gathering information: scanning, wiretapping, social engineering, espionage.
- System sabotage: unauthorized exchange of information, unauthorized access or unauthorized use of the information, denial of access, deleting data, use of vulnerabilities in devices.
- The human factor: deliberate violations of security procedures, violating binding legal regulations.
- Cyber terrorism: a terrorist crime committed in cyber space.

On the other hand, unintentional activities can be:

- Accidents and fortuitous events: hardware failures, link and software failures.
- The human factor: an unintentional violation of procedures, negligence, incorrect configuration of a device.

The events mentioned above highlight the need for the aviation community to invest not only in measures for protection of the systems to provide services, but also in the development of procedures that are able to maintain the resilience and continuity of the operations when facing an intentional or unintentional event.

These events and the catastrophic impact they may have to the aviation industry, bringing its components to a complete global, regional, national or local halt, affecting the business and normal life of billions of people at the same time, were the main incentive to the development of this research.

3.5 Vulnerabilities, trust and the research strategy

There are several documents in the literature that analyzes the vulnerabilities of systems supporting air operations. This involves onboard and ground systems. Some of them highlight the possibility of external sources intervening on onboard systems, although aircraft manufacturers deny that possibility due to the air gap between different onboard networks supporting the aircraft command domain, the information domain and the entertainment domain.

The command domain involves avionics and control systems that are safety and operation critical to flight handling and navigation. The information domain represents the business critical systems such as cabin lighting and galley power. The entertainment domain complies any system that do not support any flight safety or operation [43]. The onboard Internet or media system can be mentioned as examples for entertainment domain.

Policy-focused frameworks and guidance documents have been developed over the years addressing cyber challenges, however bridging theory to operational practice has been missing from the literature.

As the goal of this research is to propose a solution for translating infrastructure protection and resilience theories to practice under a background of system and attack related uncertainties, it is necessary to investigate with the people operating the current systems how they see the vulnerabilities. It is also necessary to investigate the challenges and possible solutions for keeping resilience and continuity in air operations. In addition, this must be done at a time when the aviation system is moving fast towards transformation through the digitalization of systems supporting aircraft operations and air traffic management.

Straus (1993) [44] highlights that the universe is living an era of extreme fluidity and this universe will not stand still for the simple reason it cannot. In this universe, new appearances and coalescence are directly linked to disappearance and fragmentation. Besides, in this universe nothing is directly determined. It is possible a partial determination if one uses a naturalistic approach that can define the roles of the human beings participating in the construction of structures that will provide the necessary support to their lives and needs.

Practical solutions for protection and mainly resilience of operations in a digitally connected and transforming environment are missing from the literature. In a revolutionary aviation world, an analysis of the grounded theory offers an opportunity to create an applied solution to the challenges faced by the aviation community to face cyber threats and attacks in a fluid environment as highlighted by Straus (1993) [44].

One of the virtues of grounded theory studies and qualitative research in general is that there are many different sources of data and information. This information can come from sources such as, interviews, applied in this research as the main instrument for data gathering, but also from historical documents, group meeting's report and observations, just to mention a few [45]. In this study, considering the problem to be investigated, the conduction of pragmatic interviews associated to analysis of published documents was the most appropriated method for data collection.

The interviews allowed this researcher to collect a rich and large amount of data and information considering that participants were free to talk about the issues pertinent to the exchange of safety and non-safety critical information between different stakeholders and they could elaborate the talking as they preferred, using direct or indirect speech. The

interviewees highlighted that this exchange of information between different stakeholders can only happens in an environment where identity is trusted, and the integrity of the messages being exchanged guaranteed at all times. The experts were able to determine their own pace to talk about the subject, in what order, and to what depth.

The decision to use the unstructured interviews was made after considering the complexity of the subject, associated to the lack of practical literature addressing the operational issues faced by the aviation community using digital connection for exchange of safety critical messages and guaranteeing continuity of operations with the hyper connectivity existing in the aviation ecosystem today.

According to Corbin and Strauss (2015) [45] an unstructured interview provides the richest source of data for theory building where participants are able to talk freely about the issues and problems pertinent to them and also give participants more control over the course of the interview.

The interviews were performed with different members of the aviation community representing different sectors of the industry participating directly or indirectly in the provision of the services to support airspace users and aircraft operations as well as the services associated to air traffic management. The interviewees were also selected from different management and operational levels in the aviation industry to allow management and technical thoughts comparison and verification of convergence or divergence.

The main objective of the interviews was to collect data and information related to the views of experts actually living the need of evolution of the aviation system in a digitally connected environment. In addition, the interviews served to evaluate the need for investments to keep the protection and resilience of the aviation system that would at the end impact safety and the business continuity and bring the benefits the society expects from the aviation industry.

These benefits cannot be achieved if the society loses confidence in the way the industry deals with safety of lives. This passes through the assurance or trust that all players in the system are identified and perform according to pre-established rules and use systems that would not jeopardize the safety or continuity of operations that could bring serious damages to the business of providing services to flying people as a whole. In addition, the damages can be from not only an asset or economic perspective but also reputational damages that could bring a service provider or aircraft operator to stop operations due to lack of confidence by the travelling public.

The notion of trust has different definitions and aspects considered by different researchers in the past. As Schneider (1999) [46] highlighted, with the constant presence of the Internet to our lives, questions related to trust and its impact and restrictions in a digital environment becomes an important subject to be discussed.

The current discussions most of the time focus on the technical and operational aspects of trusted identities in the e-commerce activities. However, the issues associated to trust can be expanded to encompass any sort of exchange of information using the cyber space.

Some authors focus on the discussion of trust related to relationships when these relationships are realized through virtual chat rooms among different groups of people. Of specific interest to the aviation community, the theories and practices related to trust in operational information management systems is still pending.

Despite different authors have an agreement that trust carries a strong psychological and social influence, the same authors can not agree to the correct place to put trust. In general, the subject has been approached in different levels. Some authors approach trust from an individual perspective as a personality trait. Others see trust as a tie between different actors, describing it from an interpersonal or relational perspective. There are some authors though that prefer to see trust from a society perspective treating it as an aspect of distinct communities as a whole.

From the different approaches mentioned before, at the individual level the trust discussions aim to cover the statement “I trust”. If the discussions are extended to interpersonal and relational perspectives, it goes towards addressing the statements of “I trust you and you and I trust each other”. Finally, if the discussions are seen from a societal perspective it goes to address the statement “we all trust” [47].

If trust is seen exclusively from an individual perspective, the subject is treated as a psychological attribute with expectations established based on experiences accumulated by different actors [48].

Interpersonal trust can be seen as the most common manifestation of trust. In the current society behaviours, it can be seen as a bond between somebody who trusts (trustor) and somebody who is trusted (trustee) [49].

In the interpersonal trust perspective, the confidence the trustor holds towards the trustee is directly influenced by the confidence by the trustors in the behaviour and expected future actions by the trustee [50].

When it comes to the relational perspective, trust must be seen as an emergent characteristic of relationships as a whole and not as a direct attitude originated in one person towards another. The relational perspective describes trust as the glue that puts people and systems together and sustains their interactions over time [51].

Trust, seen from a societal perspective, works as the most important characteristic that makes the society functioning. The societal model highlights the importance of trust that considering all factors of modern life, allows people to function in a complex society and using complex communication systems [52]. Most recently, in the modern literature, societal trust or system trust is described as a social capital.

System trust is a prerequisite for social mechanisms as well as institutions and systems [53] and the aviation system is dependent on trust between the different actors to guarantee the safe and resilient operations at the same time it contributes to continuity of operations in contingency situations.

The Convention on International Civil Aviation requires States to provide, over their areas of responsibilities, the necessary infrastructure to facilitate the air navigation. This infrastructure relates, but is not limited, to facilities to provide air traffic services, airport operational services and meteorological services. Ideally, the services to support the aviation technical and operational systems should be based in agreed international standards. At the same time, States should collaborate in international measures to secure the information being published or exchanged in support of air navigation. This highlights again the importance of societal trust for the aviation ecosystem.

Sometimes in the literature, the concepts associated to trust and confidence are mixed, however, they carry slight differences that justify a better explanation. A simplified definition of trust can be seen as the union of a person or system to which one deposits the trust (trustee), the confidence that the trust will not be betrayed and the willingness of another person or system (trustor) to take actions based on that confidence.

The concept of trust brings inherent to its definition the ones disposition to take and accept risks with consequences in the acceptance of vulnerabilities.

It is the specific characteristic of risk acceptance that differentiates trust from cooperation since cooperation can be achieved through belief or coercion. Cooperation in this case is limited to the willingness of the other to act or not on behalf of these beliefs.

The aviation system, although relying on cooperation, must have trust in its components to make aviation interoperable, safe and secure. Nowadays this is done

physically verifying identities, messages, licenses and certificates through direct local inspections and audits.

The issue comes when these verifications are not able to be performed due to the complexity of the digital and automated systems supporting the provision and consumption of services. Currently, most of these services are provided through digital information management systems storing, processing and exchanging information through online systems and applications.

As such, in this research we consider trust as the willingness of participants in a trust framework to rely on a specific other, which can be of human or technological system nature based on the confidence that one's trust will lead to positive outcomes.

The concept of trust highlights two important conditions for its definition. It entails the dependence between one agent (the trustor) on another agent (the trustee) with the recognition of both parties that this trust brings with it risks about the final results of their relationship that carries uncertainties regarding if the final outcomes are the desirable ones or not and the vulnerabilities generated in between.

This relationship between the two agents entails that one agent has a need to be fulfilled and the other has the capability to fulfil that need [54].

In the existing literature, quite often, trust is characterized in terms of the benefits that can be brought by a certain risk and the appetite to accept that risk. As such, trust is seen as the combination of vulnerabilities and uncertainties [55].

Several procedures and processes help to improve trust in systems where the direct face-to-face contact is not possible due to the physical distance between the source and the consumer of data or information. One of this process relates to the identification of both source and consumer.

Identification in the aviation context is referred to as relational trust and arises from the extent to which the trustor (consumer) and trustee (source) share a common understanding of the identity management process, goals, and values. This process relates to the cognitive dimension of trust and serves to enhance the perceived trustworthiness of the trustee in all aspects.

Trustworthiness must be perceived as the likelihood that a particular trustee will uphold one's trust. It encompasses four classes of attributes, including competence,

positive intentions, ethics, and predictability. The effect of each of these attributes is to strengthen the trustor's confidence that the trustee is willing and able to fulfill the trust.

It is widely acknowledged that trust as a construct may be applied to people, either individuals or organizations. However, there is debate over whether it is valid to speak of a technological artifact as the recipient of trust. Several researchers have argued that this is inappropriate, because technology lacks the requisite properties of a social actor. Trust requires both parties to be able to extend good will, be vulnerable and experience betrayal. It presumes that the recipient of trust possesses consciousness. Moreover, an inherent quality of trust is its transformative nature and its ability to influence the attitudes and behavior of both parties. These views dismiss the concept of trust in technology as machines cannot literally be trusted, but only be relied upon.

However, studies in human-computer interaction [56] indicate that people relate socially to computer technology, including the social relation of trust.

Trust in information systems may conform to interpersonal trust if it is invoked with respect to the specific systems with which one directly interacts, while societal trust applies to large networks of systems that are not within one's immediate purview.

The trustee is the network, the computing system, hardware and/or software, and trust entails an expectation of proper functioning, and processes and procedures to guarantee the reasonable quality and continuity of operations when using the system. The willingness to engage in trust arises because a person is free to choose an alternate system or to select an entirely different method of performing an activity that would bring the feeling of trust that the user requests.

In the aviation system and among the aviation community, the presence of risk creates a need for trust. Trust can be seen in this case as an assembly of standards, processes and procedures, agreed among the members of the community including service providers, aircraft operators and regulators to reduce risks during internal and external interactions.

The conscious acknowledgement and consideration of risk distinguishes trust from related concepts, such as confidence, blind trust, and faith [57].

Moreover, this is where an aviation trust framework for a digitally connected environment is seen as necessary to guarantee the resilience of systems that may jeopardize safety and continuity of operations, recognizing that safety and, after the pandemic of the corona virus, continuity of operations are paramount to the aviation industry.

With the goal of getting different views from different sectors of the aviation community involved in the development, maintenance, and operation of the aviation ecosystem, experts were then interviewed.

In addition, having safety, resilience and continuity of operations requirements in mind, the interviews were performed leaving the experts free to speak on the way they see the system and how they would solve the problem if they were able to take decisions at a global, regional or national level.

The start of the interviews was dictated by an introduction by the researcher on the subject. After that, the interviewee was allowed to speak from his/her experience and knowledge about resilience, safety and continuity of operations in a digitally connected environment. They were also motivated to speak on how the problem of trust could be solved in a complex aviation ecosystem involving participants clearly educated with the aviation safety culture and others that, using new flying platforms and technologies, start to interact with the aviation system but not fully engaged with the aviation safety culture.

Conversations were held with the interviewees on the use of digital technologies to support operations in the aviation ecosystem.

It is recognized that technologies facilitate the operations and bring efficiencies not possible to be achieved without them. It is also recognized that they also bring complexity to the subject of trust due to the lack of established and recognized global trusted procedures for identity management as well as clear requirements for a network to be used for the exchange of safety and non-safety critical data and information.

The analysis of the descriptions made by the experts allowed this researcher to interpret and condense the data and information and develop concepts based on their properties and the level of description. At the end, the interviews served to show the relationship between concepts and descriptions by defining the main issue related to exchange of data and information in a complex system of systems and the interaction between them and explaining how this interaction is subject to change with changes in context and relating the outcomes to the interactions.

The analysis also allowed the construction of a proposal that necessitates to be explored fully and considered from many different angles to guarantee that the aviation system remains resilient in an environment where actors interact digitally without any sort of face-to-face physical verification of their identity.

The interviews also allowed this researcher to make comparisons and decisions and act in direction of the construction of a proposal. This proposal could be applied by the aviation community to preserve the aviation industry from the threats intrinsic to a digitally connected environment and its associated issues related to preservation of trust that can be translated, among other parameters, through the confidentiality, integrity and availability of the data and information being stored, processed and exchanged among different stakeholders.

According to Glaser and Straus (1967) [58] there are different levels of theory that can lead to proposals. Theories may be substantive, middle range, or formal. Theory here is seen as a set of concepts and the postulated relationships among these, a model or framework that has implications for understanding or action.

A theory of information management derived from a specific study on human behaviour (e.g. air traffic controllers under stress) can be seen as an example of a substantive theory.

The broader concept of information management, derived from the previous study, can be used next to study other types of behaviours in different context. Studying information management in another setting will add more concepts, further develop and broaden original concepts, and potentially increase the abstraction of the core category, thereby raising the theory to a middle-range theory.

A general theory can be developed if the middle-range theory of information management is used to study disclosure and nondisclosure between two countries negotiating a return to normal operations after a crisis that brought aviation to stop for example. If the result of that study, adds more concepts and raises the level of abstraction even higher, the researcher can be seen on the way to developing a more general theory.

Formal theories are less specific to a group or place, are broader, denser, and helps to understand a wider range of concerns and problems. It is the investigation of a broad concept, such as information management in many different types of situations, which enables a substantive theory to become a formal theory and have broader applicability. Moreover, this is what this research intends to achieve; apply theories to develop a pragmatic proposal that can be applied by the entire aviation ecosystem to preserve trust among the stakeholders and guarantee resilience and continuity of operations in a digitally and vulnerable connected environment. Different stakeholders that need to develop specific local, national or regional procedures to address the needs of their communities of interest can then use that theory.

Forty-five experts were interviewed, and their views were compared to current literature and translated into inputs that served as the basis for the development of a proposal for a trust framework for aviation in a digitally connected environment. This digital connection is allowed by the digitalization and automation of systems used to support aircraft operations and provision of air navigation services. It has proven to bring efficiency gains to all stakeholders but at the same time opened vulnerabilities that were not present in the aviation system before the event of digital connectivity for the exchange of data and information.

3.6 Conclusion

The decision to use a qualitative approach to data collection and analysis was made considering the relatively new nature of the discussion on digital trust, resilience and its impact in safety and continuity of air operations.

The subject of trust has been already discussed in several fields of science, especially in human behaviour studies, however, when the studies need to link human and their interaction with digitally connected and shared systems used in support to aircraft operations and air navigation services provision, the literature is still poor.

Open interviews were conducted with members of the aviation community and the new entrants that although not directly working with the aviation industry operations are providing services in support of it. It was clear that the reason for the lack of profound literature on the subject is the lack of interest due to the wrong impression on the size of the industry. In addition, it can be mentioned the lack of knowledge on how the aviation ecosystem would behave in a digitally connected environment when sharing safety critical information through a system where digital identity could not be physically verified.

Another reason for the lack of detailed literature on the subject of digital trust and resilience in aviation was identified as the fact that most of the information on the subject is restricted in the geographic scope and covered by confidentiality protocols due to the business risks embedded in the exchange of information in a public environment.

The discussion with the experts highlighted the need of the development of global processes and procedures. All members of the aviation community can then use the processes and procedures without restriction. Only with global trust and having all members of the community following globally agreed standards, procedures and practices

it would be possible for the aviation industry to get the full benefits from digital technologies and automation without jeopardizing agreed levels of safety.

The decision to use a qualitative approach to data collection was supported by the interviewees. Unstructured interviews, in support of the development of a proposal for operations to be pursued by the aviation community, allowing the introduction and connection of digital technologies without jeopardizing safety of operations was mentioned by all interviewees as the correct approach. This approach was fully supported considering that the interviews would also subsequently lead to the opening of possibilities for development of use cases. Use cases would then demonstrate how the different stakeholders would be impacted by a common and global trust framework in support of automation and virtual connection of different systems for exchange of safety and non-safety critical data and information in and between ground-ground, air-ground and air-air systems.

However, the resource of interviews is not free of criticism. There are positive aspects such as the advantage of the possibility of being controlled by the researcher guiding the interviews towards the needs. But also disadvantages, such as mentioned by Creswell (2014) [38] where it is highlighted the fact that the presence of the interviewer can influence the content of the responses that should be unaffected in the sense of translating completely only the view of the interviewee and not be impacted by the relationship between interviewer and interviewee.

This influence of the interviewer in the results of the research compared against the validity and the generalization of the results are aspects that need to be considered [59]. As such, it was important to adopt a method of interview that would allow and incentivize the interviewee to speak freely and express what his/her expert point of view really sees and not what the interviewer wants to listen.

Regarding the type of interview to be used, there was an initial doubt if the interview should be individual or in groups or both. Considering the different points of view and sometimes the bias depending on the type of industry where the interviewee was involved with, and to avoid debates between different stakeholders with different biases it was decided to perform individual interviews to allow the interviewees to express freely and individually what was their vision on the subject.

This approach of oral interviews is seen as having an advantage over the questionnaires as reflected by Saunders et al. (2015) [59] as the interviewees prefer to speak than fill questionnaires considering the facility to think about the subject and express orally without the need to put on paper the specific thoughts.

In summary, the methodology used for the development of the proposal to reduce the cyber-attack surface and increase the resilience of the aviation system operating in a highly connected environment and as such guarantee the continuity of operations at the same time it meets the agreed levels of safety can be simplified as shown in Figure 13.

