



**UNIVERSITY
OF TURKU**

RISK DRIVEN MODELS & SECURITY FRAMEWORK FOR DRONE OPERATION IN GNSS-DENIED ENVIRONMENT

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Samuel Asiedu

Supervisors:
Dr. Antti Hakkala (University of Turku)
Dr. Tahir Mohammed (University of Turku)
Pia Taittonen (Huld Oy)

June 2023

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security

Programme: Master's Degree Programme in Information and Communication Technology

Author: Samuel Asiedu

Title: Risk driven models & security framework for drone operation in GNSS-denied environments

Number of pages: 50 pages

Date: June 2023

Flying machines in the air without human inhabitation has moved from abstracts to reality and the concept of unmanned aerial vehicles continues to evolve. Drones are popularly known to use GPS and other forms of GNSS for navigation, but this has unfortunately opened them up to spoofing and other forms of cybersecurity threats. The use of computer vision to find location through pre-stored satellite images has become a suggested solution but this gives rise to security challenges in the form of spoofing, tampering, denial of service and other forms of attacks. These security challenges are reviewed with appropriate requirements recommended.

This research uses the STRIDE threat analysis model to analyse threats in drone operation in GNSS-denied environment. Other threat models were considered including DREAD and PASTA, but STRIDE is chosen because of its suitability and the complementary ability it serves to other analytical methods used in this work. Research work is taken further to divide the drone system into units based in similarities in functions and architecture. They are then subjected to Failure Mode and Effects Analysis (FMEA), and Fault Tree Analysis (FTA). The STRIDE threat model is used as base events for the FTA and an FMEA is conducted based on adaptations from IEC 62443-1-1, Network and System Security- Terminology, concepts, and models and IEC 62443-3-2, security risk assessment for system design. The FTA and FMEA are widely known for functional safety purposes but there is a divergent use for the tools where we consider cybersecurity vulnerabilities specifically, instead of faults.

The IEC 62443 series has become synonymous with Industrial Automation and Control Systems. However, inspiration is drawn from that series for this work because, drones, as much as any technological gadget in play recently, falls under a growing umbrella of quickly evolving devices, known as Internet of Things (IoT). These IoT devices can be principally considered as part of Industrial Automation and Control Systems. Results from the analysis are used to recommend security standards & requirements that can be applied in drone operation in GNSS-denied environments.

The framework recommended in this research is consistent with IEC 62443-3-3, System security requirements and security levels and has the following categorization from IEC 62443-1-1, identification, and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events and resource availability. The recommended framework is applicable and relevant to military, private and commercial drone deployment because the framework can be adapted and further tweaked to suit the context which it is intended for. Application of this framework in drone operation in GNSS denied environment will greatly improve upon the cyber resilience of the drone network system.

Keywords: drones, drone security, risk driven models, FMEA, FTA, IEC 62443.

Table of contents

1	Introduction	1
1.1	Drones and Cybersecurity	1
1.2	Research Problem	2
1.3	Research Objectives	3
1.4	Research Methods	3
1.5	Research Design and Process	4
1.6	Scope and limitation	7
1.7	Research Contribution	7
1.8	Structure of the Thesis	7
2	Concept and Background	9
2.1	DRONES	9
2.2	FTA and FMEA	10
2.2.1	FTA	10
2.2.2	FMEA	11
2.3	GNSS NAVIGATION	11
2.4	COMPUTER VISION AND AI ASSISTED NAVIGATION	12
2.4.1	Hilla Architecture	13
2.5	FRAMEWORKS	14
2.5.1	Standards and Standard Development Organizations	14
2.6	SUITABLE LINK BETWEEN A STANDARD FRAMEWORK AND DRONE	15
3	LITERATURE REVIEW	17
3.1	Information Sources for Current Literature Review	17
3.2	Workflow of Current Literature Study	17
3.3	Year-Wise Publications	17
3.4	Security Challenges of Drones	19
3.5	Proposed Solutions for Drone Security Challenges	20
3.6	Limitations on Existing Solutions	22
3.7	Literature Review Summary	22

4	METHODOLOGY	22
4.1	FTA ANALYSIS	22
4.1.1	FTA SYMBOLS AND THE ITERATIVE PROCESS.	22
4.1.2	THE STRIDE MODEL AND FTA DIAGRAMS	23
4.2	FMEA ANALYSIS	30
4.2.1	The FMEA Process	30
4.2.2	The FMEA Table	31
4.2.3	Risk matrix and parameter definitions	33
5	Framework	35
5.1	Development of Framework	35
5.1.1	Identification and Authentication	35
5.1.2	Use Control	35
5.1.3	System Integrity	36
5.1.4	Data Confidentiality	37
5.1.5	Restricted Data Flow	37
5.1.6	Timely Response to Events	38
5.1.7	Resource Availability	38
5.2	Standards Recommendation	39
5.2.1	Identification and Authentication	39
5.2.2	Use Control	39
5.2.3	System Integrity	39
5.2.4	Data Confidentiality	40
5.2.5	Restricted Data Flow	40
5.2.6	Timely Response to Events	41
5.2.7	Resource Availability	41
6	Conclusion and Further Research	45
6.1	Conclusion	45
6.2	Further Research	46
	References	47

Abbreviations and Acronyms

AES	Advanced Encryption Standard
ATIS	Alliance for Telecommunications Industry Solutions
ASTM	American Society for Testing and Materials
CNN	Convolutional Neural Network
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
DREAD	Damage, Reproducibility, Exploitability, Affected users and Discoverability
DSRP	Design Science Research Process
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
FTP	File Transfer Protocol
FTPD	File Transfer Protocol Daemon
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HNS	Huld Navigation System
IEC	International Electrotechnical Commission
IoD	Internet of Drones
ISO	International Organization for Standardization
iTCALAS	Improved Temporal Credential-based Anonymous Lightweight User Authentication Scheme
NFV	Network Function Virtualization
PASTA	Process for Attack Simulation and Threat Analysis
RCE	Remote Code Execution
RNN	Recurrent Neural Network
SDO	Standard Developing Organization
TCALAS	Temporal Credential-based Anonymous Lightweight User Authentication Scheme

UAV	Unmanned Aerial Vehicle
UTM	Unmanned Aircraft System Traffic Management
VAST	Visual, Agile and Simple Threat modelling
VPN	Virtual Private Network
XSS	Cross-Site Scripting
XXE	Xml External Entity

List of Tables

1 Information Sources for Literary Review	17
2 Comparison of the contributions of relevant literature materials to drone security	20
3 Comparison of relevant literature materials with the research objectives of this paper	21
4 Event and Gate Symbol description	23
5 FMEA table for drone operation in a GNSS denied environment	33
6 Probability table showing parameters used for determining likelihood in risk assessment	34
7 Severity table showing parameters used for degree of impact in risk assessment	34
8 Detection table showing parameters used for how easily risks are identified in risk assessment	35
9 Risk Index table adapted from IEC 62443-3-2:2020 Annex B	35
10 Cybersecurity framework for drone operation in GNSS denied environment	43

List of Figures

1 DSRP research process model	5
2 Georeferencing processing timelines	13
3 Hilla components	14
4 Workflow of the Literature Study.....	18
5 Yearly distribution for drone security related literature	18
6 Pie chart of literary distribution	19
7 FTA diagram for Spoofing of the Drone Navigation Solution	24
8 FTA diagram for Tampering of the Drone Navigation Solution	25
9 FTA diagram for Repudiation in the Drone Navigation Solution	26
10 FTA diagram for Information disclosure in the Drone Navigation Solution	27
11 FTA diagram for Denial of Service in the Drone Navigation Solution	28
12 FTA diagram for Escalation of Privileges in the Drone Navigation Solution	29

