UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

Resilient architecture to dynamically manage unmanned aerial vehicle networks under attack

Isadora Garcia Ferrão

Dissertação de Mestrado do Programa de Pós-Graduação em Ciências
de Computação e Matemática Computacional (PPG-CMC)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Isadora Garcia Ferrão

Resilient architecture to dynamically manage unmanned aerial vehicle networks under attack

Dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Computer and Mathematical Sciences Graduate Program, for the degree of Master in Science. *FINAL VERSION*

Concentration Area: Computer Science and Computational Mathematics

Advisor: Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco

USP – São Carlos
June 2021

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

G368r Garcia Ferrão, Isadora
Resilient architecture to dynamically manage
unmanned aerial vehicle networks under attack /
Isadora Garcia Ferrão; orientadora Kalinka Regina
Lucas Jaquie Castelo Branco . -- São Carlos, 2021.
139 p.

Dissertação (Mestrado - Programa de Pós-Graduação
em Ciências de Computação e Matemática
Computacional) -- Instituto de Ciências Matemáticas
e de Computação, Universidade de São Paulo, 2021.

1. Unmanned Aerial Vehicle. 2. Security. 3.
Safety. 4. Resilient Architecture. 5. Decision
Making. I. Regina Lucas Jaquie Castelo Branco ,
Kalinka, orient. II. Título.

Isadora Garcia Ferrão

**Arquitetura resiliente para gerenciar dinamicamente redes
de veículos aéreos não tripulados sob ataque**

Dissertação apresentada ao Instituto de Ciências
Matemáticas e de Computação – ICMC-USP,
como parte dos requisitos para obtenção do título
de Mestra em Ciências – Ciências de Computação e
Matemática Computacional. *VERSÃO REVISADA*

Área de Concentração: Ciências de Computação e
Matemática Computacional

Orientadora: Profa. Dra. Kalinka Regina Lucas Jaquie
Castelo Branco

USP – São Carlos
Junho de 2021

ACKNOWLEDGEMENTS

First, I would like to thank my best friend, my greatest supporter, my inexhaustible source of strength, love and affection, my mother. I thank you for everything you have always done for me, without you none of this would have been possible. I also thank my boyfriend, Sherlon Almeida da Silva, you have always been one of my biggest supporters, my source of energy and strength. Words will never express the gratitude I have for everything you've always done for me, thank you.

I would also like to thank all the teachers who contributed to my academic journey, from elementary school to graduate school. My eternal gratitude to all these warriors.

I would like to thank my dear advisor Kalinka Regina Lucas Jaquie Castelo Branco, you are one of the most kind, competent and inspiring people I have ever met. Even before entering graduate school, I already wanted to work with you for your competence, but I was surprised by an example of a wonderful human being. Thank you for the guidance and for everything you have done for me, I admire you too much.

Finally, I would like to thank all friends from USP and friends from the laboratory, you made my afternoons happier, they were essential to keep me on track and achieve my goals.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

“Quando se nasce pobre, ser estudioso é o maior ato de rebeldia contra o sistema - autor desconhecido”

ABSTRACT

FERRÃO, ISADORA GARCIA. **Resilient architecture to dynamically manage unmanned aerial vehicle networks under attack**. 2021. 136 p. Dissertação (Mestrado em Ciências – Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

There is a growing demand for unmanned aerial vehicles (UAV) in the industry since they are being used on a large scale in various fields, such as health, security, military missions, agriculture, etc. These vehicles have the potential to increase productivity and savings. However, the increase in production and use of unmanned aerial vehicles requires improving sound decision-making principles, physical, computational security, and relevant technologies by the computing community. They must continually adapt to carry out missions where they face unpredictable problems. The increase in advanced functionality and the demand for computing capacity exposes these vehicles to different security vulnerabilities. These vulnerabilities are growing not only in number but also in sophistication. Researchers and companies have been developing multidisciplinary methodologies and approaches in recent years, trying to solve the most varied protection and safety problems around unmanned aerial vehicles. As in the past, concerns about unmanned aerial vehicles' safety were with aggressors and hijackers, now with the domain of civilian application and insertion into the network, circumstances have changed. In this context, this dissertation's objective was to advance state-of-the-art through the definition and development of a resilient architecture for unmanned aerial vehicles (STUART - reSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networksundeR atTack) that dynamically manages the network, even when subjected to an attack during a mission, integrating safety and security methods. The architecture is composed of four parts: (1) Anomaly-based detection system, (2) Triage module, (3) Decision-making module, and (4) Resilience module. This dissertation also investigated the incorporation of safety and security as a unified concept in UAV development. The developed architecture was validated by applying specific techniques in each of the parts that compose the architecture. Three tests were performed: one with a real drone and two tests using computer simulation, composed of a base station and a UAV during a vaccine transport mission for COVID-19. The results allow us to conclude that STUART is effective in detecting GPS spoofing. Unlike other architectures found in the literature that focus on specific missions or vulnerabilities, STUART proposes an organizational structure of metrics aggregated for different contexts, ranging from vulnerability detection, filtering false positives, decision-making, and mitigation. Its efficiency has been proven through computational validation using real data from a drone.

Keywords: Unmanned Aerial Vehicle, Security, Safety, Resilient Architecture, Decision Making.

RESUMO

FERRÃO, ISADORA GARCIA. **Arquitetura resiliente para gerenciar dinamicamente redes de veículos aéreos não tripulados sob ataque**. 2021. 136 p. Dissertação (Mestrado em Ciências – Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

Na indústria, há uma crescente demanda por veículos aéreos não tripulados, visto que, eles estão sendo usados em larga escala em vários campos, como saúde, segurança, missões militares, agricultura, etc. Esses veículos possuem potencial para aumentar a produtividade e a economia. No entanto, o aumento da produção e utilização desses veículos exigem o aprimoramento de princípios sólidos de tomada de decisão, segurança física, computacional e tecnologias relevantes pela comunidade de computação, pois eles devem continuamente se adaptar para realizar missões onde enfrentam problemas imprevisíveis. O aumento das funcionalidades avançadas e a demanda por capacidade computacional expõe esses veículos a diferentes vulnerabilidades de segurança. Essas vulnerabilidades estão crescendo não apenas em número, mas também em sofisticação. Como no passado as preocupações com a segurança dos VANTs estavam com agressores e sequestradores, agora com o domínio da aplicação civil e inserção na rede, as circunstâncias mudaram. Neste contexto, o objetivo desta dissertação foi avançar o estado da arte através da definição e desenvolvimento de uma arquitetura resiliente para veículos aéreos não tripulados (STUART - reSilient archiTecture to dynamically manage Unmanned aeriAl vehicle network-sundeR atTack) que gerencie dinamicamente a rede, mesmo quando submetida a um ataque, integrando métodos de segurança computacional e física. A arquitetura é composta por quatro partes: (1) Sistema de detecção baseado em anomalias, (2) Módulo de triagem, (3) Módulo de tomada de decisão e (4) (5) Módulo de Resiliência. Esta dissertação também investigou a incorporação de segurança física e computacional como um conceito unificado no desenvolvimento de UAVs. A arquitetura desenvolvida foi validada aplicando técnicas específicas em cada uma das partes que compõem a arquitetura. Três testes foram realizados: um com um drone real e dois testes por meio de simulação computacional, compostas por uma estação base e um UAV durante uma missão de transporte de vacinas da COVID-19. Os resultados permitem concluir que a STUART é efetiva na detecção de GPS spoofing e diferentemente de outras arquiteturas encontradas na literatura que focam em missões ou vulnerabilidades específicas, a STUART propõe uma estrutura organizacional de métricas que podem ser agregadas para diferentes contextos e vão desde a detecção de vulnerabilidades, filtragem de falsos-positivos, até a tomada de decisão e mitigação. A sua eficiência foi comprovada através da validação computacional utilizando dados reais de um drone.

Palavras-chave: Veículo Aéreo Não Tripulado, Segurança, Proteção, Arquitetura Resiliente, Tomada de decisão.

LIST OF FIGURES

Figure 1 – Types of UAVs	30
Figure 2 – Aircraft models used by MCAP	37
Figure 3 – UCAP Context Diagram.	38
Figure 4 – Reconfigurable flight control system architecture	39
Figure 5 – SOA enabled RFCSA	40
Figure 6 – LARISSA Profile UAS	41
Figure 7 – HAMSTER architecture hierarchical organization overview.	42
Figure 8 – SPHERE conceptual model	44
Figure 9 – SPHERE - Class diagram	45
Figure 10 – SPHERE modelling	45
Figure 11 – HAMSTER abstractions implementation examples	46
Figure 12 – Trivir - visualization system.	57
Figure 13 – Trivir classification.	58
Figure 14 – STUART architecture	62
Figure 15 – STUART activities diagram	64
Figure 16 – DDoS attack in UAVs	68
Figure 17 – STUART Sequence diagram	70
Figure 18 – Route that STUART must take.	75
Figure 19 – Illustration of the GPS Spoofing detection.	76
Figure 20 – OODA cycle.	79
Figure 21 – Resilience - Activities diagram	80
Figure 22 – Route that the UAV must take (using STUART).	85
Figure 23 – GPS spoofing with fake app.	86
Figure 24 – 3DR Solo UAV outfitted with Kodak SP360 cameras to collect 360' imagery for later surveys in the lab using virtual reality glasses	87
Figure 25 – Station HAMSTER	88
Figure 26 – UAV HAMSTER	88
Figure 27 – Solo 3DR connected with the smartphone	89
Figure 28 – (A) True location (B) Fake location	90
Figure 29 – Safe route	93
Figure 30 – False route	97
Figure 31 – Return routes for different safe deltas.	99
Figure 32 – Number of studies found in databases for the first selection.	134

Figure 33 – Proportion of studies accepted in the first selection. 135

Figure 34 – Proportion of studies accepted in the final selection. 136

LIST OF TABLES

Table 1 – The evolution of the UAV market between 2015 and 2020.	25
Table 2 – Classification of UAVs according to DoD, United States.	29
Table 3 – Requirements contemplated by MCAP	38
Table 4 – Requirements fitted by MCAP	40
Table 5 – Categories safety failures	52
Table 6 – Comparative analysis of architectures	56
Table 7 – Seed studies in TRIVIR	58
Table 8 – Cyber resilience goals	65
Table 9 – Comparison between traditional and resilient security architectures	66
Table 10 – STUART objectives	67
Table 11 – DDos attack in STUART	69
Table 12 – Comparative techniques for decision making	78
Table 13 – Scenario of test cases.	85
Table 14 – Scenario 1: Normal operation	91
Table 15 – Scenario 1: Normal operation - Security	91
Table 16 – Scenario 1: Normal operation - Safety	94
Table 17 – Scenario 2: Failure operation	95
Table 18 – Scenario 2: Failed operation - Haversine	96
Table 19 – Scenario 2: Failed operation - Safety	100

LIST OF ABBREVIATIONS AND ACRONYMS

ANAC	<i>Agência Nacional de Aviação</i>
BLOS	Beyond Line-Of-Sight
C4ISR	Reconnaissance, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCE	Container Control Environment
CJamCom	Coordinated interference technique
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSU	Central Security Unit
DDoS	Distributed Denial of Service
DECEA	<i>Departamento de Controle do Espaço Aéreo</i>
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoS	Denial of Service
ERMP	Extended Range Multi Purpose
FAA	Federal Aviation Administration
FCS	Future Combat Systems
GCS	Ground Control Station
GPS	Global Position System
HAMSTER	HeAlthy, Mobility and Security-based data communication archiTectuRe
IDS	Intrusion Detection System
LAN	Local Area Network
LARISSA	Layered Architecture model foR Interconnection of SystemS in UAVs
MCAP	Manned Unmanned Common Architecture Program
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technologies
PVT	Position Speed Time
RPA	<i>Remotely Piloted Aircraft</i>
RPAS	Remotely Piloted Autonomous Systems
RTOS	Real Time Operating Systems
SCE	Safe Control Environment

SLR	Systematic Literature Review
SMS	Systematic Mapping Study
SMU	Security Management Unit
SOA	Service Oriented Architecture
SPHERE	Security and safety Platform for HEteRogeneous systEms
SPMU	Service Provision Management Unit
STUART	reSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks undeR atTack
TCP	Transmission Control Protocol
TTCAN	Timetriggered Controller Area Network
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicles
UCAP	Unmanned Air Vehicle Common Architecture Prototype
UCAR	Unmanned Combat Aircraft Helicopter
UML	Unified Modeling Language
USP	University of São Paulo
VLOS	Visual Line–Of–Sight
VM	Virtual Machine
VTOL	Vertical take–off and Landing

CONTENTS

1	INTRODUCTION	23
1.1	Contextualization	23
1.2	Motivation and problem characterization	25
1.3	Objectives	26
1.4	Text Structure	26
2	UNMANNED AERIAL VEHICLES	27
2.1	Classification	28
2.2	Composition	29
2.3	UAVs applications	30
2.4	Final remarks	33
3	UAVS ARCHITECTURES	35
3.1	Definitions	35
3.2	UAVs Architectures and models	36
3.2.1	<i>HAMSTER – HeAlthy, Mobility and Security based data communi- cation archiTectuRe</i>	41
3.2.2	<i>SPHERE – Security and safety Platform for HEteRogeneous systEms</i>	43
3.2.2.1	<i>SPHERE implementations</i>	44
3.3	Final remarks	46
4	SECONDARY STUDY LISTINGS	49
4.1	Synthesis of Results	50
4.1.1	<i>Security threats and attacks</i>	50
4.1.2	<i>Safety failures in UAVs</i>	51
4.1.3	<i>Architectures for UAVs</i>	52
4.1.3.1	<i>Resilient architectures for UAVs</i>	53
4.1.3.2	<i>Comparative analysis</i>	55
4.2	TRIVIR: A Visualization System to Support Document Retrieval with High Recall	56
4.3	Final remarks	58
5	STUART ARCHITECTURE	61

5.1	STUART: ReSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks undeR atTack	61
5.1.1	<i>STUART composition</i>	61
5.1.2	<i>STUART goals</i>	63
5.1.3	<i>STUART Cyber resilience objectives</i>	65
5.1.4	<i>DDoS attack in STUART</i>	67
5.2	Final remarks	71
6	DESIGN OF THE STUART ARCHITECTURE TO BE RESILIENT AGAINST GPS ATTACKS	73
6.1	Anomaly-based detection system	73
6.2	Haversine	73
6.3	Non-respect of the moving zone	75
6.4	NCI - Node Criticality Index	76
6.5	Triage module	77
6.6	Decision making module	78
6.7	Cyber resilience	79
6.8	Final remarks	81
7	STUART IN A COVID-19 VACCINE TRANSPORT SCENARIO	83
7.1	STUART in a COVID-19 vaccine transport scenario	83
7.1.1	<i>Choice of mission</i>	83
7.1.2	<i>Choice of test cases</i>	84
7.1.3	<i>Choice of aircraft model</i>	85
7.1.4	<i>Implementation test scenario and analysis</i>	86
7.2	Scenario 01: GPS spoofing attack with Fake GPS Location	89
7.3	Scenario 02: Normal operation	91
7.4	Scenario 03: Failure operation	94
7.4.1	<i>Safety failure</i>	100
7.5	Final remarks	101
8	CONCLUSIONS	103
8.1	Intellectual Production	103
8.1.1	<i>Awards</i>	103
8.1.2	<i>Published papers</i>	104
8.1.3	<i>Submitted papers</i>	104
8.1.4	<i>Scientific contributions in other studies (not related to the main context of this dissertation)</i>	104
8.1.4.1	<i>Published magazine</i>	104
8.1.4.2	<i>Published paper</i>	104

8.1.4.3	<i>Submitted papers</i>	104
8.1.5	<i>Participation in events as a guest speaker</i>	105
8.2	Limitations and Difficulties	105
8.3	Contributions	105
8.4	Future works	106
BIBLIOGRAPHY		107
APPENDIX A SYSTEMATIC REVIEW		129
A.1	Planning	129
A.1.1	<i>Review objectives</i>	129
A.1.2	<i>Research Question</i>	129
A.1.3	<i>Search Strategy</i>	130
A.2	Execution	132
A.2.1	<i>Search String</i>	132
A.2.2	<i>Study Selection</i>	133

INTRODUCTION

1.1 Contextualization

As a consequence of advances in the development and miniaturization of communication technology, Unmanned Aerial Vehicles (UAV) are being used on a large scale in various fields, such as health (JORGE *et al.*, 2021; ADWIBOWO, 2021), aerial photography (HODGSON; PIOVAN, 2021; CHEN *et al.*, 2021), agriculture (VERMA; ALI; AGRAWAL, 2021; AYAMGA; TEKINERDOGAN; KASSAHUN, 2021), logistics companies (CHEN; HU; SOLAK, 2021; DOOLE *et al.*, 2021), movies (TAN *et al.*, 2021; MADEMLIS *et al.*, 2019), security (KLAUSER, 2021a; FERRÃO *et al.*, 2020a; ZHANG *et al.*, 2019a), surveillance (SHIN *et al.*, 2021; JUNG; JO; KIM, 2019), military missions (JACKMAN, 2021; CHATURVEDI *et al.*, 2019) etc. In the industry (CHOE; KIM; HWANG, 2021), the growing demand for UAV has the potential to increase productivity and economy, as it can be seen in recent research and reports (DRONEINDUSTRY, 2018; GOLDMAN, 2019; MEOLA, 2017; FROSTSULLIVAN, 2017). However, increasing the production and use of these vehicles require the improvement of solid decision-making principles, security, safety, and relevant technologies by the computing community, as they must continually adapt to face missions subject to unpredictable problems.

This improvement must consider the objective of the mission and the adaptation of the actions. In other words, the maneuvers that the UAV can perform must be adaptable to random events that arise during the mission, aiming to improve autonomy and safety for the aircraft. A failure can compromise the entire mission and, the damage can be dangerous, including the UAV fall and even injuries to human lives.

UAVs face numerous challenges to navigate autonomously in a viable and safe way (ALWATEER; LOKE; ZUCHOWICZ, 2019; HOPPE *et al.*, 2019). According to Usach *et al.* (2018), only Remotely Piloted Autonomous Systems (RPAS) can be integrated with manned aircraft in unsegregated airspace and aerodromes. To fully integrate UAVs into today's airspace, it

is necessary to work on autonomous monitoring and management technologies that are resistant to attacks, so that they provide the necessary security for the aircraft and the environment. In this context, autonomy means dealing with limited resources for processing, storage and high performance computing. However, this attribute is indispensable to guarantee the mission's success.

The increase in advanced functionalities and the demand for computing capacity exposes UAVs to different security vulnerabilities. These vulnerabilities are growing not only in number but also in sophistication (PAGANINI, 2015; HUMPHREY'S, 2012). Failure events caused by these vulnerabilities during a mission pose a serious threat to UAVs and can cause injury or loss of high-value assets. Therefore, safety (physical security) and security (logical security) are some of the main concerns around these vehicles. According to Bloomfield and Lala (2013), these non-functional requirements are increasingly difficult to be met, creating new challenges for these aircraft systems.

In recent years, researchers and companies have been developing multidisciplinary methodologies and approaches, trying to solve the most varied security and safety problems around unmanned aerial vehicles (SHAFIQUE; MEHMOOD; ELHADEF, 2021; GORREPATI; GUNTUR, 2021; FERRÃO *et al.*, 2020a; FERRÃO *et al.*, 2020b; JIANG *et al.*, 2020; SUNG *et al.*, 2020; Franco *et al.*, 2018; PAGE *et al.*, 2019; KUCHAR, 2005). In the past, concerns about UAV safety were related not only with the natural problems of the vehicle but even to attackers and hijackers, now with the domain of civilian application and insertion into the network, circumstances have changed.

In Chen *et al.* (2019), a software structure that offers resilient control to Denial of Service (DoS) attacks for UAV systems in real-time is presented. The attack occurs when there is a denial of service, in which a specific service cannot receive or process further requests. The attacker purposely spawns a large number of requisitions and sends multiple requests to the destination server to make the system unavailable.

Other attacks that pose threats to UAVs are Global Position System (GPS) and communication interference. In Spears *et al.* (2016), it is stated that GPS counterfeiting has been recognized as a serious threat to critical infrastructure applications that depend on the public GPS signal. They say it will take a few years for these technologies to mature enough to impact diminishing commercial defenses against counterfeit GPS attacks. Chen *et al.* (2019) presents a software framework that provides resilient control of DoS attacks for real-time UAV systems.

Concerning missions carried out by UAV, the dissemination of these vehicles favored the formation of collaborative swarms in order to optimize the missions (YOKOYAMA; KIMURA; MOREIRA, 2014). Cooperative applications use the location of UAVs to make decisions. In this sense, there is a risk that an attacker could deceive the system by indicating a false or inaccurate location in order to gain access to restricted resources or engage in malicious activities without being detected. This makes the systems of these aircraft sensitive and dependent on the trust of

the node's geo-temporal information in a swarm.

The certification of these vehicles depends on safety and security issues, in addition to other requirements that must be met as new vehicles are developed. Therefore, there is a clear need to investigate the extent to which current and new safety and security initiatives meet the requirements of unmanned aerial vehicles, and what gaps need to be addressed.

1.2 Motivation and problem characterization

Technological progress in electronic and avionic systems, especially about miniaturization and cost reduction, has boosted academic and economic interest in marketing and studying these aircraft. One of the main motivations of this work is focused on the future growth of the UAV market. Reports and studies foresee an important development in the commercial UAV market in the coming years [Satell \(2021\)](#), [Markets and Markets \(2017\)](#), [Shepardson \(2021\)](#).

[Table 1](#) shows the evolution of the market value of professional UAVs between 2015 and 2020. Exponential growth in the market is also noted in other recent reports, such as [DroneIndustry \(2018\)](#), [Goldman \(2019\)](#), [Meola \(2017\)](#), [Innovation and Skills \(2017\)](#), [FrostSullivan \(2017\)](#). According to [Markets and Markets \(2017\)](#), by 2022 UAVs will represent the largest share in the global market. Therefore, the rapid and growing evolution of the market must be accompanied by cutting edge solutions and with particular attention to the UAV network, thus guaranteeing its safe integration in the airspace.

Table 1 – The evolution of the UAV market between 2015 and 2020.

Domain	The evolution of the market between 2015 and 2020
Education	From \$55 million to more than \$250 million
Savvy consumers ("prosumer")	From \$220 million to more than \$830 million
Civil security	From \$50 million to more than \$210 million
Precision agriculture	From \$200 million to more nearly \$1.2 billion
Media	From \$400 million to more than \$1.3 billion
Distribution	Should reach 120 million dollars
Inspection	Should cross the threshold of one billion euros

Source: Adapted from ([CHRIKI et al., 2019a](#))

Unmanned aerial vehicles can compromise the safety of people and environment, so social and environmental concerns are also motivating factors in this work. In this way, this work aims to advance state of the art by defining and developing an architecture that dynamically manages the network and is resilient to attacks during a mission. In this context, the objective of this dissertation was to advance the state of the art through the definition and development of a resilient architecture for UAV that dynamically manages the network, even when subjected to an attack during a mission, integrating safety and security methods. The architecture consists of four parts: (1) Anomaly-based detection system, (2) Triage module (3) Decision making module, and (4) Resilience module.

1.3 Objectives

The main objective of this work was the definition and development of a resilient architecture for UAVs that dynamically manages the network, even when subjected to an attack during a mission, integrating security and safety methods in an joint way. The investigation of the interaction between safety and security during a UAV mission and, the test scenarios elaboration to validate the architecture are specific objectives of this work.

1.4 Text Structure

The remainder of this text is organized as follows. [Chapter 2](#) describes the theoretical concepts used for the work, which are related to unmanned aerial vehicles and, [Chapter 3](#) describes the concepts of UAV architectures. [Chapter 4](#) presents and discusses the literature review. [Chapter 5](#) presents the results this dissertation. Finally, [Chapter 8](#) presents the conclusions and future work.

UNMANNED AERIAL VEHICLES

This chapter aims to present the main concepts inherent to unmanned aerial vehicles that have been gaining more space in recent years and which is pointed out as a promising topic in the coming years ([PULLETI; GONIA; MAHA SENAN, 2019](#); [MAES; STEPPE, 2019](#)).

Unmanned aerial vehicle is increasingly being used by military forces and civilian applications such as surveillance ([JUNG; JO; KIM, 2019](#)), agriculture ([KIM *et al.*, 2019](#)), aerial photography ([DUAN; HU; SANG, 2019](#)), health ([CHEN *et al.*, 2019](#)), motives ([MADEMLIS *et al.*, 2019](#)), security ([ZHANG *et al.*, 2019a](#)), military missions ([CHATURVEDI *et al.*, 2019](#)), logistics companies ([RAJ; SAH, 2019](#)) etc. An unmanned aerial vehicle is a machine capable of operating without a pilot on board who directly and actively controls the device. Thus, these aircraft have control functions that can be embedded or exist in external systems ([BARNES; FIELDS; VALAVANIS, 2007](#)). Another essential term in this context is Unmanned Aircraft System (UAS) that includes the entire system, which supports the aircraft operation. This name is adopted by the US Federal Aviation Administration (FAA) and by the international academic community not only to describe the physical vehicle, but also the elements associated with its functions, such as payload, control station, communication links and support equipment ([U.S. GAO, 2008](#); [AUSTIN, 2011a](#)).

Although UAVs are associated with state of the art technologies, the first concrete experiments in the use of these vehicles occurred at the time of World War I, where radio-controlled autonomous aircraft were developed. Years later in World War II in 1951, UAVs were built for spy missions. By this time, the United States were experimenting with UAVs equipped with television cameras, capable of carrying out attacks more than 30 kilometers away ([KEANE; CARR, 2013](#)). It was common for the United States to have devices available as UAVs, such as the Bomber military aircraft. In the Vietnam War that took place from November 1, 1955 to April 30, 1975, reconnaissance UAVs were able to photograph large areas of enemy terrain. UAVs were idealized for military purposes, however, their miniaturization has led to the current interest for civilian use ([KNOBLAUCH *et al.*, 2019](#); [HUANG *et al.*, 2019](#); [SUBHAN *et al.*,](#)

2019; RESNIK; ELLIOTT, 2019; KILLE; BATES; LEE, 2019). The civil applications of UAVs will be further discussed throughout this chapter.

2.1 Classification

UAV is a pilot less aircraft that can be controlled remotely or from an on-board system. In this way it is possible to consider two types of UAVs: (1) Remotely Piloted Aircraft System – when it includes an off-board human pilot in the loop to control the flight (COOKE *et al.*, 2016). In this case, the pilot can have a Visual Line-Of-Sight (VLOS) with the aircraft, which means that the pilot can visualize it without auxiliary accessories for all procedures, or can operate the vehicle Beyond Line-Of-Sight (BLOS) with the assistance of specialized equipment, like on-board cameras and; (2) Autonomous aircraft – when it includes an on-board autopilot that allows autonomous flying without the existence of an off-board human pilot.