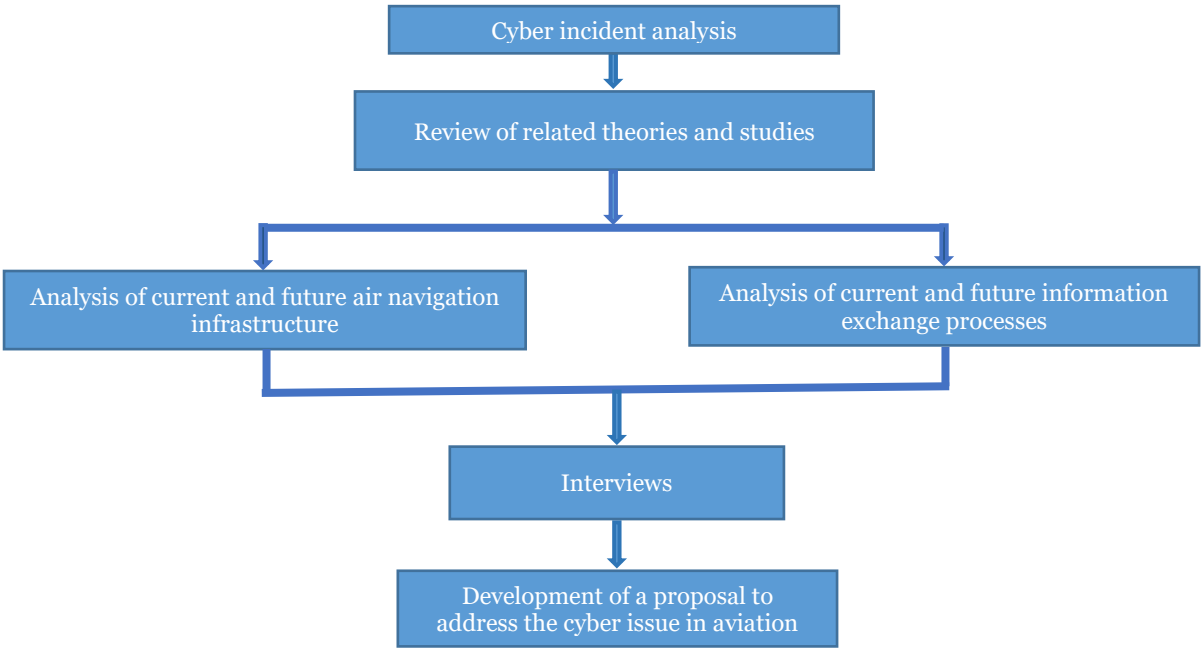

Figure 13 - Methodology used in the research. Source: Own development.

Chapter 4

Data collection

4.1 Introduction

The present chapter intends to describe the results achieved with the data collection made through interviews realized with forty-five experts from the aviation and non-aviation industry to provide views on what, when and how the industry should evolve to meet the expectations of the aviation community in a highly connected environment and the challenges associated to that evolution.

The primary method used to collect data to support the research was through unstructured interviews. This option was taken considering the novelty involved in the subject of the research and the lack of literature dedicated to it, besides the lack of global, regional or local agreements on the best option to tackle the threats faced by the aviation community while it evolves into a hyper connected environment.

According to Given (2008), if a qualitative research is to be pursued it is recommended that open questions should be prioritized considering that open questions would give the necessary freedom to the participants to voice freely their views on the subject of interest.

In this qualitative research, the use of interviews based on open-ended questions were the fundamental approach taken for data collection. According to Godoy (1995) [60] qualitative researchers do not start from pre-established hypothesis, and do not worry to find data or evidences that confirm or deny these assumptions. Qualitative researchers start from questions or points of generic interest that are explored further and become more focused and specific throughout the research. The abstractions are built from data in a bottom-up approach. The researcher taking a qualitative approach when planning to develop a theory, he/she builds a theoretical picture step by step as the data are collected and analyzed.

The exploratory research has the capability to develop, clarify and/or modify concepts improving ideas and discovering intuitions. Besides, it allows the researcher the flexibility to develop what was planned.

During the exploratory research, analysis of current and future needs of the aviation system were explored as well as recent cyber incidents and related theory and studies were reviewed.

The following table 4, adapted from Arantes (2017) [61] served as guidance on the collection, analysis and validation of the data gathered from the interviews.

Table 4 - Detailed tasks regarding data collection and report generation. Source: Adapted from [61]

Preliminary procedures	
Protocol for data collection	Used to guide the procedures used for data collection since the selection of the experts to be interviewed and first contact with the interviewees including the commitment with the confidentiality of the interview.
Means of research control	The research control was made following three processes for validation: validation of the main goals of the research through brainstorming debate with specific experts on the model and subject of the research; reliability of the research debating with specific experts the researcher's background and current activities; and establishment of a database.
Pilot test of the procedures for interview	The test was performed interviewing three different experts from three different organizations and level of technical/management involvement. The protocol for data collection was used and polished further.
Verification of data quality	The data collected during the pilot test were treated and analyzed aiming to verify if the quick-off and follow-up questions were appropriate, and the protocol was valid.

Adjustments as necessary	The protocol for data collection was slightly adjusted. This step was also important to guide the researcher on the research and study of different technical sources of information available in the aviation and non-aviation industry, especially the ones from the bank industry, which is considered well advanced in development and maintenance of a trust framework for financial transactions.
Data collection	
Contact the experts	All the experts were contacted via email or phone with a request to participate in the data collection process with an introduction on the objectives of the research and the interview and assuring the confidentiality of the process.
Data registry	The data collected during the interviews were recorded and transformed into written text to facilitate the identification of the main subjects to be further explored.
Data analysis	
Data selection and coding	The text generated by the interviews was analyzed and coded according to the main content expressed and for definition of the data registries.
Database organization	The data collected and coded were organized in an Excel spreadsheet for further analysis.
Cross analysis between different sources	Data obtained through interviews were cross-checked with the references analysed for the theoretical foundation and support to the analysis.

Production of descriptive text	The text produced relates to the data collected through the interviews and the information reviewed from the sources available.
Report production	
Definition of the scope of the issues faced by the aviation community	The analysis of the references and the results of the interviews allowed a clear definition of the scope of the issues and the achievement of the general and specific objectives of the research.
Formulation of a proposal	The data collected through the interviews were related to the references and served as the basis for the formulation of a possible solution.
Validation	The text produced was distributed to the participants of the interview process for verification of the accuracy of their views and the proposed solution by the researcher.

4.2 The interviews

To allow the participants to provide oriented point of views in the data collection for the development of this research through unstructured interviews, the same open-ended question was made to all of them. The goal of the question was to get from the participants their independent views embedded in their thoughts and based purely on their knowledge, experience and expertise in the areas of interest for the research and in such a way that could be easily understood.

Later in the process of treating the information received during the interviews, the researcher selected the most mentioned subjects by the interviewees and classified them as registry units that would support the development of a proposal regarding safe air operations in a digitally connected aviation ecosystem.

To allow the interviewees to be fully at ease with the interview, it was affirmed to them that the interview was only for data collection, a proposal for future developments related to aviation evolution and that all information being collected would be treated as confidential and no reference would be made to any names in the final text.

The unstructured interviews, as part of the research method, was useful considering that the selected experts to be interviewed were particularly articulated individuals.

The freedom given to the interviewees to take the interview through their own path allowed them to provide insights to the subject in study that a more structured interview with pre-established questions or the use of closed questions would not have allowed.

Considering the reduced number of aviation and non-aviation experts involved in the evolution of the aviation system and specifically addressing the need for measures to protect the aviation industry and make it resilient against cyber-attacks, the number of experts interviewed represented a high percentage of the existing expertise in the field.

The several experts interviewed came from aircraft manufacturing, communication service providers, security, airport and aircraft operations, air navigation services providers, air traffic management, aircraft and electronic systems maintenance, researchers from academia and others directly or indirectly involved in research and regulation development regarding technology, processes and procedures to improve the efficiency, safety and security of the aviation system.

Table 5 below shows the area and level of involvement of the interviewees in the aviation ecosystem as well as the order which the interviews were taken to improve consistency in the data collection.

In the table 5 below the area of expertise must be understood as follows:

Original Equipment Manufacturer: professionals working in development and production of new aircraft and avionic systems.

Industry developer: professionals dedicated to the development of new technologies or concept of operations to be used by the aviation industry.

Industry provider: professionals producing equipment to be used by the aviation industry.

Service provider: professionals directly involved in the provision of communication or air navigation services in support of aircraft operations.

Global organization: professionals involved in global discussions associated to aviation development and resilience.

National regulator: professionals involved in the development, application and oversight of the State regulatory framework.

Regional regulator: professionals involved in the development and application of regional regulatory framework.

International regulator: professionals involved in the development, application and oversight of the international regulatory framework.

International association: professionals representing the voice of specific groups of interest.

Research and development: professionals from industry, development programmes or academia involved in research of aviation evolutions.

Table 5 - Interviews sequence, area of work and expertise level. Source: Own development.

Interviewee order	Area	Level
1	Original Equipment Manufacturer (OEM)	Management
2	Original Equipment Manufacturer (OEM)	Management
3	Original Equipment Manufacturer (OEM)	Management
4	Original Equipment Manufacturer (OEM)	Technical
5	Original Equipment Manufacturer (OEM)	Technical
6	Original Equipment Manufacturer (OEM)	Technical
7	Original Equipment Manufacturer (OEM)	Technical
8	Original Equipment Manufacturer (OEM)	Technical
9	Industry Developer	Management
10	Industry Provider	Management

11	Industry Provider	Management
12	Industry Provider	Management
13	Industry Provider	Management
14	Industry Provider	Technical
15	Industry Provider	Technical
16	Industry Provider	Technical
17	Industry Provider	Technical
18	Service Provider	Management
19	Service Provider	Technical
20	Service Provider	Technical
21	Service Provider	Technical
22	Service Provider	Technical
23	Global Organization	Management
24	Global Organization	Management
25	National Regulator	Technical
26	National Regulator	Technical
27	National Regulator	Technical
28	National Regulator	Technical
29	National Regulator	Technical
30	National Regulator	Technical

31	Regional Regulator	Management
32	Regional Regulator	Technical
33	Regional Regulator	Technical
34	International Regulator	Management
35	International Regulator	Technical
36	International Regulator	Technical
37	International Regulator	Technical
38	International Regulator	Technical
39	International Association	Management
40	International Association	Management
41	International Association	Technical
42	International Association	Technical
43	International Association	Technical
44	Research and Development	Management
45	Research and Development	Technical

The kick-of question to all of them was the same to allow them to provide views on the same or at least close related subject. The question was:

> How do you see the evolution of the aviation industry as a system, and which are the issues related to safety and continuity of operations in a digitally connected environment?

The interviews had an average duration of 52 minutes and most of them could continuously progress without any further question to the interviewee, however, when a new incentive was necessary to get more information, an additional question was made to refresh the conversation and get more information when the researcher realized that the interviewee had more to offer. The question was the following:

> Do you think that the use of technologies associated to the Internet can bring clean benefits to the aviation industry?

4.3 The registry units

4.3.1 Trust

During the interviews and in different sources used for the research, one of the main subjects highlighted by a great majority of the interviewees, among others, was the understanding of trust in a digitally connected environment and its significance for the aviation industry.

Along the years, despite the different definitions of trust in the literature that was directly influenced by the different authors experience and the relationship with their personal projects, it is recognized that trust brings with it common characteristics or parameters when thinking exclusively about what entails trust.

Trust can be seen initially as a form of faith in other's actions that are dependent on the responsibilities of the other. If considered in an environment of uncertainty and imperfect knowledge, trust is seen as a form of belief.

Trust can also be seen as a replacement for other forms of mechanisms such as a formal contract that exists in modern societies. If trust is seen as a simplified mechanism, it can be used to reduce the complexities associated to the communication between different parties.

Trust, when established on the top of a solid foundation, is considered a precondition for the achievement of a stable society. If seen from a social perspective, trust is the mechanism that allows positive social outcomes to the participants of a society or social group.

Some authors and sociologists of the past considered that the transformation of premodern societies was directly related to the changes in the nature of trust.

In the current literature and research programs, sociologists examine trust through a series of questions. These questions are associated to what kinds of trust are able to enhance government attitudes, how relationships are affected by the culture and differences between populations that affect trust and how trust is affected by interpersonal dynamics.

There are some studies conducted by social structures that focus their research in verifying the social values of trust and looking for answer to the question on whom can be trusted.

Studies of social values and political structures frequently examine the question of whom we trust. This is considered an important aspect of the functioning of a society that is founded in imperfect knowledge and the absence of perfect mechanisms that allow individuals to verify the grounds of most knowledge or the veracity of all truth claims that could paralyze the normal activities in a social context.

However, trust is not only seen from a social perspective or a personality trait. Sciences such as economics also discuss trust as a mechanism for exchange. Political sciences investigate the impacts of trust in different types of democratic, autocratic or dictatorial governance.

Issues of trust are particularly relevant for the aviation community and the first attempt to bring the aviation industry to a common ground on trust is seen as the signature of the Chicago Convention by different States. The Convention established the minimum grounds by which aviation could operate internationally and following similar degrees of safety, security, efficiency and interoperability in different geopolitical environments with the aim of uniting peoples of the world.

With the technological evolution of processes and procedures to provide services to the aviation community and considering the technology onboard aircraft and used for ground-ground and air-ground and more recently to air-air communications, the need for a redefinition of trust in an aviation context became necessary.

Trust in an aviation context is the willingness of participants in a trust framework to rely on a specific other, which can be of human or technological system nature based on confidence that one's trust will lead to positive outcomes. It is the firm belief that the data and information being stored and exchanged is reliable, validated, and not modified while in transit and at rest.

Complex mechanisms and sometimes agreements on possible sanctions must be put in place in modern societies aiming the protection against exploitation and opportunism if

trust is nor present in daily and crucial activities realized for the common good. In the aviation community, however, the absence of trust would represent a cost that could jeopardize the business of the aviation industry and, most importantly, the agreed levels of safety that is a crucial factor in the good reputation of this mode of transportation.

An important factor to be analyzed and that characterizes trust is its fragility that allows it to be broken at any time. This can be confirmed by the societies' different structures that are in place to operate simply due to the reduced trust present in all communities. Structures such as police, surveillance, and the requirements for different types of certification can be seen as some examples. In the current socio-political scenario, the decline in the solidarity and cooperation processes that leads to consensus are seen as a consequence of the reduction in trust between different communities of interest and can also be seen as the reason for conflicts that should not otherwise exist between nations.

The changes that the society is going through nowadays with a plethora of new ways of communication and expression of feelings represented by social media can also be attributed to the changes in the dynamics of trust where individuals are forced to put their trust in automated or virtual systems and sometimes institutions.

In the aviation ecosystem, these institutions are numerous varying from air navigation and communication service providers, airlines and airport operators and different regulators besides the users of the system.

With the data obtained from the interviews, a definition of main subjects to be explored further in the development of the proposal, such as trust, were defined and became registry units.

Based on the number of times the interviewees mentioned trust as paramount to the evolution of the aviation industry in a digitally connected environment, this subject was defined as one registry unit. A registry unit here is defined as a subject that need to be further explored to allow aviation to evolve in a digitally connected environment.

The interviews also highlighted the need to address other subjects that were considered crucial for the evolution of the aviation system, and they are also considered registry units in this research. Besides trust, the main registry units derived from the interviews can be listed as relating to interoperability of systems, network resilience and safety of operations.

4.3.2 Interoperability of systems

During the interviews and from the secondary sources used, interoperability was defined as the capability of electronic systems to execute similar functions and communicate with other related systems or devices without any extra efforts from the end users. Among some functions it was mentioned the capability of different systems to exchange data that can be used by different applications without reduction in the accuracy of results, or the need of extra applications to interpret and reformat data before use independently from its origin.

The interviews also highlighted the fact that interoperability can be seen from different perspectives such as syntactic interoperability as the ability of systems to exchange information through compatible formats and protocols.

Another characteristic of interoperability highlighted by the experts in the interviews was the semantic interoperability, which is the inherent ability of systems to interpret automatically with high level of accuracy the data and or information being exchanged. The achievement of semantic interoperability is dependent upon the processes and protocols used for codification of data and information before its transmission to a different system and through different means.

When it comes to interoperability across different organizations, the interviews highlighted that this type of interoperability relates to the different requirements, policies and practices used by different organizational systems. More than simply technical devices or systems for data exchange, cross organization interoperability depend on non-technical aspects of the organization.

It was consensus among the different experts interviewed that for the growth of modern operations within the aviation industry exchange of accurate and timely data and information appears as a crucial requirement. This requirement puts pressure on the developers of systems and service providers to make available mechanisms for interoperability assurance such as compatibility tests and the use of systems and devices that follow the same standards.

Despite the recognition of all experts interviewed that the technology used is foundational for the interoperability aspects when connecting systems, other important factors to be considered were also highlighted. Among these factors and considered a hard and crucial aspect that directly affects interoperability and needs sometimes to be overcome

is culture. The aspects related to financial gain and losses by the organization influences interoperability. At the organization's level, the regulations and laws that represents the governance model has also influences in the decisions that affects interoperability.

The interviews highlighted that while some factors can be changed to facilitate interoperability, others, due to its difficult or high changing cost must be adhered to regardless the impact. The interviews with the experts led this researcher to conclude that once all aspects are considered, the one that can be seen as the most flexible is the technology to be used, however, it is recognized that the choice of technology is quite often the point by which most organizations start their projects. All experts interviewed highlighted that the registry unit of interoperability was crucial to the aviation industry.

Different experts also explored cross-domain interoperability during the interviews. It was highlighted that the existence of new information and social domains today that did not exist in previous decades, created by the information revolution being experienced by the society, are having an impact in social interactions. The presence of different types of social media and networks in the daily life of all citizens are creating the possibility of vast exchange of data and information and acting as contributing factors to the creation of new social domains that exist only in the cyber space.

According to Singer and Friedman (2013) [62] due to the appearance of new social domains, the cyber and physical worlds are united and the gaps between them were covered by the possibility of using information as the glue or the bridge between both. For the aviation industry, the domains transformation and cross-domain interferences are being accelerated due to the high speed that information and data are being exchanged and used by different stakeholders. The physical and the cyber world are under constant overlap, and this provides the opportunity by the different domains to combine and generate new domains aiming the achievement of changing objectives.

For the aviation industry, considering its international characteristics, there is a need to exchange data and information that may belong to multiple domains under the control of different stakeholders that can be separated by different boundaries such as physical, technical, political or legal.

Being a broad industry, aviation has multiple subsets within the different domains such as airports, air navigation service providers, maintenance organizations, regulators or even a single type of aircraft, among others that are emerging as function of new platforms aiming to make use of an airspace and ground before populated only by regular and very

regulated stakeholders. The interviews made clear that to make aviation a sustainable business, it is necessary the introduction and use of emerging technologies and different systems that support the functions executed by the domains and their components.

To improve their decision-making process, organizations highlight that it is necessary to use information being provided by different domains. The existence and availability of different types of information are crucial for the definition of well sounded decisions. In addition, recognizing aviation as being composed of domains that overlap to provide essential functions and are shifting and morphing at an increasing pace, a system designed for a single function is considered almost a failure and that's why the aviation domains and systems are being modified to support other domains or scrapped to make way for a replacement system. Moreover, in this evolving ecosystem the experts highlighted the need for taking a wider perspective that achieves cross-domain interoperability.

During the interviews and considering the aviation context, cross-domain interoperability was seen as the capability that allows organizations and systems to interact for provision of services and exchange of information that support cross-boundary operations. With the presence of cross-domain interoperability, the differences in the technology or the frameworks used to connect systems see their impact reduced in the operation as a whole and becomes transparent to end users.

In the aviation ecosystem, the coordination to the exchange of information in a crisis where all participants cooperate to the achievement of the high objectives of the system can be seen as an example of cross-domain interoperability. This can be achieved allowing different stakeholders to collect, process and make available critical information in a common information system where all stakeholders can access to support the final goals of the mission to be accomplished.

It was consensus among the experts that systems and procedures need an inherent interoperable framework to extend value throughout the entire aviation ecosystem and achieve the expected resilience that would at the end affect the levels of safety. The importance of cross-domain interoperability is emphasized with the changing nature of the domains that are used by different stakeholders and systems that, quite often, are not under their control but they have to interoperate with.