1 Introduction

The concept of having machines fly in the air without human inhabitation has moved from abstracts to reality and the technology of unmanned aerial vehicles continues to evolve. A drone is an unpiloted aircraft or space craft [1]. Drones gained much popularity in World War II, where miniature contraptions of unmanned aerial vehicles were used in air strikes [2]. These were radio controlled and had no other forms of technological advancements until the Vietnamese war when a camera was attached, and it was used for reconnaissance. The 2000's was when the famous Predator drone was introduced, and this marked a pivotal period for military and civilian drone development. Apart from the general use of drones for military purposes in reconnaissance and attack manoeuvres, they have other purposes like firefighting, traffic monitoring, search and rescue and weather monitoring. One main advantage of drone is the restriction of the human factor in its operation. It can survive weather conditions and move in places with little to no detection. The precision of its movement and persistence in the air for as long as there is power puts its prospects beyond the horizon. The disadvantages cannot also be ignored, like disclosure of sensitive user information during data transmission and hijacking of drones by malicious actors. The many uses that have been found for drones produces dire implications if it gets compromised. The info about users for delivery sessions, images, and geographical data it can harness can all be used for malicious purposes if it falls into the wrong hands. This is made even more apparent with how easily attackers can spoof GNSS locations and jam control signals causing the drones to malfunction [3]. Huld Oy under the AINET project has designed a solution to assist drones to minimize the reliance on GNSS [4]. The solution is made up of a drone which uses a live camera feed taking advantage of computer vision for navigation.

1.1 Drones and Cybersecurity

Drones have always been a vital component of any systems they are part of when it has been in operation. This makes it a high value target for attack, thus, not only the components of the drone, but the control station as well as the channel for communication are all attacked surfaces are exposed to threats. The issue of drones getting attacked is inevitable and there is a likelihood for them to become a pivot of attack against the wider network. This is done in fulfilling a malicious actor's desire of not only capturing the drone as a target but using it to compromise other drones and then creating a drone botnet. Some of the major cybersecurity threats caused by drone activities are GPS spoofing, downlink interception and data

exploitation [5]. GPS spoofing and downlink interception sees the drone as the target with hackers feeding drones with false GPS coordinates, inciting them to make wrong decisions and downlink interceptions in the form of abusing an unencrypted communication channel. Communication channel abuse between the drone and control station allows hackers to have access to whatever sensitive data the drone has acquired during task execution. These could be images, videos, and even coordinates of airways. Data exploitation sees the drone as a tool for extra malicious cybersecurity activities or as a pivot to move further in a compromised network. Most of the vulnerabilities in drone activities can be alleviated by some basic security practices like regular update of drone firmware and up-to-date patches. Avoiding the use of default credentials but rather use strong authentication tokens for base station app. Use of VPN or encryption of communication channel between drone and control station while enabling a failsafe mechanism for the drone like the Return-to-home feature to take over just in case the drone loses signal [6]. These recommended solutions posit that the adherence to basic IT security principles goes a long way to secure drones.

1.2 Research Problem

Most of the drone activities mentioned earlier on are heavily reliant on the use of GNSS for navigation. GNSS based navigation works by using triangulation to determine positioning using not less than three satellites. The drones have modules installed on them that act as receivers for GNSS signals. The main cybersecurity issue pertaining to this feature was the ability of malicious actors to spoof the GNSS signals to be received by the drone. Engineers have addressed this problem by developing a drone solution that is capable of navigating without a heavy reliance on GNSS by using a live camera feed with computer vision on pre-stored satellite images. There is a need to evaluate the invention to prioritize risks, apply chosen techniques, then evaluate any remaining risks using risk-driven models. As peculiar as this invention is, an appropriate risk-driven model needs to be selected for the evaluation and then the drone system classified for further Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA). Most developments in the drone industry have followed the trajectory of these drones relying on GNSS for navigation, so as there is a deviation from the norm, the drone system needs to be broken down and duly grouped into like components, factoring in the change in hardware, software, computer vision and alternate technologies that have come into play. This classification then must undergo an FMEA and FTA analysis to determine how and where it might fail, the impact of these failures and how far this system can deviate from the norm. Many standards exist regarding the use of drones, design and

manufacturing, assembly of the components and even device maintenance but none of these takes into consideration a specialized security framework for the operation of a drone without a reliance on GNSS [7][8][9]. A framework of best practices and requirements need to be established to reduce exposure to cyberattacks and to identify the areas which are most at risk for data breaches and other compromising activity perpetrated by cyber criminals. The motivation of this thesis is to develop risk driven models and recommend a security framework for drone operation in GNSS denied environments, thus, the research questions can be summarized as:

- What kind of risk/threat analysis model could be implemented to drone operation in GNSS-denied environments? **(RQ1)**
- Can the drone system be divided into units such that FMEA and FTA analysis can be performed? **(RQ2)**
- What cybersecurity standards & requirements could be applied in the drone operation in GNSS-denied environments? **(RQ3)**

1.3 Research Objectives

After successfully evaluated the research problem and subsequently posed the pertinent research questions, the following research objectives have been identified for clarity:

- To identify a risk/threat analysis model to be implemented for drone operation in GNSS-denied environments.
- Development and assessment of a Failure Mode and Effects Analysis and Fault Tree Analysis template for the research.
- To identify security standards and requirements that can be used for drone operation in GNSS-denied environments.

1.4 Research Methods

The research aims at recommending a cybersecurity framework for the operation of drones in a GNSS-denied environment along with developing risk driven models. An existing client's specifications will be used as a case study to enable the streamlining of this research and making it relevant for use for now and even in the future too. Based on this, a research approach has been selected as qualitative research, since qualitative research seeks to

understand the quality of the subject and its attributes of meaning [10]. The quality of the subject being studied is essentially affected by how it can be altered, improved, or corrected. These questions are best corresponded by design scientific, constructive research approach that is applied in the research. Design research aims to implement pragmatic solutions through its constructive research approach and aims to generate new knowledge for design and implementation [11]. The purpose of the design science research is to produce new methods or artifacts that improve the quality of the research subject. Design science research is also referred to as applied research, and therefore it is suitable for the context of this study [11]. The research utilizes the Design Science Research Process (DSRP) [12]. The research method is a case study, which examines a multi-dimensional major single-case study of the client's (cyber security) processes and their effect on drone operation in a GNSS-denied environment. Altogether, the research design of the research is based on a qualitative research approach that is applied to the design science research methodology and uses a case study as a single case study. The research's design is to be as flexible as possible, so that it enables learning in the process and if necessary, correcting the research design approaches during the research process.