The Brazil legislation regarding UAVs is established by the *Agência Nacional de Aviação* (ANAC), responsible for regulating and supervising the civil aviation and the *Departamento de Controle do Espaço Aéreo* (DECEA). According to these institutes, it must be possible for the pilot to take control of the aircraft during the entire flight, with the autonomous flight being allowed only during a remote control malfunction (ANAC, 2017; DECEA, 2016). For this reason, in this work an UAV will be also considered a *Remotely Piloted Aircraft* (RPA) and will be treated as a synonym.

UAVs are classified by ANAC and DECEA in three classes, according to the maximum take-off weight, in which the weight of the battery or fuel of the equipment and of the payload eventually transported must be considered:

- Class 1 – Maximum take-off weight greater than 150 kg;
- Class 2 – Maximum take-off weight greater than 25 kg and up to 150 kg;
- Class 3 – Maximum take-off weight up to 25 kg.

It is possible to obtain an experimental flight authorization certificate, each case being specifically analyzed by ANAC.

Although UAVs can also be classified according to different aircraft characteristics, such as size, weight or operation mode, there is no international standard classification. Therefore each country has developed its own classification. An example is the US Department of Defense (DoD), which is based on maximum take-off weight, flight altitude (relative to ground level), and speed, as shown in Table 2.

Table 2 – Classification of UAVs according to DoD, United States.

Group	Maximum take-off weight (kg)	Flight altitude (m)	Speed (m / s)
1	Up to 9.1	Up to 365.8	Up to 51.4
2	From 9.5 to 25	Up to 1066.8	Up to 128.6
3	Up to 598.7	Up to 5486.4	Up to 128.6
4	Greater than 598.7	Up to 5486.4	Varied
5	Greater than 598.7	Greater than 5486.4	Varied

Source: Department of Defense – (DOD, 2011).

Another possible classification is regarding the physical configuration, like fixed-wing aircraft, rotate wing aircraft, Vertical take-off and Landing (VTOL) vehicles, aerostats and flapping-wing aircraft (VALAVANIS; VACHTSEVANOS, 2015).

2.2 Composition

The main UAS components are (AUSTIN, 2011b; FAHLSTROM; GLEASON, 2012):

- **Aircraft** – includes fuselage, wings, tail and other physical structures, propulsion system, flight control and navigation system, communication equipment and electrical power supplies;
- **Payload** – composed by sensors related to the UAV mission or application, which could be small cameras or even complex high-power radar. Sometimes the information from these sensors can be extracted from multiple data and are processed in on-board modules;
- **Control Station** – receives and sends information from and to the aircraft, like telemetry data from sensors and commands to the actuators. It can also be the location where the mission is planned, before and during the flight, and where the support equipment is controlled;
- **Communication Links** – provide means to take control of the aircraft during the mission and allow the monitoring of its condition. The most common mediums are radio frequency and wireless communication, which offers an up-link from the Ground Control Station (GCS) to the vehicle and a down-link from the aircraft to the GCS. It is also possible to have communication links among different vehicles such as in an UAV swarming;
- **Support Equipment** – it can also be needed for the correct operation, e.g. launch, recovery and transportation equipment. This equipment usually stays within the GCS to facilitate its control.

2.3 UAVs applications

The advances in technology capabilities, regulation, and investment allow that UAVs, mainly adopted in military operations such as transportation, intelligence gathering and attacks (Hossein Motlagh; TALEB; AROUK, 2016), be also used in civilian applications. To meet the growing demand and the needs of each audience, the UAV market has several types of UAVs that have different functionalities so that each one can adapt to a specific requirement. Figure 1 illustrates some of the most popular types of UAVs found in civilian applications.

Figure 1 – Types of UAVs

Source: The author.

Each application has different needs, types of features, and equipment, UAVs can also reduce human exposure to prolonged, monotonous, dirty, or hazardous tasks, as well as provide potential financial savings and environmental benefits such as reduced fuel consumption (ELLIOTT *et al.*, 2019; PENNY *et al.*, 2019).

In agriculture, UAVs are being used for crop supervision (MATEO-AROCA *et al.*, 2019), soil, and field analysis (NUIJTEN; KOOISTRA; DEYN, 2019), spraying (HOGGENMUELLER *et al.*, 2019), among others. Formerly used satellite images that are expensive and inaccurate

today, can be replaced by high definition pictures obtained by UAVs. This technology offers a variety of crop monitoring possibilities at a lower cost and with higher quality. UAVs are also capable of accurately producing 3D maps, allowing initial soil analysis, which can be used to plan seed planting patterns. Besides, the analysis provides data for irrigation and nitrogen level management.

UAVs with hyperspectral, multispectral, or thermal sensors can identify exactly which parts of a field are missing or which need improvement (TORRES-RUA *et al.*, 2019). Also, once the crop is growing, the UAVs allow the vegetation index calculation, and others. UAV monitoring helps to assess plant health, and to detect bacterial or fungal infections in trees.

In the safety area, UAVs are widely used for surveillance in fields that need to be inspected regularly (CHOWDHURY *et al.*, 2019; SAVKIN; HUANG, 2019; HENRIO *et al.*, 2019), requiring them to be solid to operate in different weather situations and at night. In border monitoring, fixed-wing UAVs are used for highway, coastal, and boundary surveillance (ISLAM; RAZI, 2019; ABUSHAHMA *et al.*, 2019). They can help in cases of illegal border crossings (GELDENHUYS, 2019), wildlife trafficking (HAMBRECHT *et al.*, 2019) or smuggling (FILIPPOV, 2019). UAVs provide live streaming of detailed data, track objects, or intruders at a safe distance, and quickly cover a wide area (SRINIVASAN; VIJAYAKUMAR; MAKUR, 2019).

UAVs are increasingly used in the media and entertainment industry (KHOO, 2019). They are widely used in photography (CHENG, 2015), aerial filming (STANKOV *et al.*, 2019), news broadcasting at sporting events, and documentaries (PAVLIK, 2019), as well as being less expensive compared to helicopters and airplanes. They are also equipped with 4K cameras and can approach unique angles and special effects (HIGGINS; BARNETT, 2019; DELMERICO *et al.*, 2019). UAVs can serve as flying pixels performing light shows or being used in theater performances to control large statues or puppets (YOON, 2015).

In the health sector, UAVs are being used by pharmaceutical companies to distribute medicines (GATTESCHI *et al.*, 2015), vaccines in areas of difficult access (HAIDARI *et al.*, 2016), and medical equipment (CLAESSON *et al.*, 2016).

One of the beneficial factors of using UAVs to transport medicines is the cost of the trip because it tends to be lower when compared to an ambulance since it does not need fuel and does not suffer from maintenance and depreciation values of a car. Another beneficial factor is that the UAV has no worries about car flows to deliver medication, unlike an ambulance. This type of aircraft is also useful in rescuing drowned swimmers in the oceans, in addition to locating unconscious victims in sub-zero climatic conditions and people lost in fields, rivers, and mountains (SHEKARI, 2018; CLASESSON, 2018; GOTO, 2014). In 2018, there was the first case of rescue using a UAV in Australia (BBC, 2018). The episode took place on Lennox Head, a beach popular among surfers in South of Brisbane. Initially, it was UAV training in drowning events, however, it became a real rescue when someone realized that two men swimming outside the security perimeter were drowning. Lifeguards operated the equipment.

The UAV was responsible for launching a buoy for bathers to float until the boat arrived.

The list of UAV's civilian application is numerous and not limited to:

- Health (KUNOVJANEK; WANKMÜLLER, 2021; AVTAR *et al.*, 2020; CHEN *et al.*, 2019);
- Film (URIBE-MONTESDEOCA *et al.*, 2021; KIRKLAND, 2020; MADEMLIS *et al.*, 2019);
- Security (LEPPÄVIITA, 2021; WANG; CHENG, 2020; ZHANG *et al.*, 2019a);
- Aerial photography (ROCKE; RUFFELL; DONNELLY, 2021; OBANAWA; SHIBATA, 2020; DUAN; HU; SANG, 2019);
- Surveillance (YI; SUTRISNA, 2021; CAMPOS *et al.*, 2020; JUNG; JO; KIM, 2019);
- Military missions (KO *et al.*, 2021; ZHOU *et al.*, 2020; CHATURVEDI *et al.*, 2019);
- Agriculture (AYAMGA; TEKINERDOGAN; KASSAHUN, 2021; MEINEN; ROBINSON, 2020; KIM *et al.*, 2019);
- Search and rescue and policing (KLAUSER, 2021b; FOTOHI; NAZEMI, 2020; EICK, 2019);
- Disaster-response scenarios (COBAR *et al.*, 2021; THUY; WATANABE; WAKUTSU, 2020; SÁNCHEZ-GARCÍA; REINA; TORAL, 2019);
- Logistics companies (GABANI *et al.*, 2021; HERNÁNDEZ; MARTÍNEZ; SAUCEDO, 2020; RAJ; SAH, 2019).

Due to their numerous applications, UAVs will most likely be a part of our daily lives, but not without challenges. One of them is how to insert UAVs into shared airspace. UAVs must be supervised so their flying path and communication do not affect current air traffic. A collision avoidance mechanism is also necessary for a secure, safe and seamless UAV operation in the airspace (Hossein Motlagh; TALEB; AROUK, 2016).

Communication is very important for UAV applications (BEKMEZCI; SAHINGOZ; TEMEL, 2013). Another important challenge is how to ensure UAV security and safety as well as people's privacy and safety is crucial for a wide adoption of UAVs by the society (KIM; JO; SHRESTHA, 2014; Hossein Motlagh; TALEB; AROUK, 2016).

2.4 Final remarks

In this chapter, the main concepts, classifications, compositions, and applications of an unmanned aerial vehicle necessary for understanding the rest of this work. Once the concepts are defined, in the next chapter, some definitions and examples of models and architectures for UAVs will be presented.

UAVS ARCHITECTURES

As mentioned in [Chapter 2](#), there is still no global regulation that establishes a standard for the classification of Unmanned Aerial Vehicles, even less standardization for the components that compose UAVs. One of the main problem with the lack of uniformity among these vehicles is the reuse of hardware and software components. Manufacturers design and develop vehicle components on a different basis, requiring certification for each new component produced. An architectural model that guides standardization is one of the possible solutions for this problem. However, until the end of the writing of this dissertation, there is still no global standardization.

This chapter aims to detail what is an architectural model for UAV and to present examples of architectures already developed, as well as their components and operation.

3.1 Definitions

A model is a representation of abstractions from which the properties of instances can be rationally evaluated. Any model should allow to describe the set of all possible instances of the corresponding modeled concept ([GIUNCHIGLIA; WALSH, 1992](#)).

On the other hand, a reference model is not directly related to any standard, technology, or concrete implementation detail. Reference models are considered abstract frameworks where the objective is domain modeling, representing the relationship between domain entities. These models can be conceptual into ontologies ([BASS; CLEMENTS; KAZMAN, 2003a](#); [NAKAGAWA; BARBOSA; MALDONADO, 2009](#); [NAKAGAWA; OQUENDO; MALDONADO, 2014](#))

Software architecture is a structure that identifies, defines and organizes components. The relationship and design principles of the components, functions and interfaces established between subsystems can also be defined by an architecture ([GRANT, 2005](#)). On the other hand, a reference model for an architecture is an architecture where the entities, relationships and information units involved in the interactions between and within the subsystems and components

are defined and modeled. In summary, a model incorporates the basic objective or idea of the system and it can be considered as a reference for several purposes (JUN *et al.*, 2009; REGLI *et al.*, 2009). The term architectural model used in this work reflects exactly this last statement: to incorporate the basic objective and ideas of the system.

The terms architectural styles and reference architecture are also usually used interchangeably (MENDES, 2002). However, some authors such as Eickelmann and Richardson (1996) claim that the reference architecture can be seen as a structure that provides a characterization of the functionalities of the software systems of a given application domain.

Reference architectures exist for several application domains, such as: performance evaluation (BARBER; HOLT; BAKER, 2002), avionics (BATORY *et al.*, 1995), UAS (Marconato *et al.*, 2014), test environments (EICKELMANN; RICHARDSON, 1996), distributed applications (SANDKUHL; MESSER, 2000), reference architecture for electronic commerce systems (BASS; CLEMENTS; KAZMAN, 2003b) etc.

3.2 UAVs Architectures and models

Different models and architectures have been designed over the years for aerial vehicles. Although there is still no global standardization, there are models and architectures that serve as a reference. Based on this, this section presents some examples of models and architectures that serve as a reference for the design of architectural components.

A reference model to specify military rules uses and commands intuitively to a human commander has been proposed by the National Institute of Standards and Technologies (NIST) (NIST, 2002). The architecture proposed by NIST focuses on a low level of abstraction, where the layers specify what the components in a UAS should do. In Pastor, Lopez and Royo (2006) an architecture is proposed for UAS, where a Local Area Network (LAN) is used to perform the integration of the components. The architecture designers affirm the architecture facilitates the connection between the hardware components, according to the mission's need, thus being able to couple and uncouple sensors, cameras, and other devices that are necessary for the mission success.

In Wu, Ling and Dong (2009), the Timetriggered Controller Area Network (TTCAN) model is proposed. TTCAN is a protocol model for use between flight control application levels and communication levels. This model does not cover the entire architecture of a UAS. Still, it demonstrates that the division into layers and the specification of protocols help in the development of new interconnection proposals between the systems that compose the UAS.

Another architecture for UAVs is proposed in Olson and Burns (2005), called Manned Unmanned Common Architecture Program (MCAP). The US army uses MCAP in Future Combat Systems (FCS), and Reconnaissance, Command, Control, Communications, Computers,

Intelligence, Surveillance, and Reconnaissance (C4ISR). MCAP is based on electronic components, Commercial Off The Shelf (COTS), and open standards interfaces. This architecture had as its initial objective to define an architecture capable of supporting series of UAVs platforms of the American army.

The development of the MCAP included the study of three classes of UAVs: UCAR, MALE, and Extended Range / Extended Range Multi Purpose (ERMP), with aircraft being: the Unmanned Combat Aircraft Helicopter (UCAR), the Shadow 200 (FCS Class III), the Fire Scout and A-160. The classes of aircraft used, as well as the attributes studied, are illustrated in Figure 2.

Figure 2 – Aircraft models used by MCAP

<p>UCAR</p> <ul style="list-style-type: none"> Organic to UE Provided to UA for specific missions Capable of cooperative teaming with manned aircraft (MUM Ops) Mobile Strike, Close <p>Combat, BDA, Armed Recce, and Security are all expected missions</p> <ul style="list-style-type: none"> Controlled from ground, helos, A2C2S, and Mobile C3 via TCDL 	<p>Fire Scout (Class IV)</p> <ul style="list-style-type: none"> Assigned to the UA EO/IR/laser SAR/MTI Comm relay when JTRS is fitted <ul style="list-style-type: none"> Current UA O&O shows unarmed, but demos with multiple weapons are in process Controlled from ground, helos, A2C2S, and Mobile C³ via TCDL Selected by FCS as initial Class IV vehicle
<p>Shadow 200 (Class III)</p> <ul style="list-style-type: none"> In full rate production EO/IR sensors Comm Relay ConOps being <p>refined in real ops with Stryker Brigades today, in Iraq</p> <ul style="list-style-type: none"> Expected to be assigned to FCS UA Most space, weight, and power constrained Unarmed missions only today Can do limited Met survey Could drop small emergency logistics payloads 	<p>A-160 (ER/MP)</p> <ul style="list-style-type: none"> Self-deployable within the theater of operations (> 2000nmi range) Long endurance (> 24 hours) making it ideal for missions requiring persistence (i.e. Comms Relay, Surveillance) Normally assigned to UE Has capacity to insert other uninhabited vehicles (air or ground) Can also be used to deploy unattended sensors

Source: (OLSON; BURNS, 2005)

The definitions of the Department of Defense Architecture Framework (DoDAF) were used to generate various patterns of operations to be performed by the Unmanned Air Vehicle Common Architecture Prototype (UCAP) – UAV Prototype with Common Architecture. Figure 3 shows an example of a context diagram for the MCAP III mission processor system, where the circle represents the mission processor. The content of each rectangle is a representative example of possible subsystems, such as data communication links, flight sensors, weapons, and payload sensors (radars, cameras etc).

According to the authors, the MCAP architecture is simple and applicable to all UAVs

Figure 3 – UCAP Context Diagram.

Source: (OLSON; BURNS, 2005)

listed in the project. Laboratory tests were conducted with the objective of validating the ability of the mission processor architecture and the infrastructure for future services that include the four UAVs (UCAR, Shadow 200, Fire Scout, and A-160). Shadow 200 was chosen as the platform for testing. A reconnaissance mission was selected, comprising: automated route surveillance, a region of interest, and autonomous precaution against an intruder (evasive maneuver). This test allowed the authors to conclude that the project developed with architecture reduces costs, and guarantees interoperability. However, it was limited to demonstrate its use and functionality only on the mission processor. Tests in laboratory were performed only on one type of UAV. Table 3 shows the requirements fitted by the proposal (OLSON; BURNS, 2005).

Table 3 – Requirements contemplated by MCAP

Layer/Requirement	Contemplation
Monitoring and control	Partially
Navigation and services	Partially
Mission	Completely

Source: Adapted from (MARCONATO, 2014).

In Deng, Ma and Zhu (2012), a reconfigurable architecture for flight control systems is proposed, called RFCSA. The RFCSA architecture is composed by a series of models that meet five requirements:

- Interface between simple and unified modules, where the functional module must be easy to be added, removed or replaced for specific applications;

- Easy design for high-level applications, where there is a low level of need to implement details, and allows the user to develop senior applications easily;
- Hardware and Software reuse, where the hardware and software designed for an application can be ported to another without the need of significant modifications;
- Low cost, where the product must be cheap, expanding the market for small UAVs;
- Reliable, where hardware and software must be easy to develop and verify.

All modules are connected via the module interface. The module interface is unified. The model is illustrated in Figure 4, where each specific module (Processor, Sensor, Actuator, GPS, INS, Communication, and Energy) has an interface that allows its interconnection with the others.

Figure 4 – Reconfigurable flight control system architecture

Source: (DENG; MA; ZHU, 2012).

The methodology used by the authors to solve module coordination problems is Service Oriented Architecture (SOA) (KOMODA, 2006; HURWITZ *et al.*, 2009). SOA concept allows interoperability, sharing, and reuse. The system becomes more flexible, and new features can be easily integrated according to the user's needs. In this software architecture model, the

Figure 5 – SOA enabled RFCSA

Source: (DENG; MA; ZHU, 2012).

application, which runs on the processor module, sends service requests to the service Modules, as shown in Figure 5.

Finally, the requirements fitted by this architecture are presented in Table 4.

Table 4 – Requirements fitted by MCAP

Layer/Requirement	Contemplation
Air segment physics	Partially
System abstraction	Partially
Monitoring and control	Partially
Navigation and services	Partially
Mission	Partially

Source: Adapted from (MARCONATO, 2014).

Another example of architecture is Layered Architecture model for Interconnection of Systems in UAVs (LARISSA), where the components were defined based on the composition of the results from a systematic review and the comparison between different existing architectures in the literature in aerial segments, terrestrial and abstraction layer. LARISSA is divided into physical layers in the aerial part, distributed in Real Time Operating Systems (RTOS), monitoring,

and control, navigation, and mission layer. The terrestrial was divided into a physical layer and a terrestrial control station. Layered separation allows the architectural system to be divided into subsystems that may have different implementations and separate the parts that make up a complex critical embedded system at varying criticality levels. LARISSA was specified in Unified Modeling Language (UML) in the form of profiles. The layers were represented by a package, with the initial package being UAS, which is represented in the Figure 6.

Figure 6 – LARISSA Profile UAS

Source: (Marconato *et al.*, 2014).

According to Marconato *et al.* (2014), LARISSA is structured in layers, it differs from the others through low criticality, a separate configuration of the environment, improved reusability, a higher level of abstraction and interoperability, more interactive interfaces between devices and information systems.

The architecture HeAlthy, Mobility and Security-based data communication archiTecture (HAMSTER) is best suited to this dissertation's context, so it will be described in detail in the next section.

3.2.1 HAMSTER – HeAlthy, Mobility and Security based data communication archiTecture

HAMSTER is a data communication architecture designed for improving mobility, security and safety of the overall system (PIGATTO, 2017; PIGATTO *et al.*, 2016). Figure 7

presents an overview of the hierarchical organization of HAMSTER.

The HAMSTER is divided into three categories: (1) Flying HAMSTER for air vehicles, (2) Swimming HAMSTER for water vehicles, and (3) Running HAMSTER for land vehicles.

- **Flying HAMSTER:** is dedicated exclusively to air vehicles, focusing on issues of internal aircraft communication, communication between aircraft, and communication between aircraft and infrastructure;
- **Swimming HAMSTER:** was designed to deal with the aquatic vehicle segment, addressing internal communication, communication between aquatic vehicles, and also the communication of the aquatic vehicle with the infrastructure;
- **Running HAMSTER:** is dedicated to ground vehicles and addresses the issues of internal communication of ground vehicles, communication between ground vehicles, and also the vehicle with the infrastructure.

Figure 7 – HAMSTER architecture hierarchical organization overview.

Source: (PIGATTO, 2017)

HAMSTER integrates four platforms: (1) Nimble, (2) NCI, (3) NP, and (4) SPHERE.

- **Nimble** platform handles the external communication of vehicles through the use of two modules, ADHOC, and INFRA. ADHOC handles the communication among vehicles. INFRA is responsible for managing communication among vehicles, and infrastructure.
- **NCI** platform is responsible for determining the priority of nodes in the network through an index, thus guaranteeing the quality of service, safety, and security for the nodes that compose the network.
- **NP** platform is used to manage the navigation phases. It controls the state permissions and transmission rates for each of the vehicle's modules during a mission to reduce vehicle energy consumption.
- **SPHERE** platform is focused on architectural security and safety issues ([PIGATTO et al., 2015](#)). This work will cooperate with this platform. Therefore, the next section is dedicated to SPHERE details.

3.2.2 **SPHERE – Security and safety Platform for HEteRogeneous systEms**

Security and safety Platform for HEteRogeneous systEms (SPHERE) is HAMSTER's safety and security platform. Unmanned vehicles have different peripherals and modules, so they require different levels of safety, thus leading to the need to classify modules according to their importance and criticality. According to [Pigatto et al. \(2015\)](#), categorization is done in modules called primary and secondary. Primary modules have the crucial components for the aircraft to fly, to be aware of its location and to be able to make an emergency landing safely. Examples of these modules are:

- GPS receiver;
- Autopilot;
- Flight plan;
- Radar;
- Lighting and signaling;
- Barometric unit.

Secondary modules are responsible for functions considered as not critical, such as abnormal behavior in secondary actuators. For example, cameras, image processing, internet access, sprayers, among others. SPHERE is implemented by three modules: (1) CSU, (2) SMU, and (3) SPMU. as illustrated in [Figure 8](#).

Figure 8 – SPHERE conceptual model

Source: (RODRIGUES; BRANCO, 2020)

- **Central Security Unit (CSU):** is responsible for the authentication and confidentiality mechanisms of the transmitted data. It classifies the modules according to their importance for operation, assigning the appropriate security mechanisms for the applications to carry out the missions.
- **Service Provision Management Unit (SPMU):** is responsible for managing the registration, discovery, and forecasting of services, considering the security policies of sensitivity, and data trust between devices.
- **Security Management Unit (SMU):** is responsible for monitoring the integrity of the modules. It is responsible for detecting anomalies in behavior or failures and also for general control of vehicle safety. For example, if the monitoring of any part signals failure, SPHERE isolates it from other nodes in terms of communication, improving the security of the system.

Figure 9 shows the SPHERE class diagram. HAMSTER classes are not included in the diagram for better readability.

The insertion of an architecture within the SPHERE involves several challenging aspects. First, to include and validate safety, security modules, and metrics, simulation tests are required. To provide a broader validation, security threats situations must also be inserted into the simulation environment.

3.2.2.1 SPHERE implementations

According to (RODRIGUES; BRANCO, 2020), each of the HAMSTER platforms is divided into entities and objects. With that, each platform has different implementations. The implementation of the SPHERE units is illustrated in Figure 10.

Figure 9 – SPHERE - Class diagram

Source: Qualification: Mariana Rodrigues,

Figure 10 – SPHERE modelling

Source: [Rodrigues and Branco \(2020\)](#)

SPHERE Local implements HAMSTER objects through their respective modules. The

In scenarios where units must be centralized, HAMSTER super units are used. Super SPHERE contains both security and information scenarios for the service performed. The Super CSU manages the communications carried out between the entities, and the SMU provides a safety assessment. Finally, SEMU deals with the service announcement and general management of the system. Figure 11 brings a general view of HAMSTER abstractions and possible examples for each.

Figure 11 – HAMSTER abstractions implementation examples

Source: **Rodrigues and Branco (2020)**

3.3 Final remarks

In this chapter, definitions, and examples of architectures, architectural models, and reference models were presented. As it can be seen throughout the chapter, although there are several models and architectures in the literature, none of them contemplates all the requirements for making a generic UAS, that is, all focus on the definition and development of specific UASs or UAVs. In the same way, none of the architectures presents the resilient concept. Once

the concepts of Unmanned Aerial Vehicles are defined and also examples of architectures, architectural models, and reference models, the next chapter will present the literature review.

SECONDARY STUDY LISTINGS

Unmanned aerial vehicles need to be autonomous and safe, as damage can result in serious irregularities, such as: total or partial mission impairment, aircraft destruction, and even injuries to human lives. This autonomy requires to make a decision about what actions are most appropriate during a mission, aiming at ensure the aircraft safety and security, and also the mission accomplishment, even when random events occur ([ALWATEER; LOKE; ZUCHOWICZ, 2019](#); [HOPPE *et al.*, 2019](#)). According to this, the main motivation for preparing this chapter was to conduct a literature review to identify gaps in Safety and Security on UAVs and their architectures.

A Systematic Literature Review (SLR) and Systematic Mapping Study (SMS) aims to identify, analyze, and interpret all available evidence regarding a particular research question in an unbiased and repeatable manner. Through this technique, it is possible to summarize possible proof of a technology, identify gaps to suggest areas that should be investigated, clarify the state of the art for the positioning of new research, and to examine empirical results that prove or refute a given theoretical hypothesis, or that assist in the creation of new hypotheses ([KITCHENHAM; CHARTERS, 2007](#)).

The systematic or mapping review process presented in this chapter was carried out with the collaboration of the on-line tool Parsifal. Parsifal provides all necessary support to execute the systematic or mapping review protocol in a formalized, stepped way, including review objectives, research questions, keywords, synonyms, inclusion, and exclusion criteria, data extraction, among others ([KITCHENHAM; CHARTERS, 2007](#); [BIOLCHINI *et al.*, 2007](#)).