4.3.3 Network resilience

The way systems in particular and societies in general are now connected was raised as part of the modern challenges associated to the provision of a resilient system as a whole.

It was observed during the interviews and recognized by Confort, Boin and Demchack (2010) [63] that crises are difficult to manage.

The interviews demonstrated that due to increasing difficulties in solving the problems associated to connectivity, from a network perspective, three trends could be noted. First, it can be seen that threats are not limited to local or national boundaries. The range of these threats increased and the lack of physical boundaries in the cyber space allow the existence of contingencies that can jeopardize the normal functioning of a society independently of where it is located. In addition, network connectivity made societies to become more vulnerable to digital threats that can affect the physical world and not only the cyber world. Finally, the political instability in many parts of the world created a climate that limits the capability of local leaders to deal with crises. These three trends enable the appearance of a storm of events that can stop functioning of governments and global systems with unforeseen consequences.

States providing the infrastructure for the aviation industry to perform its functions in support of the development of modern societies have always confronted crises and disasters, some of them tend to visit in known guises and follow familiar disruptive or destructive patterns.

The characteristic of cyber threats that disregard local or national boundaries makes this type of threat considerably different from the traditional ones. States can experience now a higher number and impact of potential threats that can affect its normal functions considering that the reach of the threats extended as well as their capacity to generate potential situation of large destructions. This increase in range and the capacity of destruction of cyber threats are creating an environment that makes almost impossible for local or national authorities to deal with the crises in isolation and without global cooperation.

Global socio-political and economic organizations are showing that modern States have become tightly linked economically, politically, and socially. As remarked by Friedman (2005) [64], people, goods, and services now cross borders with relative ease. This facility and common pathways followed by goods and people creates also the possibilities for the risks to move across borders. What was before considered a distant local or foreign problem, due to the connectivity between people and systems can now easily make a State susceptible to the same consequences of a distant event.

The borderless characteristic of the cyber space allows a local crisis to transform into a crisis for an entire region or continent. Besides, the shape and form of threats change as

they move from one system to another creating difficulty for its detection and resolution. According to Turner (1978) [65] a glitch in one system can cross over to other systems, snowballing and cascading into a much bigger crisis.

During the interviews, it was highlighted that the necessary integration is one force to blame, mindful that critical systems have become tightly coupled as the result of increasing cooperation. Supporting systems that sustain basic societal functions such as transport networks are no longer confined to national borders, nor do they operate independently.

Modern societies have also become more complex, and a good example was mentioned as the relationship between Internet and infrastructure as the Internet relies on energy grids to power it; at the same time, energy grid controls are accessed by the Internet.

The experts also highlighted that there is some positive aspects in all this global relationship that is affecting the aviation sector. It is recognized that in the aviation sector the increased use of digital technology improved the supporting infrastructure and aviation supporting systems bringing modernizations not possible before. The same systems helped to improve the capacity of the system as a whole to deal with unexpected events. This evolution resulted in the situation that serious operational contingencies, no longer pose a real threat to modern aviation industry, however, one subject also highlighted was the discussion whether the increased capacity to deal with modern contingencies is sufficient to offset their potential damage.

As it is impossible to prevent or foresee every event or have a system that can be one hundred percent secure against the same events, experts agree that the aviation sector will have to face one eventually. The capacity of the aviation industry to absorb these events and to emerge from them with their core functions intact is identified as the core of network resilience.

4.3.4 Safety

Embedded in the evolution of the aviation industry it is always the goal that levels of safety are maintained or improved. This can only be achieved with procedures for safety management in place considering that safety management seeks to proactively mitigate safety risks before they result in aviation accidents, incidents [66] and more recently, denial of services.

Through the implementation of safety management procedures, a more integrative and structured way to address safety activities can be achieved. The optimum results in terms of aviation safety can be achieved through the prioritization of actions to address risks generated by clearly identified hazards. This anticipated identification also helps the community to manage more effectively the available resources.

In general, during the interviews, experts highlighted that there are many benefits to implementing safety management related to operations in the cyber space, including a strengthened safety culture by making visible the commitment of managers and actively involving personnel in the management of safety risk.

In addition, it was highlighted that as a help to distinct organizations on the optimization of resources for the implementation of changes, a clear definition of a system performance baseline allows better control of changes that may have impacts in systems safety.

Enhanced early detection of cyber threats and hazards is a relatively new subject for the aviation industry. It can improve the ability to detect emerging issues, which can prevent cyber events that can bring the aviation industry to a halt.

Another important aspect highlighted was the fact that a safety management system could demonstrate how management supports and enables safety, how cyber risks are identified and managed, and how safety performance is continually improved, resulting in increased confidence by the aviation community.

Safety has been treated as paramount for the aviation industry having the support of all stakeholders considering the safety of lives involved. However, experts also highlighted that due to the high levels of safety practiced nowadays by the aviation industry and the challenges being presented, safety needs also to consider possible financial savings. As an example, the interviews highlighted the fact that in the current economic environment, safety management applied to cyber threats can allow service providers and airspace users to qualify for a discount on their insurance premiums.

Through a proactive identification of cyber threats and hazards, the cost incurred due to accidents, incidents and denial of services can be avoided. In such cases, direct and indirect costs such as property damage, software and hardware recover, schedule delays,

legal actions or even worse, loss of business and damaged reputation can be anticipated and avoided or at least reduced their probabilities and effects.

As described above, four main registry units were identified and explored in this research as the basis for the proposed solution that will be described later: trust, interoperability, resilience and safety.

4.4 Data sources

Before starting the interviews for primary data collection, a review of related references was made to serve as the basis for acquisition of extra knowledge on the impacts related to evolving digital systems towards a hyper connected environment.

The references were selected from security and safety related publications as well as technical Internet related provisions. These references were reviewed to guarantee that the interviews could be progressed and interpreted in the way to cover the subjects relevant to a digitally connected aviation ecosystem.

After the review of the references used as secondary sources, the interviews were set and preliminary interviews with selected experts were made for validation purposes. These experts were selected from different levels of management and technical areas with the goal to have different points of view that could support or contradict initial assumptions that would need to be revisited.

Two different groups were interviewed for primary data collection. The first group was composed of experts in management position in their respective areas of activity related to aviation. The second group was composed of different experts in active research or technical positions in different areas of aviation ranging from aircraft operations and maintenance, air navigation and communication service providers, airport operations, airspace law specialists, and security experts with national and international experience and views.

The data collection with the experts was made through exploratory discussions and unstructured interviews and face-to-face and virtual meetings using the tools available in the market such as Zoom, Skype for Business, Microsoft Teams, GoTo Meeting or simply by phone.

The data collection followed the guidance of Yin (2011) [67] that recommends the researcher to use the principles of multiple sources: to complement and validate evidences; to establish a database; and to order thematically the evidences.

The interviews are considered important in the qualitative research due to the quality of data that can be obtained as well as the opportunity it presents to go deeper in the research subjects through the interaction between the researcher and the expert being interviewed [68].

The interviews are also important considering that the interviewees can express their impressions, and mainly, they give to the researcher the opportunity to get what was not said, but was left, sometimes intentionally, hidden in the speech.

4.5 Data analysis

The data collected can only make sense after the researcher analyse them through an accepted and adequate technique. In addition, this analysis should cover the data collected from published references as well as the ones collected in the field through the interviews.

The method of content analysis was chosen considering that it is seen as a classical procedure to analyse textual references, without importance from the source of the material [69], allowing concomitantly the understanding of the meaning of the communications, its explicit or implicit content [70].

According to Bardin (2011) [71], the content analysis is made of three steps and these steps were followed in this research - pre-analysis, review of material, and data analysis inference and interpretation - following the schema described in table 6 below.

Table 6 - Steps followed for content analysis. Source: Adapted from [61].

First step: Pre-analysis	
First contact with the subject.	a) Reading of related existing references. b) Conversation with limited number of aviation professionals to collect views on the proposed research. c) Selection of initial references to be used as information aiming the research objectives.

Second step: Material review	
Researcher's immersion into the data for definition of codification system, registry units (main idea of text), and content unities (collected contextualized information from interviews).	a) Interviews Used the unstructured interview technique where the interviewee was left free to talk about what he/she sees relevant on the subject and recording of the interviews for further reference and analysis. b) Structured decoding Intuitive and specific structuring of each interview. c) Transversal analysis Deconstruct to reconstruct. The interview material was divided in small pieces and classified into units with context meaning. Each small piece received a code that expressed its meaning related to the research. d) Registry units It is a key word that summarizes the content in the context. e) Context units Part of interview that characterizes the information.
Third step: Data analysis and interpretation	
Thematic analysis	
a) Reconstruction of pieces of text indicating alignment and misalignment with the registry units.	Verification of the codes/groups mentioned in the interviews and its frequency. Codes here means the expressions that although not mentioning directly a registry unit can be related to one.
b) Statistics	Verification of the frequency with which the registry units were mentioned by the experts directly or indirectly according to the coding.
c) Construction of text that summarizes the subject highlighted by the experts.	Transcription by the researcher of the main ideas of the interviews.
d) Validation requested by the experts.	The text generated by the researcher was sent to the experts for validation of the understandings reinforcing the commitment with the confidentiality of the information.

Interpretation	
Association of previous assumptions obtained from the references and confronted with the data obtained from the interviews accepting or rejecting previous studies.	Verification of direct citations and composition of evidences as a function of the registry units and the main objectives of the research.

The evidences obtained from the interviews were classified in five different groups and together with the registry unit's analysis are presented in two different formats. The first presentation shows a content analysis through a network that demonstrates the interrelationship between the several aspects involved in a safe, secure and resilient aviation system related to the defined group. The second format presents a table with the number of times during the interviews where the registry units were mentioned by groups of analysis. The groups of analysis were defined by the researcher based on previous discussions and conclusions during international events that highlighted their importance as well as data collected during the interviews and of related importance based on the researcher professional experience and background.

The five different groups were defined as how politics influence the evolution of the aviation system; the positive economic impacts of interconnectivity; the need for global aviation system evolution; cultural impact in evolution; and technology use.

In this context, the first group, politics, was seen as the will of decision makers to change the status in terms of risk acceptance not before experienced by the aviation industry in relation to the community they represent.

It has been identified during the interviews that this political will can direct impact how new technologies are deployed and the level of trust among different stakeholders in its use. The way political decisions are made and how they support or not the development and deployment of new technologies enabling concept of operations will have a direct impact in the resilience of the operations and as a consequence in the levels of safety practiced by the industry.

Figure 14 below shows the results of the interview's data analysis related to the first group of analysis. The relationship was derived from the information provided by the experts during the interviews. The figure shows that other related subjects were also mentioned, however they were only considered as information but not classified as registry units due to its lower direct impact in the air operations despite its indirect influence.

The interrelationship between the different mentioned subjects other than the group being analyzed were done through analysis of the information provided during the interviews where the experts mentioned the subjects as being related.

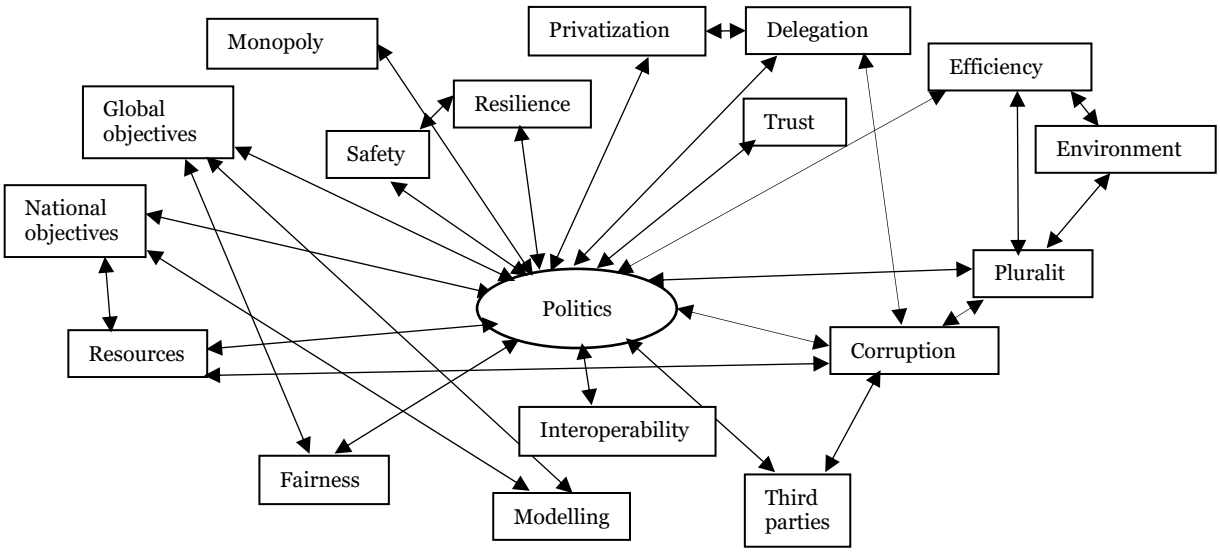

Figure 14 - Politics group analysis. Source: Own development.

Table 7 below summarizes the frequency with which the selected registry units were mentioned within the group of analysis by the experts interviewed.

Table 7 - Frequency of registry units in the first group. Source: Own development.

Group	Registry units	Total by registry	Total by group
Influence of politics in the evolution of the aviation system (Politics)	Safety	12	43
	Trust	21	
	Resilience	3	
	Interoperability	7	

Different experts made different relationships between political will and the need to develop the aviation system towards a highly connected environment that brings after it inherent advantages but also bring some new vulnerabilities that can influence performance of operations.

> "Since the beginning of the year 2000 it was realized that information management would be the most important resource to allow aviation to have a jump in terms of services quality necessary to improve efficiency of air operations. At that same time the industry realized also that for information

> management to be effective, connection between different service providers and consumers was necessary, but nobody knew if the decision makers would support this approach due to the risks associated to it." (Interviewee 6 - Safety)

Some issues related to different political interests could also affect the way aviation would approach the necessary technological evolution towards digitalization.

> "How would be the infrastructure to manage the different aspects of information management brings questions regarding State cyber sovereignty that can impact the approach to cyber security in a connected environment. The need for ICAO to be as neutral as it has been and keep all States together even when sanctions need to be made to one or a group of them to guarantee global trust in the aviation system is an important question that will have long political discussions and nuances." (Interviewee 20 - Trust)

The decision to evolve the aviation system to meet the needs of the society in general and the aviation community in particular is directly related to the capacity of the system to evolve and resist to cyber-attacks that may jeopardize safety of operations. This capability relates to the resilience of aviation infrastructure as it has been demonstrated up to now. In addition, the resilience is seen as a function of interoperable systems.

> "Aviation has demonstrated its resilience facing different crises, mainly for the fact that aviation is a factor to solve crises. What is necessary to do now is to guarantee that the necessary evolution of the aviation system does not bring other issues that will impact its resilience and as such impact safety of operations considering that at a political level safety is what matters at the same time at a technical level interoperability of systems is crucial." (Interviewee 24 - Resilience and Interoperability)

The second group relates to the positive economic impacts of interconnectivity. In the context of this research, interconnectivity is seen by the experts as a condition that needs

to be met or the aviation system may collapse for lack of capacity to accommodate different airspace users and needs economically.

Figure 15 below shows the results of the interview's data analysis related to this group and the relationship among the units was derived from the information provided by the experts during the interviews. The figure shows that other related subjects were also mentioned, however they were only considered as information but not classified as registry units due to its lower direct impact in the air operations despite its indirect influence.

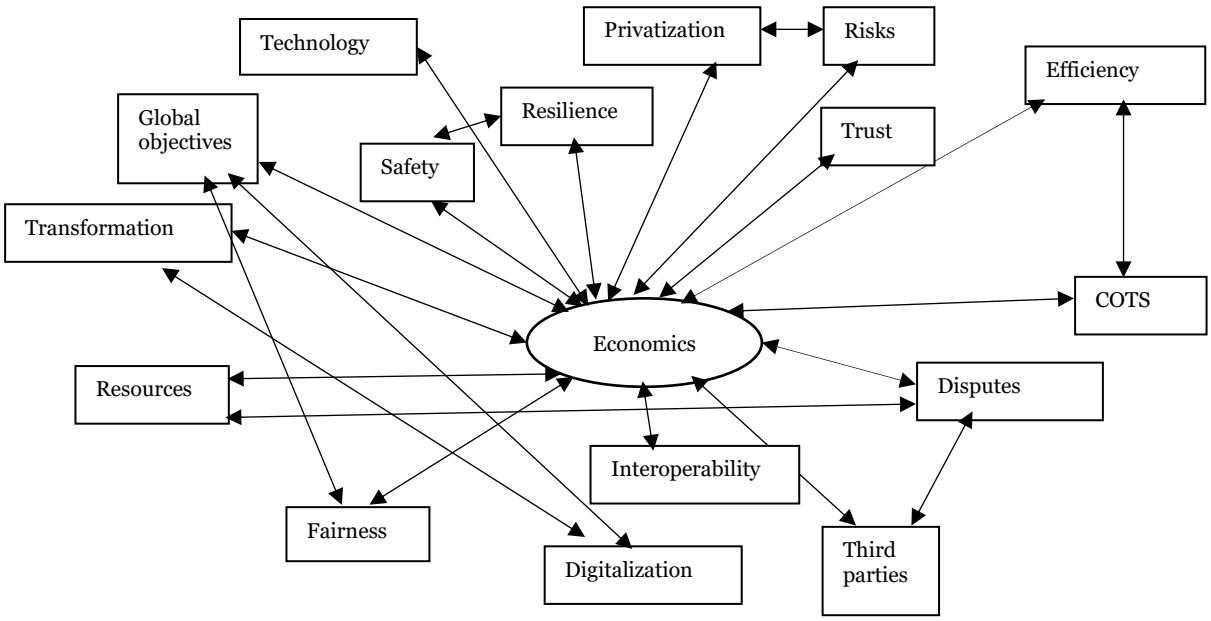

Figure 15 - Economics group analysis. Source: Own development.

Table 8 below summarizes the frequency with which the registry units were mentioned within the group of analysis by the experts interviewed.

Table 8 - Frequency of registry units in the second group. Source: Own development.

Group	Registry units	Total by registry	Total by group
Positive economic impacts of interconnectivity (Economics)	Safety	11	45
	Trust	13	
	Resilience	7	
	Interoperability	14	

Some experts highlighted that interconnectivity should not be restricted by economic factors, others agree that, without financial consideration of the evolution, technological disparities between States and regions could jeopardize interoperability and safety.

> "How the system we use today to manage air traffic would be able to support the new entrants that can reach the number of millions in the next five years is the question. If the current system, could economically accommodate the new users, the community would not need to do anything, however, the current operational restrictions point towards interconnectivity as the only technical solution for the evolution and financially viable integration of the new entrants." (Interviewee 33 - Interoperability)

Changes to the way the community deals with trust and perceives interconnectivity is crucial to shift paradigms in the current aviation system. Trust has been accepted as default by States when subscribing to the Convention on International Civil Aviation, however, the interconnectivity required nowadays if not financially viable, mainly to developing States, will jeopardize the trust built with the Convention.

> "Changes for the evolution of the aviation system as a harmonized system must occur, however, industry as users or providers, and States as regulators need to guarantee that this evolution is financially viable for all stakeholders. If interconnectivity is not financially viable not a single stakeholder would trust the way services are provided and as consequence users will not trust the system as a whole and create dedicated processes to avoid mistrust what would impact safety and resilience in the system." (Interviewee 21 - Trust)

Whatever solution is proposed to evolve the aviation system towards digital connectivity needs to be balanced to avoid bringing unsolvable or high risks related to resilience and its impacts on safety.