1.5 Research Design and Process

The DSRP model chosen for the study is the originally created to serve information system science and its specific features. The model includes a nominal research process order, which is divided in six functional steps. The steps of the DSRP model are:

1. Identifying and motivation for the problem
2. Objectives of the solution
3. Design and development
4. Presentation
5. Evaluation
6. Communication

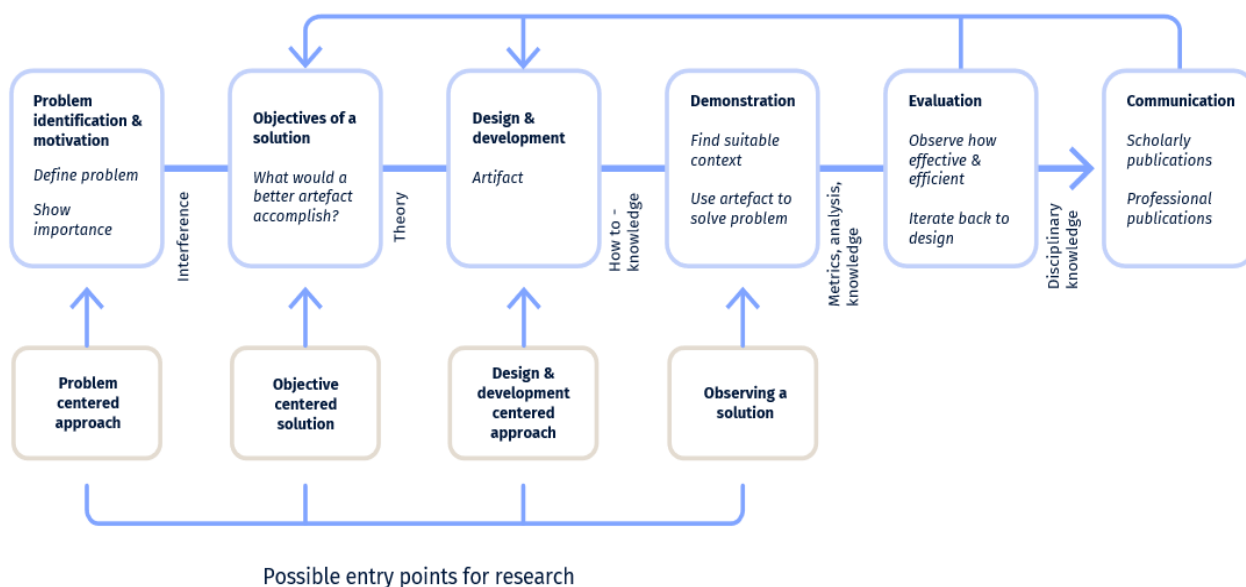


Figure 1 DSRP –research process model [12]

Concerning the flexibility need in the research design, the DSRP model is suitable due to its adaptive structure. The process model phasing is only nominally set to a specific order, allowing the researcher to dive freely from the desired point in the research process. The starting of the research from different points is structured into problem-oriented, goal-oriented, planning and development-oriented perspectives that support changes and re-evaluations during the research process. Figure 1 shows the DSRP research process model [12].

The researcher approaches the research from a problem-oriented perspective. This means diving into the research process under the heading "Identifying and motivating the problem". The reason for choosing a problem-oriented approach is that the research client has identified possible security issues or shortcomings in drone operation in GNSS-denied environments (research problem) - but these have not been systematically studied yet. The main concern of the client is that the potential security issues associated with the drone operation are realized in the operative use of customers, with may cause significant business and reputational consequences. The research pursues showing whether the feared security challenges are relevant or not. In any case, these above-mentioned issues serve as the main motivators of the research. The objectives of the research process solution are largely determined by the research problem, that is "Risk driven models and security frameworks for drone operation in GNSS denied environment". In view of the research process, the objectives of the solution are

likely to be resumed during the research process, as the potential security issues of the drone operations being investigated will be elucidated during practical testing during the research process. At this stage, the conceptual-theoretical basis for research is formulated, which is created from research publications, standards, and technology documentation in the field of information and cyber security. The objectives of the solution to be defined at this stage of the research process are Development and assessment of a Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) template, and to identify a risk/threat analysis model to be implemented for drone operation in GNSS-denied environments. The design and development phases of the research are based on the examination of the technical documentation of the solutions, modelling, and technical testing. Depending on the implementation of the research object, new implementations will be made based on what is the most appropriate for the recognized risks and on the other hand for economic profitability. For example, this phase of the study may present more options that will be introduced to the client in the next step. From the point of view of the research process, the research culminates in the demonstration and evaluation stages, where the researcher presents to his client the results obtained during the research and in practice evaluates the functionality of the new output. Depending on the new output of the study, the evaluation can be carried out for example by introducing new standards / test methods for a particular pilot cycle into the drone operations. Based on the cycle, the client gives feedback on how the new arrangement works and whether there is a need in the research process to return to the previous stages to seek a new perspective. The assessment is based on a business case formulated by the case study, which introduces risks, minimizes risks, and their operational implications for the client. From a scientific point of view, the research instructors at this stage also give feedback on the scientific merits or shortcomings of the work. The added value of research in the industry can be considered as either new information (new technological findings on vulnerabilities in a particular technology) or cumulative data (research confirms previously made observations). Demonstrating scientific evidence (technology-related) for the subject of research can be challenging because technology vendors test / monitor others' tests intensively and report any findings publicly in their own information channels. Therefore, in principle, it is more realistic to try to show, as cumulative information, that a certain technological implementation contains certain vulnerabilities that should be minimized as proposed by the research construction. The DSRP model emphasizes the importance of communication in the research process so that not only the client gets the results of the research. The importance of research needs to be widely expressed so that it can be exploited by researchers and the public. In

communication, the requirements of the client for business and product secrets must be considered.

1.6 Scope and limitation

This research is conducted with a case study in central involvement to set the scope in the broad area of drone security. The drone is assumed to be a commercial drone with a single camera. The video captured is sent to a powerful computer at the base station which houses a computer vision and AI assisted proprietary navigation solution. For matters of reference, this navigation solution will be sometimes referred to as HILLA or Huld Navigation Solution (HNS) in this research work. This powerful computer is also assumed to be capable of evolving to become a data centre. The communication between the drone and the base station is done over a 5G communication link.

1.7 Research Contribution

This research will recommend security measures for use by UAVs irrespective of the method of navigation used. The reluctance of most regulatory bodies in publishing standards for use is partly because of the quickly evolving industry of UAVs which might be young, but so agile. This research will set a baseline, regardless of the purposes or use of the drone, in order for industry experts to utilize markers when setting standards.

1.8 Structure of the Thesis

This research work is divided into five chapters. The first three chapters give the overall idea of the thesis. They also explain the idea behind the research and how the research was conducted, with a focus on topics and conceptual background.

The latter part of the thesis tries to explain how the analysis has been conducted and the data that has been generated and gathered. The research questions formulated have been answered in the last two chapters of the thesis.

- Chapter 1 presents the motivation for the research and the research problem in depth. It gives the brief idea of drones, cybersecurity, and the dependence on GNSS for navigation. It talks about the general idea of the thesis that is being presented.
- Chapter 2 gives the conceptual background of the thesis. It describes the history and evolution of drones in addition to the progression of UAV navigation. This is done

looking at GNSS dependent and independent altogether and commercial as well as military drones.

- Chapter 3 presents the literature review. It talks about the similar studies and research that have been done related to the topic. It also talks about how the different authors have assessed drone technology. At last, the research gap is identified.
- Chapter 4 is all about setting up the working environment and preparing resources for the gathering of data. The drone system is divided into components and undergoes an FTA and FMEA analysis. It also presents a review of existing cybersecurity frameworks for drones and a recommendation of a specialized one addressing drones that operate in GNSS denied environments.
- Chapter 5 presents the analysis of the findings that have been observed.
- Chapter 6 especially talks about the conclusions that have been made from the observations. It discusses all the challenges and problems that were encountered during the research and analysis. It also paves the way for future research, explains some shortcomings and presents what has been left from the overall research.