In [Appendix A](#) the systematic review protocol and the most relevant aspects of the study are presented. *Planning*, in which objectives and sources are set, as well as the selection criteria; *Execution*, in which the studies are taken from sources and verified; and *Analysis*, in which results are summarized and conclusions drawn. The phases of a systematic review are discussed in more detail ([DENYER; TRANFIELD, 2009](#)).

In this chapter are presented the result of the last step of the Systematic Review.

4.1 Synthesis of Results

In this systematic review no work precisely like this proposal has been found. The results and synthesis of the data found in the literature review process are presented in the next section.

4.1.1 Security threats and attacks

The main attacks to UAVs observed in the literature were GPS and communication interference (FOUDA, 2018; MAXWELL; BENNETT; KORPELA, 2016; RUTKIN, 2013). Communication interference is described as purposely guiding electromagnetic energy toward a communication system to destabilize or disable signal transmission (GRAHAM, 2011). Failures such as destabilization of communication signals and GPS lead to mission compromise and even destruction of the vehicle after a fall.

Interference methods, such as coordinated interference, are efficient in deteriorating transmission signals. In Wang *et al.* (2015), a communication scenario is investigated in which a communication system injects interference to interrupt enemy user transmissions, while friendly users maintain reliable communications. For this, a Coordinated interference technique (CJamCom) was developed using an MC-CDMA communication architecture. This technique is based on an MMSE linear multi-user detection algorithm. By estimating the interference covariance matrix and CJamCom's multiuser blind detection technique, friendly users were able to obtain reliable communications, while the transmission performance of enemy users was significantly reduced.

In Humphreys *et al.* (2008), the researchers demonstrated that a cheap portable software-defined GPS Location Spoofer could be built from ready-to-use components, highlighting the threat of counterfeiting. GPS spoofing is the act of producing a fake version of the GPS signal to take control of a GPS receiver's Position Speed Time (PVT) solution (SHEPARD *et al.*, 2012). In the case of military signals this type of attack is more difficult to occur because the signal is encrypted, however the civilian GPS signal, on the other hand, is considered public and easily predictable because it is not encrypted (SPEARS *et al.*, 2016).

In Spears *et al.* (2016), the authors claim that GPS counterfeiting has been recognized as a severe threat to many critical infrastructure applications that rely heavily on the public GPS signal. Also, they said there is a complete absence of any commercial defense against a GPS counterfeiting attack.

In summary, there are many studies related to GPS and signal interference and addressing different issues in the area. The contributions of these works will be necessary for the construction of this project, as some of the mentioned problems will be taken into account in the proposed

and developed architecture.

Only one work from these (FRANCO; BRANCO, 2017) is concerned with safety and security aspects together. One of the concerns in the design and development of UAV systems has been to ensure safety requirements. However, since these vehicles communicate with external entities, some architectures that were designed to provide safety requirements can present security vulnerabilities. Because of the identified gap, the architecture developed in this dissertation proposes to investigate the interaction between safety and security as a unified concept in the development of UAVs.

4.1.2 Safety failures in UAVs

Safety failures can be driven by different parts such:

- Sensors (MEI, 2021; ZHONG *et al.*, 2019);
- Sonar (MISNAN; ARSHAD; RAZAK, 2012);
- IMU (SAHAWNEH; JARRAH, 2008);
- Laser (VASCONCELOS *et al.*, 2010);
- Motor (POURPANAH *et al.*, 2018);
- Accelerometer (YOUN *et al.*, 2020);
- GPS (WARREN *et al.*, 2018);
- Beat on trees Wang *et al.* (2020), among others.

The main categories found in the literature regarding safety failures are: damages due to calculation errors, detection of sensor failures, obstacle deviation, directed attacks and accidental damage.

- **Damage due to calculation errors:** This case may occur when a UAV's mission ends up being more dangerous than planned. In 2020 in the UK, a group activity that was performing a campaign against building a third lane at Heathrow Airport piloted hundreds of UAVs within the 3-mile depletion zone to interrupt the flights. The group had no principle hurting any pedestrian, but a simple calculation error could have been catastrophic (GUARDIAN, 2020).
- **Sensor failures:** The UAV sensors do not easily detect delicate objects such as wires, tree branches, and transparent surfaces such as buildings windows. Falls by collisions with these types of items are very common or for excess of pilot trust or not even notify the obstacle's presence.

- **Obstacle deviation:** Devices of obstacles deviation are widely cited in the literature, from the deviation of buildings to trees.
- **Directed attacks:** The targeted attacks occur to cause harm to people, whether for personal or ideological reasons. In this type of attack, the UAVs with leisure are the most commonly used. Or targeted attacks to steal something that the UAV is carrying, such as an organ, food, or vaccines.
- **Accidental damage:** Accidental damage can occur when a UAV gets out of control. The cause may be the legitimate loss of control by an owner, failure of control by cyber criminalizing, or malfunction of the device hardware. Whatever the reason, a UAV falling from heaven and reaching a person will cause damage - and the bigger the UAV, the greater the damage.

Table 5 summarizes the main categories found and some studies that fall into these categories. This will be further discussed in Chapter 5.

Table 5 – Categories safety failures

Category	Studies
Damages due to calculation errors	(GUARDIAN, 2020; LASZLO; AGOSTON; XU, 2018) (HONG <i>et al.</i> , 2015; CHOWDHARY <i>et al.</i> , 2013)
Detection of sensor failures	(SCHIJNDEL; SUN; VISSER, 2021; IWASZENKO <i>et al.</i> , 2021) (MAGSINO; SAY; TAN, 2020) (WANG <i>et al.</i> , 2020; ALEMAYEHU; KIM; YOON, 2020)
Obstacle deviation	(ZAMMIT; KAMPEN, 2021; YAOMING <i>et al.</i> , 2021) (WAHID <i>et al.</i> , 2021; REN <i>et al.</i> , 2021) (BACK <i>et al.</i> , 2020)
Directed attacks	(ZHANG <i>et al.</i> , 2021; RONG-XIAO <i>et al.</i> , 2020) (HUANG <i>et al.</i> , 2020b)
Accidental damage	(KELLY, 2021; KOH <i>et al.</i> , 2018) (RUSSELL; GOUBRAN; KWAMENA, 2019)

Source: The author.

4.1.3 Architectures for UAVs

Although there are several models and architectures in the open literature, none of the models found contemplates all the requirements for making a generic and safe UAV. Most of the architectures focus on the definition and development of specific UAS or UAVs (MONDAL *et al.*, 2020; ULLAH *et al.*, 2019; ZHANG *et al.*, 2019b; HOANG *et al.*, 2019; CHRIKI *et al.*, 2019c; EMEL'YANOV *et al.*, 2016; XIONG *et al.*, 2016; SAYYED *et al.*, 2015; DENG; MA; ZHU, 2012; OLSON; BURNS, 2005; Marconato *et al.*, 2014).

4.1.3.1 Resilient architectures for UAVs

The focus of this work relies on resilient architectures taking into account that the *resilient* attribute is relevant to maintain the operation level of a stabilized UAV, even in the case of successful exploration (CHEN *et al.*, 2019; ORDOUKHANIAN; MADNI, 2019; KONG *et al.*, 2018; YOON *et al.*, 2017; ORDOUKHANIAN; MADNI, 2016; VEGA *et al.*, 2015).

Resilience in the field of engineering derives from the resilience of materials science and is characterized by the material's ability to return to its original state after deformation. In the figurative sense, it means the "ability to adapt or recover" (LEOBONS, 2017).

In Petit *et al.* (2015) the authors present several attacks on UAV, including sensors, LIDAR, and cameras. These results motivated research efforts to study the problems of intrusion detection (MITCHELL; CHEN, 2014), and attack countermeasures (YONG; ZHU; FRAZZOLI, 2015; PAJIC *et al.*, 2014; FAWZI; TABUADA; DIGGAVI, 2014). The threats to these vehicles systems are growing not only in number but also in sophistication, as demonstrated by recent attacks (PAGANINI, 2015; HUMPHREY'S, 2012). Consequently, it becomes necessary to think about security alternatives to help integrate a UAV into the airspace in a safe way.

The authors Kong *et al.* (2018) address the improvement of system resilience to emerging attacks in the controlled environment, such as sensor attacks. Consequently, the authors developed a procedure called checkpoint and recovery, using historical data to recover the failed system states. First, they proposed a new concept of physical state recovery, presented as advancing the system to the current time, starting from a consistent historical physical state to match the values of the internal elements to the states. After that, a checkpoint protocol was designed to record system states for recovery. The protocol employs a sliding window that accommodates the detection delay to improve the correction of stored states. If no failure occurs, a checkpoint is considered correct and, therefore, a trusted state. The inspection is then stored and used for possible future retrievals. The protocol stipulates that detection is performed before saving system states. This characteristic improved the correction of checkpoints and therefore brought good results for the recovery likelihood. However, this work's results were evaluated only in a simulator environment, with no real data or concrete implementations of an avionic architecture being used.

In Yoon *et al.* (2017), authors proposed a framework aimed at achieving resilient control of the unmanned aircraft system against cyber attacks, even presenting security vulnerabilities. Two control environments were used: the user control with advanced features and the security control, including only a limited set of features. Usually, a framework manages the inbound and outbound operations, monitors the security detection and threat protection and, ultimately, the recovery or physical control when an incident occurs. The secure control environment has been added to a security monitoring module that checks the system physical and logical states. As soon as a threat is detected, the secure control environment takes control of the UAV and limits

its operations until corrective actions take place. To select normal and safe control environments, a built-in processor that features hardware-assisted virtualization technology is used. Sensor, actuator, and communicator virtualization have been introduced to protect against potential threats to integrity and availability by abstracting low-level details and controlling access.

The results demonstrated that the framework provides an integrated way to address multiple security threats that require potentially conflicting requirements. Nevertheless, one structure still presents challenges for practical use as the tests were performed with an autopilot and typical controllers for safety purposes only. Ideally, run selected control software from Safe Control Environment (SCE) and implement a high-security driver. The high latency introduced by the virtual machine makes it impossible to import more resource control in real-time. Besides, a structure cannot handle complex manipulations on sensors, such as a fake GPS.

Likewise, [Chen et al. \(2019\)](#) presented the ContainerDrone framework that proposes resilient control of DoS attacks for real-time UAV systems using containers. Container technology is an open source and offers software isolation ([PREETH et al., 2015](#); [MERKEL, 2014](#)), and abstraction of many features in the Linux kernel. System isolation using containers leads to less execution overhead, less memory usage, and less footprint. When compared to Virtual Machine (VM), containers have advantages in lightness issues ([CHEN et al., 2019](#)) because they share the host kernel while the virtual machine needs a hypervisor to communicate with the kernel. In terms of efficiency, the container is about tens of MB, while a VM easily exceeds GB. ContainerDrone provides support mechanisms for three system resources, namely the Central Processing Unit (CPU), communication channel, memory, and also offers resilient control to DoS attacks for real-time UAVs.

The container-based software framework is composed of two distinct control environments, one for verified host control that ensures security with basic functionality and the other potentially vulnerable control environment that provides access to advanced functionality. By simulating sensors and drivers in the container, a security monitor continuously checks for Denial of Service attacks through communication channels. Upon detection of a safety rule violation, the structure changes to the safety controller to mitigate the attack. To validate a quadcopter prototype with commercially available hardware COTS and open-source software was implemented.

The ContainerDrone framework has proven to be reliable in protecting against DoS attacks launched within the container by limiting attacker access to three critical system resources: CPU, memory, and communication channel. Experiments have shown that the proposed structure can be effective against various types of Container Control Environment (CCE) DoS attacks launched effectively. In this study, the authors had not considered physical component failures, software failures caused by bugs and logic failures, or any other attack than DoS.

As noted in the study mentioned above, an effective way to improve attack resilience is to develop methods that can estimate system states with sufficient precision for control, regardless

of compromised components. An advantage is that it informs the state of the system, even when some elements have been compromised, allowing the use of the same controllers as in case without attacks. Resilient state estimation in deterministic linear systems has recently been mapped in the optimization problem of ten (PASQUALETTI; DÖRFLER; BULLO, 2013; FAWZI; TABUADA; DIGGAVI, 2014). However, the proposed techniques consider noise-free systems and in case of the exact model of system dynamics is known. These studies will be useful in defining the resilience attribute applied in the definition and specification of the architecture proposed in this project.

Finally, taking into account the contribution of the cited studies, the proposed architecture in this dissertation aims to design and develop a resilient architecture. This will be discussed further in the next chapter.

4.1.3.2 Comparative analysis

For the comparative analysis presented in Table 6, the studies architecture were [1] Chen *et al.* (2019), [2] Kong *et al.* (2018), [3] Yoon *et al.* (2017), [4] Pigatto *et al.* (2016) and [5] STUART (the architecture proposed and developed in this dissertation).

The following features were selected to compare the architectures:

- **Resilience:** Resilient architectures should be highlighted (KONG *et al.*, 2018; CHEN *et al.*, 2019; YOON *et al.*, 2017) because they are seen as a relevant security attribute to maintain the operation level of a stabilized UAV system, even under a successful attacks (ORDOUKHANIAN; MADNI, 2019; ORDOUKHANIAN; MADNI, 2016; VEGA *et al.*, 2015).
- **Safety and Security:** One of the concerns in the UAV design and development is to ensure safety requirements. However, since these vehicles communicate with external entities, architectures that are designed to ensure safety requirements can present security flaws and security requirements can present safety flaws. Therefore, it is necessary to investigate and treat safety and security together in UAV architecture.
- **Automatic detection:** This feature refers to the act of automatically identifying an intrusion. To ensure UAV security on the network and prevent the compromising of the mission, the architecture has to detect attacks and failures.
- **Network monitoring:** Network monitoring in a UAV architecture is responsible for identifying anomalies in the network and informing the central point of the architecture when a problem occurs. Such failures fall into the category of integrity. Integrity is an important feature to ensure that internal and external communication from various modules that compose a UAV architecture are not compromised.

- **Decision making:** The increase in the production and use of UAV requires a significant improvement in built-in decision-making capabilities, as UAV must continually adapt to missions and detect unexpected internal problems or external dangers. These decisions should consider the objective of the mission and adjust the choice of actions to achieve it according to random events related to the context of the mission, the health of the entire system, and dealing with the risk, and mission security.

Table 6 – Comparative analysis of architectures

Feature	Architecture				
	[1]	[2]	[3]	[4]	[5]
Resilience	Totally	Totally	Totally	Incompletely	Totally
Safety and Security (aggregates)	Incompletely	Incompletely	Incompletely	Totally	Totally
Automatic Detection	Partially	Incompletely	Partially	Incompletely	Partially
Network Monitoring	Totally	Totally	Totally	Incompletely	Totally
Decision making	Partially	Incompletely	Partially	Incompletely	Totally

Source: The author.

As shown in [Table 6](#), although there are several architectures in the open literature, none of the models presented contemplates all the requirements for making a generic and safe UAV. In the comparative analysis, only the work [4], and the one here proposed [5] are concerned with aspects of safety and security together. However, the work [4] is the only architecture that does not include the resilience characteristic.

The proposed work [5], study [1], and [3] are the architectures that propose to detect out attacks automatically in a network of a UAV. However, all of them detects only partially because physically, it is still not feasible to ensure that all the countless types of attacks are identified.

4.2 TRIVIR: A Visualization System to Support Document Retrieval with High Recall

Trivir is an interactive tool powered by an information retrieval mechanism that implements an active learning protocol to support information retrieval ([DIAS; MILIOS; OLIVEIRA, 2019](#)). The system integrates graphical visualizations through Projection and Force Layout to collect documents, including a similarity map obtained with multidimensional projection techniques. The system overview is presented in [Figure 12](#)

According to [Dias, Milios and Oliveira \(2019\)](#), TRIVIR offers two main advantages over other existing information retrieval systems: it provides an output to the machine learning

Figure 12 – Trivir - visualization system.

Source: The author.

algorithm through visualization, offering user interactions in an accessible way, and also improves the convergence of the best documents after the interaction with the user. The second reason is that it provides a vocabulary synonymous with terms found within the collection of documents.

Throughout the research period, the Trivir system was used to update the reading of new studies and read helpful articles from other years that were not included in the period since 2015, included in the systematic review. The system offered support based on the recommendation of works and made it possible to create a projection with the articles read, suggested, relevant, unimportant, and unread. Trivir also makes it possible to export the results during the research and learning phase. Figure 13 shows the result before (A) and after (B) the reading and training process of the system.

A total of 259 studies were read, 25 of which were classified as seed, highly relevant to the work. Table 7 presents the seed works and their respective years of publication. One hundred twenty-four studies were classified as appropriate, and 110 of these studies were not relevant to this dissertation's context. The file¹ exported after selecting the documents shown in the Figure 13 shows the articles' names and the classification categories they belong.

Finally, it is essential to note that Trivir was an important tool to facilitate and streamline the reading and review process carried out throughout this research.

¹ <https://drive.google.com/file/d/11xD8j-1H82BR22MKwRfpIuPE4lyDj0fz/view?usp=sharing>

Figure 13 – Trivir classification.

Source: The author.

Table 7 – Seed studies in TRIVIR

Year	Seed Studies
2014	(PIGATTO <i>et al.</i> , 2014; MEJRI; BEN-OTHTMAN; HAMDI, 2014) (AJMAL <i>et al.</i> , 2014)
2015	(IKEDA; HONDA; BAROLLI, 2015; BERGIN, 2015), (HAMIDA; NOURA; ZNAIDI, 2015; GUPTA; JAIN; VASZKUN, 2015)
2016	(PIGATTO <i>et al.</i> , 2016; JAVED; HAMIDA; ZNAIDI, 2016)
2017	(SCHOLLIERS; SAMBEEK; MOERMAN, 2017), (SIEGEL; ERB; SARMA, 2017)
2018	(LIN <i>et al.</i> , 2018)
2019	(CHRIKI <i>et al.</i> , 2019b; SINGH; NANDI; NANDI, 2019), (VOCHIN; ZOICAN; BORCOCI, 2019; WANG <i>et al.</i> , 2019), (KHELIFI <i>et al.</i> , 2019)
2020	(GUPTA; KUMARI; TANWAR, 2020; SAFADINHO <i>et al.</i> , 2020), (ISLAM; SHIN, 2020; ROSENDE <i>et al.</i> , 2020), (HUANG <i>et al.</i> , 2020a)
2021	(GUPTA; KUMARI; TANWAR, 2021; GUPTA <i>et al.</i> , 2021), (KUMAR <i>et al.</i> , 2021)

Source: The author.

4.3 Final remarks

This chapter presented a systematic review on safety issues and UAVs architectures. The main objective was to identify relevant, similar studies, and gaps to guide this research.

The studies presented in this chapter helped to define the reasons for building a resilient architecture for UAVs. Attacks linked to GPS and signal interference are regularly cited in the

literature and addressed different problems in the area. Therefore, they were taken into account in the architecture proposed in this work.

Only one work among those found ([FRANCO; BRANCO, 2017](#)) is concerned with safety and security aspects in an aggregate way. Therefore, the architecture proposed took into account the interaction between safety and security together in the context of a UAV.

Next Chapter addresses the reSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks undeR atTack (STUART). It also describes a case study scenario and the results obtained with the implemented architecture.

STUART ARCHITECTURE

As seen in the previous Chapter, developing a resilient architecture for dynamically managed UAV networks is a research area to explore. Therefore, in this Chapter, a resilient architecture for UAVs named STUART is presented, together with the results obtained through its development.

5.1 STUART: ReSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks undeR atTack

STUART is an architecture that manages the network dynamically, even in the face of an attack. It consists of four parts: (1) Anomaly-based detection system, (2) Triage module, (3) Decision making module, and (4) Cyber resilience. [Figure 14](#) illustrates the main architecture components and their interactions. Below are detailed each of the components that make up the architecture.

5.1.1 STUART composition

The parts that compose STUART, as well as their connections are illustrated in [Figure 14](#). These main components have different functionalities:

1. **Anomaly-based detection system:** This module is responsible for checking and detecting anomalies on the network. One of the concerns in the design and development of UAV systems has been to ensure safety requirements. However, since these vehicles communicate with external entities, some architectures designed to provide safety requirements can present security flaws, and security requirements can have safety flaws. Therefore, it is necessary to investigate and treat safety and security together in a UAV architecture.

Figure 14 – STUART architecture

Source: The author

Based on this, the anomaly-based detection system is concerned with detecting safety and security anomalies in an integrated manner.

2. **Triage module:** This module receives both security and safety alerts. Security and safety are interdependent, i.e. security can affect the safety and reversely the safety can affect the security. For example, if the intrusion detection system malfunctions due to an hardware failure, the security of the system is impacted. In the same way, if the intrusion detection system falsely classify the GPS traffic as a GPS spoofing attack, the response to this attack could deactivate the GPS and have a high impact on the safety of the system. Sometimes some attacks trigger two alerts: one from the security manager and one from the safety manager. Both of these alerts may be contradictory and confuse the decision making system. The triage module filters the wrong alert. The attack that triggers this alert has consequences on the system. If these consequences are similar to the one detected by the safety system, the safety alert is a false positive and can be removed. If the consequences are different, both alerts are valid.

3. **Decision making module:** The increase in the production and use of UAVs requires a significant improvement in built-in decision making capabilities (making the UAV "intelligent"). The UAVs must continually adapt to missions to solve unexpected internal problems or external dangers. Therefore, this architecture's decision making module is responsible for deciding which actions are most suitable for the UAV to complete a given mission when it undergoes an attack attempt. It makes the decision autonomously, through random events that arise during a mission. This module is responsible for ensuring the autonomy of the UAV through autonomous decision making.
4. **Resilient module:** Bearing in mind that malicious people can exploit safety and security flaws, STUART architecture includes a resilience module. The resilience module is responsible for the recovery and restoration of the UAV if subjected to deformation. Resilience is a relevant security attribute to maintain the level of system operation of a stabilized UAV, even in successful exploration.

Figure 15 shows the activities diagram carried out by STUART, elucidating the activities executed by the architecture.

To be considered resilient, an architecture must satisfy some goals and objectives (BODEAU *et al.*, 2015). A resilient architecture must fulfill the goals and, meet those goals, the objectives are the actions to be deployed.

5.1.2 STUART goals

Acordding to Bodeau *et al.* (2015), the main goals that an architecture must contain to be resilient are:

- **Anticipate:** This goal refers to an architecture's ability to be prepared in advance to detect and resist malicious events.
- **Withstand:** The architecture must absorb the impacts of adverse events such as system failures, hardware, and cyber bugs and continue essential functions.
- **Evolve:** The architecture must have the power to decide and adapt the desired mission functions to an acceptable level within a reasonable time.
- **Recover:** The architecture must have the ability to restore operations or functionality even after being subjected to an attack. Ideally, recovery also includes the system's ability to "adapt" to reduce the impact of future adverse events.

The way STUART achieves these goals is shown in Table 8.

Figure 15 – STUART activities diagram

Source: The author

For an architecture to be considered resilient, the first goal it must fulfill is to maintain a state of information prepared for adversity. STUART accomplishes this goal with the anomaly-based detection system and triage module. Both metrics are inserted in the architecture to check every moment if there is any adversity and perform the filtering of false positives.

The second goal says that a UAV must continue its mission even in the face of adversity. To fulfill this objective, STUART has as one of the possible decisions of the Decision-making module the function of isolating the vulnerable part so that the mission continues to be executed.

The third goal for an architecture to be resilient is to adapt mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat envi-

Table 8 – Cyber resilience goals

Goal	Description	STUART
Anticipate	Maintain a state of informed preparedness for adversity	Anomaly-based detection system and Triage Module
Withstand	Continue essential mission/business functions despite adversity	Decision making: Act: Isolate the vulnerable part for recovery and continue performing
Evolve	Adapt mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments	Decision making module
Recover	Restore mission/business functions during and after adversity	Cyber resilience

Source: The author

ronments. STUART achieves this goal with the decision-making module, whose function is to decide in the face of anomaly what the cyber resilience module should perform to adapt to the vulnerable part and not prevent the mission from completing successfully.

Finally, the goal of restoration should be achieved with the objective of restore mission / business functions during and after an adversity. STUART contemplates this goal through the resilience module, responsible for reestablishing the UAV after an attempt or attack.

STUART focuses on recovering or fighting safety and security failures against unpredictable attacks and events. This means that STUART needs to maintain essential resources, regardless of the threats they face. Thus, the resilience used at STUART is much more than merely building a safer UAV architecture, as it requires the capacity and planning to recover from dangerous events, whether they are known or unexpected. Table 9 provides a comparison of why the security of resilient architectures differs from conventional cybersecurity architectures.

5.1.3 STUART Cyber resilience objectives

In the same way, according to Bodeau *et al.* (2015), some objectives still must be fulfilled for the architecture to fit as resilient. These objectives are:

1. **Understand:** The first is to understand, that is, maintain useful representations of mission dependencies and resources status for possible adversity. This objective is accomplished with the four goals present in STUART, anticipate, withstand, evolve and finally, recover.
2. **Prepare:** The second is always to maintain a set of realistic courses of action that address predicted or anticipated adversity. This objective, like the previous one, is also fulfilled

Table 9 – Comparison between traditional and resilient security architectures

Attributes	Resilient architectures	Traditionally secure architectures
Business advantage	It focuses on real-time operations, ensuring the mission's success, thus preventing companies from having losses with the aircraft or compromising the mission, which can cost of dollars.	Focused primarily on protecting assets, mostly preventative with intense moments of reaction; considers what valuable business assets need to be protected
Prioritization of the C-I-A triad (confidentiality, integrity, availability)	Focused on availability with assumed integrity and little regard for confidentiality	Focused on retaining confidentiality of data along with integrity, and less priority on availability.
Scale of the complexity challenge	Complex interactions lead to poorly understood emergent behaviors	Interactions might be complicated but are mostly linear, leading to well-understood behaviors
Systems view: people, processes, and technology	These social-technical systems require nearly constant inputs from sensors to monitor and control.	Mostly focused on technical security solutions and data security

Source: Adapted from ([MAILLOUX; GRIMAILA, 2018](#))

with all the goals present at STUART, mentioned in the previous chapter: anticipate, withstand, evolve and recover.

3. **Prevent/avoid:** The third is to prevent and avoid the successful execution of an attack or the realization of adverse conditions. Again, this objective is met by all goals present at STUART.
4. **Continue:** The fourth, where the duration and viability of essential mission/business functions during adversity should be maximized, STUART achieves, withstand, evolve, and recover.
5. **Constrain:** The fifth concerns the changes in the architecture to achieve limited damage from adversity. In this case, withstand fills this gap by isolating the vulnerable parts and recovering them by performing UAV resilience.
6. **Reconstitute:** In the sixth, only recover fits since it is responsible for restoring as much mission/business functionality as possible after adversity.
7. **Transform:** The goal of transforming present at STUART is when the architecture can transform mission functions to deal with adversity more effectively. STUART can cover this objective with the goals mentioned in the previous chapter, evolve and recover.