> "The required changes brought by globalization are pushing the aviation community towards solutions that can be globally acceptable and deployed in short term due to the pressure of the new entrants. The aviation community needs more than ever be smart to deploy solutions that will face the challenges

> associated to digitalization as a requirement for connectivity balancing these requirements with the need to keep the safety risks at a level that can be accepted by the society, and this also involves the financial viability of proposed solutions. And to satisfy the requirements of the society, internally, the aviation community needs to create a cyber resilient infrastructure, and this is seen as a major challenge considering the old thoughts still remaining in the community that every single State or regulator needs to have full control of the whole operations, what in a digitally connected environment is not possible." (Interviewee 31 - Safety and Resilience)

The third group relates to the need for global aviation system evolution. All the experts interviewed were unanimous affirming that the current status of aviation technology and regulatory framework need to evolve to meet the needs of current and future aviation demands.

Since 1944 with the advent of the Chicago Convention, the aviation industry has been developing based on concepts and technologies that despite increased evolutions that served very well the industry purposes up to now, are becoming obsolete due to the need to meet requirements not before foreseen. Unmanned aircraft systems, space operations are among the ones requesting support from the aviation industry and regulators due to the differences in operations when compared to traditional manned aviation. Moreover, this evolution needs global harmonization or hazards will be created that may generate risks incompatible with the ones that can be accepted by the society in general and the aviation community in particular.

Figure 16 below shows the results of the interview's data analysis related to the third group. The relationship was derived from the information provided by the experts during the interviews and the figure shows that other related subjects were also mentioned; however, they were only considered as information but not classified as registry units due to its lower direct impact in the air operations despite its indirect influence.

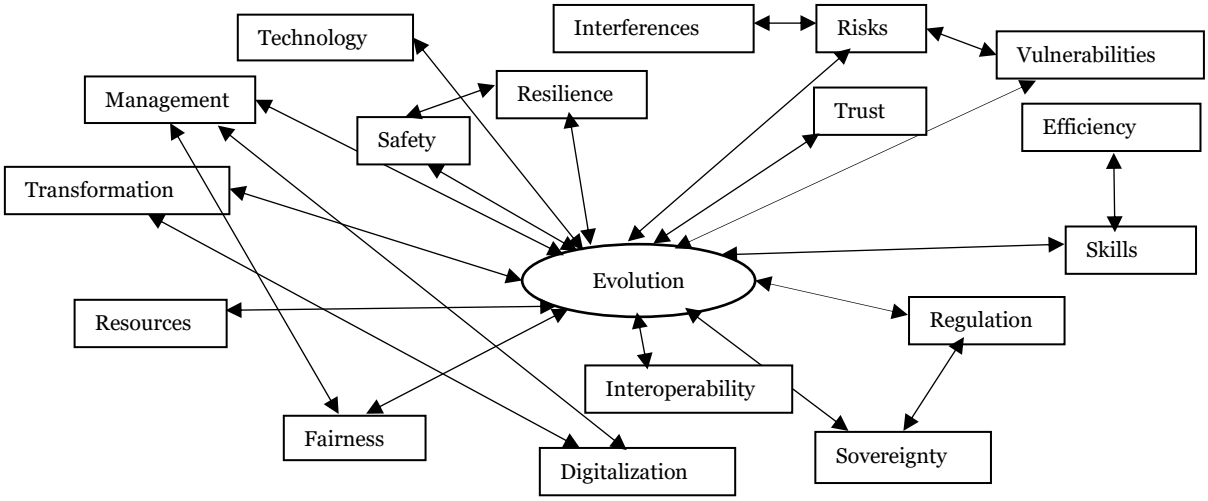

Figure 16 - Evolution group analysis. Source: Own development.

Table 9 below summarizes the frequency with which the registry units were mentioned within the group of analysis by the experts interviewed.

Table 9 - Frequency of registry units in the third group. Source: Own development.

Group	Registry units	Total by registry	Total by group
Global aviation system evolution (Evolution)	Safety	15	43
	Trust	11	
	Resilience	10	
	Interoperability	7	

Despite the fact that the aviation system needs to evolve to meet the expectations and mission needs of different stakeholders, mainly the ones operating new flying platforms, the interviews highlighted the challenges associated to evolution versus keeping the safety risks at the agreed levels. One of the issues highlighted by the experts is that the current agreed levels of safety never considered the new flying platforms, and it is necessary a new evaluation and verification of the risk appetite of the society considering the new aviation landscape compared to the past century.

> "What the aviation community needs to analyze and decide is if we are going to continue to operate with the same level of safety when only traditional manned aviation was operating or if we need to adjust the society expectations with the introduction of new flying platforms. Obviously, what we are pursuing is to maintain or increase the levels of safety, but the diversity of the environment where the

> new platforms will be flying such as urban environments creates the need for a review of the agreed levels of safety or we may make these types of operation not viable." (Interviewee 45 - Safety)

One of the expectations of the aviation community is that despite the challenges associated to the use of new technologies, the level of safety is maintained and/or improved. This maintenance or improvement of safety levels is directly dependent on the resilience of the system to unlawful or unintentional interferences.

> "The evolution of the aviation system passes necessarily through the need to improve the way information is exchanged. The problem is that these new ways to exchange information will not be effective without a high level of connectivity and consequently, a domino effect becomes a risk in the communication system, at the same time it can be used to improve the resilience of the operations. This balance is where the community should focus the attention to guarantee that evolution happens in a harmonized and safe way." (Interviewee 2 – Resilience)

In a digitally connected environment, where due to the volume of information exchanged and the geographical location of providers and consumers of services, face-to-face relationships barely happen, the degree of trust among different stakeholders rises as a crucial requirement for any type of evolution.

> "How can we trust people that we don't see, we don't know and sometimes we don't even know if they are who they say they are and what the qualifications they have to provide a service that the community needs raise several questions regarding the process to guarantee identity management. Without a strong process in place for identity management, trust cannot be guaranteed in a digitally connected system as a whole." (Interviewee 29 - Trust)

In a system of systems such as aviation, the evolution and integration of each component providing different services to the community and the economic benefits for the aviation industry is highly dependent on the interoperability of the systems that together makes the sky seamless.

> "What all the aviation community stakeholders need to have in mind is that the technological evolution of aviation systems will not work if it creates disparities between States and regions. Isolated evolutions will create differences in levels of development, and this will create interoperability issues that may make aviation to take backward steps instead of forward towards meeting expectations. The democracy in the evolution if we want to guarantee interoperability must be pursued by the community or face risks that will jeopardize safety and resilience." (Interviewee 27 - Interoperability)

The fourth group relates to the cultural impact in the evolution of the aviation system. All the experts interviewed highlighted that one of the most challenging aspects of the evolution of the aviation system is the necessary change in some cultural aspects developed since the first commercial airplane took-off. Commercial aviation was born and developed based in cultural aspects that heavily influenced how the aviation system is shaped today. Isolation of systems, local protection avoiding domino effects, heavy sovereignty values as outlined in the first article of the Chicago Convention, the need to see or directly talk to verify identity, are among some aspects that helped to shape aviation as we know it today.

The evolution of today's systems, besides requiring heavy technology investments, also demands some cultural changes to allow the introduction of new regulations and concept of operations to create an environment where all stakeholders, from users to service providers, can take advantage of what the technological evolution can offer to the whole community.

Figure 17 below shows the results of the interview's data analysis related to the fourth group. The relationship was derived from the information provided by the experts during the interviews and the figure shows that other related subjects were also mentioned; however, they were only considered as information but not classified as registry units due to its lower direct impact in the air operations despite its indirect influence.

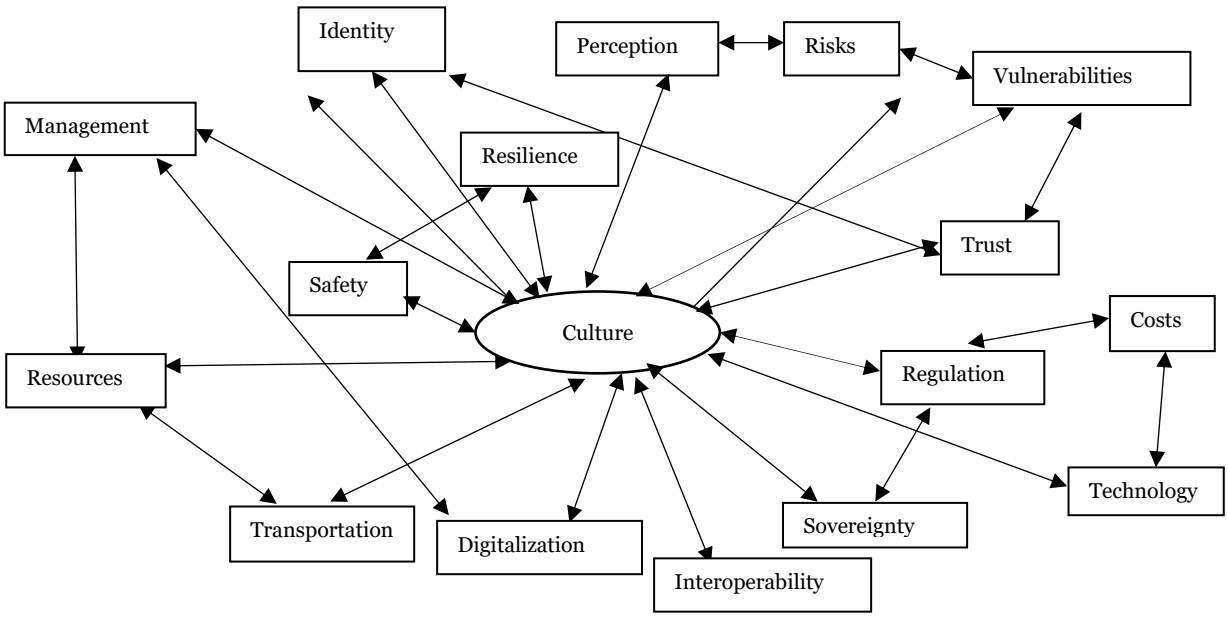

Figure 17 - Culture group analysis. Source: Own development.

Table 10 below summarizes the frequency with which the registry units were mentioned within the group of analysis by the experts interviewed.

Table 10 - Frequency of registry units in the fourth group. Own development.

Group	Registry units	Total by registry	Total by group
Cultural impact in the evolution (Culture)	Safety	16	45
	Trust	21	
	Resilience	4	
	Interoperability	4	

With the evolution of the aviation system towards a highly connected environment where transactions are made simultaneously from different places contributing to the same operation, without any sort of physical interaction such as voice communication, it demands a change in the culture in the aviation community to accept services being provided remotely and sometimes without direct human intervention or verification.

This represents a need for change in the culture of a community who grew up having full control of the services being provided and knowing immediately the sources of the information being consumed and the processes associated to the production and distribution of that information.

> "Hopefully our aviation community will understand and accept the changes that are necessary. And they

> relate not only in the technological area but mainly in the culture on how to see safety and how to accept services that are available in the cyber space and that need to be trusted despite the fact that the consumer doesn't have full control on the origin and processing of that information provided by the service." (Interviewee 34 – Safety and Trust)

Seeing culture as a social heritage of an organized community or society which is a pattern of responses that have been discovered and invented when the group has interacted, which is a combination of beliefs and customs, among other aspects, can potentially have a great impact on education and acceptance of changes in the community.

The aviation community has a wide range of culture that exists with it. This is because the community is composed of several many small communities with different cultures. However, these differences have also similarities that keep the stability of the culture that depends on how similar the community acts or behaves.

The orchestrated behaviour of the aviation community is evolving to a more choreographed behaviour where its elements act without the need of a master conductor. This behaviour guarantees that if any piece of the system fails it allows other interconnected pieces to take its place to guarantee that the system continues to perform according to the needs of the community delivering the same results with one less piece in the orchestra.

This needed behaviour change represents a big difference from the current aviation culture. These changes value the existence and need of every single piece working to allow the provision of services or contingency plans, that limit the services, are put in place with sometimes a high impact in the performance of the system due to the low level of interconnectivity between system and services.

> "What needs to be realized by the aviation community is that despite the fact that all pieces are necessary to keep the system running, the pieces may not need to be simultaneously in operation. They may not be as necessary as they think in a certain moment. Interconnectivity will allow the resilience of the system to failures of some of its components without jeopardizing the continuity of operations and the levels of safety. This represents a shift in the

> culture that all are needed all the time. As long as the interconnectivity exist and the elements interconnected can be trusted, the system will continue to perform, and the users will not be impacted. The acceptance of that new environment will request a change in the localized culture of the community to a more globalized culture." (Interviewee 25 – Resilience)

In an interconnected and choreographed system, the link between the different elements becomes a crucial condition for its work. System of systems such as aviation, and being international by definition, needs all pieces working seamlessly and this requires interoperability of all component systems and technologies. How to achieve interoperability though becomes a challenge with the diversity of developers and implementers in the aviation ecosystem. The ability of all aviation supporting systems to cooperate in the production, exchange and use of information dictates how seamless the system will be.

> "What we can see from the current developments and evolutions is still isolated pools of developments that may represent a challenge when all the systems are connected. The aviation community, mainly in the cyber area, needs to act local but think global or the evolution through new systems may bring more problems than solutions to the community as a whole." (Interviewee 37 - Interoperability)

The last, but not less important group of analysis relates to the technology use. Several companies are developing technologies for generic usage, however, quite often, the technologies need to be seen in use in a specific environment to be fully trusted and used correctly.

State, culture, and sometimes even religion have a great impact on how technology is used in different environments. Sometimes technology products fail because designers did not understand or foresee the context of usage.

With the increased use of commercial of-the-shelf technologies to develop dedicated aviation systems, the risks associated to the correct usage raises as a concern among different members of the aviation community. For some of them it is transparent, however,

for some it is crucial that the technology in use is developed or adapted to the environment it is to be inserted.

The awareness of the technology purpose and the correct training of the users to make the best use of the technology in a specific environment becomes crucial for safe and secure interconnectivity and consequently raises an important aspect to be considered in the evolution of the aviation ecosystem towards a digitally connected one.

Figure 18 below shows the results of the interview's data analysis related to the fifth and last group of analysis related to technology usage. The relationship between the different elements was derived from the information provided by the experts during the interviews and the figure shows that other related subjects were also mentioned; however, they were only considered as information but not classified as registry units due to its lower direct impact in air operations despite its indirect influence.

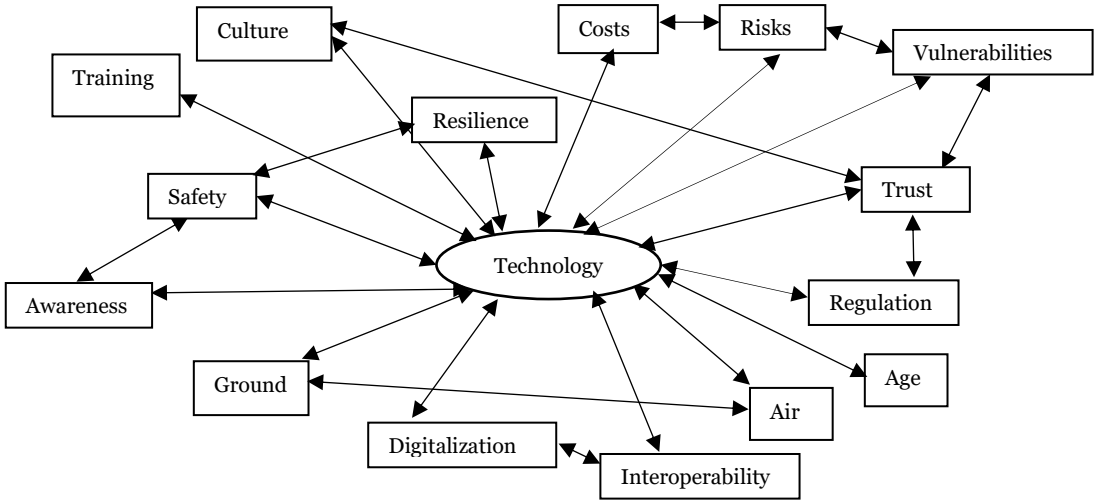

Figure 18 - Technology use group analysis. Source: Own development.

Table 11 below summarizes the frequency with which the registry units were mentioned within the group of analysis by the experts interviewed.

Table 11 - Frequency of registry units in the fifth group. Own development.

Group	Registry units	Total by registry	Total by group
Technology use (Technology)	Safety	7	43
	Trust	11	
	Resilience	2	
	Interoperability	23	

The speed with which new technologies are being developed and used by different members of the aviation community highlights the need for a harmonized approach to its deployment, besides the need for customization of some systems to meet specific aviation requirements.

The search and deployment of new systems, which can bring efficiency to aircraft operations and service provisions, generated a patchwork of systems and networks not always interoperable or following aviation established requirements, what can affect the agreed levels of safety for the aviation system as a whole.

> "Nowadays we see airlines and air navigation service providers investing in emerging technologies to improve efficiency in their operations and reduce the associated costs. The issue comes from the fact that the investments are made in an uncoordinated way. The proliferation of new technologies, not specifically developed for the aviation industry use creates pockets of vulnerabilities that can later be explored by bad actors and affect the agreed levels of safety in a way that can jeopardize the perception of the community regarding how safe is to fly." (Interviewee 14 – Safety)

In an environment where different systems are connected, it is accepted that coordination for their deployment needs to happen at local, regional or sometimes global level to ensure that the seamless connection happens, and the interoperability is guaranteed. If this coordination is not made from the start of planning for deployment the necessary investments to fix interoperability problems later can make the use of new technologies not viable from an economic or operational perspective.

> "The different stakeholders including States and service providers are always looking for the best solution for their own specific safety or efficiency problems. The issue is that isolated investments for implementation of new technologies may create gaps or overlaps in services between different airspaces or airports with direct impact in the interoperability of systems and the associated operational costs to

> international carriers." (Interviewee 35 – Interoperability)

The use of some evolving technologies is necessary to support the aviation ecosystem growth. Investments by all stakeholders show the good will of the aviation community to provide even better services for customers and airspace users, independently of their interest or mission to accomplish.

The high level of investments in emerging technologies pushes the aviation community towards digitalization and systems are able to interconnect and services provided independently from where the provider or the consumer of such services are located.

However, the lack of immediate identification of different providers or consumers, the lack of confidence in the data or information being exchanged and the capability of the providers raises a crucial question on how to trust the system without knowing who or from where the information or data is coming from and the processes associated to their production.

> "In a hyper connected environment, airspace users and sometimes service providers are providing or consuming data and information with a speed that becomes almost impossible to verify sources and quality of data. Mechanisms must be in place to allow the use of data and information with the trust that do not request verification of everything by all or the environment for message exchange becomes heavy enough to make the use of new technologies for data and information storage, processing and exchange not viable or mistrusted." (Interviewee 36 – Trust)

The aviation community accepts the fact that isolated systems do not provide the quality or the efficiency requested by the aviation system to operate seamlessly and with the levels of safety that are requested by the society. This comes from the fact that the services to be provided may use different technologies but need to follow international standards, procedures and agreements and despite their local production and use, systems will be connected and the failure of one of them should not jeopardize the performance of the system as whole.

If safety is to be guaranteed and the global performance of the system acceptable by the community, the different connected or isolated systems must be resilient to any sort of event that can make isolated systems stopping to work. In a hyper connected ecosystem, resilience raises as the most important characteristic that can impact safety of operations.