2 Concept and Background

In this chapter, we discuss the concept and background of the research. We look at the evolution of drones and how they diversify into military and commercial groups. The discussion then moves on to how GNSS is used as a baseline for navigation and how various innovations are seeking to alleviate that with specific consideration of computer vision and AI assisted navigation. This chapter ends with a look at the existing frameworks guiding drone operations in general and a look at how they impact in isolation, the operation of drones in GNSS-denied environments.

2.1 DRONES

The evolution of drones from medieval contraptions to contemporary IoT devices has been a stellar one. Drones have already been defined in this document as an unmanned aircraft that can be controlled remotely or operate autonomously with a layman's label as a flying robot appropriate in this instance. The first instance of this application was in military technology when Austria attacked Venice in the 1850's [13]. They were mere flying balloons that carried bombs intended to be dropped onto Venice, but they were blown off course by a change in wind. No matter how crude the contraptions were, the inventors of that time must be commended for their innovation. Then quadcopters came into play at the beginning of the twentieth century. Then came the first world war when the first pilotless aircraft was built for yet again, the purpose of dropping bombs. Archibald Low was the inventor, and this was also the first drone to use a radio guidance system. The 1930's saw the continuance of the development of unmanned aircraft judging from the success in the first world war. Curtiss N2C-2, Radioplane OQ-2 and V-1 Doodlebugs played prominent roles in the war with the use of radio-control and remote control [14]. However, the first patent for an invention that uses a ground terminal to track movements of airplanes were assigned to Edward Sorenson. Most of these devices employed a guidance system that used a simple autopilot to control altitude and airspeed; a pair of gyroscopes-controlled yaw and pitch; the azimuth was maintained using a magnetic compass; a barometric device was used to control altitude. The gyros, rudder, and elevator were controlled using pressurized air. The Vietnam war was the first instance cameras were used along with drones for reconnaissance. Drone development was beefed up afterwards with the US and Israel taking lead roles. The RQ2 Pioneer was developed as a medium sized reconnaissance aircraft with drone developers looking at alternate sources of power with the obvious choice being solar power [14]. The predator which was launched in

2000 is considered the true mother of all contemporary drones with small-sized, fixed-wing surveillance drones taking centre stage afterwards. Generally, drones have the following parts:

1. Copter frame
2. Motors
3. Electronic Speed Controllers
4. Flight Controller Boards
5. Propellers
6. Radio Transmitter
7. Battery, Electronics, and Power Distribution Cables
8. Camera
9. Landing Gear

For the purposes of this research the following components have rather been adapted for classification:

1. Drone hardware (propellers, motors, camera, battery, remote controller)
2. Drone software (drone firmware, remote controller OS)
3. Network/ Network link
4. Laptop/ Data Centre
5. GeoServer/ Map Source
6. HNS

The classification above partly answers the research question RQ2. The components have been classified with the similarity in their make and function to simply the analysis of threats and risks that exist against this drone system.

2.2 FTA and FMEA

2.2.1 FTA

FTA also known as Fault Tree Analysis, is a popular method industry experts use to evaluate an undesired state that can occur in a system [15]. It was first developed and used in Bell Laboratories in the USA by H.A Watson. It has been used mostly for safety and reliability engineering across many industries like aerospace, nuclear power, pharmaceutical and petrochemicals. FTA has many uses like assisting in designing a system, functioning as a diagnostic tool, understanding the processes and logic that leads to an event. It has gone through various evolutions and developmental changes to become a leading tool in Process Hazard Analysis. In this research however, its use has been tweaked for cybersecurity

purposes only with a shift in the analytical process, enhancing the evaluation on vulnerable drone parts and allowing researchers to get a clearer view on how a cybersecurity attack against these parts compromise the whole drone system. This method of analysis was chosen in comparison to the Reliability Block Diagram and Markov Analysis because of the top-down method which allows researchers to analyze vulnerabilities in a system holistically and the analytical process allows the incorporation of risk assessment methods like what is defined in IEC 62443-3-2, security risk assessment for system design.

2.2.2 FMEA

FMEA also known as Failure Mode and Event Analysis is a systemised approach for eliminating failure during product development. It has become a pre-requisite for manufacturers and experts in the product development industry. From its inception in the 1960's by the US military along with its constant use and evolution, has given rise to three main types, that is, Functional FMEA, Design FMEA and Process FMEA. FMEA allows researchers to discover all that could possibly go wrong with a system, remedial actions to take to prevent such failures or to prevent the consequences of both probabilistic and deterministic failures [16]. The FMEA was chosen as a complementary tool to the FTA because the down-to-top approach serves as a counterbalance for the FTA which uses a top-to-down method. The FMEA also allows the inculcation of IEC 62443-3-2, security risk assessment for system design, with an emphasis on applying a risk matrix to determine severity and probability of a failure along with an opportunity to take retrospective action. The FMEA in this research does not consider functional failure per se, but how cybersecurity attacks can compromise the drone system.

2.3 GNSS NAVIGATION

Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The GNSS navigation is done through a process called trilateration. A GNSS receiver comprises two elements, a processor, and an antenna. The antenna picks up the signal, and the processor decodes the necessary information. When a satellite broadcasts, it transmits the time it sends that signal encoded in the signal information. The receiver then uses the difference in time from when the signal was broadcasted to when they received it, considering the time delay caused by the earth's surrounding layers. Then using the speed of light, it measures the

distance travelled by the signals from three different satellites. The receiver can deduce its location with the satellite's initial location information. An atomic clock synced to a GNSS, or a fourth satellite is needed to time the signal transmission. Another satellite also provides more than one combination of three satellites that can be used for trilateration. The performance of GNSS is measured by the following four metrics which are Availability, Integrity, Continuity and Accuracy. There are various satellite systems that offer navigation systems and are namely:

1. GPS [17]
2. GLONASS [18]
3. BeiDou [18]
4. Galileo [18]
5. NAVIC [19]
6. QZSS [20]

2.4 COMPUTER VISION AND AI ASSISTED NAVIGATION

Computer Vision is a branch of engineering that allows machines to make meaning of visual inputs such as photos and videos. AI comes to play here in a descriptive sense as to how computer vision uses convolutional neural networks (CNNs) to processes visual data at the pixel level and deep learning recurrent neural network (RNNs) to understand how one pixel relates to another [21].

Huld is developing a computer vision solution called Hilla that enables real-time georeferencing of observable terrain in unmanned aerial vehicles (UAV) using a single camera sensor. The developed solution combines modern deep learning and edge computing with classical remote sensing to enable autonomous, spatially aware flying platforms.

In addition to enabling accurate autonomous navigation based on visual sensory input, this technology allows precisely locating arbitrary objects in the UAV's field of vision. The video feed or images taken by a UAV can be georeferenced based on a reference map that can originate from satellite imagery, airborne image acquisition, or even a pre-recorded flight video.

The solution uses neural networks as the feature extractors for georeferencing images. Features in the video frames are matched with the features in the reference map [22].

2.4.1 Hilla Architecture

Hilla is a Huld developed software written in Python. It can be thought as a single executable, that when started, processes input video either from a file in the local filesystem or waits for incoming frames in the specified RTMP-stream.

Once new video frames are available, the main geolocation loop executes. The main loop works in two stages, where the first stage estimates the absolute geolocation. While the following absolute geolocation estimations are running, the system updates the geolocation estimate through visual odometry. The absolute/relative estimation cycle is shown in Figure 2.