8. **Re-architect:** Re-architecture is about the power to modify and restore architecture, even after a successful attack. This guarantees its ability to re-architect. This last objective is fulfilled by the goals of evolve and recover.

Table 10 summarize the necessary objectives to achieve the goals handled by STUART.

Table 10 – STUART objectives

Objective	Description	Goals STUART			
Understand	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity				
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity				
Prevent/Avoid	Preclude the successful execution of an attack or the realization of adverse conditions				
Continue	Maximize the duration and viability of essential mission/business functions during adversity				
Constrain	Limit damage from adversity				
Reconstitute	Restore as much mission/business functionality as possible subsequent to adversity				
Transform	Modify mission / business functions and supporting processes to handle adversity more effectively				
Re-architect	Modify architectures to handle adversity more effectively				

Source: The author

5.1.4 DDoS attack in STUART

This section describes the generic behavior of STUART when subjected to a Distributed Denial of Service (DDoS) attack. This type of attack occurs when several machines send many requests to a UAV system at the same time. Taking into account that avionics systems have a limited number of users that can be served at the same time, this large number of traffic makes it impossible for the UAV to be able to fulfill any request (GARG *et al.*, 2019; CHOUDHARY *et al.*, 2018). Then, the UAV can restart or even get stuck depending on the resource that was victimized. The Figure 16 illustrates this attack.

Table 11 shows the steps of STUART in the face of a DDoS attack. Assuming that the attacker already knows the vulnerability of the UAV and has already gained privileged access to the system, this means that it already controls several machines, which, in turn, can control a large number of other machines. It is from these machines that a large number of requests are triggered in a specific period of time, usually a short period. With this, the result is not only the saturation of the UAV network system, but mainly the shutdown of its essential services. However, at STUART this type of attack can be avoided through the modules that compose the architecture.

Figure 16 – DDoS attack in UAVs

Source: The author

The **Anomaly-based detection** system module is responsible for detecting anomalies on the network, so when there is a sudden change in requests in a short period of time, it will inform the triage module that there is a problem and inform the characteristics of the problem.

The **triage module**, in turn, verifies that it is not a false positive and is a DDoS attack, as reported by the previous module. Then, it issues an alert to the other modules that make up STUART informing about the attack.

The **decision module** checks the part that needs to be isolated, for example, a specific port or the GPS sensor. Then, it tells cyber resilience to apply that measure. Also, it assesses the possibilities to solve the problem and informs the cyber resilience which action to take to restore the compromised party.

Cyber resilience, in turn, applies isolation to the vulnerable part and performs the

Table 11 – DDos attack in STUART

DDoS attack	Description	Stuart	
		Goal	Module
After obtaining privileged access to the UAV system, several machines start sending multiple requests in a short period of time	STUART finds that several requests are being sent in a short time	Anticipate	Anomaly-based detection system
	The triage module identifies that it is not a false positive and sends the alert to the modules.		Triage Module
Failure attack!	The vulnerable part of the system where the Anomaly-based detection system identified is isolated to be treated, for example, a door system specific	Withstand	Decision making Act: isolation of vulnerable parts
Failure attack!	The decision making checks the actions possible to solve the problem and informs cyber resilience	Evolve	Decision making
Failure attack!	First it will isolate the vulnerable part defined by the decision making and then, finally, cyber resilience performs the restore action, for example, in this case of a DDoS, there could be blocking of requests from machines that sent a large number of requests within the time period reported by anomaly-based detection system.	Recover	Cyber resilience

Source: The author

recovery action. In this case, one of the possible actions would be to block requests from machines (blocking the doors) that have sent a large number of requests within the time reported by cybersecurity. Then, the modules communicate that the mission can continue and there is no more threat of problems on the network at that moment. The operating sequence of the modules that make up STUART are shown in the [Figure 17](#).

It is worth emphasizing that this is just an example of application and restoration and STUART is not limited to it, other techniques of detection, classification, isolation, decision making and restoration can be applied for different types of attacks, including other techniques for the DDoS attack.

Figure 17 – STUART Sequence diagram

Source: The author

5.2 Final remarks

This chapter presented a new resilient architecture named STUART to allow the recovery of a UAV network under attack. Aiming to provide the dynamical recovery, the architecture uses a resilient model, which integrates security and safety in a unique system named anomaly-based detection system.

To provide dynamic recovery, the architecture uses a resilient model that allows the integration of techniques that enable the UAV to be autonomous and make decisions in the face of adversities encountered during the mission. In the next chapter, different techniques are proposed to illustrate the architecture potentials to prevent GPS spoofing attacks.

DESIGN OF THE STUART ARCHITECTURE TO BE RESILIENT AGAINST GPS ATTACKS

As previously seen in [subsection 5.1.1](#), STUART is composed of four parts: (1) Anomaly-based detection system, (2) Triage module (3) Decision making module, and (4) Resilience module. Thus, each of them requires at least a different technique to be implemented. In this chapter, it is presented each method used to validate the four parts of STUART.

6.1 Anomaly-based detection system

One of the concerns in the design and development of UAV systems has been to ensure safety requirements. However, since these vehicles communicate with external entities, some architectures designed to provide safety requirements can present security flaws. And security requirements can have safety flaws. Therefore, it is necessary to investigate and treat safety and security together in a UAV architecture. STUART architecture explores the incorporation of security and safety metrics as a unified concept in UAV development.

This dissertation comprises two security metrics: Haversine and non-respect of the moving zone and, one safety metric: the NCI (Node Criticality Index). The metrics are detailed in the next sections and used to detect GPS SPOOFING attack

6.2 Haversine

When collecting information, the UAV control system is responsible for informing the module what data is being received, such as GPS positioning (Latitude and Longitude) and when the action occurred (hour and minute).

After the data is collected, the Haversine formula ([ROBUSTO, 1957](#)) is applied. The Haversine formula is an equation used in navigation to provide distance between points. In the

specific case of STUART, the points are obtained through the acquisition of its geographical coordinates (Latitudes and Longitudes). It is used to calculate the distance of the largest circle between two points, i.e. the shortest distance on the earth's surface, giving a distance "as the crow flies" between the points (ignoring any hills they fly).

The formula works as follows: two points on a sphere (of radius R) with Latitudes ϕ_1 and ϕ_2 , $\phi_{separation} : \phi_{Latitude} = \phi_2 - \phi_1$, and separation of $\lambda : Final\lambda = \lambda_2 - \lambda_1$, where the angles are in radians. The **distance** D can be obtained either by the simple application of the inverse Haversine or by the use of the arccosine function (inverse of the sine).

The Haversine central angle can be calculated between two points with R as the radius of the earth, D as the distance between two points Latitude (ϕ_1 and ϕ_2) and Longitude (λ_1 and λ_2) using the Equation 6.1:

$$\text{Haversine}\left(\frac{D}{R}\right) = \text{haversine}(\phi_2 - \phi_1) + \cos(\phi_1)\cos(\phi_2)\text{haversine}(\lambda_2 - \lambda_1) \quad (6.1)$$

To calculate the distance between two geographical coordinates, the Haversine formula must be derived as follows:

$$\begin{aligned} A &= \sin^2\left(\frac{\phi_{Difference}}{2}\right) + \cos(\phi_1)\cos(\phi_2) \\ &\quad \sin^2\left(\frac{\lambda_{Difference}}{2}\right) \\ C &= 2 \arctan(\sqrt{A}, \sqrt{1-A}) \\ R &= 6371 \\ D &= R \cdot C \end{aligned} \quad (6.2)$$

Where,

- $\phi_{Difference} = \phi_1 - \phi_2$ (latitude difference);
- $\lambda_{Difference} = \lambda_1 - \lambda_2$ (longitude difference);
- R is the radius of the earth, that is, 6,371 km;
- D is the calculated distance between two points.

Finally, after applying Haversine, the average UAV speed, s , can also be calculated from the time collected as t (Equation 6.3). From that, we have the timestamp information (hour and minute), distance, and speed, which are used in this dissertation to verify the security of GPS (Global Position System) in the UAV. For example, a UAV flies at a maximum speed of 80 km/h.

In a given time, the station passes on data that, after calculating Haversine and the average speed, concludes that the UAV is advancing at an average speed of 200 km/h, representing an anomaly.

$$s = \frac{d}{t} \quad (6.3)$$

6.3 Non-respect of the moving zone

The rules to detect a digression from the moving zone is calculated with the circumference limit. As the architecture already knows the distance between the base station and the arrival point, two circumferences between the two points (start and end) are calculated. This circumference is illustrated in [Figure 18](#).

Figure 18 – Route that STUART must take.

Source: The author

The median point between the two circles serves to guide the limit (radius) where the UAV can travel. Let's say that the distance is 143 meters, so in this metric, it is checked if the UAV has not crossed the circumference limit and is in the permitted zones. To verify this, a line is drawn between the starting point and the current one and at each displacement a set of rules are checked.

Let's assume I is the starting point, F the ending point and X the current position of the UAV. D being the distance between an initial point I and an end point F , the UAV is correctly positioned if:

$D(I, X) \leq d$ then it is within the region

$(D(I, X) < D) \& (D(F, X) < D)$ then stable UAV, illustrated in [Figure 19 \(B\)](#)

So, the rules to detect a GPS spoofing attack are:

If $D(I, X) > d$ then it is outside the I region

If $D(I, X) \leq d$ then it is within the I region

If $D(F, X) > d$ then it is outside the F region

If $(D(I, X) > D) \& (D(F, X) > D)$ then GPS SPOOFING, illustrated in Figure 19 (A)

If $Lat(X) < Lat(I)$ then GPS SPOOFING, illustrated in Figure 19 (C)

If $Lat(X) > Lat(F)$ then GPS SPOOFING, illustrated in Figure 19 (D)

Figure 19 – Illustration of the GPS Spoofing detection.

Source: The author

6.4 NCI - Node Criticality Index

The metric used to ensure safety in this dissertation will be the Node Criticality Index (NCI) (PIGATTO, 2017). The NCI is the specification of a formal criticality classification responsible for determining the nodes priority through an index. The reason for choosing this metric is twofold: 1) NCI measures the quality of service, safety, and security for the nodes that make up the network, and 2) NCI provides valuable information to the system that can influence the decision making of tasks.

The determination of each score takes into account the need for different approaches. Although the scope of this dissertation does not include the automatic attribution of this score, it

is an open research topic for future integration. The fact that it requires human intervention is not necessarily a problem, as it is performed only once before the operation of the unmanned vehicle begins. Scoring is carried out first during a configuration phase and then automatically updated as a result of changes and events during system operation. The score assignment must be a number within a range of 0 to 1, meaning common and critical data, respectively.

The $NCIm_i^{Saf}$ is the safety metric for a module i of this architecture. The $NCIm_i^{Saf}$ will be used as a safety metric to measure the health of the module and can be found by calculating the average between the *health* index and the *modulePriority* index, as shown in Equation 6.4. *Health* represents a score between [0,1] that indicates the health status of a module. The *modulePriority* is a score [0,1] that identifies the importance of a module for the overall security of the system.

$$NCIm_i^{Saf} = average(health_i, modulePriority_i) \quad (6.4)$$

6.5 Triage module

To perform the vulnerability filtering, an algorithm with an Intrusion Detection System (IDS) structure was used (SUJATHA; DHARMAR; BHUVANESWARAN, 2012; WANG *et al.*, 2017). An IDS can investigate system activity, recognize known attack patterns and identify abnormal network activity. Sometimes some attacks trigger two alerts: one from the security manager and one from the safety manager. Both of these alerts may be contradictory and confuse the decision making system. The triage module filters the wrong alert.

The detection of GPS attacks is a very complex task. Low deviation (slowloris attack (DURAVKIN; LOKTIONOVA; CARLSSON, 2014)) in GPS positioning is rarely detected by an anomaly-based intrusion detection system. Therefore, to detect this type of attack, it is proposed a new signature-based intrusion detection system. The main advantage of signature-based intrusion detection system, compared to anomaly-based IDS, is to detect attacks without returning false-positives (QUINCOZES; KAZIENKO, 2020). This point is very important because false-positive alerts can be misinterpreted and have an impact on the safety of the system. To design the rules to detect GPS attacks, the position of the UAV has to be known.

An IDS algorithm has types of reactivity in each system, which can be passive when providing alerts or reporting on the occurrence of the event, or active when implementing mechanisms to respond to attacks such as resources to disable Transmission Control Protocol (TCP) connections (TANENBAUM; WETHERALL, 2010), modify routing tables or firewall rules, thereby preventing the attack from actually occurring or from taking on more significant proportions. In this dissertation, the structure of a passive IDS is used. That is, when it identifies that the vulnerability is not a false positive, it issues an alarm to the administrator (decision making module) to take measures for preventing the invasion from continuing.

6.6 Decision making module

The technique used for decision making is guided by the OODA cycle (ROUSSEAU; BRETON, 2004), one of the models studied in several strategic areas, despite being developed in the military environment. This technique was determined after an analysis of the existing techniques, shown in Table 12.

Table 12 – Comparative techniques for decision making

Drawbacks	Multiple Criteria Decision Making	Mixed Observability MDP	Partially Observable MDP	Game Theory	OODA cycle
Need manually information	Yes	Yes	No	No	No
Intentions are assumed unchangeable. Different modelling required for each environment	Yes	Yes	No	No	No
Continuous belief space may lead to large number of samples and large computational effort	Yes	Yes	Yes	No	No
Perfect information assumed	Yes	Yes	No	Yes	No
Perfect information required	Yes	Yes	No	Yes	No

Source: The author

The OODA cycle is comprised of (1) OBSERVE, (2) ORIENT, (3) DECIDE and (4) ACT.

- **OBSERVE:** is responsible for acquiring odometry data from the UAV;
- **ORIENT:** is responsible for performing the necessary calculations for decision making based on OBSERVE data. These calculations are: (1) Return to the base by a known path; (2) Time to return to the base in a known way; (3) Return to the base by a faster way; (4) Time to return to the base by a faster route; (5) Recovery through historical data;
- **DECIDE:** chooses decisions based on data calculated by OBSERVE. For example, if the UAV needs to go back to the base, ORIENT calculates two routes considering the amount of battery. It is then up to DECIDE to verify which strategy to adopt and inform ACT;
- **ACT:** is the one who tells cyber resilience what action to take.

Figure 20 illustrates the main idea of this cycle. Possible actions include landing (in case of a safety problem), recovering from a safe state, or returning to the base (in case of a security problem) and isolation of the vulnerable part (in case of a security or safety problem) .

Figure 20 – OODA cycle.

Source: (ROUSSEAU; BRETON, 2004).

6.7 Cyber resilience

The resilience module is the last to be executed at STUART. It is structured in a state machine and works as follows after being invoked by decision-making:

- **Loading:** in this part, the four information passed on by the decision-making are loaded, which are: (1) Action to be performed, (2) Quantity of battery, (3) Reset data (current and known to be safe geographic coordinates), and, (4) Number of reinstatements;
- **Verification:** checks the number of recovers. If this number is greater than 3, it forwards to State 03. If not, it verifies the action to be performed and forwards to States 04 and 05 in the case of a security problem or State 06 in case of a safety problem;
- **Return to the base:** this action returns to the base calculated by the decision-making;
- **Isolation:** this action performs the isolation of the vulnerable part indicated by the decision-making. This action is essential to avoid making other essential functions vulnerable;
- **Recovery:** action will send the UAV to a consistent physical state to match the values of the elements internal to the states and thus be able to recover the UAV. Essential operation is defined as advancing the system to the current time, starting from a consistent

historical physical state (in other words, verifying where a consistent physical state was and advancing the time to the current time, as if now (current time) the UAV was in that position).

Figure 21 shows the activities diagram carried out by resilience module, elucidating the activities executed. In the first activity, the information is loaded and sent to the verification activity, where the number of recovers is checked. If the number is greater than 3, it goes into returning to the base. However, if in the verification the number is less than 3, it goes to the isolation activity, where the vulnerable part is isolated. Finally, the isolation activity leads to the recovery activity, where the UAV is recovered. Also, in the verification activity, there is a third activity that can be performed, which is the Land. Still, it is only performed if the problem is a safety problem because, in this case, there is no possibility of recovery.

Figure 21 – Resilience - Activities diagram

Source: The author

6.8 Final remarks

In this chapter, different techniques were proposed to illustrate the architecture potentials to prevent GPS spoofing attacks, being: Haversine, Non-respect of the moving zone, NCI, IDS, OODA Cycle and recovery and rollback through historical data. As can be seen, the NCI is an index that can be applied to prioritize communication and safety purposes due to its sub-indices. On the other hand, Haversine is an ally for calculating the distance and verifying sudden location changes. The tour of the mobile zone makes it possible to detect slow spoofing GPS attacks. The three metrics complement each other to ensure that the mission is safe.

A new security metric was also presented to help in the detection of GPS spoofing attack and, a new signature-based for an IDS, helping in the diagnosis of a slowloris GPS attack detection.

Finally, in the next chapter, these techniques were validated through a case study simulation, covering all the architecture's main component behaviors.

STUART IN A COVID-19 VACCINE TRANSPORT SCENARIO

In this chapter it is presented the validation of the four parts of STUART in a COVID-19 vaccine transport case study where the aircraft is subjected to a GPS attack.

7.1 STUART in a COVID-19 vaccine transport scenario

The development of this study comprised the accomplishment of tasks divided into four stages: choice of mission, choice of test cases, choice of aircraft models, implementation scenario of tests and analysis of results.

7.1.1 *Choice of mission*

In December 2019, COVID-19 began to be detected in the Chinese city of Wuhan (PAN *et al.*, 2020; TIAN *et al.*, 2020). Because of the virus, more than 100 million people around the world have already been infected and more than 2 million have died (ANAC, 2021). The most common symptoms of this disease are fever (CHACÓN-AGUILAR *et al.*, 2020), dry cough (SCHWARTZ *et al.*, 2020), tiredness (MOEIN *et al.*, 2020), pain and discomfort (MAJUMDAR; BISWAS; SAHU, 2020), loss of taste or smell (MENNI *et al.*, 2020), among others. More severe symptoms include difficulty in breathing or shortness of breath, chest pain or pressure, and loss of speech or movement (JAIN; YUAN, 2020; POYRAZ *et al.*, 2021).

Despite all the damage caused by the pandemic, the first mass vaccination program started in early December 2020, and as of May 13, 2021, 1.37 billion doses of vaccine were administered (ITA, 2021). At least seven different vaccines are being administered around the world. Despite advances in developing new vaccines for COVID-19, their safe distribution, especially in remote and hard-to-access areas, has not yet evolved significantly. Thanks to technological advances in

healthcare, UAVs are being used as a possible solution to the distribution problem, not only for vaccines for COVID-19 but for other types of vaccines and medicines (KIM; KIM; HWANG, 2021; CHAMOLA *et al.*, 2020).

The advances of UAV in such scenario are numerous. They can operate in difficult terrains with faster results due to the fact that they do not follow terrestrial traffic rules (and do not face congestion, for instance) (BARMPOUNAKIS; GEROLIMINIS, 2020). They also reduce the labor cost because they are autonomous and do not require to be remotely controlled. Recent studies (HAIDARI *et al.*, 2016; MICHAEL *et al.*, 2019; HII; COURTNEY; ROYALL, 2019) show that they are very suitable to distribute vaccine doses to health care providers. They can slightly improve the vaccine availability and significantly reduce the logistic cost.

However, due to the rarity of vaccine, it may be very profitable for attackers to steal the UAVs and the doses that they carry. As they are autonomous, these vehicles are exposed to many cyber threats. To hijack a UAV and steal the doses that they carry, GPS spoofing attacks can be used. Therefore, this test scenario was chosen to validate STUART.

7.1.2 Choice of test cases

The main scenario is the station located at the UFSCar University hospital (São Carlos, SP - Brazil) to the Santa Casa hospital (São Carlos, SP - Brazil) to deliver 120 doses of COVID-19 vaccines developed by the university's laboratory and referred to vaccinate hospital health professionals. Figure 22 illustrates the path the UAV must take.

This study is divided into three test scenarios: a real UAV test and the next two being computer simulations. In the first case, a real UAV is used to test if it is vulnerable to a GPS spoofing attack. GPS spoofing is considered one of the most recurring threats to UAVs (GASPAR *et al.*, 2018; KERNS *et al.*, 2014; SHEPARD *et al.*, 2012). The principle behind the GPS counterfeit attack is that, by sending the UAV's false geographic coordinates to the control system, it is possible to trick the on-board system that hijacks the vehicle in a different location is commanded (KERNS *et al.*, 2014).

In practice, there are GPS "spoofers" that create false GPS signals to trick receivers into thinking that they are in a different location or at other times. An example of a spoofer is FakeGPS (2020), an application for android phones that falsifies the position by rewriting the location. In this test case, the Fake GPS Location app was used to analyze whether the aircraft was vulnerable to this type of attack and to collect data from the UAV for use in the following two tests, computer simulations. This test scenario is illustrated in Figure 23.

The test scenarios are shown in Table 13. The two computer simulations are composed by:

1. An aircraft acquires the data normally, without problems, and can deliver the vaccines to

Figure 22 – Route that the UAV must take (using STUART).

Source: The author

the indicated location.

2. The aircraft is subjected to a GPS attack, where an attacker tries to trick the UAV into taking a different route to steal vaccines.

Table 13 – Scenario of test cases.

Scenario	Type of test	An aircraft
Case 1	Test with a real UAV	GPS spoofing attack with Fake GPS Location
Case 2	Computational simulation	A normal operation with an aircraft acquiring data
Case 3	Computational simulation	An aircraft is subjected to a gps spoofing attack

Source: The author.

7.1.3 Choice of aircraft model

The aircraft model chosen was the 3DR Solo Quadcopter and it is illustrated in Figure 24. The reason for choosing the aircraft is that it has an autopilot, ideal for transport cases.

Solo is considered the world's first smart UAV, weighs 11.7 pounds, and measures 16.4 x 16.5 x 9.2 inches. The packaging is standard and contains the following components: the

Figure 23 – GPS spoofing with fake app.

Source: The author

quadcopter, camera gimbal for stable photos, self-tightening propellers in the dimensions of 10 inches x 4.5 inches, remote control, Li-Po Solo battery of 5200 mAh, rechargeable battery of the 2600 mAh capacity controller and backpack to carry the UAV (AMAZON, 2020). It is worth mentioning that the Solo 3DR stopped being produced. However, it can be considered for evaluating and demonstrating what is possible to accomplish by applying safety techniques.

7.1.4 Implementation test scenario and analysis

STUART architecture was implemented in C++ language in the HAMSTER based data communication architecture. HAMSTER is a data communication architecture designed for improving mobility, security, and safety of the overall system (PIGATTO, 2017; PIGATTO *et al.*, 2016). As a means of validating security (at CSU) and safety (at SMU) metrics, we performed the test scenario through concrete implementations of the HAMSTER abstractions, mentioned earlier in subsection 3.2.1.

All HAMSTER units use elliptical curve encryption algorithms implemented by the RELIC (ARANHA *et al.*, 2000) version 0.3.3 toolkit built with a 160-bit key. The test environment consists of a station (HAMSTER Super Entity) and one HAMSTER Entity (UAV1), an autopilot, and a unit sensor. HAMSTER units were implemented as different processes on a Windows 10 desktop, communicating over TCP sockets on localhost. Ethernet also communicates

Figure 24 – 3DR Solo UAV outfitted with Kodak SP360 cameras to collect 360° imagery for later surveys in the lab using virtual reality glasses

Source: (CRUTSINGER; SHORT; SOLLENBERGER, 2016)

the station with an instance of the Message Queuing Telemetry Transport (MQTT).

The validation scenario works as follows: UAV authenticates with their central unit and provides telemetry data. The public station requests the UAV data on a server that another client accesses. Then the customer can receive telemetry data from the UAV. The UAV station communication links are managed by the HAMSTER Platform, while the data exchange is done by Message Queue Telemetry (RODRIGUES; BRANCO, 2020). Communication and interface abstraction is implemented using a TCP network.

The test environment consists of a station (HAMSTER Super Entity) and one HAMSTER Entity (UAV1), an autopilot, and a unit sensor. HAMSTER units were implemented as different processes on a Windows 10 desktop, communicating over TCP sockets on localhost. Ethernet also communicates the station with an instance of the MQTT.

When connecting to the Station, the UAV sends its ID and a public cryptographic key. The Station connects to the UAV in the same way, creating a bidirectional connection. After the link is completed, UAV sends REQ ENTITY ACCESS with its authorization information, and the CSU and SMU modules that contain the metrics are invoked, as illustrated in Figure 25.

If the data was plausible and the GPS is working correctly during the whole trip, the Station responds with the message ENTITY ACC GRANTED and presents the flight history. Otherwise, the SMU or CSU alerts the central Station that GPS spoofing is taking place, as illustrated in Figure 26. Then, the Station prioritizes communication through the wifi transmitter and informs the decision-making module that an action must be taken.

Figure 25 – Station HAMSTER

```

800000010058? *?? ?Z3??10c?h?k??J/D?a?GF&???' 6????e9u?*s?1????>??A?1???la?n???
^???)0
38303030303030313030353803ad2a06a9b27c5a33b8dd6c4f63a568d66bf10cc11e2e4a2f448502
61da474626b68714cc89272036f61ec9c7d0653975cd2a007314c03185d5151a843c3ee3961e41b6
318f8be35d6195136e9df9bb605edfbbbe7d3016
0000027 [DETAILS] getPeerFromHandler() pointer find = 0x800067b10
0000028 [DEBUG] HAMSTER_UNIT_ID received.
0000029 [ERROR] Could not hash, error code = 6
MESSAGE BUFFER:
0000000200011
3030303030303032303030303131
0000031 [DETAILS] getPeerFromHandler() pointer find = 0x800067b10
0000032 [DEBUG] Message other than HAMSTER_UNIT_ID received.
MESSAGE BUFFER:
0000000200012
30303030303030323030303132
0000033 [DETAILS] getPeerFromHandler() pointer find = 0x800067b10
0000034 [DEBUG] Message other than HAMSTER_UNIT_ID received.
MESSAGE BUFFER:
0000000200013
30303030303030323030303133
0000035 [DETAILS] getPeerFromHandler() pointer find = 0x800067b10
0000036 [DEBUG] Message other than HAMSTER_UNIT_ID received.