> "We are working today with so many different pieces of technology that it becomes almost impossible to control who does what. However, at the same time diversity can bring benefits depending on where the technology is used and how it is managed, it raises the need of procedures in place that allows the diversity of systems but guarantee the resilience of the aviation system as a whole if the agreed levels of safety needs to be preserved." (Interviewee 11 - Resilience)

4.6 Conclusion

This chapter aimed at showing the results of the interviews with experts from different sectors linked to aviation and non-aviation industries. The main objective of the interviews was to collect their views on how aviation must evolve to meet the expectations of the society in general and the aviation community in particular, and which are the main aspects that need to be considered and the challenges associated to this necessary evolution in a hyper connected environment.

The interviews highlighted areas categorized as groups. These groups were aligned with the secondary references used to gain knowledge and insights on the challenges expected by the aviation community in a hyper connected environment. The interviews also allowed the definition of registry units that describe the main aspects of an aviation system that intends to meet the needs of the aviation community in particular and the society in general in the 21st century and beyond.

The first group related to politics and was seen as the will of decision makers to change the status in terms of risk acceptance by the aviation industry in relation to the community they represent.

The second group related to the positive economic impacts of interconnectivity and was seen as a condition that needs to be met to avoid the collapse of the aviation system as

a whole due to the lack of capacity to accommodate different airspace users and needs in an economically viable environment.

The third group related to the need for global aviation system evolution in terms of technology use and regulatory framework that need to evolve to meet the current and future aviation demands and expectations.

The fourth group related to the cultural impact in evolution considering that aviation was born and developed based in cultural aspects that heavily influenced how the aviation system is shaped today including isolation of systems, local protection and heavy sovereignty values.

The fifth group related to the technology use and was seen as the analysis of risks associated to the correct usage of some crucial technologies not specifically developed for aviation purpose and how they perform in the environment they are inserted to.

Table 12 below provides the details on the data collection on the groups, registry units and other technical aspects highlighted during the interviews.

Table 12 - Groups and registry units identified in the interviews. Own development.

Groups	**Registry units**					**Total references by interviewees**
	Trust	Interoperability	Resilience	Safety	Others	
Politics	21	7	3	12	13	56
Economics	13	14	7	11	12	57
Evolution	11	7	10	15	13	56
Culture	21	4	4	16	12	57
Technology	11	23	2	7	11	54

Total	280	280

From the groups mentioned by the different experts, was possible to define registry units being the main aspects that need to be considered and addressed to allow the aviation industry to evolve in a connected environment and preserving the main values of the aviation community.

These registry units were defined based on the information and data gathered through the analysis of the interviews. The dialogue with the experts and the study of the secondary sources were used as the basis to develop a proposal for the evolution of the aviation system in a digitally connected environment. A proposal to address the challenges faced by the aviation community is described in the next chapter.

Chapter 5

A proposal for an international aviation trust framework

5.1 Introduction

The present chapter describes a proposal for the evolution of the infrastructure to support information exchange in a safe and secure digitally connected environment. Based on the evolutions, concepts and issues described in the previous chapters and on the discussions with the experts during the data collection phase of the research, this chapter describes a proposed global solution for the secure exchange of information within a global resilient aviation trusted system.

This evolution is necessary to allow efficiencies to be brought to the aviation industry without jeopardizing the levels of safety and resilience defined and agreed by the aviation community.

This proposal recognizes the need for evolution of the aviation industry towards a highly connected environment and addresses the specific challenges associated to it, mainly the ones derived from the possible new vulnerabilities that can result in disruptive cyber-attacks that may bring the industry to a halt at local, regional or even global level.

The World Economic Forum 2018 Global Risk Report, which identifies and analyses the most pressing global risks [72, p. 6], identifies cyber risks as one of the four key risk areas:

> "Cyber security risks are growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cyber security breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Another growing trend is the use of cyber-attacks to target

> critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."

This trend was confirmed in the World Economic Forum 2021 Global Risk Report [73, p. 7] which informs that:

> "Among the highest likelihood risks of the next ten years are extreme weather, climate action failure and human-led environmental damage; as well as digital power concentration, digital inequality and cyber security failure. Among the highest impact risks of the next decade, infectious diseases are in the top spot, followed by climate action failure and other environmental risks; as well as weapons of mass destruction, livelihood crises, debt crises and IT infrastructure breakdown."

The Allianz Global Corporate & Specialty [74] ranks business interruption (BI) as one the most important risks that can affect the normal functioning of specific systems and the society in general considering, among other aspects, the possible impacts that business interruption can have in the revenue generating activities. Industries are seeing risks growing due to the high level of connectivity and digitalization of systems supporting the different activities that keep their activities and the society at large functioning. These risks, despite not bringing, normally, the same physical damages as natural disasters or fires in installations can bring, come with high level of financial losses.

From a customer point of view, cyber incidents raise the biggest concerns considering the possibility of a cyber event to cause business interruptions that directly affects perception of safety and also the high possibility of financial losses that follows a cyber incident. The increase in the number of cyber incidents and particularly the ones that involves ransomware have the potential to disrupt operations through business interruption to large geographical areas or number of systems.

According to the information available through official media and specialized cyber reports, society is seeing an increase in cyber incidents and the possibility of attackers disrupting large numbers of companies simultaneously, like a natural disaster, is also increasing.

Besides financial losses and safety risks, another damage suffered by companies that are subject to a cyber incident is the reputational damage. The data available in the secondary sources of information for this research shows that 75% of the companies that were affected by a cyber-attack also suffered reputational damage with or without media coverage [74]. Trust among stakeholders can be destroyed if sensitive data is leaked or compromised.

It is recognized that digitalization and connectivity are transforming the lives of everyone and changing business models. This digital transformation presents several benefits to the functioning of societies, however, at the same time, experts highlights that this transformation is also making systems that support critical infrastructure such as transportation more vulnerable to cyber-attacks. The move towards digitalization of operations and supply chains as well as business transactions and associated services are contributing to this increase in the cyber threats.

The aviation community, due to its particular relationship to safety of lives, to manage efficiently and effectively service provisions, needs to be proactive in dealing with cyber threats to its critical infrastructure.

Despite aviation being operated with high levels of safety and low levels of disruptions since its first flight in the 20th century, it lives today in a different environment where cyber-attacks are aiming to disrupt business and operations through interferences to its digital and physical communications infrastructure. These attacks have different motivations, but in general, they can potentially harm the aviation industry and bring financial losses not only to the aviation industry but also to the world economy as a whole.

The same way a successful attack can damage the aviation industry, the community recognizes that even potential threats can have similar devastating effects and for this reason the community needs to act fast to avoid consequences that can jeopardize safety of operations and the trust of the society in the air transportation system.

To avoid the mistrust and guarantee or improve safety of operations, the aviation community needs to develop a system that can guarantee resilience and safety of operations under any circumstance. At the same time, the aviation industry needs to use available and developing technologies to improve its efficiency and meet the expectations of the aviation community in particular and the society in general.

To face the increasing risks associated to the use of the cyber space, this research proposes the evolution of the principles of the Chicago Convention to the 21st century

through the establishment of an international aviation trust framework. The trust framework aims to reduce the probabilities of cyber events that can bring the aviation industry to a halt or jeopardize safety of operations through tampering of safety critical information.

Two elements can be considered the core of an international aviation trust framework that would reduce the attack surface and increase resilience. These elements, made of different components, relate to a global network to exchange data and information and a system to guarantee the identity of the participants in the exchanges.

At the end of the chapter, a brief description of the envisaged full operation is provided as an attempt to put all elements together in an operational environment.

5.2 Global resilient aviation network

Exchange of information on a global basis must use connected, secure and resilient networks to allow reaching all corners of the globe with reduced cyber risks.

In this research, it is proposed a layered approach to the protection of networks, systems and applications. This layered approach aims to reduce the cyber risks to all elements of the infrastructure at the same time it allows the necessary flexibility for the definition of individual protections depending on the environment the system, network or application is operating.

Networks

The aviation ecosystem in this research proposed scenario should be formed by a number of interconnected networks operating as a single global interoperable network as illustrated in Figure 19 below.

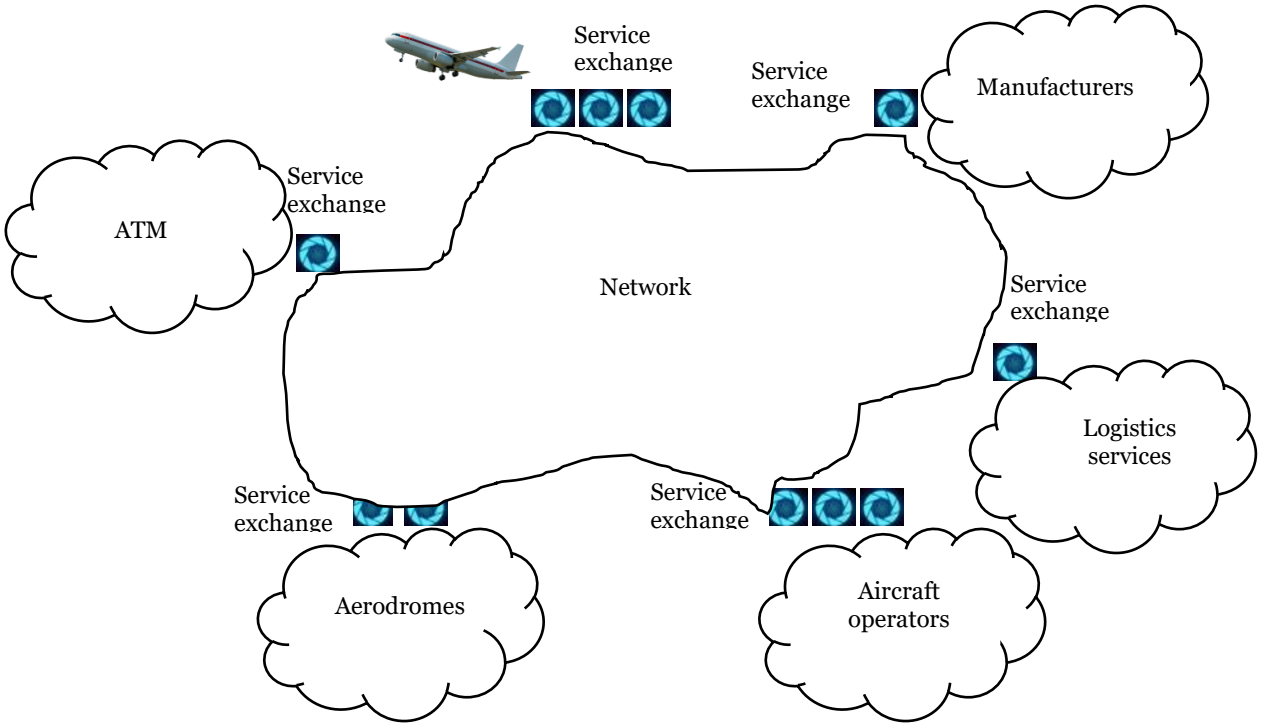

Figure 19 - The global interoperable network. Source: Own development.

The aviation community has agreed that communications infrastructure enabling the connections of different applications to support different network functions in the air navigation system should be done through the Internet protocol suite due to the low processing costs associated to this communication capability and the minimal bandwidth required [75].

In an environment where IP network service is used, the specification of the network will have a direct impact on the confidentiality, integrity and availability of the messages being exchanged. The proposal is that when a message needs to be exchanged between networks, initially they should go to a Service Exchange that should consist of multiple cyber processes and controls. It is assumed that these cyber processes and controls to be implemented can vary for different Service Exchanges due to the different cyber threats' exposure, however a full set of controls would be available to guarantee that the appropriate response can be given in case of changing threats.

A basic process that can be used by the Service Exchange is the white list that aims to deny the capability to outsiders from accessing controls with high processing activities. To enforce even more the controls, processes to do message sanity checks before the messages are routed through the networks can also be performed by each Service Exchange through policy enforcement points. At the receiving network, another policy enforcement point to verify also the messages can be established to improve the effectiveness of the controls.

Similar to the verification made by applications on the integrity of the messages being processed by those same applications, policy enforcement points could improve the way checks are made. These improvements are enabled through additional verification and correlation that can be made between the messages that are exchanged, its source and identity and other aspects such as message frequency and common destination and time of exchanges, among others. Policy enforcement points should also be able to quickly deploy message access and flow control rules. This dynamic process would allow better protection of applications, network and systems against evolving cyber threats.

Systems

To enhance the security aspects of the network, configuration of systems should be done in a way that limits access only to pre-defined ports that are process or application specific logical resources and that serves as end-point communications being used by the transport layer protocols of the Internet protocol suite. Examples of these protocols are the user datagram protocol and the transmission control protocol as explained in chapter 2.

Aiming to reduce the exposure of applications in the network, ports should be associated with, and identify specific applications. This approach would reduce the probability of and attacker to access an application host system due to the increased difficult to access the operating system considering that the system would only expose selected applications to the network. To eliminate the possibility of cyber-attacks through malware or other sources, remote access to the operating system should also be disabled and this access could only happen through secure and authenticated accesses.

Applications

Applications need to communicate among themselves to perform desired and essential functions associated with aircraft and air traffic management operations. The connection of applications, to avoid them being redirected to a rogue application by an attacker, must be done only after mutual authentication is completed. This authentication must be done through the use of processes to guarantee verification of digital identities.

The exchange of messages between different applications allows them to connect and communicate. Some characteristics of these messages would help to create a pattern that can be used later for verification of authenticity and provide correct levels of protection. These characteristics are related to, among others, the length of the message, the type of data being transported and the integrity signature that can be all included in the header of the message. The generation of message integrity signatures by the applications originating

the message would guarantee that the message is not replayed by and attacker or even modified.

Encryption is another technique that can be used by the applications originating messages. Encryption should be used when the confidentiality of the messages should be preserved. With encryption in place, the application receiving the message would be able, through the header of the message, to verify the integrity and authenticity of the message, avoiding the possibility of the application to process corrupted or spoofed messages. Through this verification, the application receiving a message would have the capability to drop it if the message integrity signature does not match the content or the header of the message is incorrect.

In case of applications using commercial-of-the-shelf message exchange protocols that do not allow verification of message integrity signature, the originating and receiving applications being used for the exchange of messages should have an architecture, design and configuration that would allow them to create a virtual private network (VPN) through the use of the transport layer security (TLS).

The use of the transport layer security would allow the verification of the message integrity signature. In addition, the verification of the message integrity signature would be transparent to the application and if, while in transit, a message is modified or spoofed, the transport layer would be able to discard it.

With a secure network achieved through the use of layers of defense, the probabilities of a successful cyber-attack would be reduced, however, there is no system or network one hundred percent secure and as such, resilience becomes the most important aspect for the aviation industry operating in the cyber space and should cover all its elements or enablers.

After listening several experts involved in the protection and operation of digital systems used for message exchange, a public key infrastructure (PKI), a dedicated IP addressing and domain name system (DNS), as well as an information security management system (ISMS), are considered in this research basic enablers for a resilient network.

Information Security Management System

To provide for initial and over time protection for a global resilient aviation interoperable network infrastructure against cyber-attacks, networks should be planned and deployed with characteristics of security and resilience by design.

A secure network operation should be achieved through regular re-assessment of the risks that the operations are subjected to. This constant assessment would allow the implementation or review of existing cyber security related processes to reduce probabilities of cyber events and close vulnerability gaps.

The continuous monitoring against cyber related events of operational networks, as part of an information security management system, is crucial for the control of the message exchanges and the occurrence of possible cyber-attacks. Through monitoring processes, possible vulnerabilities can be discovered before intruders use them to perpetrate an attack. Considering the interconnection and interdependency between systems operating through a network, sharing information regarding vulnerabilities among the participants, using a correct protocol for those exchanges to guarantee agreed levels of confidentiality, will help to reduce the number of weak links in the infrastructure and leverage lesson learned.

Public Key Infrastructure

When the community needs to guarantee integrity of digital identities and the confidentiality and integrity of information being exchanged, and the use of simple passwords does not meet the authentication performance criteria established, a public key infrastructure (PKI) comes as and affordable and secure option. A public key infrastructure is made of a set of policies and procedures to manage encryption and revoke digital certificates to facilitate the secure digital transfer of information between systems.

People and organizations have their respective identities linked to public keys when using a PKI arrangement. The establishment of processes for registration and issuance of certificates by an authorized certificate authority (CA) will link the identities to the organizations participating in a PKI.

Before the issuance of a certificate to a specific organization, and through a registration authority (RA), which is a specific function in the PKI infrastructure, the authentication of the identity of the organization requesting a certificate is performed and based on the information collected about an organization requesting a certificate, the organization will be uniquely identified.

As part of the PKI arrangement, and to verify if a particular key really belongs to a specific organization, processes and procedures for the creation, storage and distribution of digital certificates are put in place. The digital certificates serve then to map organizations to specific public keys and are stored in central repositories that allow their revocation in case of breaches in their confidentiality.

A PKI to support the aviation community while using the cyber space for services provision should consist of [76]:

- A registration authority (RA) - verifies the identity of organizations requesting their digital certificates.
- A certificate authority (CA) - stores, issues and signs the digital certificates.
- A central directory - a secure location where keys are indexed and stored.
- A certificate management system - manages the access to stored certificates or the delivery of the certificates.
- A certificate policy – a document that states the PKI's requirements to allow auditors to analyse the PKI's trustworthiness.

Certificate Authority

A certificate authority represents the function that digitally sign and publish a public key that is linked to a specific organization. The certificate authority uses its own private key to sign and publish the organizations public key. This arrangement puts a strong responsibility on the performance of the certificate authority which will dictate how much trust is entitled to a certain public key issued by that authority by the different participating organizations in the PKI considering that the binding between key and organizations is highly dependent on the level of assurance the mentioned binding has. This binding can be established by human supervision or automated systems.

Another important role of the certificate authority that allows participants of a PKI the verification of the status of a public key is the maintenance of online certificate status protocol (OCSP). This arrangement is crucial for the different organizations' verification of keys no longer valid and as such identify the message exchanges that cannot be blindly trusted anymore.

If a certificate authority decides to have an organizational structure that allows other authorities to sign and publish certificates, this delegation of authority to sub-certificate authorities does not relieve the original certificate authority, in this case a root certificate authority, of its accountability for the published public keys.

Bridge Certificate Authority

The idea of creating a global PKI to support the aviation ecosystem as a whole, brings with it three possible architectural arrangements:

1. The aviation community can create a single root certificate authority with the establishment of sub-CA's for each State, region or organization.
2. The community can define a root CA for each State, region or organization and defines bi-lateral agreements for cross certification between each root CA.
3. The community can also create a bridge certificate authority (BCA) with a single member root or distinct BCA's for each State, region or organization. The BCA in this option would provide bi-directional cross certification between each root CA and itself.

The first architectural arrangement with a single root CA to support the aviation ecosystem would require that current running CAs be adapted to sub-CAs what would require them to reconfigure all their using PKI systems to comply with the new hierarchy. This arrangement would also concentrate all the liability related to a PKI on the hands of a single root authority.

In the second type of arrangement where a single root CA is created for each State, region or organization would result in the need of the establishment and maintenance of N x (N-1) / 2 number of bi-lateral agreements between the root CA's where N is the total number of root CA's in the PKI. Based on the difficulties associated to the development and agreement between different entities when several different parameters and mainly interests are involved, this process would be long and complex. The risks that the aviation community is facing today due to cyber vulnerabilities request more expedite decisions. Besides, it would be necessary the discovery and validation of N x (N-1)/2 number of path's which is prone to error and time consuming.

According to the interviews with experts presented in Chapter 4 of this research, the establishment of a bridge certificate authority is considered the most feasible arrangement, considering it can unify the already existing PKI and pave the way for future PKIs. This arrangement would keep the liabilities of current operating CAs for signing and publishing their own keys. The validation of the keys would still be a complex process, however, with only one validation path.