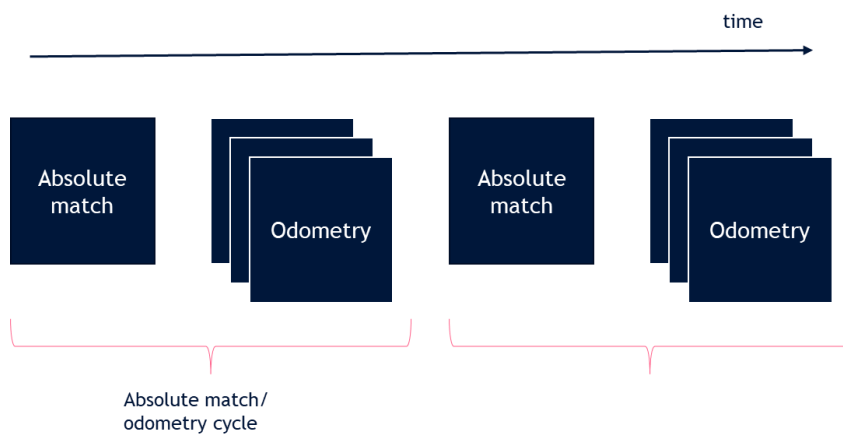


Figure 2 Georeferencing Processing Timeline

As a part of trying to find the absolute match for the geolocation, HNS requests reference maps of the area from a locally running GeoServer instance. The reference maps are queried based on the initial GPS-location estimate or previous estimations for the drone's location. A prerequisite for using this navigation solution is thus uploading and configuring the local GeoServer instance with the correct reference maps of the area of the drone. The rough initial guess for the location of the drone must be within few hundred meters from the actual location.

The interfaces for the navigation solution are shown in Figure 3. The current solution supports georeferencing video streams as well as single still images. The results of the georeferencing can easily be seen from the output video feed, which has an overlay of the OpenStreetMap layer. The results are also stored in a separate file which can be used for further visualisations.

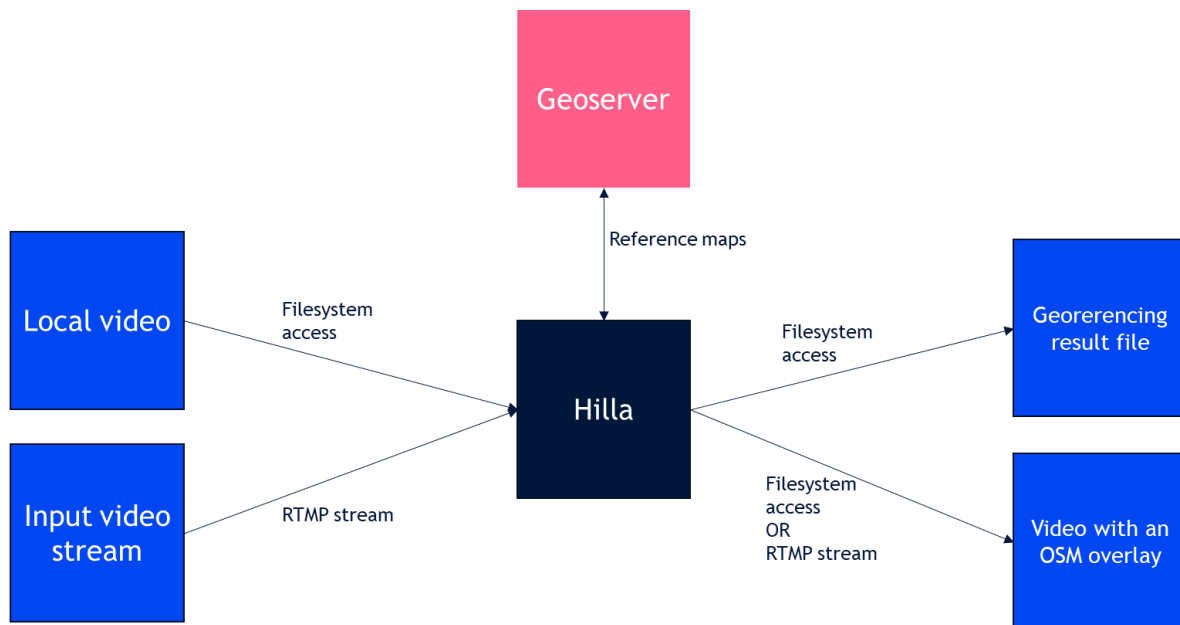


Figure 3 Hilla components

The software is containerised for easier deployment. The entire system, with a running GeoServer instance can be started using docker compose.

2.5 FRAMEWORKS

The widespread adoption of drone technology has posed issues, in addition to security, in terms of liability, privacy, and regulation. Reduced-sized UAVs offer several advantages in shipping, distribution, and privacy such that drone technology has become a part of daily lives. The security and privacy of these drones, on the other hand, are a major concern. Most of drone operations are categorized under hobby, private or commercial activities. The general ideology is to develop a framework where regardless of the purpose of the drone, once there is a navigation under GNSS denied conditions, there are a set of proper recommendations that exist concerning privacy, data transfer and security. A cybersecurity framework is a collection of best practices that are recommended to be followed to manage cybersecurity risk. The goal of the framework is to reduce exposure to cyberattacks, and to identify the areas most at risk for data breaches and other compromising activity perpetrated by cyber criminals.

2.5.1 Standards and Standard Development Organizations

A Standards Development Organization (SDO) is an organization whose primary function is developing, coordinating, revising, interpreting, or otherwise contributing to the usefulness of

technical standards to those who employ them. A cyber security standard defines both functional and assurance requirements within a product, system, process, or technology environment. Most standards are voluntary in the sense that they are offered for adoption by people or industry without being mandated in law. Some standards become mandatory when they are adopted by regulators as legal requirements in particular domains, often for the purpose of safety or for consumer protection from deceitful practices and they are sometimes called formal standards. An example of an SDO is the International Standards Organization (ISO) and an example of a framework that has become a formal standard is ISO 27001. ISO set up a drone framework that is including, but not limited to, classification, design, manufacture, operation (including maintenance) and safety management of UAS operations. ISO released a couple of drone standards in 2019 but recalled the ISO/IEC WD 22460 and subsequently deleted from the market. There are several others like the ISO/IEC AWI 22460-3, ISO/IEC DIS 4005-4 which are still under development and touch on critical areas such as logical data structures, access control, authentication, and integrity validation for drone operations.

The International Electrotechnical Commission (IEC) is another standardization organization that sets standards on manufacture and testing of finished goods unlike ISO which concentrates on materials and process control. The IEC 62443 series is an international series of standards for operational technology in industrial automation and control systems. Specifically, the IEC 62443-3 and 62443-4 series, addresses technical security requirements for systems and components and risk assessment methodology. Though these standards do not explicitly refer to drones, drones can be considered as IoT devices which enables it to fall under the Industrial Automation and Control Systems (IACS) family.