```

Source: The author

Figure 26 – UAV HAMSTER

```

0000029 [EVENT] Message HAMSTER_UNIT_ID sent.
Message Payload:
800000010058? *?? ?Z3??10c?????J?<=?r? ?B????4ä??=K??9U???P?~??h??x?p????\YF?PF?
rpW?8??x??1^0
0000030 [VERBOSE] CSU state = WAITING_CENTRAL_UNIT
0000031 [VERBOSE] Leave customExecution()
testando...
0000032 [VERBOSE] entered customExecution()
0000033 [EVENT] UAV is now sending telemetry data.
Latitude: 44.2760089 Longitude: -94.0903 Altitude:295
Roll: -1062 Pitch: -227 Yaw: 17357
NCI safety: 0.5
Horario = 15:30
Preparando para voo...
0000034 [DEBUG] CommBroker parse message. Code = USER MESSAGE
0000035 [DEBUG] CommBroker push external message
0000036 [DEBUG] CommBroker leavinfParse
testando...
0000037 [DEBUG] Message in CommInterface. Code = USER MESSAGE
0000038 [DEBUG] CommInterface parse message. Message USER MESSAGE
0000039 [DEBUG] External message parsed. Code = USER MESSAGE
0000040 [VERBOSE] Encrypting.....
0000041 [VERBOSE] sendMessageToPeer(ComInterface)
0000042 [EVENT] Message USER MESSAGE sent.
Message Payload:
0000000200011
0000043 [DEBUG] External message sent.
0000044 [DEBUG] CommInterface leave ParseMessage
0000045 [VERBOSE] Leave customExecution()
testando...
0000046 [VERBOSE] entered customExecution()
0000047 [EVENT] UAV is now sending telemetry data.
Latitude: -22.0057600 Longitude: -47.8961 Altitude:295
Roll: -1062 Pitch: -228 Yaw: 17356
NCI safety: 0.5
Horario = 15:31
Verificacao de GPS: ativada...
ALERTA DE GPS SPOOFING...

```

Source: The author

7.2 Scenario 01: GPS spoofing attack with Fake GPS Location

First, the Fake GPS application was installed on a smartphone with an Android operating system. Then the 3DR Solo UAV was connected to the smartphone via WiFi. Figure 27 illustrates the Solo after being connected with the smartphone.

Figure 27 – Solo 3DR connected with the smartphone

Source: The author

The initial location indicated on the UAV's GPS was correct and was the same indicated by the Fake GPS on the smartphone, being in the city of São Carlos, SP - Brazil, at 17:32, as shown in Figure 27 (A). A minute later, at 17:33, the GPS location in the Fake GPS application was changed to Pará, located in northern Brazil, as shown in Figure 28 (B). It was then verified that 3DR Solo also indicated that it was in Pará, i.e. if this were real, it would have moved a distance of 2,350 km in one minute. However, no alerts to the UAV's central command were issued. The video of the attack can be seen on Youtube ¹.

¹ Demo Attack: <https://youtu.be/hjs-9yuA7II>

Figure 28 – (A) True location (B) Fake location

Source: The author

In this scenario, the vaccines of COVID-19 would be easily stolen and would compromise the entire mission, from the theft of doses to the aircraft itself. However, now let's think about a situation where the 3DR Solo contains the structure of STUART.

Applying the Haversine metric, this UAV would have been able to check the sudden change of route and would be able to detect GPS Spoofing. The distance would be calculated and the average speed too, so it would be easily possible to conclude that the UAV has gone a very long way in a short time. Or even if the architecture had the NCI, the module's integrity containing the GPS would reflect this variation, increasing the health score to the value of 1 [min: 0, max: 1]. The value 1 represents the most critical value. Therefore, an alert would be issued in the architecture, and the appropriate action should take place. Applying just one of these STUART metrics, it would already be possible to detect GPS spoofing and calculate possible forms through decision-making to be used by the resilience module, thus not compromising the entire mission.

This concludes that a malicious person emitting a signal with a simple smartphone could falsify the real location of a UAV like the 3DR Solo. It can be concluded, then, that techniques that help UAVs to detect and mitigate this type of attack are still absent in many aerial vehicle

architectures, although they are essential to guarantee the completion of a mission.

7.3 Scenario 02: Normal operation

In this scenario, the 3DR Solo communicates with a base station via a WiFi transmitter. The Solo has an Inertial Measurement Unit (IMU), a GPS to identify its location and an autopilot that powers the camera, motors, and WiFi transmitter/receiver.

In [Table 14](#) we have the test case for a normal vaccine transport. The UAV is launched at time 15:31:00. Then the formulas are applied. First, the security calculation is performed, followed by the safety calculation. The steps that will take place during the normal operation test are detailed below.

Table 14 – Scenario 1: Normal operation

Time	Action	STUART
15:31:00	The UAV leaves the base station and starts to move (flight)	Calculates anomaly-based detection system
15:31:03		Triage module receives information report
15:31:04		OBSERVE saves historical data
15:38:00	The actions continue until they reach the end point	

Source: The author.

The first step is to calculate the Haversine metric. In [Table 15](#) we have the test for Haversine. Latitude and longitude corresponding to the starting point (at 15:31:00), the median distance point (at 15:35:02), and the arrival point (at 15:38:00). After converting the angles for radians, applying Haversine, and collecting time, we have the result of the average speeds. The 3DR Solo reaches 80km/h, so it is concluded that the flight is stable, that is, in an acceptable distance covered in the indicated time range.

Table 15 – Scenario 1: Normal operation - Security

Time	Security Metric for GPS			
	Latitude	Longitude	Haversine	Km/h
15:31:00	-021.59.33.6	-047.53.24.4	0	0
15:35:02	-021.59.54.1	-047.53.34.1	691 meters	10.37 km/h
-	The mission continues	-	-	-
15:38:00	-022.00.42.7	-047.54.03.5	675 meters	13.5km/h

Source: The author.

The main implementation of the Haversine for security metrics can be seen in [Source code 1](#).

Source code 1 – Haversine Code

```

1: /* Haversine Code for Security */
2: int firstTime = ((hr1*60)+min1);
3: int secondTime = ((hr2*60)+min2);
4: totalTime = secondTime - firstTime;
5: //conversion to degree
6: lat1 = ((lat1 * pi)/180.0);
7: long1 = ((long1 * pi)/180.0);
8: lat2 = ((lat2 * pi)/180.0);
9: long2 = ((long2 * pi)/180.0);
10:
11: double Lat = lat2 - lat1;
12: double Long = long2 - long1;
13: double val1 = 6371;
14: //Calculates the angle and the derivative
15: double val2 = sin(Lat/2)*sin(Lat/2)+cos(lat1)*cos(lat2)*sin(Long/2)*sin(Long
    /2);
16: val2 = 2 * atan2(sqrt(val2), sqrt(1 - val2));
17: dist = val1 * val2;
18: avgSpeed = (dist/totalTime);

```

The second step is to calculate the second security metric, also known as the mobile zone tour. As the architecture already knows the distance between the base station and the arrival point (2043m), two circumferences between the two points (start and end) are calculated. The median point between the two circles serves to guide the limit where the UAV can travel. In this specific case, the UAV fell under the second verification rule, where

If $D(I, X) \leq d \rightarrow$ It is within the region, can be seen in [Figure 29](#)

The path taken by Solo 3DR can be seen in [Figure 29](#) (Note: The UAV has a green circle around it to highlight the image). Thus, the UAV is in area *I* and within the permitted radius, so it is safe. No alerts are issued from the security metrics, so the safety metric is the next one to be calculated.

The third step is to calculate the safety metric with NCI. For that, some values were stipulated initially, as presented in [Table 16](#). The IMU and autopilot manipulate data related to the Solo positioning, so their priority is set to 0.5. If Solo is forced to land, it is necessary to establish WiFi communication to locate and retrieve the UAV, which justifies its value of 0.5 as a priority.

GPS is responsible for sending the location signals, in this case, of paramount importance for the mission, so its priority is 1. The remaining modules do not deal with any data that could be considered risky for the UAV, so they are defined with priority 0. Regarding safety, all modules are working correctly in regular operation, so health is set to 0.

Figure 29 – Safe route

Source: The author

Table 16 – Scenario 1: Normal operation - Safety

Module	NCI Safety		
	health	priority	total
GPS	0	1	0.5
IMU	0	0.5	1
Camera	0	0	0
Autopilot	0	0.5	0.25
Motor	0	0	0
Wifi	0	0.5	0.25

Source: The author.

The main implementation of the NCI for safety metrics can be seen in [Source code 2](#):

Source code 2 – NCI Code

```

1: /* NCI Code for Safety */
2: void ReceiveDataHealth (sample::FlightData DataHealth){
3:     double modulePriority = healthData.get_priority_GPS();
4:     double health=DataHealth.get_health();
5:     average(modulePriority, health);
6: }
7: void average(double modulePriority, double health){
8:     double nci_safety = ((health+modulePriority)/2);
9:     cout << "\t NCI safety: " << nci_safety << endl;
10: }
```

After calculating the three metrics of the anomaly-based detection system, it is responsible for notifying the triage module that there are no anomalies on the network. This, in turn, warns the other modules (decision-making module and cyber resilience) that there are no problems to be solved. Finally, the OBERSE of the OODA cycle present in the decision-making keeps the odometry data safe. These data are latitude (at the current time) and longitude (at the current time). All the steps mentioned, from the verification in the anomaly-based detection system to saving the odometry data, are repeated every moment until the operation is successful when reaching its final destination and, finally, delivering vaccines at the hospital.

7.4 Scenario 03: Failure operation

In this test scenario, the aircraft is subjected to a GPS attack, where an attacker tries to trick the UAV into taking a different route to steal vaccines. GPS spoofing is considered to be one of the most recurring threats to UAVs. [Table 17](#) shows the steps concerning how STUART reacts to this situation. It is worth mentioning that there are several ways to perform GPS spoofing. In this test scenario, we are working with the simulation of false location, but the scenario could be replicated for other cases, such as no signal on the network.

Table 17 – Scenario 2: Failure operation

Time	Action	STUART
15:31:00	The UAV leaves the base station and starts to flight	Calculates Anomaly-based detection system
15:31:52		Triage module receives information report
15:31:54		OBSERVE saves historical data
15:32:00	UAV advances a greater radius than allowed in a few seconds	Calculates anomaly-based detection system
15:32:02		Triage module receives information report
15:32:10		Triage module sends an alert to the other modules!
15:32:50		The observer informs the data when orienting it and decides for its choice to restore from the last consistent historical data. Then, ACT sends that order to resilience.
15:32:52		The vulnerable part is isolated, in this case, the GPS.
15:32:59		Resilience restores the GPS location

Source: The author.

As in the previous study in a normal operation, in this one again, the Haversine is the first metric to be calculated. The Haversine converts the angles for radians, collects the time that has passed from the launch (at 15:31:00) to the first position / current position (at 15:31:30), and calculates the distance between the two points. Until then, the UAV is on a stable path. However, after passing some coordinates forward, at 15:31:52, an attempt is made to steal the UAV by falsifying its current position. The average speed is calculated and compared with the average speed supported by the UAV. The 3DR Solo reaches 80 km/h, and in this case, the result was 110.45 km/h. This information is then reported to the triage module.

The second metric is also calculated and is outside the permitted radius zone. The path taken by Solo 3DR can be seen in [Figure 30](#). In this specific case, the UAV fell under the second verification rule, where

Table 18 – Scenario 2: Failed operation - Haversine

Time	Security Metric for GPS			
	Latitude	Longitude	Haversine	Km/h
15:31:00	-021.59.33.6	-047.53.24.4	0	0
15:35:02	-021.59.54.1	-047.53.34.1	691 meters	10.37 km/h
-	The mission continues	-	-	-
15:31:52	-022.00.07.1	-047.54.14.3	675 meters	110.45 k/h

Source: The author.

If $D(I, X) > d \rightarrow$ It is outside the I region

This means that it indicated a location outside the two regions (circumference of the starting point I and circumference of the ending point F). Only with the previous case anomaly would it be enough for the UAV to alert the triage module. However, in this validation scenario, the type of attack and the medium explored was applied in two security metrics.

If we assume that the change of location is not sudden and the UAV is in an acceptable time range, it did not follow the informed route and is outside the region. The tour of the mobile zone would also detect this type of failure. This would be a case of slow spoofing GPS, not addressed in this work's tests, but it is important to note that the STUART modeled with this metric would also detect this attack case. As anomaly has already been detected in insurance cases, notifications are already sent to the triage module because, while the attacker is carrying out the attack, the faster the intrusion is detected and passed on to the decision-making module, the smaller the damage caused. Even some attacks persist for some time, so the faster the IDS reports, the better it will be for the avionics system. The behavior of the NCI in the event of a safety fault was explained in [section 6.4](#). However, it does not apply to this case.

As it has already been informed that there are vulnerabilities in the network, the triage module performs the filtering with the IDS to verify that it is not a false positive. The detection of IDS by signature will seek specific characteristics about the type of attack, in this case, traveling a long distance in a short period of time, and in addition, still outside the permitted mobile zone. Signature IDS has a more favorable index for detecting false positives when compared to anomaly detection, however, it has the limitation of being able to detect only attacks that are in its database. The specific false-positive tests in this dissertation were limited to the characteristics of GPS spoofing. In this scenario, the following steps were performed:

- **Information capture:** this function is responsible for saving the information received by the anomaly detection system;
- **Extraction:** has the function of extracting the characteristics of the information received so that they can be inserted in the attacks table. These characteristics are then sent to the

Figure 30 – False route

Source: The author

characteristic analyzer;

- **Characteristics analyzer:** is responsible for checking if the characteristics match the table of known attacks. If the analyzer does not detect any anomalies, the attack is excluded from the attack table. But in this test case, it is identified that it is GPS spoofing. In this work, the structure of a passive IDS is used (DEVOTI *et al.*, 2020; TIAN *et al.*, 2018). When it identifies that the vulnerability is not a false positive, it issues an alarm to the administrator (decision-making module) to prevent the invasion from continuing. Then, the triage module generates an alert to the other modules for a recovery decision to be executed.

After completing the filtering of the triage module, the decision module begins to perform its actions. During the route, the UAV position is acquired from odometry data. The battery level is also achieved. As the decision making was invoked to solve GPS spoofing, OBVERSE sends data from safe and unsafe locations to ORIENT. When facing GPS spoofing, ORIENT has four options:

1. **Land:** if it is a safety problem, it must land;
2. **Isolate:** if it is a security problem, it should isolate the GPS module from the other essential functions;
3. **Recover:** if it is a security problem and GPS spoofing, it should be restored most three times;
4. **Return base:** if the problem repeats more than three times, then the ORIENT is ordered to return to the home station and ignore any other commands. This was determined because the UAV's chances of being stolen and losing control are high since the attacker could access it repeatedly. If the UAV decides to return to the home station, the possible paths are calculated by varying the safe delta, illustrated in Figure 31.

Therefore, the UAV must decide which route to take to return to the home station, based on the battery amount. The UAV may choose to be more conservative and only fly over previously traveled areas, or it may decide to take more risk and move through areas not previously traveled to arrive at the home quickly. For this type of action, an algorithm was implemented at STUART that traverses its base of safe points (those through which the UAV passed before losing the connection) and verifies which ones are within the radius delimited by the safe delta. Some possible cases with different values for the safe delta are illustrated in Figure 31.

In this way, it is possible to identify all possible safe movements from the point where the UAV is. Finally, from these points, the closest thing to the position the UAV wants to reach is evaluated, and its coordinates are used as a target for the next movements. So on, it is done until

Figure 31 – Return routes for different safe deltas.

Source: Adapted from (BISCEGLIE *et al.*, 2019)

the complete route is established so that the UAV can reach the home station. But this case was not applied in this simulation scenario, as GPS spoofing occurred for the first time. In this case, the DECIDE of the OODA cycle decided to apply the method of recovery through historical data. Recovery is performed by the resilience module².

The resilience module is the last one to be executed at STUART after being invoked by decision-making (detailed in Section 6.7). In this test scenario, the states determined were **isolate**: to isolate the GPS's functionality to not compromise the other parts of the vehicle. In short, the isolation of the GPS (or the vulnerable part) works by preventing the GPS from receiving external commands until it receives the notification that it can continue to execute. This means that the victimized part is no longer exploited. Otherwise, it could even allow the attacker to exploit the vulnerability and access other internal components of the architecture. While the vulnerable party is isolated, the decision-making module looks at how to resolve the problem. Then, the last state is invoked, being that of recovery. Recover the UAV through the consistent

² The checkpoint and recovery are reactive procedures that need to be used with the existing detection mechanisms (anomaly-based detection system and triage module). The recovery of the physical or computational state is triggered for execution if the mechanisms discover any compromise. Otherwise, the system follows the checkpoint protocol to record the states (in the OODA OBSERVE cycle)

historical data that were saved during the trip.

A checkpoint and recovery concept was used through historical data modeled on a state machine to recover the failed system states. This forward roll operation has a much lower overhead than the conventional rollback operation in the context of recovering physical states. The recovery state accommodates the detection delay to improve the accuracy of the stored states (NORRIS *et al.*, 2020; FERRÃO *et al.*, 2020a).

7.4.1 Safety failure

Let's say that the GPS sensor stops sending information to the station, or suffers a deformity in any other part of the body, in this case STUART sends an alert through the NCI, reporting that the GPS has a malfunction, not following the predefined route. It is possible to notice the importance of the safety and security modules working together.

In this case of GPS failure in Table 19, it results in a change in the health value of the damaged GPS to 1, which is reflected in its end, which increases to 1. As a consequence, this affects the NCI and creates an alert to prioritize communication. Therefore, a new mission is defined for the damaged 3DR Solo to maintain communication as long as possible. Consequently, the WiFi transmitter/receiver's priority is changed to 1, raising its NCI to 0.5.

Table 19 – Scenario 2: Failed operation - Safety

Module	NCI Safety		
	health	priority	total
GPS	1	1	1
IMU	0.8	0.5	0.65
Camera	0	0	0
Autopilot	0.8	0.5	0.65
Motors	0	0	0
Wifi	0	1	0.5

Source: The author.

In the case of a safety fault, no restoration task is applied since after a UAV has been compromised, there are still no known ways to recover it physically. However, landing is a chance that the UAV will not be totally lost.

As can be seen, the NCI is an index that can be applied to prioritize communication and for safety purposes due to its sub-indices. For example, prioritizing communications due to a failure in an entity can be dealt with quickly, as in scenario 2, where there was a failure in the mechanism. An alert was issued to prioritize its communication. On the other hand, when it comes to ensuring the safety of an entity, SPHERE SMU can take the appropriate measures based on the increase in the health index. Although very specific, this case study can be seen in many unmanned vehicle applications, and this validation can be extended to other scenarios.

7.5 Final remarks

This chapter showed a practical study with the 3DR solo, and two validation tests through simulation. STUART was disposed of in a scenario to allow vaccines COVID-19 to be delivered with greater security and safety, even in more remote areas.

The results allowed us to conclude that STUART is effective for at least two types of attacks, DDoS and GPS spoofing. The 3DR solo UAV, despite being a very popular avionic model, still does not have enough metrics to prove safety, thus emphasizing the importance of treating these metrics.

The codes for implementing these scenarios are available at <https://github.com/IsadoraFerraio/ICUAS-2021-Stuart-architecture> and can be widely used and cited.

Next chapter presents the conclusions of this work and the future work.

CONCLUSIONS

This dissertation presents a new resilient architecture for unmanned aerial vehicles called STUART. STUART's main differential with other architectures found in the literature is that it has the entire scope for detecting and mitigating vulnerabilities, different from those found that deal only with autonomy or detection. Aiming to provide dynamical recovery, the architecture uses a resilient model that integrates security and safety in a unique system named anomaly-based detection.

Three studies were carried out to analyze the architecture, one with a real UAV and two using computer simulations. The results allowed us to conclude that STUART is effective for at least two types of attacks, DDoS and GPS spoofing. The 3DR solo UAV, despite being a very popular avionic model, still does not have enough metrics to prove safety, thus emphasizing the importance of treating these metrics. The test scenario was the delivery of COVID-19 vaccines. Although this case is very specific, STUART is not limited to it and can be applied in other scenarios.

Finally, different metrics have been proposed for each of the parts that compose STUART. In the anomaly detection system, the safety and security vulnerabilities were addressed and highlighted, showing the importance of the architecture to have mechanisms to detect and mitigate both types. It is expected that these results will serve as a reference not only for UAV architectures but also for embedded and critical systems to adopt an integrated approach to both safety and security visions.

8.1 Intellectual Production

8.1.1 Awards

- Best paper award, WoCCES Organizing Committee.

- Scholarship Grace Hopper Celebration, Anita Borg Institute.

8.1.2 Published papers

- Ferrão, I. G., Pigatto, D. F., Fontes, J. V., Silva, N. B., Espes, D., Dezan, C., & Branco, K. R. (2020, July). STUART: ReSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks undeR atTack. In 2020 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-6). IEEE ([FERRÃO et al., 2020a](#)).
- Ferrão, I. G., da Silva, S. A., Pigatto, D. F., & Branco, K. R. (2020, November). GPS Spoofing: Detecting GPS Fraud in Unmanned Aerial Vehicles. In 2020 Latin American Robotics Symposium (LARS), 2020 Brazilian Symposium on Robotics (SBR) and 2020 Workshop on Robotics in Education (WRE) (pp. 1-6). IEEE ([FERRÃO et al., 2020b](#)).

8.1.3 Submitted papers

- Isadora G. Ferrão, Daniel F. Pigatto, Natassya B. F. Silva, Catherine Dezan, David Espes and Kalinka R. L. J. C. Branco; A resilient UAV architecture for transporting COVID-19 vaccines. IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR, 2021)

8.1.4 Scientific contributions in other studies (not related to the main context of this dissertation)

8.1.4.1 Published magazine

- Ferrão, I. G., Chervinski, J. O., da Silva, S. A., Kreutz, D., Immich, R., Kepler, F., Righi, R. D. R. (2019). Urnas Eletrônicas no Brasil: linha do tempo, evolução e falhas e desafios de segurança. Revista brasileira de computação aplicada.

8.1.4.2 Published paper

- Ferrão, Isadora Garcia, et al. "Robotic assistance for autism: a literature review." 2020 Latin American Robotics Symposium (LARS), 2020 Brazilian Symposium on Robotics (SBR) and 2020 Workshop on Robotics in Education (WRE). IEEE, 2020.

8.1.4.3 Submitted papers

- Andréa Sabedra Bordin, Isadora G. Ferrão, Kalinka R. L. J. C. Branco; Women in Technology: Uma análise bibliométrica dos últimos cinco anos; Women in Information Technology (WIT, 2021).

8.1.5 Participation in events as a guest speaker

- 6th IFMT Computer Week. The real life of a computer scientist. 2020.
- XX SEMAC - Semana da Computação da UNESP. SEMAC. 2020

8.2 Limitations and Difficulties

Due to the vast literature of studies that address aerial vehicles' safety, it was quite a lot of studies to read and compute all articles between the years selected in the systematic review due to study being done manually. In addition, obtaining knowledge about UAVs' functioning proved to be quite complex because it has many technical terms.

Another difficulty encountered was the installation and understanding of the codes and the HAMSTER architecture's organizational structure, because it is an architecture resulting from several master's and doctoral works, it has a very vast structure and several implementation cycles derived from different researchers.

Finally, one of the most significant difficulties was proposing and testing a safety metric since it is not feasible to use a real UAV with a safety fault to carry out the tests. Any sequence of instructions could cause the loss of avionics architecture. However, it was possible to perform the test with sensor data in a computer simulation.

Other kinds of attacks (different from DDoS and GPS Spoofing) were not treated and can't be detected.

Simulation is a limitation, the implementation of the metrics and the entire architecture in a real UAV is a limitation of this study.

8.3 Contributions

The main contributions of this dissertation are:

1. Idealization and implementation of a resilient architecture that manages the network even in the face of attacks;
2. Advancing state of the art through the joint investigation of safety and security;
3. The advance of the logical part regarding the security of the HAMSTER architecture;
4. Advance in state of the art through the implementation of different metrics that together detect GPS spoofing in UAVs and
5. Creation of a new metric for detecting GPS spoofing in a mobile zone area.

8.4 Future works

For future work, the following research possibilities were listed but not limited to:

- Implement and test STUART metrics within Solo;
- Perform tests with the metrics proposed in other types of attacks;
- Implement route planning algorithms for the UAV and carry out tests to verify which has greater effectiveness and less computational cost (an example of an algorithm that will be analyzed is the ant colony-based routing) and
- Propose new metrics for STUART to recognize other types of attacks.

BIBLIOGRAPHY

ABUSHAHMA, R. I. H.; ALI, M. A.; RAHMAN, N. A. A.; AL-SANJARY, O. I. Comparative features of unmanned aerial vehicle (uav) for border protection of libya: a review. In: IEEE. **2019 IEEE 15th International Colloquium on Signal Processing & Its Applications (CSPA)**. [S.l.], 2019. p. 114–119. Citation on page 31.

ACM. **ACM Digital Library**. 2020. <<https://dl.acm.org/>>. Accessed: 2020-01-20. Citation on page 130.

ADWIBOWO, A. Assessments of heavy lift uav quadcopter drone to support covid 19 vaccine cold chain delivery for indigenous people in remote areas in south east asia. **medRxiv**, Cold Spring Harbor Laboratory Press, 2021. Citation on page 23.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Requisitos gerais para aeronaves não tripuladas de uso civil**. [S.l.]: Agência Nacional de Aviação Civil, 2017. Citation on page 28.

AJMAL, S.; RASHEED, A.; QAYYUM, A.; HASAN, A. Classification of vanet mac, routing and approaches a detailed survey. **J. UCS**, v. 20, n. 4, p. 462–487, 2014. Citation on page 58.

ALEMAYEHU, T. S.; KIM, J.-H.; YOON, W. Fault-tolerant uav data acquisition schemes. **Wireless Personal Communications**, Springer, v. 114, p. 1669–1685, 2020. Citation on page 52.

ALWATEER, M.; LOKE, S. W.; ZUCHOWICZ, A. Drone services: issues in drones for location-based services from human-drone interaction to information processing. **Journal of Location Based Services**, Taylor & Francis, v. 13, n. 2, p. 94–127, 2019. Citations on pages 23 and 49.

AMAZON. **3DR Solo Quadcopter**. 2020. Available: <<https://www.amazon.com/3DR-Solo-Quadcopter-No-Gimbal/dp/B00ZPM7BOG>>. Citation on page 86.

ARANHA, D. F.; GOUVÊA, C. P. L.; MARKMANN, T.; WAHBY, R. S.; LIAO, K. **RELIC is an Efficient Library for Cryptography**. 2000. <<https://github.com/relic-toolkit/relic>>. Citation on page 86.

AUSTIN, R. **Unmanned aircraft systems: UAVS design, development and deployment**. [S.l.]: John Wiley & Sons, 2011. (Aerospace Series, v. 54). ISBN 9780470664803. Citation on page 27.

_____. **Unmanned Aircraft Systems: UAVS Design, Development and Deployment**. [S.l.]: Wiley, 2011. ISBN 978-0-470-05819-0. Citation on page 29.

AVTAR, R.; SUAB, S. A.; YUNUS, A. P.; KUMAR, P.; SRIVASTAVA, P. K.; RAMAIAH, M.; JUAN, C. A. Applications of uavs in plantation health and area management in malaysia. In: **Unmanned Aerial Vehicle: Applications in Agriculture and Environment**. [S.l.]: Springer, 2020. p. 85–100. Citation on page 32.