The physical arrangement for a bridge certificate authority should be one that enables communities to get together to unify and harmonize the processes and procedures, including its governance, associated to the achievement of a trusted digital identity.

The model to be used for governance should allow clear allocation of liabilities, and a supporting structure for sharing, validating and auditing the liabilities. At the same time,

the BCA would be the element to link organizations and enable the recognition of CA credentials when they are issued by different organizations.

Through the use of cross certification processes, a bridge certificate authority would be able to validate a credential presented by any organization participating in the PKI arrangement.

To operate and support a common operating environment, a trust framework becomes necessary. This trust framework would establish specific standards for cyber safety and resilience, as well as policies and governance principles for a globally connected aviation ecosystem.

Digital Certificate/Identity

The ownership of a public key is proved through an electronic document know as a key certificate or as some authors call it, a digital certificate or prove of digital identity. The digital certificate includes the digital signature of an organization who verified the contents of the certificate. These contents will show the information about the key and information about the identity of the owner itself. To allow the secure connection and exchange of messages in a secure digital environment, a confirmation of the validity of the signature in the certificate and the confirmation that the system trusts the contents of the certificate is necessary.

In the aviation daily operational scenario, digital identities serve to identify different stakeholders, including airspace users and the different equipment used in the support of aircraft and airport operations. From an aircraft perspective, the digital identity can be used to uniquely identify the airframe itself as well as any of the different components of the aircraft.

From an airspace management perspective, any object may also have an alias to allow its specific identification in the context of the parties participating in the interaction. This can be seen as similar to the use of flight numbers to identify a flight for operational purposes or the tail number for fleet management and maintenance purposes.

One of the requirements to be applied to digital identity is the requirement to be unique, invariant and persistent. This uniqueness would allow the digital tracking when the aircraft move from one operator to another. It would also allow the tracking of the aircraft components as they can also move from one aircraft to another such as the engines. This can be done in a similar way as it is done today through serial numbers that are affixed to different parts of the aircraft.

Internet Protocol (IP) Addressing

To allow the communication between different systems or devices through the routing of IP messages in a global network such as the one supporting the aviation operations, it is necessary that all devices and/or systems have a unique identifier represented by a logical numeric IP address.

The IP addresses are located in the header of the messages and have the goal to identify the origin and destination of an IP message. To use a comparison, we can see the use of IP addresses the same way we use civic addresses that individually identify a location where one lives. The difference relies on the methods used to deliver the message that in the case of a digital message, it flows through routing in an IP network.

Despite the existence of two different version of IP protocols for address definition and messages routing, IP version four (IPv4) and IP version 6 (IPv6), due to the exhaustion of IPv4 addresses and the security issues associated to it, the community is migrating to IPv6.

For a global system such as aviation that depends on safe and secure communication systems, experts identified that IPv4 is not suitable for the proposed use and recommended the use of IPv6.

One of the parameters that recommends the use of IPv6 instead of IPv4 in the aviation industry is the far larger number of unique addresses that can be obtained with its use. While IPv4 uses 32 bits for address composition, allowing the definition of 2^{32} addresses, IPv6 uses 128 bits allowing the definition of 2^{128} and this is equal to 340 trillion trillion trillion IP addresses. This much higher number of possible addresses guarantees the uniqueness necessary for routing through safe networks.

Besides uniqueness, and the capability of having built-in security standards, the use of IPv6 allows another important characteristic of IP messages routing that relates to its capability of multicasting operations, where one message can be routed simultaneously to several different locations while in IPv4 the messages are only possible to transit from unique point-to-point.

Due to the differences between the two versions, it results that the two are not totally compatible. The communications in different networks using IPv4 and IPv6 addresses can only be made between addresses using the same protocol. IPv4 can only communicate with another IPv4 address and IPv6 can only communicate with another IPv6 address. Being aviation a system of systems that were and continue to be defined locally and in different

times to meet the expectations of sometimes specific national or regional communities, it is necessary to develop a transition to allow all systems to be connected in a trusted, seamless and interoperable way.

Dedicated IPv6 address block

As seen in previous sections, the use of a trusted digital identity to identify securely the participants in an exchange of messages transiting through the cyber space is crucial for the confidentiality and integrity of the respective messages. However, just the identification is not sufficient to guarantee the resilience and consequently the safety and interoperability performance required in the aviation industry.

One method that is vastly used by the industry to reduce vulnerabilities and minimize the possibility of a cyber-attack is the address control. Address control also helps the aviation industry with the challenges associated to the integration of public and private networks.

The use of a unique block of IPv6 addresses to support the needs of the aviation industry, allows the internet service providers to create an extra layer of information security by rejecting messages routed to that block unless they are coming from inside the block. The use of dedicated address block precludes these addresses of being routed through the public Internet, and as such reduces the probability of these addresses being attacked or used for an attack.

Among the advantages of operating the aviation industry using a dedicated block of IPv6 addresses it can be mentioned [76]:

- The possibility of direct link between private and public networks.
- Possible use of the dedicated addresses for operations particularly defined for internal process within a specific organization.
- Organizations can use their dedicated block of addresses for internal and external applications.
- Reduces the risk to an integrated infrastructure by limiting the number of addresses to be managed.
- Is scalable allowing the growth of the communications infrastructure as the needs come to support new functions and/or applications.
- Allows the use of white lists of IP addresses to help simplifying the protection of the supporting networks.

During the interviews as presented in Chapter 4, experts highlighted the fact that, despite necessary, the transition to a dedicated IPv6 addressing schema presents some challenges for the aviation community. One of the challenges is associated to the costs of configuration and testing of legacy equipment and systems.

Domain Name System (DNS) and Generic Top-Level Domain (gTLD)

The use of a generic top-level domain is seen by the experts as another layer of protection against cyber-attacks, not only from a technical perspective but also from a political point of view. The use of a specific top-level domain for the aviation industry would limit the exposure of the aviation industry to public networks through the use of specific technical standards and processes for governance.

Another capability that has not been in the list of worries of the aviation community until the event of hipper connectivity being experienced nowadays, where anything that can be connected is being connected, relates to the use of DNS services, considering that most of the current aviation networks are private and isolated ones. However, in a fully connected environment through the cyber space where different DNS services are used for message routings and location discoveries, uncoordinated DNS services will bring inefficiencies to all stakeholders and the aviation system as a whole.

The main function of a DNS is to provide a service that converts technical numerical addresses into human readable addresses that can be remembered easily for further applications. The translation between numerical and human readable address allows the use of Internet domains through the use of names instead of numbers and vice-versa.

The name servers are the main infrastructure supporting the DNS services. They represent the communication and computing systems of a DNS and contain, each of them, small portions of the information related to a domain name space. The data provided by a DNS allows any device to be available on the Internet.

To ensure the integrity and authenticity of the domain name and information while in transit, the DNS uses source authentication processes. This can be considered one of the primary goals of a DNS.

Being an essential service for connectivity between systems and despite the security measures in place, DNS services are vulnerable to attackers aiming to hijack traffic to tamper the information being exchanged and for this reason, it is critical the protection of the DNS to ensure the trust in the services provided in the networks. Some techniques can be used for DNS protection such as the combination of:

- Use of protected DNS service such as DNSSEC (DNS Security Extensions) which are a group of minimum standard specifications aiming the security of the information in the DNS used in networks.
- Limiting the access to applications outside the aviation domain through the use of private DNS services.

The use of a private and secure DNS service associated to a generic top-level domain for the aviation industry would contribute to limit the risks of a cyber-attack. When combined with the use of a dedicated block of address, this architecture would reduce significantly the probabilities of an attacker to penetrate the system without being detected in advance.

This approach cannot be considered new or experimental. It has been in use by different industries and governments to protect sensitive communications. One of the examples that can be mentioned is the use of the domain ".mil" used by States to protect the sensitive military exchanges and guarantee the sovereignty of their territory and security of their populations.

The validation system to be used relies on the fact that an application can be put in place to approve if a message or request for connection is coming from a valid and approved DNS and address and reject the request if necessary. These layers of verification create a net of protection against publicly accessible domains and infrastructure and can be implemented easily by any supporting system.

Experts highlight that with the expansion of interconnectivity and use of IP connection in the aviation system, some common services used for IP connection by other industries will need to be adopted. One example, as mentioned before, is the use of domain name systems.

Another underlying service, although not considered in this research as a basic enabler for a resilient aviation network, but that would help to increase the layers of defense, is a generic Top-Level Domain (gTLD). A generic Top-Level domain is a top-level domain (TLD) maintained by the Internet Corporation of Assigned Names and Numbers (ICANN) for use in the Domain Name System of the Internet. A top-level domain is the last level of every fully qualified domain name.

Although not being considered a basic enabler from a technical perspective, the interviews with the experts, as highlighted in Chapter 4, indicated that to improve the levels

of security and resilience of the aviation ecosystem, a gTLD should also be pursued in support of and international aviation trust framework.

The gTLD acquisition and maintenance by the aviation community relates to its political impact in a trust framework environment and the resilience aspects involved when a community of interest has the control of a gTLD.

Considering the basic enablers of a cyber-resilient network, resilience in the international aviation trust framework context can be achieved through six components: compliance, identification, protection, detection, mitigation and recovery.

Compliance

Networks and organizations operating them must demonstrate their compliance to the established policies and procedures related to cyber security. Through qualified organizations to provided audit services, networks and operators can be audited and certified regularly to guarantee compliance that may be considered the start of a segregation to support safety and resilience. This process, when the results of the audit are shared with the different network operators in the system, allows each participant to decide on the continuity of sharing information or not depending on the information security parameters verified for compliance with the established rules.

Identification

Information about versioning of the devices and systems used to support critical functions need to be managed by each participant and the respective cyber hazards and vulnerabilities used to define the risks associated to their use must be identified.

All the cyber vulnerabilities, hazards and risks identified by the participants in a global network to support aviation operations and its critical functions need to have the information and respective approaches taken to resolve the issue shared to avoid the same issue repeated times in different locations.

Certificate authorities, network service providers, including domain name system operators and communication service providers, due to their critical role played in the aviation ecosystem, besides application developers, are important players and see as crucial the processes associated to identification of vulnerabilities.

In addition, not only the identification of vulnerabilities is identified as crucial, but also the sharing of related information among the different participants considering the need to strength the cyber resilience of the aviation system through a trusted network.

Protection

Some procedures can be used to protect aviation assets or limit the impact of cyber events that can disrupt operations. Among them, it can be highlighted procedures for access control and/or authentication of different interested parties, information and data security, the use of protective technology as well as the regular maintenance of software and hardware.

All participants of a trust framework should implement access control at application, system and network levels. Despite the possibility of the differences in the application of technologies for access control, as long as they comply with the established minimum performance requirements, they would maintain the protection level at the required one.

In a communication process, it is crucial that the receiving side can correctly identify the originator of the message or request for access. Access could then be only granted if the receiving part can authenticate the origin of the request. For this purpose, participants in a communication process need to perform mutual authentication through the exchange of digital identities that can be trusted by both ends. In the particular case of the aviation system, these identities need to be trusted globally due to the inherent international aspects of aviation. The use of non-trusted identities would mandate the development of complex systems with the possibility of generation of gaps and vulnerabilities that could be exploited by attackers.

Procedures for data security would contribute to guarantee, when necessary, the confidentiality of the messages exchanged and in all cases the integrity of the messages. This can be achieved by signing or encrypting the data, if necessary, after the participants perform mutual authentication through their respective digital identities.

To protect critical assets and services in the aviation ecosystem, each stakeholder needs to define and document what security processes will be used for data control. Considering the inherent international character of the aviation system, the procedures to be used should follow internationally agreed procedures to guarantee their harmonization and reduce their impacts in the interoperability of systems.

Based on the state of the assets and the vulnerabilities identified, all stakeholders of the aviation ecosystem, interacting through and international aviation network, should have

detailed procedures in place to update and/or upgrade their hardware, software and applications as well as the security configurations of the systems operating in support of critical functions.

As mentioned in previous sections, and to be used as another protective layer, measures such as the use of policy enforcement points, intrusion detection and protection systems, among other options, should be used by all stakeholders of the aviation ecosystem. The application of these protection measures should be consistent with the level of risk identified by each stakeholder depending on their network architecture and the cyber risks identified through their risk assessment process.

Detection

In order to protect the aviation applications, the systems put in place for network protection must provide the capability of early detection of cyber events. This function is only valid if all stakeholders participating in a global network have the capability to detect timely possible intrusions. This early detection would allow the isolation of the anomalies stopping its propagation to other connected systems.

Among the different actors and functions, contributing for early detection of cyber events, it can be mentioned the role of certificate authorities who must be able to identify anomalous identity discovery and requests for validation. Also, bridge certificate authorities, must be able to identify erroneous requests for certificate policy mapping as well as erroneous request for cross-certificate validation. The process of cross-certificate validation can be achieved based on the analysis of some parameters associate to the different messages and requests such as origin, destination, time and frequency.

At the application level, the capability of identifying erroneous request for access, authentication and issues regarding the integrity of messages should also be implemented. Network service providers must be able to early detection of anomalous attempts of network flows, attempts to denial of services or any other intrusion that can stop systems and services to work as expected. The correlation of the mentioned events will allow the early detection of a potential cyber-attack.

Mitigation or Response

The reduction of the impact of a cyber event is identified as mitigation or response. Mitigation can be achieved through clear documentation of the appropriate activities that need to be performed in case of a potential cyber event. Mitigation processes, including how

to isolate or block a cyber-attack and the communication process to be applied between stakeholders during and after a cyber event must be documented.

Based on the involvement of different stakeholders in a cyber-attack, and as part of the response to the incident, certificate authorities may need to revoke some digital identities. In this research proposed architecture for an international aviation trust framework, if there is a notification that a certificate authority has been compromised, all identities of this entity may have the cross certification revoked by the bridge certificate authority. In addition, based on the criteria of trustworthiness, a policy domain may have its certificate policy mapping limited by the bridge certificate authority.

From a network perspective, network service providers, to avoid a distributed denial of service against a series of networks connected for the provision of global services, may block the flow from a specific network.

Recovery

As important as the activities for provision and management of services for the aviation industry, are the processes put in place by the aviation community related to the reestablishment of services when they are affected by a cyber-attack. The activities to recover the system, including the communication recovery plan, must be all documented considering that the same event can repeat in different times or location and the lessons learned during one attack can be used to avoid another similar one.

5.3 Global Trusted Identity

Since its initial developments, commercial and general aviation have been recognized as a global business considering that aircraft cross borders consistently for the provisions of transport services to a global community. These services are dependent on a strong capability of all stakeholders to exchange information that can be trusted by all participants. Moreover, to guarantee the trust in the information and the actors participating in the exchanges, it is crucial that trust is put on the identity of the participants and in the integrity of the information provided and messages being exchanged.

With the investments associated to the digital transformation of the aviation system, as highlighted by several experts interviewed and as described in Chapter 4, the digitalization of infrastructure and automation of services, despite the benefits they provide also bring new challenges to the aviation community.

To allow the necessary digital transformation of the aviation industry, exchanges of operational information of any kind need to be trusted. This evolution requests that the trust framework represented by the Chicago Convention evolve and adapt to the new technological scenario.

As part of the mentioned evolution, and to continue to meet the expectations of the global aviation community, an international aviation trust framework, following the guidance provided by the Chicago Convention, needs to follow some principles. Moreover, as this new way of trust will be done through the cyber space, the principles should consider that the provision of services should have its safety, efficiency and interoperability preserved or improved if compared to current operations. Some crucial principles can be listed as:

- A seamless and efficient service for message exchange on a system-wide basis must be implemented and guarantee interoperability between all participants.
- Through compartmentalization of a global network, and the use of layers of protection for the supporting infrastructure, the services should have their resilience guaranteed to avoid disruptions in large scale.
- Trust in the system must be based on strong processes, procedures and documentation for identification, authentication and authorization.

A fundamental aspect for the establishment of trusted communications between the different stakeholders, as an enabler for the evolution of the aviation system, is the capability to trust the information being exchanged. With the inherent complexity associated to this evolution, a trusted information exchange environment becomes crucial for the maintenance or improvement of the current levels of safety applied by the aviation industry and accepted by the aviation community, as well as for the improvements in the performance of the system as a whole.

Cryptography can be used in an international aviation trust framework as an element to support trust among different participants. However, as highlighted in previous sections, other elements are also necessary if this trust is to be established and maintained in a digitally connect environment. Strong processes associated to cyber hygiene and a trusted digital identity are among them.

Cyber hygiene

Some basic care would be necessary, since the beginning, from all stakeholders in the process of connecting networks and exchanging trusted information in a system-wide basis.

To all stakeholders to be able to trust networks and applications developed and operated by different States and companies, basic cyber hygiene procedures must be in place and demonstrated by the different parties.

Cyber security policies published by different standard making organizations dealing with operations in the cyber space can be used to guarantee that the minimum cyber hygiene processes are in place [77].

Trusted digital identity

Figure 20 below shows a simplified view of the documentation, organizational and operational aspects related to the trusted digital identities. The elements showed in the figure are necessary for States, air navigation and communication service providers, airspace users and other participants of the aviation community to trust each other's digital identities.

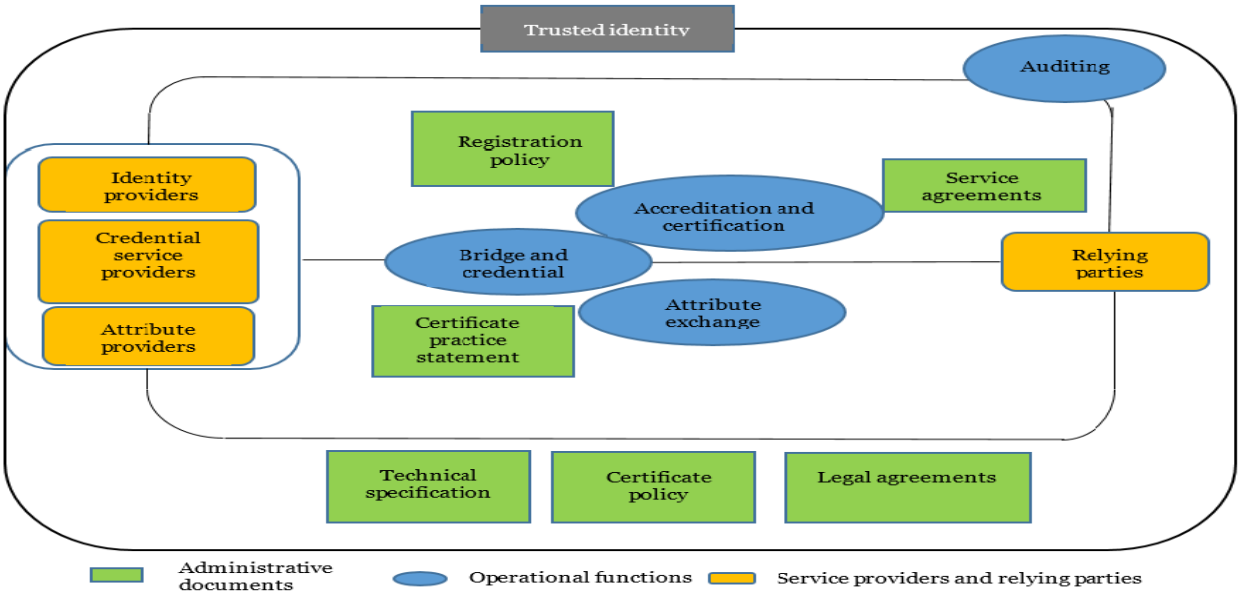

Figure 20 - Trusted digital identity framework. Source: Own development.