2.6 SUITABLE LINK BETWEEN A STANDARD FRAMEWORK AND DRONE

Some of frameworks are set by independent standard organizations and others too are set by government or governmental bodies. Upon all these, there is a lack of a specific framework that consulted drone professionals, academics, businesses, and the public to regulate the operations of drones in a GNSS denied environment. ISO 21384-3 [23], Unmanned aircraft systems – Part 3: Operational procedures and other frameworks do not address asset management, risk assessment, access control, continuous monitoring, and recovery for the type of drones that are subject to this research. Taking into consideration a section of a framework like continuous monitoring, most industry players would not like to wholesale

change their security posture to include analysis and response planning. There are a lot of different cybersecurity risk practices that suit different organizations with different security requirements. They will just look at adding a few new categories with minor tweaks without embarking on wholesale changes. This is because the fact cannot be denied that drones are an extension of the user's network and thus, most information security management practices can be applied but the metamorphosis is required when computer vision and AI is adapted for navigation, and data processing is done inflight on the drone or by a datacentre somewhere with data exchange on a 5G network link. The following chapter looks at review of appropriate and reliable documents relevant to the research.

3 LITERATURE REVIEW

3.1 Information Sources for Current Literature Review

Major information sources are explored for literature study of drone security materials. Instead of searching through internet, direct databases are accessed to get relevant studies. However, some other sources are also searched to get all possible relevant materials. These materials are filtered and only the ones found relevant are studied for this review. The sources of these literary works are shown in Table 1 below.

Information Source	Web link
IEEE Xplore	http://ieeexplore.ieee.org/Xplore/
ACM Digital Library	http://dl.acm.org/
Springer	http://www.springerlink.com/
Science Direct	https://www.sciencedirect.com/
Other Sources	Conferences, books, and webpages

Table 1 Information Sources for Literary Review

3.2 Workflow of Current Literature Study

This literature study is carried out in different steps. Different actions are performed at each stage to get accurate and relevant proposed solutions. In this first step, literature review is performed with drone security in general and the security challenges they face. These security challenges are categorized and discussed accordingly. In next step, solutions for these threats are discussed and security issues are identified. Limitations for existing solutions are identified in these papers. A new solution is proposed to overcome these limitations. Fig. 4 shows the workflow of the current literature study.

3.3 Year-Wise Publications

The statistics for analysis of publications in this chapter is considered only from IEEE Xplore with the key words used for the queries as “drone security” and “standards”. The following graph shows the year-wise publications list. In 2015 relevant studies were 9 which are considered in the bar chart shown in Fig 5. This number increases continually for each year. In 2022, relevant studies are increased which include drone security, challenges and security frameworks are described for the selection of papers. There is also a pie chart in Fig. 6 below which shows a distribution of the relevant materials across the eight-year period of analysis

with this including conference proceedings, journals, magazines, books, and early access articles.