AYAMGA, M.; TEKINERDOGAN, B.; KASSAHUN, A. Exploring the challenges posed by regulations for the use of drones in agriculture in the african context. **Land**, Multidisciplinary Digital Publishing Institute, v. 10, n. 2, p. 164, 2021. Citations on pages 23 and 32.

BACK, S.; CHO, G.; OH, J.; TRAN, X.-T.; OH, H. Autonomous uav trail navigation with obstacle avoidance using deep neural networks. **Journal of Intelligent & Robotic Systems**, Springer, v. 100, n. 3, p. 1195–1211, 2020. Citation on page 52.

BARBER, K. S.; HOLT, J.; BAKER, G. Performance evaluation of domain reference architectures. In: PROC. OF THE 14TH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING AND KNOWLEDGE ENGINEERING. [S.l.]: ACM Press, 2002. p. 225–232. Citation on page 36.

BARMPOUNAKIS, E.; GEROLIMINIS, N. On the new era of urban traffic monitoring with massive drone data: The pneuma large-scale field experiment. **Transportation research part C: emerging technologies**, Elsevier, v. 111, p. 50–71, 2020. Citation on page 84.

BARNES, L.; FIELDS, M.; VALAVANIS, K. Unmanned ground vehicle swarm formation control using potential fields. In: IEEE. **2007 Mediterranean Conference on Control & Automation**. [S.l.], 2007. p. 1–8. Citation on page 27.

BASS, L.; CLEMENTS, P.; KAZMAN, R. **Software architecture in practice**. [S.l.]: Addison-Wesley Professional, 2003. Citation on page 35.

_____. **Software architecture in practice. The SEI Series in Software Engineering**. 2. ed. [S.l.]: Addison-Wesley Publishing Company, 2003. Citation on page 36.

BATORY, D.; COGLIANESE, L.; GOODWIN, M.; SHAFER, S. Creating reference architectures: an example from avionics. In: SSR '95: PROC. OF THE 1995 SYMPOSIUM ON SOFTWARE REUSABILITY. New York, NY: ACM Press, 1995. p. 27–37. Citation on page 36.

BBC. **Drone saves two Australian swimmers in world first**. 2018. <<https://www.bbc.com/news/world-australia-42731112>>. Accessed: 2020-01-20. Citation on page 31.

BEKMEZCI, I.; SAHINGOZ, O. K.; TEMEL, Ş. Flying ad-hoc networks (fanets): A survey. **Ad Hoc Networks**, Elsevier, v. 11, n. 3, p. 1254–1270, 2013. Citation on page 32.

BERGIN, D. L. Cyber-attack and defense simulation framework. **The Journal of Defense Modeling and Simulation**, SAGE Publications Sage UK: London, England, v. 12, n. 4, p. 383–392, 2015. Citation on page 58.

BIOLCHINI, J. C. de A.; MIAN, P. G.; NATALI, A. C. C.; CONTE, T. U.; TRAVASSOS, G. H. Scientific research ontology to support systematic review in software engineering. **Advanced Engineering Informatics**, Elsevier, v. 21, n. 2, p. 133–151, 2007. Citation on page 49.

BISCEGLIE, B. D.; TELLES, F.; ALMEIDA, G.; COSTA, G.; FLORIANO, L. Suporte para tomada de decisão em veículos autônomos [embraer]. **Embraer**, 2019. Citation on page 99.

BLOOMFIELD, R.; LALA, J. Safety-critical systems: The next generation. **IEEE Security & Privacy**, IEEE, v. 11, n. 4, p. 11–13, 2013. Citation on page 24.

BODEAU, D.; GRAUBART, R.; HEINBOCKEL, W.; LADERMAN, E. **Cyber resiliency engineering aid-the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques**. [S.l.], 2015. Citations on pages 63 and 65.

CAMPOS, M. G. Santos de; SOUZA, U. de; EDUARDO, P.; CHANEL, C. P. C.; LACAN, J. Blockchain-based multi-uav surveillance system. 2020. Citation on page [32](#).

CHACÓN-AGUILAR, R.; OSORIO-CÁMARA, J. M.; SANJURJO-JIMENEZ, I.; GONZÁLEZ-GONZÁLEZ, C.; LÓPEZ-CARNERO, J.; PÉREZ-MONEO, B. Covid-19: fever syndrome and neurological symptoms in a neonate. In: ELSEVIER. **Anales de pediatria**. [S.l.], 2020. Citation on page [83](#).

CHAMOLA, V.; HASSIJA, V.; GUPTA, V.; GUIZANI, M. A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. **Ieee access**, IEEE, v. 8, p. 90225–90265, 2020. Citation on page [84](#).

CHATURVEDI, S. K.; SEKHAR, R.; BANERJEE, S.; KAMAL, H. Comparative review study of military and civilian unmanned aerial vehicles (uavs). **INCAS Bulletin**, INCAS-National Institute for Aerospace Research "Elie Carafoli", v. 11, n. 3, p. 183–198, 2019. Citations on pages [23](#), [27](#), and [32](#).

CHEN, H.; HU, Z.; SOLAK, S. Improved delivery policies for future drone-based delivery systems. **European Journal of Operational Research**, Elsevier, 2021. Citation on page [23](#).

CHEN, J.; FENG, Z.; WEN, J.-Y.; LIU, B.; SHA, L. A container-based dos attack-resilient control framework for real-time uav systems. In: IEEE. **2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)**. [S.l.], 2019. p. 1222–1227. Citations on pages [24](#), [53](#), [54](#), and [55](#).

CHEN, J.; XIU, S.; CHEN, X.; GUO, H.; XIE, X. Flounder-net: An efficient cnn for crowd counting by aerial photography. **Neurocomputing**, Elsevier, v. 420, p. 82–89, 2021. Citation on page [23](#).

CHEN, Q.; WEN, X.; WU, F.; YANG, Y. Defect detection and health monitoring of steel structure based on uav integrated with image processing system. In: IOP PUBLISHING. **Journal of Physics: Conference Series**. [S.l.], 2019. v. 1176, n. 5, p. 052074. Citations on pages [27](#) and [32](#).

CHENG, E. **Aerial photography and videography using drones**. [S.l.]: Peachpit Press, 2015. Citation on page [31](#).

CHOE, J. Y.; KIM, J. J.; HWANG, J. Innovative marketing strategies for the successful construction of drone food delivery services: Merging tam with tpb. **Journal of Travel & Tourism Marketing**, Taylor & Francis, v. 38, n. 1, p. 16–30, 2021. Citation on page [23](#).

CHOUDHARY, G.; SHARMA, V.; GUPTA, T.; KIM, J.; YOU, I. Internet of drones (iod): Threats, vulnerability, and security perspectives. **arXiv preprint arXiv:1808.00203**, 2018. Citation on page [67](#).

CHOWDHARY, G.; JOHNSON, E. N.; CHANDRAMOHAN, R.; KIMBRELL, M. S.; CALISE, A. Guidance and control of airplanes under actuator failures and severe structural damage. **Journal of Guidance, Control, and Dynamics**, American Institute of Aeronautics and Astronautics, v. 36, n. 4, p. 1093–1104, 2013. Citation on page [52](#).

CHOWDHURY, S.; MARUFUZZAMAN, M.; TUNC, H.; BIAN, L.; BULLINGTON, W. A modified ant colony optimization algorithm to solve a dynamic traveling salesman problem: a case study with drones for wildlife surveillance. **Journal of Computational Design and Engineering**, Elsevier, v. 6, n. 3, p. 368–386, 2019. Citation on page [31](#).

CHRIKI, A.; TOUATI, H.; SNOUSSI, H.; KAMOUN, F. Centralized cognitive radio based frequency allocation for uavs communication. In: IEEE. **2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)**. [S.l.], 2019. p. 1674–1679. Citation on page 25.

_____. Fanet: Communication, mobility models and security issues. **Computer Networks**, Elsevier, v. 163, p. 106877, 2019. Citation on page 58.

_____. Uav-gcs centralized data-oriented communication architecture for crowd surveillance applications. In: IEEE. **2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)**. [S.l.], 2019. p. 2064–2069. Citation on page 52.

CLAESSION, A.; FREDMAN, D.; SVENSSON, L.; RINGH, M.; HOLLENBERG, J.; NORDBERG, P.; ROSENQVIST, M.; DJARV, T.; ÖSTERBERG, S.; LENNARTSSON, J. *et al.* Unmanned aerial vehicles (drones) in out-of-hospital-cardiac-arrest. **Scandinavian journal of trauma, resuscitation and emergency medicine**, BioMed Central, v. 24, n. 1, p. 124, 2016. Citation on page 31.

CLASESSON, A. Emergency drone system displays effective ems and rescue applications. **Journal of Emergency Medical Services**, 2018. Citation on page 31.

COBAR, M. J.; MONTALVO, C. J.; BENNETT, M.; BUCKNER, C.; HENRY, C. Disaster response fixed wing uav for gulf of mexico field campaign. In: **AIAA Scitech 2021 Forum**. [S.l.: s.n.], 2021. p. 1408. Citation on page 32.

COOKE, N.; ROWE, L.; BENNETT, W.; JORALMON, D. **Remotely Piloted Aircraft Systems: A Human Systems Integration Perspective**. USA: Wiley, 2016. (Aerospace Series). ISBN 9781118965917. Citation on page 28.

CRUTSINGER, G. M.; SHORT, J.; SOLLENBERGER, R. **The future of UAVs in ecology: an insider perspective from the Silicon Valley drone industry**. [S.l.]: NRC Research Press <http://www.nrcresearchpress.com>, 2016. Citation on page 87.

DELMERICO, J.; CIESLEWSKI, T.; REBECQ, H.; FAESSLER, M.; SCARAMUZZA, D. Are we ready for autonomous drone racing? the uzhfpv drone racing dataset. In: **IEEE Int. Conf. Robot. Autom.(ICRA)**. [S.l.: s.n.], 2019. Citation on page 31.

DENG, Z.; MA, C.; ZHU, M. A reconfigurable flight control system architecture for small unmanned aerial vehicles. In: 2012 IEEE INTERNATIONAL SYSTEMS CONFERENCE (SYSCON). Vancouver: IEEE, 2012. p. 1–4. Citations on pages 38, 39, 40, and 52.

DENYER, D.; TRANFIELD, D. Producing a systematic review. Sage Publications Ltd, 2009. Citation on page 49.

DEVOTI, F.; SCIANCALEPORE, V.; FILIPPINI, I.; COSTA-PEREZ, X. Pasid: Exploiting indoor mmwave deployments for passive intrusion detection. In: IEEE. **IEEE INFOCOM 2020-IEEE Conference on Computer Communications**. [S.l.], 2020. p. 1479–1488. Citation on page 98.

DIAS, A. G.; MILIOS, E. E.; OLIVEIRA, M. C. F. de. Trivir: A visualization system to support document retrieval with high recall. In: **Proceedings of the ACM Symposium on Document Engineering 2019**. [S.l.: s.n.], 2019. p. 1–10. Citation on page 56.

DOD, D. of D. The unmanned systems integrated roadmap. In: DEPARTMENT OF DEFENSE (DOD). [S.l.], 2011. p. 2011–2036. Citation on page 29.

DOOLE, M.; ELLERBROEK, J.; KNOOP, V. L.; HOEKSTRA, J. M. Constrained urban airspace design for large-scale drone-based delivery traffic. **Aerospace**, Multidisciplinary Digital Publishing Institute, v. 8, n. 2, p. 38, 2021. Citation on page 23.

DRONEINDUSTRY. **The European Drone Industry**. 2018. <<https://www.droneii.com/wp-content/uploads/2018/06/The-European-Drone-Industry-v1.1.pdf>>. Accessed: 2019-11-23. Citations on pages 23 and 25.

DUAN, T.; HU, P.; SANG, L. Research on route planning of aerial photography of uav in highway greening monitoring. In: IOP PUBLISHING. **Journal of Physics: Conference Series**. [S.l.], 2019. v. 1187, n. 5, p. 052082. Citations on pages 27 and 32.

DURAVKIN, I.; LOKTIONOVA, A.; CARLSSON, A. Method of slow-attack detection. In: IEEE. **2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology**. [S.l.], 2014. p. 171–172. Citation on page 77.

EICK, V. Glocal pacification by vertical means: The case of droneland policing. **Geopolitics**, Taylor & Francis, v. 24, n. 4, p. 811–838, 2019. Citation on page 32.

EICKELMANN, N. S.; RICHARDSON, D. J. An evaluation of software test environment architectures. In: PROC. OF THE 18TH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING. Berlin, Germany: IEEE Computer Society Press, 1996. p. 353–364. Citation on page 36.

ELLIOTT, K. C.; MONTGOMERY, R.; RESNIK, D. B.; GOODWIN, R.; MUDUMBA, T.; BOOTH, J.; WHYTE, K. Drone use for environmental research [perspectives]. **IEEE Geoscience and Remote Sensing Magazine**, IEEE, v. 7, n. 1, p. 106–111, 2019. Citation on page 30.

EMEL'YANOV, S.; MAKAROV, D.; PANOV, A. I.; YAKOVLEV, K. Multilayer cognitive architecture for uav control. **Cognitive Systems Research**, Elsevier, v. 39, p. 58–72, 2016. Citation on page 52.

FAHLSTROM, P.; GLEASON, T. **Introduction to UAV Systems**. 4. ed. [S.l.]: Wiley, 2012. ISBN 978-1-119-97866-4. Citation on page 29.

FAKEGPS. **Fake GPS Location**. 2020. Available: <https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=pt_BR>. Citation on page 84.

FAWZI, H.; TABUADA, P.; DIGGAVI, S. Secure estimation and control for cyber-physical systems under adversarial attacks. **IEEE Transactions on Automatic control**, IEEE, v. 59, n. 6, p. 1454–1467, 2014. Citations on pages 53 and 55.

FERRÃO, I. G.; PIGATTO, D. F.; FONTES, J. V.; SILVA, N. B.; ESPES, D.; DEZAN, C.; BRANCO, K. R. Stuart: Resilient architecture to dynamically manage unmanned aerial vehicle networks under attack. In: IEEE. **2020 IEEE Symposium on Computers and Communications (ISCC)**. [S.l.], 2020. p. 1–6. Citations on pages 23, 24, 100, and 104.

FERRÃO, I. G.; SILVA, S. A. da; PIGATTO, D. F.; BRANCO, K. R. Gps spoofing: Detecting gps fraud in unmanned aerial vehicles. In: IEEE. **2020 Latin American Robotics Symposium (LARS), 2020 Brazilian Symposium on Robotics (SBR) and 2020 Workshop on Robotics in Education (WRE)**. [S.l.], 2020. p. 1–6. Citations on pages 24 and 104.

FILIPPOV, S. The smuggling of tobacco products in europe: Criminogenic potential capacity. **Baltic Journal of Law & Politics**, Sciendo, v. 12, n. 1, p. 35–61, 2019. Citation on page 31.

FOTOHI, R.; NAZEMI, E. An agent-based self-protective method to secure communication between uavs in unmanned aerial vehicle networks. Preprints, 2020. Citation on page 32.

FOUDA, R. M. Security vulnerabilities of cyberphysical unmanned aircraft systems. **IEEE Aerospace and Electronic Systems Magazine**, IEEE, v. 33, n. 9, p. 4–17, 2018. Citation on page 50.

Franco, M. L.; Branco, K. R. J. L.; Braga, R. T. V.; Oliveira, A. L. d.; Dezan, C.; Diguët, J. Model-based dependability analysis of unmanned aerial vehicles - a case study. In: **2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)**. [S.l.: s.n.], 2018. p. 263–270. Citation on page 24.

FRANCO, M. L.; BRANCO, K. R. L. J. C. **UVESAFER - Explorando Safety e Security em veículos aéreos não tripulados**. Master's Thesis (Master's Thesis) — Universidade de São Paulo, 2017. Accessed: 2019-11-19. Citations on pages 51 and 59.

FROSTSULLIVAN. **Analysis of the Global Commercial UAS Market to 2020**. 2017. <<https://ww2.frost.com/event/calendar/analysis-global-commercial-uas-market-2020/?eID=1606>>. Accessed: 2019-11-23. Citations on pages 23 and 25.

GABANI, P. R.; GALA, U. B.; NARWANE, V. S.; RAUT, R. D.; GOVINDARAJAN, U. H.; NARKHEDE, B. E. A viability study using conceptual models for last mile drone logistics operations in populated urban cities of india. **IET Collaborative Intelligent Manufacturing**, Wiley Online Library, 2021. Citation on page 32.

GARG, S.; AUJLA, G. S.; KUMAR, N.; BATRA, S. Tree-based attack–defense model for risk assessment in multi-uav networks. **IEEE Consumer Electronics Magazine**, IEEE, v. 8, n. 6, p. 35–41, 2019. Citation on page 67.

GASPAR, J.; FERREIRA, R.; SEBASTIÃO, P.; SOUTO, N. Capture of uavs through gps spoofing. In: IEEE. **2018 Global Wireless Summit (GWS)**. [S.l.], 2018. p. 21–26. Citation on page 84.

GATTESCHI, V.; LAMBERTI, F.; PARAVATI, G.; SANNA, A.; DEMARTINI, C.; LISANTI, A.; VENEZIA, G. New frontiers of delivery services using drones: A prototype system exploiting a quadcopter for autonomous drug shipments. In: IEEE. **2015 IEEE 39th Annual Computer Software and Applications Conference**. [S.l.], 2015. v. 2, p. 920–927. Citation on page 31.

GELDENHUYS, K. Border security-technology as a solution. **Servamus Community-based Safety and Security Magazine**, SARP Publishers, v. 112, n. 8, p. 20–22, 2019. Citation on page 31.

GIUNCHIGLIA, F.; WALSH, T. A theory of abstraction. **Artificial intelligence**, Elsevier, v. 57, n. 2-3, p. 323–389, 1992. Citation on page 35.

GOLDMAN. **Goldman Sachs Research Report**. 2019. <<https://www.goldmansachs.com/insights/technology-driving-innovation/drones/>>. Accessed: 2019-11-25. Citations on pages 23 and 25.

GORREPATI, R. R.; GUNTUR, S. R. Dronemap: An iot network security in internet of drones. **Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead**, Springer International Publishing, p. 251–268, 2021. Citation on page 24.

GOTO, R. Emerging technologies in lifesaving. In: **Drowning**. [S.l.]: Springer, 2014. p. 299–301. Citation on page 31.

GRAHAM, A. **Communications, Radar and Electronic Warfare**. [S.l.]: John Wiley & Sons, 2011. Citation on page 50.

GRANT, T. Unifying planning and control using an ooda-based architecture. In: ANNUAL RESEARCH CONFERENCE OF THE SOUTH AFRICAN INSTITUTE OF COMPUTER SCIENTISTS AND INFORMATION TECHNOLOGISTS ON IT RESEARCH IN DEVELOPING COUNTRIES, REPUBLIC OF SOUTH AFRICA: SOUTH AFRICAN INSTITUTE FOR COMPUTER SCIENTISTS AND INFORMATION TECHNOLOGISTS. [S.l.], 2005. p. 159–170. Citation on page 35.

GUARDIAN, T. **Heathrow third runway ruled illegal over climate change**. [S.l.]: <https://www.theguardian.com/environment/2020/feb/27/heathrow-third-runway-ruled-illegal-over-climate-change>, 2020. Citations on pages 51 and 52.

GUPTA, L.; JAIN, R.; VASZKUN, G. Survey of important issues in uav communication networks. **IEEE Communications Surveys & Tutorials**, IEEE, v. 18, n. 2, p. 1123–1152, 2015. Citation on page 58.

GUPTA, R.; KUMARI, A.; TANWAR, S. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. **Transactions on Emerging Telecommunications Technologies**, Wiley Online Library, p. e4009, 2020. Citation on page 58.

_____. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5g communications. **Transactions on Emerging Telecommunications Technologies**, Wiley Online Library, v. 32, n. 1, p. e4176, 2021. Citation on page 58.

GUPTA, R.; NAIR, A.; TANWAR, S.; KUMAR, N. Blockchain-assisted secure uav communication in 6g environment: Architecture, opportunities, and challenges. **IET Communications**, Wiley Online Library, 2021. Citation on page 58.

HAIDARI, L. A.; BROWN, S. T.; FERGUSON, M.; BANCROFT, E.; SPIKER, M.; WILCOX, A.; AMBIKAPATHI, R.; SAMPATH, V.; CONNOR, D. L.; LEE, B. Y. The economic and operational value of using drones to transport vaccines. **Vaccine**, Elsevier, v. 34, n. 34, p. 4062–4067, 2016. Citations on pages 31 and 84.

HAMBRECHT, L.; BROWN, R. P.; PIEL, A. K.; WICH, S. A. Detecting ‘poachers’ with drones: Factors influencing the probability of detection with tir and rgb imaging in miombo woodlands, tanzania. **Biological conservation**, Elsevier, v. 233, p. 109–117, 2019. Citation on page 31.

HAMIDA, E. B.; NOURA, H.; ZNAIDI, W. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. **Electronics**, Multidisciplinary Digital Publishing Institute, v. 4, n. 3, p. 380–423, 2015. Citation on page 58.

HENRIO, J.; DELIGNE, T.; NAKASHIMA, T.; WATANABE, T. Route planning for multiple surveillance autonomous drones using a discrete firefly algorithm and a bayesian optimization method. **Artificial Life and Robotics**, Springer, v. 24, n. 1, p. 100–105, 2019. Citation on page 31.

HERNÁNDEZ, E. J. U.; MARTÍNEZ, J. A. S.; SAUCEDO, J. A. M. Optimization of the distribution network using an emerging technology. **Applied Sciences**, Multidisciplinary Digital Publishing Institute, v. 10, n. 3, p. 857, 2020. Citation on page 32.

HIGGINS, R. F.; BARNETT, J. The drone racing league: Building the sport of the future. 2019. Citation on page 31.

HII, M. S. Y.; COURTNEY, P.; ROYALL, P. G. An evaluation of the delivery of medicines using drones. **Drones**, Multidisciplinary Digital Publishing Institute, v. 3, n. 3, p. 52, 2019. Citation on page 84.

HOANG, T. V.; PHUNG, M. D.; DINH, T. H.; HA, Q. P. System architecture for real-time surface inspection using multiple uavs. **arXiv preprint arXiv:1907.03305**, 2019. Citation on page 52.

HODGSON, M. E.; PIOVAN, S. E. An indoor landscape for instruction of 3-d aerial drone imagery. **Journal of Geography in Higher Education**, Taylor & Francis, p. 1–15, 2021. Citation on page 23.

HOGGENMUELLER, M.; HESPANHOL, L.; WIETHOFF, A.; TOMITSCH, M. Self-moving robots and pulverized urban displays: Newcomers in the pervasive display taxonomy. In: **Proceedings of the 8th ACM International Symposium on Pervasive Displays (PerDis' 19)**. [S.l.: s.n.], 2019. Citation on page 30.

HONG, Z.; TONG, X.; CAO, W.; JIANG, S.; CHEN, P.; LIU, S. Rapid three-dimensional detection approach for building damage due to earthquakes by the use of parallel processing of unmanned aerial vehicle imagery. **Journal of Applied Remote Sensing**, International Society for Optics and Photonics, v. 9, n. 1, p. 097292, 2015. Citation on page 52.

HOPPE, M.; KOSCH, T.; KNIERIM, P.; FUNK, M.; SCHMIDT, A. Are drones ready for takeoff? reflecting on challenges and opportunities in human-drone interfaces. In: . [S.l.: s.n.], 2019. Citations on pages 23 and 49.

Hossein Motlagh, N.; TALEB, T.; AROUK, O. Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives. **IEEE Internet of Things Journal**, v. 4662, n. c, p. 1–1, 2016. ISSN 2327-4662. Available: <<http://ieeexplore.ieee.org/document/7572034/>>. Citations on pages 30 and 32.

HUANG, C.; YANG, Z.; KONG, Y.; CHEN, P.; YANG, X.; CHENG, K.-T. T. Learning to capture a film-look video with a camera drone. In: IEEE. **2019 International Conference on Robotics and Automation (ICRA)**. [S.l.], 2019. p. 1871–1877. Citations on pages 27 and 28.

HUANG, H.; ZHENG, X.; YANG, Y.; LIU, J.; LIU, W.; WANG, J. An integrated architecture for intelligence evaluation of automated vehicles. **Accident Analysis & Prevention**, Elsevier, v. 145, p. 105681, 2020. Citation on page 58.

HUANG, X.; TIAN, Y.; HE, Y.; TONG, E.; NIU, W.; LI, C.; LIU, J.; CHANG, L. Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: A threat to swarm intelligence. **Security and Communication Networks**, Hindawi, v. 2020, 2020. Citation on page 52.

HUMPHREY'S, T. **Demonstration of a remote unmanned aerial vehicle hijacking via GPS spoofing**. 2012. Available: <<https://www.youtube.com/watch?v=6qQXVUze8oE>>. Citations on pages 24 and 53.

HUMPHREYS, T. E.; LEDVINA, B. M.; PSIAKI, M. L.; O'HANLON, B. W.; KINTNER, P. M. Assessing the spoofing threat: Development of a portable gps civilian spoofer. In: **Radionavigation laboratory conference proceedings**. [S.l.: s.n.], 2008. Citation on page 50.

HURWITZ, J. S.; BLOOR, R.; KAUFMAN, M.; HALPER, F. **Service Oriented Architecture (SOA) for Dummies**. [S.l.]: John Wiley & Sons, 2009. Citation on page 39.

IEEE. **IEEE Xplore**. 2020. <<https://ieeexplore.ieee.org/Xplore/home.jsp>>. Accessed: 2020-01-20. Citation on page 130.

IKEDA, M.; HONDA, T.; BAROLLI, L. Performance of optimized link state routing protocol for video streaming application in vehicular ad-hoc networks cloud computing. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, v. 27, n. 8, p. 2054–2063, 2015. Citation on page 58.

INNOVATION, D. of B.; SKILLS. **The uk value stream for remotely piloted civil aircraft systems**. 2017. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/590985/remotely-piloted-civil-aircraft-systems-rpas-uk-value-research.pdf>. Accessed: 2019-11-23. Citation on page 25.

ISLAM, A.; SHIN, S. Y. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in internet of things. **Computers & Electrical Engineering**, Elsevier, v. 84, p. 106627, 2020. Citation on page 58.

ISLAM, S.; RAZI, A. A path planning algorithm for collective monitoring using autonomous drones. In: IEEE. **2019 53rd Annual Conference on Information Sciences and Systems (CISS)**. [S.l.], 2019. p. 1–6. Citation on page 31.

ITA, K. Coronavirus disease (covid-19): Current status and prospects for drug and vaccine development. **Archives of medical research**, Elsevier, v. 52, n. 1, p. 15, 2021. Citation on page 83.

IWASZENKO, S.; KALISZ, P.; SŁOTA, M.; RUDZKI, A. Detection of natural gas leakages using a laser-based methane sensor and uav. **Remote Sensing**, Multidisciplinary Digital Publishing Institute, v. 13, n. 3, p. 510, 2021. Citation on page 52.