Documentation

The documentation to ensure a trusted identity as presented in figure 20 above should consist of a set of rules, agreements and procedures to be applied for the management of a trust framework for aviation:

- The liability and legal, commercial and operational risks should be described in the legal agreements signed or accepted by the different participants.
- Procedural and operational requirements associated to the digital identities, including, among other aspects, its validation and verification must be defined in the certificate policy and are applied to all organizations participating in a trust framework.
- The operation of a framework to guarantee the trust in the identities of different participants requires the specification of technical standards, tools and interfaces.

To guarantee that the operations in general and all participants in particular are behaving in conformance to the agreed upon certificate policy, there is a need for the entity regulating the trust framework to perform regular audits. The goal of the audits is to verify compliance with the different aspects described in the certificate policy, the technical specifications and legal agreements.

Organizations

The first organization identified in figure 20 is the registration authority. These organizations collect and verify the information for the creation of a digital identity and as such are called identity providers.

The second organization described is the certificate authority to manage and issue digital identities. Based on information received from the registration authorities, the certificate authorities issue the digital identities to the organization requiring them. These digital identities are issued in the form of public and private key certificates.

The figure also shows entities that can provide supplemental information aiming to increase the trustworthiness of the identity. These are considered attribute providers.

Last, the figure shows the applications using the digital identities for mutual authentication as well as generation of digital integrity signature. These encompass all relying parties.

Operations

The operations of a framework for digital identity management consist of not only operational functions but also administrative documents.

Relevant administrative documents are listed below:

- The document that describes how, and based on which requirements, identity providers verify the physical identity of entities and register the relevant attributes before issuing a digital identity is the registration policy.
- The practical processes and requirements used by the credential provider to issue and validate digital identities are described in the certificate practice statement.
- The functional and performance requirements for the services and technical interfaces from service providers are documented in the service agreement.

Operational Functions

- To describe, evaluate and validate a digital identity, an accreditation and certification process is put in place.
- To guarantee trust between digital identities issued by different certificate authorities, a bridge and credential exchange function for cross certification is operationalized.
- A real-time exchange of identity attributes between different service providers is performed by the attribute exchange function.

5.4 Operations

A consortium formed by traditional and new network communication service providers is foreseen for the provision of network services. These network service providers should involve the ones providing also services through low earth orbit satellites and long-term evolution technologies.

International standards for network services, as well as network interfaces and security would guide the provision of services by the consortium. At the same time, network users and providers would follow the agreed standards and procedures.

Aiming the achievement of a global resilient aviation interoperable network, the interconnection of networks will be done in accordance with a multilateral agreement. This agreement will enable seamless exchange of network traffic.

Network providers will be able to manage the bandwidth they sell to network users according to the user's needs in terms of global services being consumed or provided.

For the aviation community to follow already tested and approved procedures for network traffic exchanges based on demand and capacity for services, reducing that way the potential risks of failures, the successes history of the Internet must be considered, and relevant procedures applied.

The first step for an aviation user to get a service to support its operations is for this user to obtain a digital identity. An example can be given as one air navigation service provider or aircraft operator that wants to know the position of an aircraft performing a flight.

The user, as a first step, registering its actual identity with the respective registration authority, can obtain the digital identity. After the validation of the actual identity, the information is passed to the certification authority. Being the certification authority a participant of the trust framework, it is able to issue the digital identity in the form of a digital certificate.

As a next step, it is necessary for the user to obtain a connection from a network provider participating in the global aviation interoperable network. The user needs to provide proofs that its system or network that needs connection complies with the network security and interface requirements to be connected to the global network, as well as that it is compliant to the operational policies.

These steps would enable any network provider to connect its systems or networks to the global aviation network and keep the interoperability of operations while providing or consuming services. The establishment of the network connection allows the users of the network to obtain the requested services.

Network services

The requirements adopted for the network services, defined at least by the parameters listed below, establish a standard set of services that can be provided by each participant to the network consortium:

- Bandwidth.
- Maximum latency.
- Availability.
- Supporting protocols.

- Scope that can be global or local.

Based on the parameters listed above, network service providers can develop a catalogue of services available for provision that can be chosen by different users based on their operational and technical needs.

Network interface requirements and policy

To provide the guidance to network providers on how to interconnect their networks, the network requirements and policy are defined.

Among the requirements, it would be the ones related to network interfaces between network providers and users as well as the use of the dedicated block of addresses in the aviation ecosystem.

The processes describing how to obtain and assign the dedicated addresses to the network must be described in the policy associated to the use of the global aviation network. In addition, roles, responsibilities and liabilities of each network provider must be described in the policy.

Network security requirements and policy

The definition of standards to be followed by the security controls applied by users and network providers must be defined in the network security requirements. A process must also be implemented to guarantee that users and providers are compliant to the security policy.

5.5 Conclusion

As described in the previous sections, aviation is a safety critical business that needs to evolve to continue bringing to the society in general and the aviation community in particular the benefits of physically connecting people and allowing the growing of societies in isolated parts of the world.

To continue to provide these benefits, the aviation system needs to evolve towards a digitally connected environment for services provision, which will allow a better decision-making process bringing safety and efficiency benefits to all stakeholders involved.

This evolution involves, necessarily, better ways to exchange information and automation of processes where human is involved considering that human involvement

comes sometimes in detriment of accuracy, efficiency and/or effectiveness due to the inherent characteristics of the human process for decision-making.

With this in mind, experts from all over the world have been researching better ways for information exchange and it is unanimity that considering the status of availability of new technologies, the use of the cyber space is a goal to be pursued.

However, it is also unanimity the view that the use of the cyber space, besides bringing the benefits expected for better ways of information exchange, also brings challenges. These challenges in some areas can jeopardize the high levels of safety practiced by the aviation industry in the last decades if not addressed in the right way and at the right time.

These challenges are mostly associated to the need of strong processes and procedures to reduce the cyber-attack surface and provide high levels of resilience to systems in case unexpected events happen to one of its components that can disrupt large operational areas.

A solid process for identity management in a digitally connected environment and a resilient network for exchange of information are the main components to be addressed considering the lack of physical means for identity verification when using the cyber space and the number of interconnected networks to provide a global resilient network for connectivity.

With the goal of providing a solid digital identity management and a resilient network, the aviation community needs to get together and work in different components as enablers that would allow the achievement of the mentioned goals.

From a network perspective, the implementation of specific cyber controls and processes based on local impact threat analysis is necessary to ensure rapid response to changing threats.

The use of white lists as a firewall for access control will avoid non participants of the trust framework to access the more processing and important intensive controls. Policy enforcement points can be used as an additional layer of protection through message sanity checks that must be performed before the message is routed to and from the intended destination.

To increase the difficulty for an external actor in attacking the application host system, systems should only expose specific applications to the network, thus an attacker

would not have direct access to the operating system. This would be possible considering that the same systems would be configured to limit access only to pre-defined network ports serving as a communication end-point. Network ports should be associated with and identify specific applications.

Mutual authentication processes using digital identities must be performed before two parties start a communication session. This authentication is necessary to guarantee that the parties have not been redirected to a rogue application aiming to harm the system.

To avoid messages being replaced by an attacker, the message header should follow a pattern. This pattern would define the message length and type of data. Besides, using the digital identities of the parties, the integrity of the signature created by the sender would be verified.

Basic enablers for a resilient network should be put in place involving information security management systems, public key infrastructure, dedicated internet protocol addressing and a secure domain name system.

The operationalization of information security management systems would enable the implementation of processes for monitoring operations and detecting potential cyber threats before they can become a real cyber-attack. The discovery of vulnerabilities can also be done through the same monitoring processes. Aiming to reduce the risks of an attack, these vulnerabilities must be shared with the participants of the trust framework to leverage lessons learned and reduce the number of weak links in the supporting infrastructure.

Rules, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption can be achieved through a public key infrastructure. Where the use of simple passwords does not fulfill the requirements for secure identification, the use of a public key infrastructure comes as an option to guarantee the secure exchange of digital information between systems and devices.

The public key infrastructure arrangement would bind public keys with respective identity of entities. A process of registration and issuance of certificates at and by a certificate authority would be used to establish the binding that depending on the assurance level can be carried out by an automated process or human supervision.

The use of internet protocol address control minimizes the exposure to cyber-attacks across the public infrastructure. This extra layer of network assets protection can be

achieved through simple white lists. These controls also allow the secure connectivity between public and private infrastructures.

The definition and use of a dedicated address block to be applied uniquely by the members of the aviation community and when necessary by the supporting supply chain, would enable an additional layer of protection. This additional layer would enable the rejection of messages directly routed to the dedicated block.

Another layer of protection to be implemented for an effective use of the Internet across the global aviation community can be the creation of a private domain name system linked to a specific aviation generic top-level domain. This layer of protection would help to limit and isolate some of the cyber risks associated to the use of the cyber space.

All the enablers mentioned above would contribute to a cyber-resilient network.

To achieve an acceptable level of resilience in an international aviation trust framework, different participants would need to be compliant with the established policies and procedures related to cyber security.

Participants should also contribute to resilience of operations by performing identification of resources that support critical functions and their related cyber vulnerabilities.

Finally, the development of protection, detection and mitigation measures to contain the impact of a cyber event and ways to restore any functions that were affected or totally disrupted by a cyber event would reinforce the resilience of the aviation system through an international aviation trust framework.

Chapter 6

Conclusions

6.1 Initial considerations

This chapter presents the final considerations about the subject of this research. Initially the results in light of the literature and interviews used as the basis for the research and the evolution of the aviation system are presented. Later, the general and specific objectives of the research are assessed and the proposal in this research is analyzed based on the results achieved. The limitations of the research are highlighted and proposals for future work related to the subject of this research are recommended.

6.2 Synthesis

Since the invention of the airplane, aviators and pioneers of aviation have been trying to improve the efficiency and safety of operations and mainly after the signature of the Chicago Convention and the creation of the International Civil Aviation Organization, the aviation community have been harmoniously trying to develop and apply new technologies to aircraft operations and air traffic management.

The evolution of the infrastructure in support of aviation related activities came as a need and very early, but mainly after the Second World War aviation reached a tipping point. During its evolution, several forms of technologies related to navigation, surveillance and communication were developed very fast due to the increase in the demand for air transportation considering its benefits to the global economy and the society in general.

After solving the problems related to lift, control and propulsion of a machine to perform a flight heavier than the air, the community focused on other systems to support aircraft operations. These developments, besides the benefits they represented, brought new challenges to the aviation community in terms of the performance of the systems to cope with the society expectations. The challenges could be observed in all technological areas and the supporting infrastructure for air traffic management, as well as challenges associated to the role of human in the loop that could jeopardize safety and continuity of operations in a similar way as a failure in technical systems.

Communication, navigation, surveillance and air traffic management systems evolved to a point where the harmonious use of the installed infrastructure required

exchange of information between the different actors and components to guarantee its efficiency. Then improved systems for information management started to be developed and deployed.

Point to point communications have dominated the exchange of information until a moment where the system became more complex due to the increase in the occupation of the airspace and the different flying platforms using the same airspace. This airspace occupation resulted in dependent operations among different airspace users, and automated systems to support decision-making became necessary as the air traffic management system started not to be able to provide the society with the levels of safety and efficiency in accordance with the community expectations.

With the strong requirements for automation also came the need for connectivity. In a highly connected environment, information management becomes crucial. Its role in defining the best real-time picture supports the correct decision-making and its role in defining future scenarios can be used to anticipate technical and operational situations that could influence safety and efficiency of flight operations if not acted in advance.

Several benefits are brought to the aviation ecosystem by the processes and procedures associated to information management. Among them, it is worth to highlight the direct benefits brought by increased availability of information. These benefits have consequential benefits in the performance levels of the system in terms of safety and efficiency. At the same time, information management processes and procedures guarantee the continuity of operations under circumstances that deny the capability of primary sources to provide the users with the expected information to manage air operations.

In the current scenario with the increasing levels of digitalization and automation of the air traffic management related processes and procedures, timely and accurate information need to be available where they are critical for decision-making. This environment where information is available to all parties in need of it, defines the principle of seamlessness of information in a secure, flexible and scalable aviation ecosystem.

With the transformation from point to point communication to a system-wide exchange of information using the Internet infrastructure, attention is called to the fact that the confidentiality, integrity and availability of the information can be compromised if measures to protect the exchange of information are not taken in a proactive manner.

For the successful digital transformation of the aviation system, processes and procedures associated to secure exchange of information on a global basis is crucial. This

secure exchange can only be enabled by the use of a resilient network that must be built upon a trust framework. This highlights the importance of information security as an enabler of safety and resilience.

The current situation of the aviation system where isolated solutions are being planned and implemented for information security can also bring risks the same way as doing nothing. These risks can be eliminated if a global approach is taken on the subject and interoperable solutions are adopted. The development and deployment of a global resilient aviation interoperable network through cooperation among all members of the aviation community, using layers of defense against cyber-attacks is the most suitable approach to be taken to guarantee the performance of different systems contributing to the performance of the aviation system as a whole.

Since 1969, when a message travelled for the first time from one computer to another, at that time through a telephone line, the internetworking we all benefit today was born.

The basic network established that connected the University of California and the Stanford Research Institute was the precursor of the high number of nodes that started to connect static and mobile organizations and devices.

With the development of a large number of networks, the problem shifts from connecting computers to connecting networks. Internetworking then becomes the moto of experts around the world. With the development of the Transmission Control Protocol/Internet Protocol (TCP/IP) all networks can now connect to each other, whatever the internal structure of the networks and this creates the Internet, a network of networks.

From the origin to the target destination, data and information travel along routers and a large series of connections keeps the structure linked through optical fibres, telephone lines, satellite connections and other means that all together configure a network.

Networks can then be categorized depending on size, complexity, level of security, or geographical range they support. From personal area networks to wide area networks, they all provide means of connections and they are all subject to similar challenges.

Through specific protocols, networks of different ranges and models are connected to each other forming a system of connected networks or a system of systems (SoS). This SoS is not limited to technological systems and devices. It also involves people and processes and, in this context, the term system must be broadly understood.

At its beginning, the aviation system was not identified as a target for cyber-attacks. It was assumed by the aviation community that attackers would not have the capability or will to use aviation as a vehicle for political demonstration or as a source for illegal revenues. Consequently, the threat models used to define the levels of risk to aviation have not considered cyber-attacks as a possible threat. However, with the evolution of the aviation system and the digital transformation that is affecting processes moving them from manual execution to automation and connecting systems and devices that supports aviation functions, the situation has changed. Aviation is, as many other industries nowadays, a target for cyber-attacks and is suffering critical consequences.

As being a safety focused business and considering the dependence between different systems that form the aviation ecosystem, for the aviation industry is paramount that no interference with one of its components change the overall system performance.

Considering the many interactions in the aviation system to keep it running seamlessly, it becomes a complex task its protection against attacks that come from the cyber space and that do not follow known rules.

With multiple stakeholders interacting for the provision of common services necessary to conduct safe and seamless air operations, the need for trust and confidence are some characteristics that need to be observed to guarantee continuity of services under any circumstances.

Trust in the aviation context is seen as the anticipation of one entity in the expected behaviour of another entity. This can be translated, for example, in the expectation that all participants in the aviation system will only produce and share information that can be trusted and not deliberately produce false information.

At the same time, the capability that one entity has to evaluate the behaviour of another entity and control and scrutinize that behaviour is defined as confidence.

In the aviation context three levels of confidence/trust must be observed to guarantee its safety and resilience. First, it is the confidence that participants in the communication process are positively identified and that the data and information they are exchanging were not modified when at rest or while in transit between origin and destination (Technical trust). Second is the confidence by the different components of a system that the infrastructure put in place by the different participants is resilient to electronic interference in accordance with the services expected to be delivered by each participant (Organizational trust). The third and final level of confidence is the necessary

uncompromised information provision. This relates to an expectation on the behaviour of the originator of any type of information (Societal trust).

In the case of technical trust, the main challenge associated to the assurance of the right originator providing information with the expected level of integrity relates to the system or processes and procedures in place to guarantee the digital identity of the participants in the process. This passes through the existence of a system to verify and validate the identity of the originator of the message that can be done through a recognition of an electronic signature.

The challenge associated to the assurance of organizational trust relates to the system or processes and procedures in place to oversee and approve the operations of another organization, which includes the infrastructure available in the organization to be overseen. The process in place needs to be sufficiently robust to guarantee that and organization involved in the provision of a certain service to the benefit of the community operates under a certain level of trustworthiness.

The scenario is a bit more complicate when it relates to societal trust considering that there are no possible controls that can be used by the aviation community. In this case, there is a need of blind trust.

The need to fulfill the expectation that an organization or system is who it claims to be and that the same organization or system presents the behaviour as expected by other organizations participating in the same SoS is highlighted. Any system or device engaged in the exchange of digital data need to follow some basic requirements. These requirements are related to the need of every system or organization involved in a process of exchanges of trusted digital information to have a digital identity. At the same time, a robust process need to be in place to assure the validity of this digital identity and guarantee that the identity can be trusted.

Furthermore, the process associated to the decommissioning of an identity when for any reason this identity cannot be trusted anymore is crucial. Trust in digital identities is directly related to the process associated to its verification. If the process in place does not bring the level of trust that is necessary for the exchange of data and information in a digital environment, the established identities are not trustworthy.

To solve the trust challenges associated to any kind of operation in the cyber space, a trust framework is necessary and being aviation a global business, it highlights the need of a global trust framework to guarantee seamlessness throughout the aviation ecosystem.

Considering the different behaviours in the global society and the challenges associated to societal trust due to different geo-political scenarios, it becomes crucial the definition of global requirements for technical and organizational trust.

Using a pragmatic paradigm, because pragmatism is not committed to any system of philosophy or reality, the research focused on what and how of the research problem. As such, pragmatism provided the underlying philosophical framework for the qualitative research method. With the pragmatic paradigm, the research problem was used as central and applied all approaches to understanding the problem.

An active research was pursued in this work considering that its main goal was the investigation of a current and real problem affecting the levels of safety in the aviation system caused by cyber threats. The research investigated the problem starting with its clear identification, developing a proposal and planning the observation of the results to be able to change it, if necessary, to meet the expected performance. The implementation of the proposal and observation of the changes are to be developed as part of a use case scenario for the proposal in the future.

The use of the pragmatic paradigm provided an opportunity for different methods, views and assumptions. It allowed also the use of different forms of data collection and analysis.

The pragmatic approach to the consequences of hyper connectivity brought with it a wide spectrum of possibilities to the analysis of posed cyber threats to civil aviation. Cyber events are not always intentional considering that in a digitally connected environment even an unintentional event can stop or harm essential systems and services.

The possibility of cyber events highlights the need for the aviation community to invest not only in measures for protection of the systems to provide services, but also in the development of procedures that are able to maintain the resilience and continuity of the operations when facing an intentional or unintentional event.

These events carry the possibility of catastrophic impact to the aviation industry, bringing its components to a complete global, regional, national or local halt, affecting the business and normal life of billions of people at the same time.

Through unstructured interviews with experts from different segments of the aviation industry and academia, the possibilities were analysed and confirmed that there is a need for investments to keep the protection and resilience of the aviation system that would at the end impact safety of operations and business continuity.

It is consensus that the society needs to keep confidence in the way the aviation industry deals with safety of lives. This passes through the assurance or trust that all players in the system are identified and perform according to pre-established rules and use systems that would not jeopardize the safety or continuity of operations.

As established by the Chicago Convention, it is necessary that each State responsible for the provision of air navigation services and facilities over a designated area of responsibility, including its sovereign airspace, provide them in accordance with global agreed standards. It is also necessary procedures in place to secure the information being published or exchanged in support of air navigation. This highlights the importance of trust for the aviation system.

It is of utmost importance the trust among different actors considering that damages can come from not only an asset or economic perspective but also reputational damages that could bring a service provider or aircraft operator to stop operations due to the lack of confidence by the travelling public.