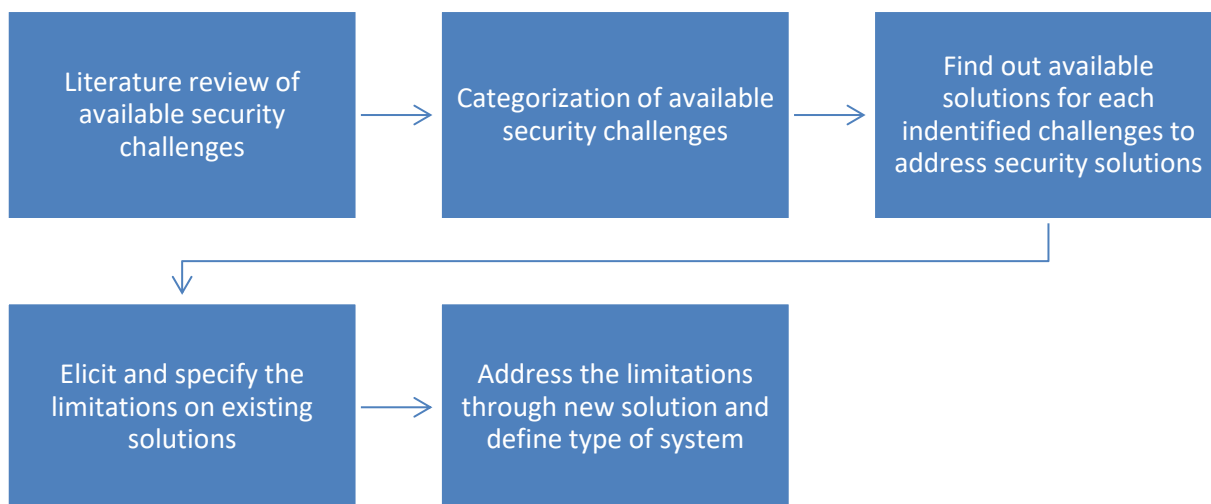


Figure 4 Workflow of the Literature Study

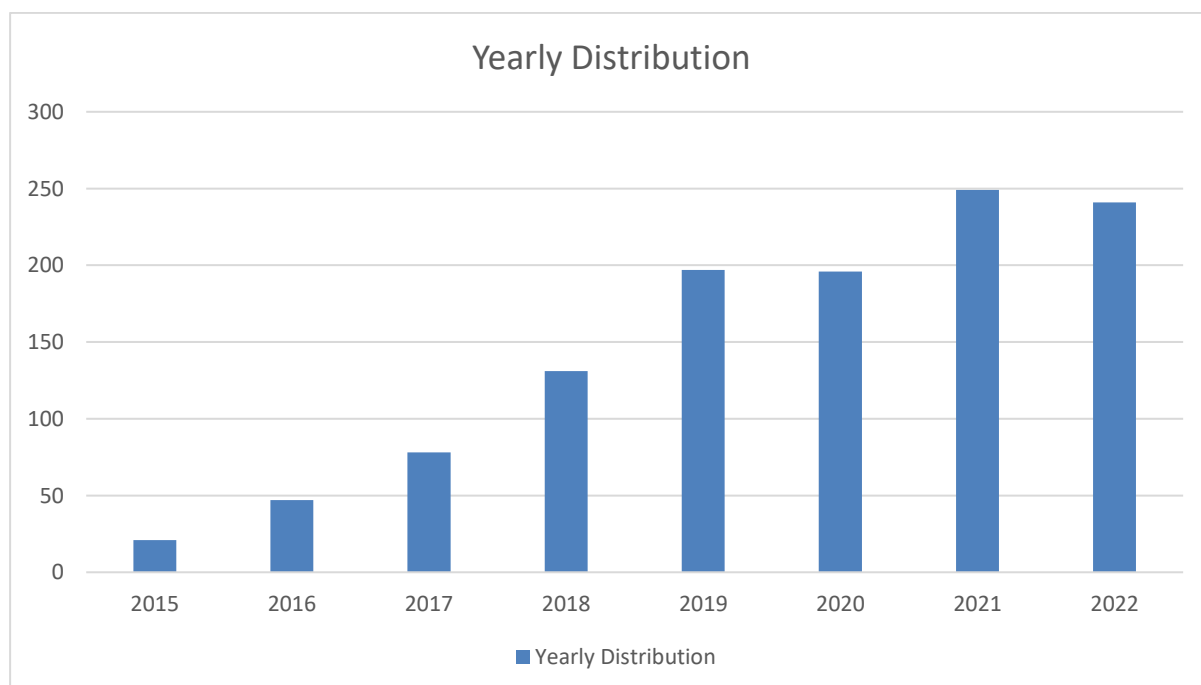


Figure 5 Yearly distribution for drone security related literature

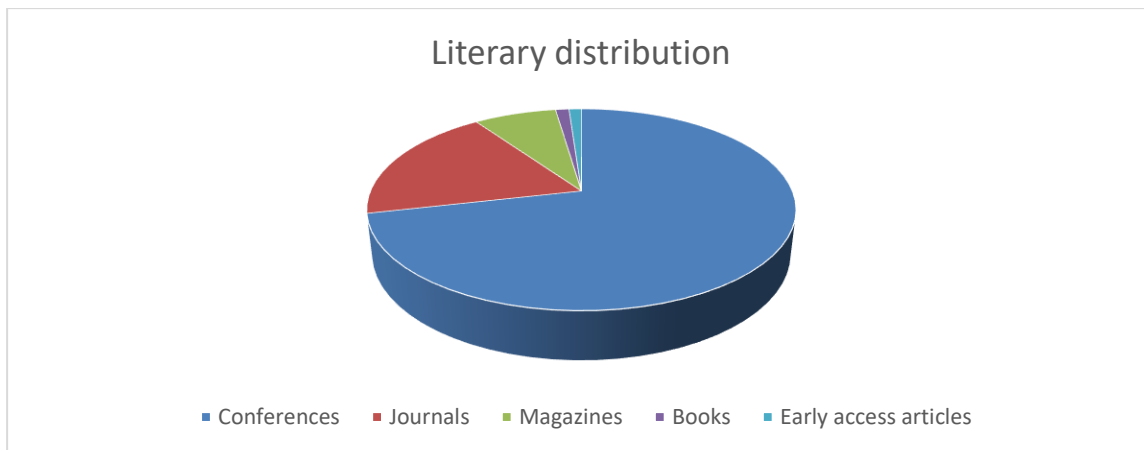


Figure 6 Pie chart of literary distribution

3.4 Security Challenges of Drones

A lot of literary work has been done on the threats, risks, and general security issues of drones. [24] assesses the DBPOWER U818A WIFI quadcopter family of drones which is a popular brand, highly re-purposed and sold by a variety of drone vendors. A vulnerability was discovered and assigned as CVE- 2017-3209. This vulnerability was known to allow attackers to have anonymous FTP access over the drone's own local access point with full file permissions. This could result in attackers flying away with the drones, taking the drone down, looking the legitimate owner out, or stealing user data.

[25] makes extensive use of the term "internet of drones", IoD, which is a derivative of the term, internet of things, IoT. It is discussed that this makes most of the threats and vulnerabilities affecting IoTs inherent to IoDs. Various scenarios are then used to assess the impact and affected security parameters that are seen as challenges for drones. A taxonomy of different types of known attacks in IoD is listed in terms of relations to privacy, integrity, confidentiality, availability, and trust. Privacy and trust are new parameters other than confidentiality, integrity and availability that make up the popular cybersecurity triad. Third party violations, key loggers, location tracing and data capturing are noted as some of the attacks prevalent on privacy and trust in that research.

[26] focus research on opportunities for drones in the civil and military industries. There is further analysis of architectural, security and safety issues which lists the challenges facing these intelligent devices in security and privacy of data. A further review of drone communications in this research work reveals four drone communication classifications, namely, drone-to-drone, drone-to-ground, drone-to-network, and drone-to-satellite

communications. An identification of threats and vulnerabilities that are susceptible to these industrial and military drones are grouped as protocol-based attacks, sensors-based attacks, compromised components and jammers.

[27] surveys the main security, privacy, and safety aspects associated with the use of civilian drones in airspaces. There is an identification of both the physical and cyber threats of such systems and a discussion of the security properties required by their critical operation environment. This survey categorizes cyber-physical threats according to the power of the adversary and names them as revelation capabilities, knowledge capabilities and disruption capabilities. The attacks are then further grouped into two. Attacks on the flight controller and ground control station have examples as spoofing GPS data, spoofing UAV transmissions and injecting falsified sensor data. Attacks on the datalink have some examples such as denial of service and unauthorized disclosure of information.

3.5 Proposed Solutions for Drone Security Challenges

Vast work has been done on the threats and vulnerabilities drones face. This has seen a culmination in the proposal of solutions for these threats. [28] conducted a survey to categorise the UAV threat landscape for connections between UAVs, ground control stations, and personal pilot devices. There is then an analysis of conventional and novel UAV routing protocols, indicating the advantages and disadvantages from the cybersecurity perspective. The solutions recommended for the threats identified include multi-hierarchical routing, data centric routing, optimized link state routing and temporally ordered routing algorithm.

Lightweight and energy-efficient symmetric-key cryptographic algorithms have been recommended to be deployed on devices that are resource constrained. [29] implemented Elgamal and AES to encrypt location information, which provides confidentiality and traceability for mobile devices. [30] designed TCALAS, a temporal credential based anonymous lightweight user authentication mechanism for the IoD. This was proven to be resistant to known authentication attacks. [31] improved TCALAS by using lightweight symmetric key primitives and temporal credentials to secure against traceability as well as stolen verifier attacks. The researchers proposed scheme, ITCALAS, is lightweight and can work with multiple IoD flying zones or clusters.

To safeguard drones from DoS or spoofing attacks, [27] suggest an anonymous intrusion detection system that differentiates between genuine communications and those corrupted by

DoS attacks. [32] use an intelligent deep learning-based IDS to distinguish between spoofed or original GPS signals. This allows drones to identify intruders and ensure a safe return-to-home if required. Simulations indicate the IDS can provide high levels of accuracy, sensitivity, and specificity against a range of cyber security attacks.

Alliance for Telecommunications Industry Solutions (ATIS) is the North American Organisational Partner for 3GPP. 3GPP Standards added some elements to mobile cellular networks to support UAV communication [33] using LTE and 5G radios. The related works are detailed in 3GPP Release 15 [34], 16 [35] as well as 17 [36] and includes UAVs ranging from low altitude to high altitude (8 km-50 km). These works cover issues such as up-link power control, interference detection, radio performance improvement, identification, initial UAV pilot authorization, UAV traffic management, identity broadcasting when piloting BLoS.

American Society for Testing and Materials (ASTM) F38 [37] is a committee that develops UAS standards and guidance, including topics relating to safety, performance as well as flight proficiency. There are thirteen active standards in subcommittee F38.01 [38] and five proposed new standards waiting for jurisdiction. These standards are UAS registration and marking (ASTM F2851-10) [39], small and lightweight UAS design (ASTM F2910-14) [7], construction and verification (ASTM F3298-19) [8], specification in designing command and control systems in small UAS (ASTM F3002-14a) [9], and detection as well as avoidance in small UAS BVLOS (ASTM WK62669) [43].

ISO Technical Committee (TC) 20, Subcommittee (SC) 16 are a set of standards in UAS areas containing, but not restricted to classification, design, manufacture, and operation [44]. Since 2019, there are five published standards about commercial UAS operation requirements (ISO 21384-3:2019) [23], definition of relevant terms in UAS (ISO 21384-4:2020) [45], a classification tool of UAS (ISO 21895:2020) [46], a survey on UAS traffic management (UTM) (ISO/TR 23629-1:2020) [47] and methods for training people who operate UAVs (ISO 23665:2021) [48]. Providing Operations of Drones with Initial UAS traffic Management (PODIUM) [49] provides a U-space service (a European ecosystem assisting UAV operation), methods and technologies in three European countries. PODIUM gives advice regarding standards, regulations, and future UAV use with partners like Airbus, DSN, DELAIR, Drones Pari Region, and Unifly. PODIUM is contributed to by EUROCONTROL which is an

organisation serving European aviation. EUROCONTROL also presents a series of projects and initiatives [50] about UAS operations, UTM, satellite navigation and flight control.