JACKMAN, A. Visualizations of the small military drone: normalization through 'naturalization'. **Critical Military Studies**, Taylor & Francis, p. 1–26, 2021. Citation on page 23.

JAIN, V.; YUAN, J.-M. Systematic review and meta-analysis of predictive symptoms and comorbidities for severe covid-19 infection. **medRxiv**, Cold Spring Harbor Laboratory Press, 2020. Citation on page 83.

JAVED, M. A.; HAMIDA, E. B.; ZNAIDI, W. Security in intelligent transport systems for smart cities: From theory to practice. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 16, n. 6, p. 879, 2016. Citation on page 58.

JIANG, C.; FANG, Y.; ZHAO, P.; PANNEERSELVAM, J. Intelligent uav identity authentication and safety supervision based on behavior modeling and prediction. **IEEE Transactions on Industrial Informatics**, IEEE, 2020. Citation on page 24.

JORGE, H. G.; SANTOS, L. M. González de; ÁLVAREZ, N. F.; SÁNCHEZ, J. M.; MEDINA, F. N. Operational study of drone spraying application for the disinfection of surfaces against the covid-19 pandemic. **Drones**, Multidisciplinary Digital Publishing Institute, v. 5, n. 1, p. 18, 2021. Citation on page 23.

JUN, L.; ZHIQIANG, Y.; JIANZHONG, Q.; SHUKUAN, L. A role-based reference model for the service properties of service oriented architecture. In: IFITA '09: INTERNATIONAL FORUM ON INFORMATION TECHNOLOGY AND APPLICATIONS. [S.l.], 2009. p. 341–349. Citation on page 36.

JUNG, S.; JO, Y.; KIM, Y.-J. Aerial surveillance with low-altitude long-endurance tethered multirotor uavs using photovoltaic power management system. **Energies**, Multidisciplinary Digital Publishing Institute, v. 12, n. 7, p. 1323, 2019. Citations on pages 23, 27, and 32.

KEANE, J. F.; CARR, S. S. A brief history of early unmanned aircraft. **Johns Hopkins APL Technical Digest**, Citeseer, v. 32, n. 3, p. 558–571, 2013. Citation on page 27.

KELLY, L. Threats to civilian aviation since 1975. Institute of Development Studies, 2021. Citation on page 52.

KERNS, A. J.; SHEPARD, D. P.; BHATTI, J. A.; HUMPHREYS, T. E. Unmanned aircraft capture and control via gps spoofing. **Journal of Field Robotics**, Wiley Online Library, v. 31, n. 4, p. 617–636, 2014. Citation on page 84.

KHELIFI, H.; LUO, S.; NOUR, B.; MOUNGLA, H.; FAHEEM, Y.; HUSSAIN, R.; KSENTINI, A. Named data networking in vehicular ad hoc networks: State-of-the-art and challenges. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 1, p. 320–351, 2019. Citation on page 58.

KHOO, O. Drone feminism: technology, surveillance and entanglement in laura poitras' astro noise. **Feminist Media Studies**, Taylor & Francis, p. 1–11, 2019. Citation on page 31.

KILLE, T.; BATES, P. R.; LEE, S. Y. **Unmanned Aerial Vehicles in Civilian Logistics and Supply Chain Management**. [S.l.]: IGI Global, 2019. Citations on pages 27 and 28.

KIM, J.; KIM, S.; JU, C.; SON, H. I. Unmanned aerial vehicles in agriculture: A review of perspective of platform, control, and applications. **IEEE Access**, IEEE, v. 7, p. 105100–105115, 2019. Citations on pages 27 and 32.

KIM, J. J.; KIM, I.; HWANG, J. A change of perceived innovativeness for contactless food delivery services using drones after the outbreak of covid-19. **International Journal of Hospitality Management**, Elsevier, v. 93, p. 102758, 2021. Citation on page 84.

KIM, Y.; JO, J.; SHRESTHA, S. A Server-Based Real-Time Privacy Protection Scheme against Video Surveillance by Unmanned Aerial Systems. In: **International Conference on Unmanned Aircraft Systems (ICUAS)**. Orlando, USA: IEEE, 2014. p. 684–691. ISBN 978-1-4799-2376-2. Available: <<http://dx.doi.org/10.1109/ICUAS.2014.6842313>>. Citation on page 32.

KIRKLAND, B. R. **VOODIO: Proposal for an Online Video Content Creation Tool**. Phd Thesis (PhD Thesis) — Virginia Tech, 2020. Citation on page 32.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. Citeseer, 2007. Citation on page 49.

KLAUSER, F. Police drones and the air: Towards a volumetric geopolitics of security. **Swiss Political Science Review**, Wiley Online Library, 2021. Citation on page 23.

_____. Policing with the drone: Towards an aerial geopolitics of security. **Security Dialogue**, SAGE Publications Sage UK: London, England, p. 0967010621992661, 2021. Citation on page 32.

KNOBLAUCH, A. M.; ROSA, S. de la; SHERMAN, J.; BLAUVELT, C.; MATEMBA, C.; MAXIM, L.; DEFAWE, O. D.; GUEYE, A.; ROBERTSON, J.; MCKINNEY, J. *et al.* Bi-directional drones to strengthen healthcare provision: experiences and lessons from madagascar, malawi and senegal. **BMJ Global Health**, BMJ Specialist Journals, v. 4, n. 4, p. e001541, 2019. Citations on pages 27 and 28.

KO, Y.; KIM, J.; DUGUMA, D. G.; ASTILLO, P. V.; YOU, I.; PAU, G. Drone secure communication protocol for future sensitive applications in military zone. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 21, n. 6, p. 2057, 2021. Citation on page 32.

KOH, C. H.; LOW, K.; LI, L.; ZHAO, Y.; DENG, C.; TAN, S. K.; CHEN, Y.; YEAP, B. C.; LI, X. Weight threshold estimation of falling uavs (unmanned aerial vehicles) based on impact energy. **Transportation Research Part C: Emerging Technologies**, Elsevier, v. 93, p. 228–255, 2018. Citation on page 52.

KOMODA, N. Service oriented architecture (soa) in industrial systems. In: IEEE. **2006 4th IEEE international conference on industrial informatics**. [S.l.], 2006. p. 1–5. Citation on page 39.

KONG, F.; XU, M.; WEIMER, J.; SOKOLSKY, O.; LEE, I. Cyber-physical system checkpointing and recovery. In: IEEE. **2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)**. [S.l.], 2018. p. 22–31. Citations on pages 53 and 55.

KUCHAR, J. K. Safety analysis methodology for unmanned aerial vehicle (uav) collision avoidance systems. In: **USA/Europe Air Traffic Management R&D Seminars**. [S.l.: s.n.], 2005. v. 12. Citation on page 24.

KUMAR, A.; VARADARAJAN, V.; KUMAR, A.; DADHEECH, P.; CHOUDHARY, S. S.; KUMAR, V. A.; PANIGRAHI, B.; VELUVOLU, K. C. Black hole attack detection in vehicular ad-hoc network using secure aodv routing algorithm. **Microprocessors and Microsystems**, Elsevier, v. 80, p. 103352, 2021. Citation on page 58.

KUNOVJANEK, M.; WANKMÜLLER, C. Containing the covid-19 pandemic with drones- feasibility of a drone enabled back-up transport system. **Transport Policy**, Elsevier, 2021. Citation on page 32.

LASZLO, B.; AGOSTON, R.; XU, Q. Conceptual approach of measuring the professional and economic effectiveness of drone applications supporting forest fire management. **Procedia engineering**, Elsevier, v. 211, p. 8–17, 2018. Citation on page 52.

LEOBONS, C. M. O conceito de resiliência aplicado a sistemas de transportes. In: . [S.l.: s.n.], 2017. p. 12. Citation on page 53.

LEPPÄVIITA, N. J. Creation of drone education curriculum for security guards and security officers. 2021. Citation on page 32.

LIN, C.; HE, D.; KUMAR, N.; CHOO, K.-K. R.; VINEL, A.; HUANG, X. Security and privacy for the internet of drones: Challenges and solutions. **IEEE Communications Magazine**, IEEE, v. 56, n. 1, p. 64–69, 2018. Citation on page 58.

MADEMLIS, I.; NIKOLAIDIS, N.; TEFAS, A.; PITAS, I.; WAGNER, T.; MESSINA, A. Autonomous uav cinematography: A tutorial and a formalized shot-type taxonomy. **ACM Computing Surveys (CSUR)**, ACM, v. 52, n. 5, p. 105, 2019. Citations on pages 23, 27, and 32.

MAES, W. H.; STEPPE, K. Perspectives for remote sensing with unmanned aerial vehicles in precision agriculture. **Trends in plant science**, Elsevier, v. 24, n. 2, p. 152–164, 2019. Citation on page 27.

MAGSINO, E. R.; SAY, M. F.; TAN, J. A. Achieving complete uav delivery in the presence of motor failures. In: IEEE. **2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)**. [S.l.], 2020. p. 1–5. Citation on page 52.

MAILLOUX, L. O.; GRIMAILA, M. Advancing cybersecurity: The growing need for a cyber-resiliency workforce. **IT Professional**, IEEE, v. 20, n. 3, p. 23–30, 2018. Citation on page 66.

MAJUMDAR, P.; BISWAS, A.; SAHU, S. Covid-19 pandemic and lockdown: cause of sleep disruption, depression, somatic pain, and increased screen exposure of office workers and students of india. **Chronobiology International**, Taylor & Francis, v. 37, n. 8, p. 1191–1200, 2020. Citation on page 83.

MARCONATO, E. A. **Modelo de arquitetura em camadas para interconexão de sistemas em SANT**. Phd Thesis (PhD Thesis) — Universidade de São Paulo, 2014. Citations on pages 38 and 40.

Marconato, E. A.; Pigatto, D. F.; Branco, K. R. L. J. C.; Branco, L. H. C. Larissa: Layered architecture model for interconnection of systems in uas. In: **2014 International Conference on Unmanned Aircraft Systems (ICUAS)**. [S.l.: s.n.], 2014. p. 20–31. Citations on pages 36, 41, and 52.

MARKETS; MARKETS. **Le cabinet MarketsandMarkets annonce de belles perspectives de croissance annuelle pour ce marché mondial dans les 5 ans à venir, prévoyant notamment la multiplication rapide des applications commerciales**. 2017. <<http://www.mesures.com/vision-industrielle/item/13721-une-croissance-proche-de-20-sur-le-marche-des-drones>>. Accessed: 2019-11-25. Citation on page 25.

MATEO-AROCA, A.; GARCÍA-MATEOS, G.; RUIZ-CANALES, A.; MOLINA-GARCÍA-PARDO, J. M.; MOLINA-MARTÍNEZ, J. M. Remote image capture system to improve aerial supervision for precision irrigation in agriculture. **Water**, Multidisciplinary Digital Publishing Institute, v. 11, n. 2, p. 255, 2019. Citation on page 30.

MAXWELL, P.; BENNETT, D.; KORPELA, C. The cyber defense review a joint production of the army cyber institute and marine corps forces cyber command battlefield asymmetric robotic threat. **Cyber Defense Review**, 02 2016. Citation on page 50.

MEI, R. Robust control for the suspension cable system of the unmanned helicopter with sensor fault under complex environment. **Complexity**, Hindawi, v. 2021, 2021. Citation on page 51.

MEINEN, B. U.; ROBINSON, D. T. Mapping erosion and deposition in an agricultural landscape: Optimization of uav image acquisition schemes for sfm-mvs. **Remote Sensing of Environment**, Elsevier, v. 239, p. 111666, 2020. Citation on page 32.

MEJRI, M. N.; BEN-OTHTMAN, J.; HAMDI, M. Survey on vanet security challenges and possible cryptographic solutions. **Vehicular Communications**, Elsevier, v. 1, n. 2, p. 53–66, 2014. Citation on page 58.

MENDES, A. **Arquitetura de Software: Desenvolvimento orientado para arquitetura**. [S.l.]: Campus, 2002. Citation on page 36.

MENNI, C.; VALDES, A.; FREYDIN, M. B.; GANESH, S.; MOUSTAFA, J. E.-S.; VISCONTI, A.; HYSI, P.; BOWYER, R. C.; MANGINO, M.; FALCHI, M. *et al.* Loss of smell and taste in combination with other symptoms is a strong predictor of covid-19 infection. **MedRxiv**, Cold Spring Harbor Laboratory Press, 2020. Citation on page 83.

MEOLA, A. **Drone market shows positive outlook with strong industry growth and trends**. 2017. <<https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts-2017-7>>. Accessed: 2019-11-22. Citations on pages 23 and 25.

MERKEL, D. Docker: lightweight linux containers for consistent development and deployment. **Linux Journal**, v. 2014, n. 239, p. 2, 2014. Citation on page 54.

MICHAEL, O. T.; OLUSEGUN, A.; PAUL, O. A.; FELIX, S. O.; KANIKI, F. R.; AYOSANMI, O. S.; WADE, D.; FAITH, A. O.; TERNA, G. Z.; MUSA, A. *et al.* The use of uav/drones in the optimization of nigeria vaccine supply chain. **International Journal of Scientific & Engineering Research**, v. 10, n. 10, p. 1273–1279, 2019. Citation on page 84.

MISNAN, M. F. bin; ARSHAD, N. M.; RAZAK, N. A. Construction sonar sensor model of low altitude field mapping sensors for application on a uav. In: IEEE. **2012 IEEE 8th International Colloquium on Signal Processing and its Applications**. [S.l.], 2012. p. 446–450. Citation on page 51.

MITCHELL, R.; CHEN, I.-R. A survey of intrusion detection techniques for cyber-physical systems. **ACM Computing Surveys (CSUR)**, ACM, v. 46, n. 4, p. 55, 2014. Citation on page 53.

MOEIN, S. T.; HASHEMIAN, S. M.; MANSOURAFSHAR, B.; KHORRAM-TOUSI, A.; TABARSI, P.; DOTY, R. L. Smell dysfunction: a biomarker for covid-19. In: WILEY ONLINE LIBRARY. **International forum of allergy & rhinology**. [S.l.], 2020. v. 10, n. 8, p. 944–950. Citation on page 83.

MONDAL, S.; WILLIAMSON, A.; XU, Z.; TSOURDOS, A. Autonomous architecture for uav-based agricultural survey. In: **AIAA Scitech 2020 Forum**. [S.l.: s.n.], 2020. p. 2298. Citation on page 52.

NAKAGAWA, E. Y.; BARBOSA, E. F.; MALDONADO, J. C. Exploring ontologies to support the establishment of reference architectures: An example on software testing. In: IEEE. **2009 Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture**. [S.l.], 2009. p. 249–252. Citation on page 35.

NAKAGAWA, E. Y.; OQUENDO, F.; MALDONADO, J. C. Reference architectures. **Software Architecture 1**, Wiley Online Library, p. 55–82, 2014. Citation on page 35.

NIST. **4D/RCS: Reference Model Architecture for Unmanned Vehicle Systems Version 2.0**. [S.l.], 2002. Citation on page 36.

NORRIS, M.; CELIK, B.; VENKATESH, P.; ZHAO, S.; MCDANIEL, P.; SIVASUBRAMANIAM, A.; TAN, G. Iotrepair: Systematically addressing device faults in commodity iot. In: **IEEE. 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)**. [S.l.], 2020. p. 142–148. Citation on page 100.

NUIJTEN, R. J.; KOOISTRA, L.; DEYN, G. B. D. Using unmanned aerial systems (uas) and object-based image analysis (obia) for measuring plant-soil feedback effects on crop productivity. **Drones**, Multidisciplinary Digital Publishing Institute, v. 3, n. 3, p. 54, 2019. Citation on page 30.

OBANAWA, H.; SHIBATA, H. Applications of uav remote sensing to topographic and vegetation surveys. In: **Unmanned Aerial Vehicle: Applications in Agriculture and Environment**. [S.l.]: Springer, 2020. p. 131–142. Citation on page 32.

OLSON, L.; BURNS, L. A common architecture prototype for army tactical and fcs uavs. In: **THE 24TH DIGITAL AVIONICS SYSTEMS CONFERENCE. DASC 2005**. Washington: IEEE, 2005. p. 8.B.5–1 – 8.B.5–11. Citations on pages 36, 37, 38, and 52.

ORDOUKHANIAN, E.; MADNI, A. M. Resilient multi-uav operation: key concepts and challenges. In: **54th AIAA Aerospace Sciences Meeting**. [S.l.: s.n.], 2016. p. 0475. Citations on pages 53 and 55.

_____. Model-based approach to engineering resilience in multi-uav systems. **Systems**, Multidisciplinary Digital Publishing Institute, v. 7, n. 1, p. 11, 2019. Citations on pages 53 and 55.

PAGANINI, P. **A hacker developed Maldrone, the first malware for drones**. 2015. <<http://securityaffairs.co/wordpress/32767/hacking/maldrone-malware-for-drones.html>>. Accessed: 2019-11-20. Citations on pages 24 and 53.

PAGE, V.; WEBSTER, M.; FISHER, M.; JUMP, M. Towards a methodology to test uavs in hazardous environments. 2019. Citation on page 24.

PAJIC, M.; WEIMER, J.; BEZZO, N.; TABUADA, P.; SOKOLSKY, O.; LEE, I.; PAPPAS, G. J. Robustness of attack-resilient state estimators. In: **IEEE COMPUTER SOCIETY. ICCPS'14: ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014)**. [S.l.], 2014. p. 163–174. Citation on page 53.

PAN, A.; LIU, L.; WANG, C.; GUO, H.; HAO, X.; WANG, Q.; HUANG, J.; HE, N.; YU, H.; LIN, X. *et al.* Association of public health interventions with the epidemiology of the covid-19 outbreak in wuhan, china. **Jama**, American Medical Association, v. 323, n. 19, p. 1915–1923, 2020. Citation on page 83.

PASQUALETTI, F.; DÖRFLER, F.; BULLO, F. Attack detection and identification in cyber-physical systems. **IEEE transactions on automatic control**, IEEE, v. 58, n. 11, p. 2715–2729, 2013. Citation on page 55.

PASTOR, E.; LOPEZ, J.; ROYO, P. An embedded architecture for mission control of unmanned aerial vehicles. In: 9TH EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN ARCHITECTURES, METHODS AND TOOLS. Dubrovnik: IEEE Computer Society, 2006. p. 554–560. Citation on page 36.

PAVLIK, J. V. **Journalism in the age of virtual reality: How experiential media are transforming news**. [S.l.]: Columbia University Press, 2019. Citation on page 31.

PENNY, S. G.; WHITE, R. L.; SCOTT, D. M.; MACTAVISH, L.; PERNETTA, A. P. Using drones and sirens to elicit avoidance behaviour in white rhinoceros as an anti-poaching tactic. **Proceedings of the Royal Society B**, The Royal Society, v. 286, n. 1907, p. 20191135, 2019. Citation on page 30.

PETIT, J.; STOTTELAAR, B.; FEIRI, M.; KARGL, F. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. **Black Hat Europe**, v. 11, p. 2015, 2015. Citation on page 53.

PIGATTO, D. F. **HAMSTER healthy, mobility and security-based data communication architecture for unmanned systems**. Phd Thesis (PhD Thesis) — Universidade de São Paulo, 2017. Citations on pages 41, 42, 76, and 86.

PIGATTO, D. F.; GONÇALVES, L.; PINTO, A. S. R.; ROBERTO, G. F.; FILHO, J. F. R.; BRANCO, K. R. L. J. C. Hamster-healthy, mobility and security-based data communication architecture for unmanned aircraft systems. In: IEEE. **2014 International Conference on Unmanned Aircraft Systems (ICUAS)**. [S.l.], 2014. p. 52–63. Citation on page 58.

PIGATTO, D. F.; GONÇALVES, L.; ROBERTO, G. F.; FILHO, J. F. R.; SILVA, N. B. F. D.; PINTO, A. R.; BRANCO, K. R. L. J. C. The hamster data communication architecture for unmanned aerial, ground and aquatic systems. **Journal of Intelligent & Robotic Systems**, Springer, v. 84, n. 1-4, p. 705–723, 2016. Citations on pages 41, 55, 58, and 86.

PIGATTO, D. F.; SMITH, J.; LUCAS, K. R.; BRANCO, J. C. Sphere: A novel platform for increasing safety & security on unmanned systems. In: IEEE. **2015 International Conference on Unmanned Aircraft Systems (ICUAS)**. [S.l.], 2015. p. 1059–1066. Citation on page 43.

POURPANAH, F.; ZHANG, B.; MA, R.; HAO, Q. Anomaly detection and condition monitoring of uav motors and propellers. In: IEEE. **2018 IEEE SENSORS**. [S.l.], 2018. p. 1–4. Citation on page 51.

POYRAZ, B. Ç.; POYRAZ, C. A.; OLGUN, Y.; GÜREL, Ö.; ALKAN, S.; ÖZDEMİR, Y. E.; BALKAN, İ. İ.; KARAALI, R. Psychiatric morbidity and protracted symptoms after covid-19. **Psychiatry research**, Elsevier, v. 295, p. 113604, 2021. Citation on page 83.

PREETH, E.; MULERICKAL, F. J. P.; PAUL, B.; SASTRI, Y. Evaluation of docker containers based on hardware utilization. In: IEEE. **2015 International Conference on Control Communication & Computing India (ICCC)**. [S.l.], 2015. p. 697–700. Citation on page 54.

PULLETI, U. K.; GONIA, P.; MAHASANAN, A. V. **Generating a three-dimensional model of an industrial plant using an unmanned aerial vehicle**. [S.l.]: Google Patents, 2019. US Patent 10,250,821. Citation on page 27.

QUINCOZES, S. E.; KAZIENKO, J. F. Machine learning methods assessment for denial of service detection in wireless sensor networks. In: IEEE. **2020 IEEE 6th World Forum on Internet of Things (WF-IoT)**. [S.l.], 2020. p. 1–6. Citation on page 77.

RAJ, A.; SAH, B. Analyzing critical success factors for implementation of drones in the logistics sector using grey-dematel based approach. **Computers & Industrial Engineering**, Elsevier, v. 138, p. 106118, 2019. Citations on pages [27](#) and [32](#).

REGLI, W. C.; MAYK, I.; DUGNA, C. J.; KOPENA, J. B.; LASS, R. N.; MODI, P. J.; MONGAN, W. M.; SALVAGE, J. K.; SULTANIK, E. A. Development and specification of a reference model for agent-based systems. **IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews**, v. 39, n. 5, p. 572–596, 2009. Citation on page [36](#).

REN, X.; TAN, L.; JIAQI, S.; LIAN, X. Multi-target uav path planning based on improved rrt algorithm. In: IOP PUBLISHING. **Journal of Physics: Conference Series**. [S.l.], 2021. v. 1786, n. 1, p. 012038. Citation on page [52](#).

RESNIK, D. B.; ELLIOTT, K. C. Using drones to study human beings: ethical and regulatory issues. **Science and engineering ethics**, Springer, v. 25, n. 3, p. 707–718, 2019. Citations on pages [27](#) and [28](#).

ROBUSTO, C. C. The cosine-haversine formula. **The American Mathematical Monthly**, JSTOR, v. 64, n. 1, p. 38–40, 1957. Citation on page [73](#).

ROCKE, B.; RUFFELL, A.; DONNELLY, L. Drone aerial imagery for the simulation of a neonate burial based on the geoforensic search strategy (gss). **Journal of Forensic Sciences**, Wiley Online Library, 2021. Citation on page [32](#).

RODRIGUES, M.; BRANCO, K. R. L. J. C. Cloud–sphere: Towards secure uav service provision. **Journal of Intelligent & Robotic Systems**, Springer, v. 97, n. 1, p. 249–268, 2020. Citations on pages [44](#), [45](#), [46](#), and [87](#).

RONG-XIAO, G.; JI-WEI, T.; BU-HONG, W.; FU-TE, S. Cyber-physical attack threats analysis for uavs from cps perspective. In: IEEE. **2020 International Conference on Computer Engineering and Application (ICCEA)**. [S.l.], 2020. p. 259–263. Citation on page [52](#).

ROSENDE, S. B.; SÁNCHEZ-SORIANO, J.; MUÑOZ, C. Q. G.; ANDRÉS, J. F. Remote management architecture of uav fleets for maintenance, surveillance, and security tasks in solar power plants. **Energies**, Multidisciplinary Digital Publishing Institute, v. 13, n. 21, p. 5712, 2020. Citation on page [58](#).

ROUSSEAU, R.; BRETON, R. The m-ooda: A model incorporating control functions and teamwork in the ooda loop. In: CITESEER. **Proc. Command and Control Res, & Tech. Symp.** [S.l.], 2004. Citations on pages [78](#) and [79](#).

RUSSELL, L.; GOUBRAN, R.; KWAMENA, F. Emerging urban challenge: Rpas/uavs in cities. In: IEEE. **2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)**. [S.l.], 2019. p. 546–553. Citation on page [52](#).

RUTKIN, A. H. spoofers use fake gps signals to knock a yacht off course. **MIT Technology Review**, 2013. Citation on page [50](#).

SAFADINHO, D.; RAMOS, J.; RIBEIRO, R.; FILIPE, V.; BARROSO, J.; PEREIRA, A. Uav landing using computer vision techniques for human detection. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 20, n. 3, p. 613, 2020. Citation on page [58](#).

SAHAWNEH, L.; JARRAH, M. Development and calibration of low cost mems imu for uav applications. In: IEEE. **2008 5th International Symposium on Mechatronics and Its Applications**. [S.l.], 2008. p. 1–9. Citation on page 51.

SÁNCHEZ-GARCÍA, J.; REINA, D.; TORAL, S. A distributed pso-based exploration algorithm for a uav network assisting a disaster scenario. **Future Generation Computer Systems**, Elsevier, v. 90, p. 129–148, 2019. Citation on page 32.

SANDKUHL, K.; MESSER, B. Towards reference architectures for distributed groupware applications. In: 8TH EUROMICRO WORKSHOP ON PARALLEL AND DISTRIBUTED PROCESSING. Rhodes, Greece, 2000. Citation on page 36.

SATELL, M. **Ultimate List of Drone Stats for 2021**. [S.l.]: <https://www.phillybyair.com/blog/drone-stats/>, 2021. Citation on page 25.

SAVKIN, A. V.; HUANG, H. Asymptotically optimal deployment of drones for surveillance and monitoring. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 19, n. 9, p. 2068, 2019. Citation on page 31.

SAYYED, A.; ARAÚJO, G. M. D.; BODANESE, J. P.; BECKER, L. B. Dual-stack single-radio communication architecture for uav acting as a mobile node to collect data in wsns. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 15, n. 9, p. 23376–23401, 2015. Citation on page 52.

SCHIJNDEL, B. S. van; SUN, S.; VISSER, C. de. Fast fault detection on a quadrotor using on-board sensors and a kalman filter approach. **arXiv preprint arXiv:2102.06439**, 2021. Citation on page 52.