In this context trust comes as the confidence in the outcomes as planned and expected by the community as well as the willingness by the different participants in the digital transformation of the aviation system to modify behaviours to achieve the outcomes.

In this process of improving the system for the provision of better services using the cyber space, trust involves the people and systems who need to trust (trustor) and the people and systems to whom the trust is directed (trustee). Besides, to have complete trust, the willingness of the involved participants to act on and upheld that confidence is necessary.

Issues come when verifications are not able to be performed due to the complexity of the systems supporting the provision and consumption of services using digital systems for storage, processing and exchange of information through applications connected in the cyber space.

In the aviation ecosystem, trust is the willingness of participants in a trust framework to rely on a specific other, which can be of human or technological system nature based on confidence that one's trust will lead to positive outcomes.

Among the aviation community, the presence of risk creates a need for trust. Trust in this case is an assembly of standards, processes and procedures, agreed among the members of the community including service providers, aircraft operators and regulators to reduce risk and improve performance during processing and exchange of information as well as internal and external interactions.

What differentiates the concept of trust from other related concepts such as faith is the conscious acknowledgement and evaluation of the risks involved. The consideration of risks justifies why an aviation trust framework for a digitally connected environment is necessary as an element to support the resilience of systems that may affect safety and continuity of operations.

During the development of this research, two elements were considered the core of an international aviation trust framework that would reduce the attack surface and increase resilience of the aviation system. These elements, made of different components, relate to a global network to exchange data and information and a system to guarantee the identity of the participants in the exchanges.

To have a global resilient network and reduce the cyber risks, the pragmatic approach used in this research proposes the implementation of layers of individual defenses for networks, systems and applications. This proposal comes from the fact that the expected scenario is the one where different networks will be connected to support systems and applications as it were only a single interoperable network supporting the services provision for aviation.

The specifications of the IP network service used is crucial for the performance of the systems exchanging messages. In the exchange of messages transiting among different networks, the messages pass through different services exchange environment. In this environment, different cyber controls are in place to guarantee the security of the information in transit. Despite the fact that at each service exchange the implemented cyber controls may differ, considering they depend on the local cyber threat analysis, processes and controls would be available to guarantee a rapid response in case of threats' changes.

To avoid intruders to affect the more intensive controls, white lists can be used as first level protection. For the message's control, and before they are routed through the network, sanity checks would be performed by policy enforcement points. The process of verification is repeated after the message is routed at the destination network boundary by another policy enforcement point.

Specific attributes of the messages can be used for the integrity check of the messages from one source. The process consists of the correlation of the identity of the source with more specific message attributes such as its frequency, destination, time and location of the source among other aspects.

To protect systems, applications and the network itself against cyber-attacks, policy enforcement points are able to deploy flow control and message access rules quickly.

To increase the difficulty for an external actor in attacking the application host system, systems should only expose specific applications to the network, thus an attacker would not have direct access to the operating system. This would be possible considering that the same systems would be configured to limit access only to pre-defined network ports serving as a communication end-point. Network ports should be associated with and identify specific applications.

Mutual authentication processes using digital identities must be performed before two parties start a communication session. This authentication is necessary to guarantee that the parties have not been redirected to a rogue application aiming to harm the system.

To avoid messages being replaced by an attacker, the message header should follow a pattern. This pattern would define the message length and type of data. Besides, using the digital identities of the parties, the integrity of the signature created by the sender would also be verified.

The encryption of messages using digital identities can also be performed by a sender when the aspect of confidentiality is necessary to be enforced to a specific message or set of data. Through this process, the authenticity and integrity of the messages can be verified by the receiving system what would prevent the processing of spoofed or corrupted messages. If after the verification, the message integrity signature does not relate to its content or the message header is incorrect, the message is dropped.

Through the use of layers of defense, a secure network is achieved and the probability of a successful cyber-attack is reduced, however, as there is no system or network one hundred percent secure, procedures for resilience becomes an important aspect for the aviation industry using the cyber space.

Basic enablers for a resilient network should be put in place involving information security management systems, public key infrastructure and dedicated internet protocol addressing and domain name system. The combination of processes, procedures and applied technologies, allows the system to continue running despite the occurrence of a cyber event that impacts operations.

The operationalization of information security management systems would enable the implementation of processes for monitoring operations and detecting potential cyber threats before they can become a real cyber-attack.

Rules, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption can be achieved through a public key infrastructure. As part of this infrastructure, the establishment of a bridge certificate enables cross certification and seamless recognition of digital identities system-wide without the need of one to one agreement.

IP address control helps to minimize cyber exposure across public infrastructure. The definition and use of a dedicated address block to be applied uniquely by the members of the aviation community and when necessary by the supporting supply chain, would enable an additional layer of protection. This additional layer would enable the rejection of messages directly routed to the dedicated block from addresses outside the block.

A private domain name system (DNS) associated to an aviation dedicated top-level domain (TLD) allow the effective utilization of the Internet protocol communication across the global aviation community limiting and isolating cyber risks.

The use of the technologies and architectures mentioned above through global standards and procedures for compliance, identification, protection, detection, mitigation and recovery, allow the establishment of a global secure network for exchange of digital information. This network will then operate in accordance with the levels of safety required by the aviation community to support the transformation of the aviation industry towards a fully connected digital environment that is secure, safe and resilient to cyber events.

6.3 Limitations of this research

This research was performed with the understanding that aviation is a global business and that a system-wide information management is necessary to support current and future operations. In addition, two fundamental aspects for system-wide information exchanges must be observed at all times. These aspects relate to the assurance of the digital identities of the involved parties and the integrity of the messages being exchanged among them. This limitation was necessary considering that the full process to achieve trust between different stakeholders involves also geo-political, economic and social aspects that are not under the control of any entity and are influenced, among other aspects, by the culture established within different organizations or technical and political entities.

Not considering the geo-political, economic and social aspects related to trust impose a limitation to this research considering that important aspects of trust are dependent on the organized civil society that are influenced by important aspects that must also be analyzed.

The results achieved with this research are limited to the primary data collected through a group of experts from management and technical levels that were interviewed as well as secondary data obtained from different sources available from different segments of the aviation industry and academia. Despite the fact that it is assumed that the proposal in this research is the most appropriated one, it opens the possibility for the research to be expanded to other groups of professionals and the use of different secondary sources to expand the subject.

The aviation industry is made of specific requirements considering the criticality of its operations dealing with safety of lives. This poses a restriction to the use of other already agreed approaches from other industries due to its differences in functions criticality. In this research, other industry initiatives were used, and this poses certain limitations to the results achieved and approach proposed to be taken.

Last, but not least, it is worth to highlight that the discussion with experts on the subject is as important as the methodology followed. The more time the researcher spends in this phase, debating conclusions and points of views with different experts, representatives from academia and general public, more mature will be his/her approach to the analysis of the data obtained in the field and more mature will be his/her conclusions and final considerations. The COVID-19 pandemic put some restrictions to the number of people consulted and could be expanded in future work.

6.4 Future work

This research was meant to provide, based on the expected developments of civil aviation, a proposal to address the risks of the use of the cyber space for the exchange of safety and business critical information.

This research did not address all aspects of a proposed international aviation trust framework due to the limitations associated to an academic research. However, this research shows that to reduce the cyber-attack surface and contribute to the resilience of the aviation system in a digitally connected environment, the industry needs to evolve and develop processes and procedures to guarantee technical and organizational trust among a variety of aviation stakeholders.

The primary and secondary sources used in this research demonstrated that only with trust among the different stakeholders, the aviation industry will continue to have the confidence of the society considering the aspects related to safety of lives involved in the air traffic management procedures in support of aircraft operations.

The direct participation of the industry in the development and operation of an international aviation trust framework is crucial to guarantee technical and organizational trust. This arrangement does not exclude the participation of international organizations as trust anchors.

As this research also intends to open other areas for future research work, below there is a list of proposed areas for further research:

- Application of the trust framework as part of a use case involving different stakeholders from aviation and non-aviation industry.
- There are different technologies that can be used for identity management. A new research could focus on the evaluation of these new technologies.
- Implication of the use of public and private DNS with DNSSEC as part of a trust framework.
- The impact of the use of blockchain for the confidentiality, integrity and availability of safety critical information.
- A possible public key infrastructure architecture for a global trust framework.
- The best governance options for a global trust framework from an operational and political perspective.
- A threat model for hazard identification and risk analysis.
- An information security management system customized for the aviation industry needs.
- The risks associated to the use of satellite communications in a trusted environment.
- Cyber vulnerabilities and solutions to ADS-B as surveillance technology.
- Cyber vulnerabilities and solutions for controller-pilot data-link communication.

References

[1] International Civil Aviation Organization, *Aviation Security Global Risk Context Statement (Doc10108-Restricted),* Montreal, Canada: ICAO, 2018.

[2] S. Preetha, P. Lalasa and P. R., "A Comprehensive Overview on Cybersecurity: Threats and Attacks," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 10, no. 8, pp. 98-106, 2021.

[3] E. C. Vivian, A History of Aeronautics, New York, USA: BiblioLife, 2008.

[4] R. Curley, The complete history of aviation, New York, USA: Britannica Educational Publishing, 2012.

[5] International Civil Aviation Organization, *Convention on International Civil Aviation,* Montreal, Canada: ICAO, 2006, p. 1.

[6] International Civil Aviation Organization, *Annex 11 - Air Traffic Services,* Montreal, Canada: ICAO, 2018.

[7] H. V. Sudarshan, Seamless Sky, Hampshire, UK: Ashgate Publishing Limited, 1988.

[8] International Civil Aviation Organization, *Procedures for Air Navigation Services, Air Traffic Management,* Montreal: ICAO, 2016.

[9] International Civil Aviation Organization, *Aviation benefits,* Montreal, Canada: ICAO, 2017.

[10] International Civil Aviation Organization, *Global ATM Operational Concept,* Montreal, Canada: ICAO, 2005.

[11] Mimecast, "Securing the enterprise in the COVID world," Mimecast, London, United Kingdom, 2021.

[12] International Civil Aviation Organization, *Global Air Navigation Plan,* Montreal, Canada: ICAO, 2019.

[13] S. J. d. Silva, *A comprehensive strategy for air navigation: Endorsement of the updated global air navigation plan,* Montreal, Canada: ICAO, 2019.

[14] S. J. d. Silva, *Cyber resilience,* Montreal, Canada: ICAO, 2018.

[15] S. J. d. Silva, *Trust framework for a digital environment,* Montreal, Canada: ICAO, 2019.

[16] Deloite, *Future of cyber,* London, United Kingdom: Deloite LLP, 2020.

[17] G. C. Catanzaro and M. Catanzaro, Networks, London, UK: Oxford University Press, 2012.

[18] G. A. Donahue, Network Warrior, Sebastopol, USA: O'Reilly Media Inc., 2007.

[19] D. Groth and T. Skandier, Network+ Study Guide, Fourth Edition, Indianapolis, USA: Sybex, Inc., 2018.

[20] B. Forouzan, Data Communications and Networking, 5th Edition, New York, USA: McGraw-Hill, 2013.

[21] A. L. Russel, "IEEE Spectrum," 30 July 2013. [Online]. Available: https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt. [Accessed 17 November 2021].

[22] FS.com, "TCP/IP vs. OSI: What's the Difference Between the Two Models?," 3 November 2017. [Online]. Available: https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html. [Accessed 17 November 2021].

[23] International Organization for Standardization, *ISO/IEC/IEEE 15288 Annex G, Systems and software engineering,* Geneva, Switzerland: ISO, 2015.

[24] M. W. Maier, "Architecting Principles for Systems-of-Systems," *System engineering,* vol. 1, no. 4, pp. 267-284, 1998.

[25] J. Dahman and K. Baldwin, "Implications of Systems of Systems on System Design and Engineering," in *6th International Conference on System of Systems Engineering,* Albuquerque, USA, 2011.

[26] EUROCAE, "ED-203A Airworthiness Security Methods and Considerations," EUROCAE, Paris, France, 2018.

[27] RTCA, "RTCA DO-356 Airworthiness Security Methods and Considerations," RTCA, Washignton, USA, 2014.

[28] EUROCONTROL, *Considerations about cybersecurity in aviation,* Montreal, Canada: ICAO, 2018.

[29] M. Honan, "Wired," 08 June 2018. [Online]. Available: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/. [Accessed 17 November 2021].

[30] A. Avizienis, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on dependable and secure computing - Volume 1,* pp. 1-23, 31 March 2004.

[31] Gartner Inc., "Gartner research," 24 May 2017. [Online]. Available: https://www.gartner.com/en/documents/3727718. [Accessed 15 November 2021].

[32] L. M. Given, The SAGE Encyclopedia of Qualitative Research Methods, Thousand Oaks, California, USA: SAGE Publications, Inc., 2008.

[33] M. Punch, "Politics and Ethics in Qualitative Research," in *Handbook of Qualitative Research*, vol. 1, Thousand Oaks, USA, Sage, 1994, pp. 83-97.

[34] J. McMillan and S. (. e. Schumacher, Research in Education, Boston, USA: Pearson Education, 2006.

[35] D. Bluhm, W. Harman, T. Lee and T. Mitchell, "Qualitative Research in Management: A Decade of Progress," *Journal of Management Studies,* vol. 48, no. 8, pp. 1866-1891, 2011.

[36] A. R. D. G. S. Baltazar, *Erro Humano e Erro Organizacional nas Atividades de Manutenção das Aeronaves na Perspetiva da Grounded Theory: O Caso Nacional,* Lisbon, Portugal: Lisbon University, 2018.

[37] N. Mackenzie and S. Knipe, "Research dilemmas: Paradigms, methods and methodologies," *Issues in educational research,* vol. 16, no. 2, pp. 193-205, 2006.

[38] J. W. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches. (4th ed.), Thousand Oaks, USA: Sage, 2014.

[39] A. Stander and J. Ophoff, "Cyber security in civil aviation," *Imam Journal of Applied Sciences,* vol. 1, no. 1, 2016.

[40] T. D. Zan, F. d'Amore and F. D. Camillo, *The Defence of Civilian Air Traffic Systems from Cyber Threats,* Rome, Italy: Instituto Afari Internazionali, 2016.

[41] C. Lynch, D. Oliver and J. Lowe, *Overcome the silent threat - Building cyber resilience in airports,* London, UK: PA Consulting, 2018.

[42] J. Nowak, K. Ogonowski and M. Kustra, "Selected threats to civil aviation," *Scientific Journal of Silesian University of Technology,* vol. 102, pp. 141-150, 2019.

[43] A. R. Bryant, J. R. Lopez and R. F. Mills, "Cyberterrorists bringing down airplanes: Will it happen soon?," in *12th International conference on cyber warfare and security*, Dayton, USA, 2017.

[44] S. Strauss, "Theories of learning and development for academics and educators," *Educational psychologist,* vol. 28, no. 3, pp. 191-203, 1993.

[45] J. C. Strauss and A. Strauss, Basics of qualitative research - Techniques and procedures for developing grounded theory - 4th edition, London, UK: Sage publications, 2015.

[46] F. B. Schneider, Trust in cyberspace, Washington, USA: National Academy Press, 1999.

[47] K. C. Wallace and A. William, "Trust in Electronic Environments," in *36th Hawaii International Conference on System Sciences*, Washignton, USA, 2003.

[48] J. B. Rotter, "Generalized expectancies for interpersonal trust," *American Psychologist,* vol. 26, no. 5, p. 443–452, 1971.

[49] R. C. Mayer, F. D. Schoorman and J. Davis, "An integrative model of organizational trust," *Academy of Management Review,* vol. 20, no. 3, pp. 709-734, 1995.

[50] K. Blomqvist, "The many faces of trust," *Scandinavian Journal of Management,* vol. 13, no. 3, pp. 271- 286, 1997.

[51] A. B. Seligman, The Problem of Trust, New Jersey, USA: Princeton University Press, 1997.

[52] N. Luhmann, Trust and Power, Chichester, UK: John Wiley & Sons, 1979.

[53] F. Fukuyama, Trust: The Social Virtues and the Creation of Prosperity, New York, USA: Free Press, 1995.

[54] D. M. Rousseau, S. B. Sitkin, R. S. Burt and C. Camerer, "Not so different after all: a cross discipline view of trust," *Academy Management Review,* vol. 23, no. 3, pp. 393-404, 1998.

[55] B. H. S. Sherman and M. Dana, "The Grammars of Trust: A Model and General Implications," *The Academy of Management Review,* vol. 23, no. 3, pp. 422-437, 1998.

[56] B. Friedman, Human Values and the Design of Computer Technology, Stanford, USA: Center for the Study of Languge and Information, 1997.

[57] C. A. Heimer, "Solving the problem of trust," in *Trust in society*, New York, USA, Russell Sage Foundation, 2001, pp. 40-88.

[58] B. G. Glaser and A. L. Strauss, The Discovery of Grounded Theory: Strategies for Qualitative Research, Chicago, USA: Aldine, 1967.

[59] M. N. Sauders, P. Lewis and A. Thornhill, Research Methods for Business Students, Edinburgh, Scotland: Pearson, 2015.

[60] A. S. Godoy, "Introdução a pesquisa qualitativa e suas possibilidades," *Revista de Administração de Empresas,* pp. 57-63, 1 April 1995.

[61] E. C. Arantes, *O design estratégico da concesão aeroportuaria no Brasil*, Curitiba, Brazil: Pontificia Univesrsidade Católica do Paraná, 2017.

[62] P. Singer and A. Friedman, Cybersecurity and cyber war, Oxford, UK: Oxford University Press, 2013.

[63] L. K. Comfort, A. Boin and C. C. Demchack, Designing resilience: Preparing for Extreme Events, Pittsburgh, USA: Pittsburgh University Press, 2010.

[64] T. L. Friedman, The world is flat: A brief history of the 21st century, New York, USA: Farrar, Straus and Giroux, 2005.

[65] B. A. Turner, Man-made disasters, London, UK: Wykeham Publications, 1978.

[66] International Civil Aviation Organization, *Safety Management Manual*, Montreal, Canada: ICAO, 2018.

[67] R. K. Yin, Estudo de caso. Planejamento e métodos, Porto Alegre, Brazil: ARTMED Editora S.A, 2001.

[68] V. Oliveira, M. Martins and A. Vasconcelos, *Entrevistas em profundidade na pesquisa qualitativa em administração: pistas teóricas e metodológicas.,* São Paulo, Brazil: Simpósio de Administração da Produção, Logística e Operações Internacionais-SIMPOI, 2012.

[69] U. Flick, Introdução à metodologia de pesquisa: um guia para iniciantes., Porto Alegre, Brazil: Penso Editora Ltda, 2009.

[70] A. Chizziotti, Pesquisa qualitativa em ciências humanas e sociais, Petrópolis, Brazil: Editore Vozes, 2006.

[71] L. Bardin, Análise de conteúdo, Lisboa, Portugal: Edições 70, LDA, 2010.

[72] World Economic Forum, "Global Risk Report," WEF, Geneva, Switzerland, 2018.

[73] World Economic Forum, "Global Risks Report," WEF, Geneva, Switzerland, 2021.

[74] Allianz Global Corporate & Specialty, "Allianz Risk Barometer – Top risk business for 2018.," Allianz Global Corporate & Specialty SE, Munich, Germany, 2018.

[75] International Civil Aviation Organization, *Annex 10 - Aeronautical Telecommunications, Volume 3*, Montreal, Canada: ICAO, 2007.

[76] International Civil Aviation Organization, *Draft of the Global Resilient Aviation Network Concept of Operations,* Montreal, Canada: ICAO, 2018.

[77] International Organization for Standardization, *Information technology — Security techniques — Information security management systems — Overview and vocabulary,* Geneva, Switzerland: ISO, 2018.