SCHOLLIERS, J.; SAMBEEK, M. V.; MOERMAN, K. Integration of vulnerable road users in cooperative its systems. **European transport research review**, Springer, v. 9, n. 2, p. 15, 2017. Citation on page 58.

SCHWARTZ, K. L.; MURTI, M.; FINKELSTEIN, M.; LEIS, J. A.; FITZGERALD-HUSEK, A.; BOURNS, L.; MEGHANI, H.; SAUNDERS, A.; ALLEN, V.; YAFFE, B. Lack of covid-19 transmission on an international flight. **Cmaj**, Can Med Assoc, v. 192, n. 15, p. E410–E410, 2020. Citation on page 83.

SCOPUS. **Scopus Lybrary**. 2020. <<https://www.scopus.com/standard/marketing.uri>>. Accessed: 2020-01-20. Citation on page 130.

SHAFIQUE, A.; MEHMOOD, A.; ELHADEF, M. Survey of security protocols and vulnerabilities in unmanned aerial vehicles. **IEEE Access**, IEEE, v. 9, p. 46927–46948, 2021. Citation on page 24.

SHEKARI, A. M. Ocean savior from above: Small unmanned aircraft systems (suas) operations during near-shore ocean rescues. **McNair Scholars Research Journal**, v. 5, n. 1, p. 1, 2018. Citation on page 31.

SHEPARD, D. P.; BHATTI, J. A.; HUMPHREYS, T. E.; FANSLER, A. A. Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks. In: **Radionavigation Laboratory Conference Proceedings**. [S.l.: s.n.], 2012. Citations on pages 50 and 84.

SHEPARDSON, D. **U.S. commercial drone use to expand tenfold by 2021: government agency**. [S.l.]: <https://www.reuters.com/article/us-usa-drones-idUSKBN16S2NM>, 2021. Citation on page 25.

SHIN, Y.-H.; KIM, D.; SON, S.; HAM, J.-w.; OH, K.-Y. Vibration isolation of a surveillance system equipped in a drone with mode decoupling. **Applied Sciences**, Multidisciplinary Digital Publishing Institute, v. 11, n. 4, p. 1961, 2021. Citation on page 23.

SIEGEL, J. E.; ERB, D. C.; SARMA, S. E. A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas. **IEEE Transactions on Intelligent Transportation Systems**, IEEE, v. 19, n. 8, p. 2391–2406, 2017. Citation on page 58.

SINGH, P. K.; NANDI, S. K.; NANDI, S. A tutorial survey on vehicular communication state of the art, and future research directions. **Vehicular Communications**, Elsevier, v. 18, p. 100164, 2019. Citation on page 58.

SISTEMAS de Aeronaves Remotamente Pilotadas e o Acesso ao Espaço Aéreo Brasileiro. Brazil: Departamento de Controle do Espaço Aéreo, 2016. Citation on page 28.

SPEARS, A.; HUNT, L.; ABDULRAHIM, M.; SANDERS, A.; GRZYWNA, J. A trusted autopilot architecture for gps-denied and experimental uav operations. In: . [S.l.: s.n.], 2016. Citations on pages 24 and 50.

SRINIVASAN, A.; VIJAYAKUMAR, A.; MAKUR, A. Compressive sensing-based on-board intrusion detection for a surveillance drone. In: IEEE. **2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)**. [S.l.], 2019. p. 1–5. Citation on page 31.

STANKOV, U.; KENNEL, J.; MORRISON, A. M.; VUJIČIĆ, M. D. The view from above: The relevance of shared aerial drone videos for destination marketing. **Journal of Travel & Tourism Marketing**, Taylor & Francis, p. 1–15, 2019. Citation on page 31.

SUBHAN, I.; GHAZI, S. S.; NABI, S. *et al.* Use of drones (unmanned aerial vehicles) for supporting emergency medical services in india. **Apollo Medicine**, Medknow Publications, v. 16, n. 1, p. 61, 2019. Citations on pages 27 and 28.

SUJATHA, K.; DHARMAR, V.; BHUVANESWARAN, R. Design of genetic algorithm based ids for manet. In: IEEE. **2012 International Conference on Recent Trends in Information Technology**. [S.l.], 2012. p. 28–33. Citation on page 77.

SUNG, Y.-H.; KIM, H.-Y.; HAN, J.-H.; LEE, D.-K. Self-learning mav under safety-guaranteed flight test environment. In: **AIAA Scitech 2020 Forum**. [S.l.: s.n.], 2020. p. 0261. Citation on page 24.

TAN, L. K. L.; LIM, B. C.; PARK, G.; LOW, K. H.; YEO, V. C. S. Public acceptance of drone applications in a highly urbanized environment. **Technology in Society**, Elsevier, v. 64, p. 101462, 2021. Citation on page 23.

TANENBAUM, A. s; WETHERALL, D. J. Computer networks. Pearson, 2010. Citation on page 77.

THUY, C. T.; WATANABE, A.; WAKUTSU, R. Cloud-based 3d data processing and modeling for uav application in disaster response and construction fields. In: **Geotechnics for Sustainable Infrastructure Development**. [S.l.]: Springer, 2020. p. 1177–1182. Citation on page 32.

TIAN, H.; LIU, Y.; LI, Y.; WU, C.-H.; CHEN, B.; KRAEMER, M. U.; LI, B.; CAI, J.; XU, B.; YANG, Q. *et al.* An investigation of transmission control measures during the first 50 days of the covid-19 epidemic in china. **Science**, American Association for the Advancement of Science, v. 368, n. 6491, p. 638–642, 2020. Citation on page [83](#).

TIAN, Z.; LI, Y.; ZHOU, M.; LI, Z. Wifi-based adaptive indoor passive intrusion detection. In: IEEE. **2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)**. [S.l.], 2018. p. 1–5. Citation on page [98](#).

TORRES-RUA, A.; ABOUTALEBI, M.; WRIGHT, T.; NASSAR, A.; GUILLEVIC, P.; HIPPS, L.; GAO, F.; JIM, K.; ALSINA, M. M.; COOPMANS, C. *et al.* Estimation of surface thermal emissivity in a vineyard for uav microbolometer thermal cameras using nasa hytes hyperspectral thermal, and landsat and aggieair optical data. In: INTERNATIONAL SOCIETY FOR OPTICS AND PHOTONICS. **Autonomous Air and Ground Sensing Systems for Agricultural Optimization and Phenotyping IV**. [S.l.], 2019. v. 11008, p. 1100802. Citation on page [31](#).

ULLAH, S.; KIM, K.-I.; KIM, K. H.; IMRAN, M.; KHAN, P.; TOVAR, E.; ALI, F. Uav-enabled healthcare architecture: Issues and challenges. **Future Generation Computer Systems**, Elsevier, v. 97, p. 425–432, 2019. Citation on page [52](#).

UNMANNED aircraft systems: federal actions needed to ensure safety and expand their potential uses within the national airspace system. [S.l.]: U.S. Government Accountability Office, 2008. Citation on page [27](#).

URIBE-MONTESDEOCA, S.; ARIAS-FLORES, H.; RAMOS-GALARZA, C.; JADÁN-GUERRERO, J. Using drones for tourism: Exploring exciting places in ecuador. In: SPRINGER. **International Conference on Intelligent Human Systems Integration**. [S.l.], 2021. p. 786–791. Citation on page [32](#).

USACH, H.; VILA, J. A.; TORENS, C.; ADOLF, F. Architectural design of a safe mission manager for unmanned aircraft systems. **Journal of Systems Architecture**, Elsevier, v. 90, p. 94–108, 2018. Citation on page [23](#).

VALAVANIS, K. P.; VACHTSEVANOS, G. J. **Handbook of Unmanned Aerial Vehicles**. USA: Springer Publishing Company, Incorporated, 2015. ISBN 9048197082, 9789048197088. Citation on page [29](#).

VASCONCELOS, J. F.; SILVESTRE, C.; OLIVEIRA, P.; GUERREIRO, B. Embedded uav model and laser aiding techniques for inertial navigation systems. **Control Engineering Practice**, Elsevier, v. 18, n. 3, p. 262–278, 2010. Citation on page [51](#).

VEGA, A.; LIN, C.-C.; SWAMINATHAN, K.; BUYUKTOSUNOGLU, A.; PANKANTI, S.; BOSE, P. Resilient, uav-embedded real-time computing. In: IEEE. **2015 33rd IEEE International Conference on Computer Design (ICCD)**. [S.l.], 2015. p. 736–739. Citations on pages [53](#) and [55](#).

VERMA, M.; ALI, S. I.; AGRAWAL, G. Uav—a boon towards agriculture. In: SPRINGER. **Proceedings of Second International Conference on Smart Energy and Communication**. [S.l.], 2021. p. 299–303. Citation on page [23](#).

VOCHIN, M.; ZOICAN, S.; BORCOCI, E. Intelligent vehicle navigation system with assistance and alerting capabilities. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, v. 31, n. 22, p. e4402, 2019. Citation on page [58](#).

WAHID, M. A.; OTHMAN, N.; ZAIN, M. Z. M.; SHAHARUDDIN, N. M. R. Control and simulation of obstacle avoidance for a quadcopter. **Journal of Aeronautics, Astronautics and Aviation**, Aeronautical and Astronautical Society of the Republic of China, v. 53, n. 2, p. 251–256, 2021. Citation on page [52](#).

WANG, D.; LI, W.; LIU, X.; LI, N.; ZHANG, C. Uav environmental perception and autonomous obstacle avoidance: A deep learning and depth camera combined solution. **Computers and Electronics in Agriculture**, Elsevier, v. 175, p. 105523, 2020. Citation on page [51](#).

WANG, H.; YAO, Y.-D.; WANG, R.; SHEN, L. Coordinated jamming and communications in an mc-cdma system. **IEEE Transactions on Aerospace and Electronic Systems**, IEEE, v. 51, n. 4, p. 3151–3160, 2015. Citation on page [50](#).

WANG, R.; LIU, H.; WANG, H.; YANG, Q.; WU, D. Distributed security architecture based on blockchain for connected health: architecture, challenges, and approaches. **IEEE Wireless Communications**, IEEE, v. 26, n. 6, p. 30–36, 2019. Citation on page [58](#).

WANG, W.; SHENG, Y.; WANG, J.; ZENG, X.; YE, X.; HUANG, Y.; ZHU, M. Fast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. **Ieee Access**, IEEE, v. 6, p. 1792–1806, 2017. Citation on page [77](#).

WANG, Y.; WANG, X.; ZHAO, S.; SHEN, L. A hierarchical collision avoidance architecture for multiple fixed-wing uavs in an integrated airspace. **arXiv preprint arXiv:2005.14455**, 2020. Citation on page [52](#).

WANG, Z.; CHENG, C. Discussion on the application of 5g network uav in public security of smart cities. In: **Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA 2019)**. [S.l.]: Springer, 2020. p. 1945–1953. Citation on page [32](#).

WARREN, M.; GREEFF, M.; PATEL, B.; COLLIER, J.; SCHOELLIG, A. P.; BARFOOT, T. D. There's no place like home: visual teach and repeat for emergency return of multirotor uavs during gps failure. **IEEE Robotics and Automation Letters**, IEEE, v. 4, n. 1, p. 161–168, 2018. Citation on page [51](#).

World meter. **COVID-19 coronavirus pandemic**. [S.l.]: Agência Nacional de Aviação Civil, 2021. Citation on page [83](#).

WU, X.; LING, H.; DONG, Y. On modeling and verifying of application protocols of ttcan in flight-control system with uppaal. In: **INTERNATIONAL CONFERENCE ON EMBEDDED SOFTWARE AND SYSTEMS - ICESS '09**. Hangzhou: IEEE Computer Society, 2009. p. 572–577. Citation on page [36](#).

XIONG, M.; ZENG, D.; YAO, H.; LI, Y. A crowd simulation based uav control architecture for industrial disaster evacuation. In: **IEEE. 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)**. [S.l.], 2016. p. 1–5. Citation on page [52](#).

YAOMING, Z.; YU, S.; ANHUAN, X.; LINGYU, K. A newly bio-inspired path planning algorithm for autonomous obstacle avoidance of uav. **Chinese Journal of Aeronautics**, Elsevier, 2021. Citation on page [52](#).

YI, W.; SUTRISNA, M. Drone scheduling for construction site surveillance. **Computer-Aided Civil and Infrastructure Engineering**, Wiley Online Library, v. 36, n. 1, p. 3–13, 2021. Citation on page [32](#).

YOKOYAMA, R. S.; KIMURA, B. Y. L.; MOREIRA, E. dos S. An architecture for secure positioning in a uav swarm using rssi-based distance estimation. **ACM SIGAPP Applied Computing Review**, ACM, v. 14, n. 2, p. 36–44, 2014. Citation on page 24.

YONG, S. Z.; ZHU, M.; FRAZZOLI, E. Resilient state estimation against switching attacks on stochastic cyber-physical systems. In: IEEE. **2015 54th IEEE Conference on Decision and Control (CDC)**. [S.l.], 2015. p. 5162–5169. Citation on page 53.

YOON, H. Use of drones in the cultural industries. **Journal of the Korea Society of Digital Industry and Information Management**, Korea Society of Digital Industry and Information Management, v. 11, n. 4, p. 99–112, 2015. Citation on page 31.

YOON, M.-K.; LIU, B.; HOVAKIMYAN, N.; SHA, L. Virtualdrone: virtual sensing, actuation, and communication for attack-resilient unmanned aerial systems. In: ACM. **Proceedings of the 8th International Conference on Cyber-Physical Systems**. [S.l.], 2017. p. 143–154. Citations on pages 53 and 55.

YOUN, W.; CHOI, H.; CHO, A.; KIM, S.; RHUDY, M. B. Accelerometer fault-tolerant model-aided state estimation for high-altitude long-endurance uav. **IEEE Transactions on Instrumentation and Measurement**, IEEE, v. 69, n. 10, p. 8539–8553, 2020. Citation on page 51.

ZAMMIT, C.; KAMPEN, E.-J. V. 3d real-time path planning of uavs in dynamic environments in the presence of uncertainty. In: **AIAA Scitech 2021 Forum**. [S.l.: s.n.], 2021. p. 1956. Citation on page 52.

ZHANG, D.; FENG, G.; SHI, Y.; SRINIVASAN, D. Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances. **IEEE/CAA Journal of Automatica Sinica**, IEEE, v. 8, n. 2, p. 319–333, 2021. Citation on page 52.

ZHANG, G.; WU, Q.; CUI, M.; ZHANG, R. Securing uav communications via joint trajectory and power control. **IEEE Transactions on Wireless Communications**, IEEE, v. 18, n. 2, p. 1376–1389, 2019. Citations on pages 23, 27, and 32.

ZHANG, Q.; JIANG, M.; FENG, Z.; LI, W.; ZHANG, W.; PAN, M. Iot enabled uav: Network architecture and routing algorithm. **IEEE Internet of Things Journal**, IEEE, v. 6, n. 2, p. 3727–3742, 2019. Citation on page 52.

ZHONG, Y.; ZHANG, W.; ZHANG, Y.; ZUO, J.; ZHAN, H. Sensor fault detection and diagnosis for an unmanned quadrotor helicopter. **Journal of Intelligent & Robotic Systems**, Springer, v. 96, n. 3, p. 555–572, 2019. Citation on page 51.

ZHOU, Y.; ZHAO, H.; CHEN, J.; JIA, Y. A novel mission planning method for uavs' course of action. **Computer Communications**, Elsevier, 2020. Citation on page 32.

SYSTEMATIC REVIEW

A.1 Planning

As previously mentioned in [Chapter 4](#), a systematic review is divided into three phases: (1) planning, (2) execution, and (3) analysis. The first phase of the process and also described in this section is planning. The planning phase is where the protocol is defined and evaluated by specialists. The protocol definitions imply defining the objectives that will guide the inspection in the literature, defining the research questions, search sources, search strings, and the inclusion and exclusion criteria. The evaluation carried out by the experts, on the other hand, is necessary to ensure that all the planning, well as the predefined definitions and objectives, are correct and in accordance with the focus of the proposal.

A.1.1 *Review objectives*

The main objectives of this systematic review are:

- Identify common characteristics and gaps among architectures currently developed for unmanned aerial vehicles with the focus on safety and security;
- Identify security and safety gaps in unmanned aerial vehicles architectures;
- Identify studies that do not propose architectures themselves, but that reflect new features that can be incorporated into architectures for unmanned aerial vehicles.

A.1.2 *Research Question*

The research question is formulated to determine the focus of the investigation, that is, to perform a more specific review. The systematic review was planned in order to answer this main question:

Is it possible to apply resilience to an unmanned aerial vehicle after it has been attacked¹ during a mission?

The result for this question is answered in [Chapter 5](#).

A.1.3 Search Strategy

The search strategy was performed to determine the criteria for the studies selection:

1. search sources;
2. languages;
3. search methods;
4. keywords;
5. inclusion criteria;
6. exclusion criteria.

(1) In order to select the sources utilized in the review, the following criteria were established: coverage, availability, versatility to export the results, and usability. For coverage were considered only search sources with a great number of studies. Only studies with full-text access were reviewed in the availability criterion. For versatility were determined sources that exported the studies in an automated way. Finally, accepted search engines were also considered applying the usability criterion that is easy to understand and operate. Based on the above criteria, the search sources were:

- IEEE Xplore Digital Library ([IEEE, 2020](#))
- ACM Digital Lybrary ([ACM, 2020](#))
- Scopus ([SCOPUS, 2020](#))

(2) The languages determined for the systematic review were English and Portuguese. Portuguese is the native language used at the University of São Paulo (USP) and also to contemplate and value Brazilian research. English was also used since it is the worldwide adopted language for scientific research.

(3) The search method chosen was automatic, performed through search engines.

(4) For the systematic review, the following keywords and their synonyms were chosen:

¹ In this dissertation, attack can be interpreted as a security or safety issues.

- **Security:** safety, security, cybersecurity, proteção, segurança e cibersegurança
- **Vehicles:** UAVs, unmanned aerial vehicle, unmanned vehicle, autonomous intelligent vehicles, intelligent vehicles, veículos aéreos não tripulados, veículo não tripulado, veículos autônomos inteligentes e veículos inteligentes.
- **Architecture:** architecture, resilient architecture, arquitetura e arquitetura resiliente.

(5) The inclusion, exclusion, and quality criteria were defined during the planning phase in order to ensure the credibility of the review, keeping the focus on selection. The inclusion criteria for the identified studies were:

- Studies that address safety and security aspects in UAVs;
- Studies showing resilient architectures for unmanned and autonomous air vehicles;
- Studies showing the type of test used to evaluate UAVs in the network.

(6) The defined exclusion criteria were:

- Studies that do not have a clear structure of objectives and outcomes;
- Studies that have no relevance to the central theme;
- Studies that discuss UAVs but do not address safety or security issues;
- Studies that do not present an objective methodology;
- Incomplete Studies;
- Studies that are not written in English or Portuguese.

At the end of the planning process and before starting the execution of the systematic review, it is necessary to validate the protocol with specialists, thus certifying the quality in the remaining of the search. The evaluation carried out by the experts is to ensure that all planning, as well as, the definitions and predefined objectives are correct, and following the proposal focus. In this way, the protocol developed was evaluated by two specialists, namely, Professor Dra. Kalinka Regina Lucas Jaquie Castelo Branco (specialist in the area of security, embedded, and critical systems) and by the doctoral student Anderson Yoshiaki Iwazaki (specialist in software engineering and systematic literature review). Both specialists analyzed each of the stages of the planning process and contributed to improvements. It is worth mentioning that all the recommendations were considered.

A.2 Execution

The systematic review begins with the process of identifying the primary studies using the search strategies defined in the planning phase. For this, in the first step, it is necessary to create the search strings. The search strings were designed from the keywords defined earlier in the planning phase of the review protocol. The second step consists of the preliminary studies selection by reading the titles and abstracts, assessing whether the work fits the inclusion and exclusion criteria. In the third step, the final selection occurs through the complete reading of the selected studies and the data extraction. Finally, in the fourth step, the data are synthesized and analyzed.

A.2.1 Search String

The search string was created respecting the specifications of each database, using "AND" and "OR" operators to group synonyms. It was also restricted to searches for terms in the title and summary ensuring focus on the process of studies identification. The search strings created with the terms in English and Portuguese were:

- **Base String (EN)** : (“Safety” OR “Security” OR “Cybersecurity”) AND (“UAVs” OR “Unmanned aerial vehicle” OR “Unmanned vehicle” OR “Autonomous intelligent vehicles” OR “intelligent vehicles”) AND (“Architecture” OR “Resilient architecture”);
- **Base String (PT-BR)** : (“Proteção OR “Segurança” OR “Cibersegurança”) AND (“UAVs” OR “Veículo aéreo não tripulado” OR “Veículo não tripulado” OR “Veículos autônomos inteligentes” OR “Veículos inteligentes”) AND (“Arquitetura” OR “Arquitetura resiliente”);
- **IEEEExplore Digital Library (EN)** : (("Document Title":"Safety" OR "Document Title":"Security" OR "Document Title":"Cybersecurity") AND ("Document Title":"UAVs" OR "Document Title":"Unmanned aerial vehicle" OR "Document Title":"Unmanned vehicle" OR "Document Title":"Autonomous intelligent vehicles" OR "Document Title":"Intelligent vehicles") AND ("Document Title":"Architecture" OR "Document Title":"Resilient architecture")) OR (("Abstract":"Safety" OR "Abstract":"Security" OR "Abstract":"Cybersecurity") AND ("Abstract":"UAVs" OR "Abstract":"Unmanned aerial vehicle" OR "Abstract":"Unmanned vehicle" OR "Abstract":"Autonomous intelligent vehicles" OR "Abstract":"Intelligent vehicles") AND ("Abstract":"Architecture" OR "Abstract":"Resilient architecture"))
- **IEEEExplore Digital Library (PT-BR)** : (("Document Title":"Proteção" OR "Document Title":"Segurança" OR "Document Title":"Cibersegurança") AND ("Document Title":"UAVs" OR "Document Title":"Veículo aéreo não tripulado" OR "Document Title":"Veículo não tripulado" OR "Document Title":"Veículos autônomos inteligentes" OR "Document Title":"Veículos inteligentes") AND ("Document Title":"Arquitetura"

OR "Document Title": "Arquitetura resiliente")) OR (("Abstract": "Proteção" OR "Abstract": "Segurança" OR "Abstract": "Cibersegurança") AND ("Abstract": "UAVs" OR "Abstract": "UVeículo aéreo não tripulado" OR "Abstract": "Veículo não tripulado" OR "Abstract": "Veículos autônomos inteligentes" OR "Abstract": "Veículos inteligentes") AND ("Abstract": "Arquitetura" OR "Abstract": "Arquitetura resiliente"))

- **ACM Digital Library (EN)** : Title : ("Safety" OR "Security" OR "Cybersecurity") AND Title : ("UAVs" OR "Unmanned aerial vehicle" OR "Unmanned aircraft system" OR "Autonomous intelligent vehicles" OR "Intelligent vehicles") AND Title : ("Architecture" OR "Resilient architecture") OR Abstract : ("Safety" OR "Security" OR "Cybersecurity") AND Abstract : ("UAVs" OR "Unmanned aerial vehicle" OR "Unmanned vehicle" OR "Unmanned aircraft system" OR "Autonomous intelligent vehicles" OR "Intelligent vehicles") AND Abstract : ("Architecture" OR "Resilient architecture");
- **ACM Digital Library (PT-BR)** : Title : ("Proteção" OR "Segurança" OR "Cibersegurança") AND Title : ("UAVs" OR "Veículo aéreo não tripulado" OR "Veículo não tripulado" OR "Veículos autônomos inteligentes" OR "Veículos inteligentes") AND Title : ("Arquitetura" OR "Arquitetura resiliente") OR Abstract : ("Proteção" OR "Segurança" OR "Cibersegurança") AND Abstract : ("UAVs" OR "Veículo aéreo não tripulado" OR "Veículo não tripulado" OR "Veículos autônomos inteligentes" OR "Veículos inteligentes") AND Abstract : ("Arquitetura" OR "Arquitetura resiliente");
- **Scopus (EN)** : TITLE-ABS-KEY(("Safety" OR "Security" OR "Cybersecurity") AND ("UAVs" OR "Unmanned aerial vehicle" OR "Unmanned vehicle" OR "Autonomous intelligent vehicles" OR "Intelligent vehicles") AND ("Architecture" OR "Resilient architecture"));
- **Scopus (PT-BR)** : TITLE-ABS-KEY(("Proteção" OR "Segurança" OR "Cibersegurança") AND ("UAVs" OR "Veículo aéreo não tripulado" OR "Veículo não tripulado" OR "Veículos autônomos inteligentes" OR "Veículos inteligentes") AND ("Arquitetura" OR "Arquitetura resiliente"));

A.2.2 Study Selection

After performing the search in repositories with the search strings, a total of 545 studies were identified. Their information was exported from the databases in Bibtex format and imported on the Parsifal platform. After removing duplicate studies identified by the tool itself, 465 studies remained. The database with the most significant number of studies related to the topic was Scopus, followed by the IEEEExplore Digital Library, and ACM Digital Library. The proportion of studies found in each of the databases is illustrated in Figure 32. Nine studies were identified in ACM (1,7%), 86 in IEEE (15,8%), and 450 in Scopus (82,6%).

Figure 32 – Number of studies found in databases for the first selection.

Source: The author.

The first selection was made by reading the titles and abstracts, identifying the inclusion and exclusion criteria. The studies accepted were those that met at least one of the inclusion criteria, and the rejected studies were those that met at least one exclusion criterion. In the end, 119 studies were accepted, and 346 were refuted. Distribution of the selected studies in each of the bases can be observed in the graph of [Figure 33](#). Although the ACM Digital Library database contains relevant studies on the large area of UAVs, there are not many studies on safety and security in unmanned aerial vehicles using resilient architectures. The most significant number of studies were found in the Scopus database, followed by the IEEEExplorer Digital Library database.

After primary study selection, each accepted article was read in its totality and re-matched to an inclusion or exclusion criteria. During the full reading, summaries were generated as results. The number of studies accepted in the final selection stage can be seen in [Figure 34](#). The most significant number of studies found and consequently accepted was on Scopus. In total, 52 works were selected (69,7%), followed by IEEE, with 28 accepted studies (27,7%), and only 2 from ACM entered the list (2,5%).

Among the accepted studies, the criterion that received the highest level of acceptance was that of studies that presented safety and security aspects in UAVs. Works with resilient architectures criterion were less found and, consequently, less accepted. Regarding the exclusion

Figure 33 – Proportion of studies accepted in the first selection.

Source: The author.

criteria, the most significant was the criterion of studies that have no relevance to the central theme. Most of them did not have characteristics relevant to the focus of the research.

In the last step of the systematic review, a discursive synthesis of the results was produced to expose the results found and the research gaps. This synthesis is presented in [section 4.1](#).

Figure 34 – Proportion of studies accepted in the final selection.

Source: The author