3.6 Limitations on Existing Solutions

The research above has made valuable contributions to the UAV industry but there is a long road to tow for industry experts before the optimal standard can be achieved. [28], [29], [30] and many others have made recommendations for solutions to the threats that UAVs face. These recommendations, however, address the technological vulnerabilities these systems face and not issues that come up because of the system's operation. The standards recommended by the regulatory bodies were a step in the right direction but many of them are not matured for the industry and are GNSS operational biased. ASTM and ISO have such frameworks in the pipeline but are not ready for public use as of the time of this research. There is a gap in the operational phase for UAV devices which can be filled with a mature security framework for operations.

3.7 Literature Review Summary

Table 2 shows the summary of materials used for the literature review. There are details of the type of materials, the contribution made to drone security, criteria of research and further work to be done on each research. Some materials gave technological solutions that lacked research for operational implementations while the rest made operational solutions but were GNSS biased. Table 3 continues a rendition of the summary but examines relevant literature materials in relation to the research objectives of this paper. Some of the papers made use of standard models for threat analysis or performed a risk analysis for a use case of a drone system but none of them performed an FTA or FMEA of a drone system in a cybersecurity context.

Citation	Type of Literature	Criteria	Contribution	Further work
Valente et al., 2017 [24]	Research work	Vulnerability Research	Vulnerability Discovery in U818A drones	Security research in other types of drones
Choudhary et al., 2018 [25]	Research work	Vulnerability Research	Threat modelling for internet of drones.	Threat mitigation mechanisms and vulnerability assessments methods for loD.
Majeed et al., 2021 [26]	Journal	Cybersecurity Research	Evaluation of drone security as part of an IoT system.	Security solution improve authentication and access control mechanisms in drone security.
Tsao et al., 2022 [28]	Survey	Technological solution	Network resilience	Operational implementation
Ni et al. [29]	Conference Paper	Technological solution	Encryption and cryptography	Operational implementation
Altawy et al. [27]	Survey	Technological solution	IDS implementation	Operational implementation
Srinivas et al. [30]	Research work	Technological solution	Cryptographic scheme for drone authentication	Operational implementation
Ali et al. [31]	Research work	Technological solution	Improved cryptographic scheme for drone authentication	Operational implementation
ASTM F2500 [38]	International Standard	Operational Solution	Flight operations for UAVs	Yet to be published
ISO 21384-3:2019 [23]	International Standard	Operational Solution	UAV Risk assessment and ISMS	GNSS biased
This research work	Research	Operational solution	Cybersecurity FTA and FMEA of UAVs	Security framework for operation in GNSS denied environment

Table 2 Comparison of the contributions of relevant literature materials to drone security.

Citation	Standard threat model	Risk analysis	Drone parts classification	Recommendation of security framework
Valente et al., 2017 [24]	✓	✓	✗	✗
Choudhary et al., 2018 [25]	✓	✓	✗	✗
Majeed et al., 2021 [26]	✓	✓	✓	✗
Tsao et al., 2022 [28]	✓	✓	✗	✗
Ni et al. [29]	✗	✗	✗	✓
Altawy et al. [27]	✗	✓	✗	✗
Srinivas et al. [30]	✗	✓	✓	✓
Ali et al. [31]	✗	✓	✗	✓
This research work	✓	✓	✓	✓

Table 3 Comparison of relevant literature materials with the research objectives of this paper.

4 METHODOLOGY

After successfully dividing the drone system into components, this chapter looks to subject the components to FTA and FMEA thoroughly. RQ1 asks what kind of risk/threat analysis model could be implemented to drone operation in GNSS-denied environment? This question requires a need to fully explore all causes of what could compromise a drone operation in a GNSS denied environment. The Fault Tree Analysis is the primary tool used for analysis in this research and Failure Mode and Effects Analysis is the secondary tool used to mop out the remainder of components that were not included in the FTA. These two forms of analysis are seen as a complement to each other and would be less effective for our research if used in isolation. The assumptions here is that all drone operations are conducted in GNSS denied environments. These conditions will help propose risk driven models and scenarios where the threats and risks posed will be used to design a security framework.

4.1 FTA ANALYSIS

Fault tree analysis is a tool used to explore the causes of system level failures [15]. It uses Boolean logic to combine a series of lower-level events and it is basically a top-down approach to identify the component level failures that cause a system to fail. FTAs mainly consists of two elements, “events” and “logic gates” which connect the events to identify the cause of the failure at the top of the hierarchy. FTA is different from FMEA by focusing on all possible system failures- of an undesired top event, whereas FMEA conducts analysis to find all possible system failure modes irrespective of their severity. FTA is relevant to this research because of its ability to perform all types of system level risk assessments and its ability to effectively identify causes of system failure and mitigate the risks before it occurs. For a system as complex as a drone system, this is an invaluable tool that visually displays the logical way of identifying the problem and as an additive, improving system efficiency.

4.1.1 FTA SYMBOLS AND THE ITERATIVE PROCESS.

FTA diagrams have numerous symbols but a few that will be relevant to our research have been listed below. The FTA analysis gives room for the DSRP where the analysis is problem-oriented and development-oriented that supports change from the state of the system to the primary or basic failure event where changes and re-evaluations during the research process may be needed. From the problem identification and motivation to the final stage where the solution will be proposed, change is inevitable.



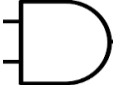
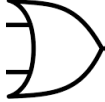
Event / Gate Symbol	Description
	Primary or basic failure event. It is random event and sufficient data is available.
	State of system, subsystem, or component event.
	AND Gate – the output event occurs when all the input events occur
	OR Gate – the output event occurs when at least one of the input events occur.

Table 4 Event and Gate Symbol description

The STRIDE MODEL which lists various threats that could develop into faults in the drone system are used as the states of the system or component events in the FTA and are discussed below along with their corresponding FTA diagrams.

4.1.2 THE STRIDE MODEL AND FTA DIAGRAMS

The STRIDE model is used extensively as a framework for threat analysis of various systems. It was chosen because in comparison with other threat models, STRIDE provides suitable scenarios that presents the existing threats against the drone parts in a logical and realistic manner. Other threat models like PASTA, VAST and DREAD were considered for the FTA but were not suitable for this research because of a lack of clearly defined attack vectors and because outright threat modelling is beyond the scope of this research, it was imperative that the threat model chosen, provides a suitable foundation as base events for the FTA. STRIDE therefore became the obvious choice and though it is not the main tool in use here, it serves as the foundation from which the various base failure events for the FTAs will be built from. From vast literature review, it has been identified that FTA has never been used in a cybersecurity implementation but only for safety purposes. To the best of our knowledge, this is a novel implementation of FTA for drone cybersecurity analysis in research. The STRIDE model is made up from six components namely:

1. Spoofing
2. Tampering
3. Repudiation

4. Information disclosure
5. Denial of service
6. Elevation of privilege

The components of the drone system listed in chapter 2 have been divided and analysed in the diagrams below.

4.1.2.a Spoofing

Spoofing is a security concept where a trusted entity is imitated [51]. For this system under consideration there are various components that attackers can imitate. The powerful laptop or scalable data centre that will be in place can be spoofed during the communication between it and the drone. This navigation technology makes use of pre-stored satellite images which involves the heavy use of maps. Maps as an external source can be spoofed when the source of reference is altered. The technology allows a downloading of offline maps to be directly uploaded to the drone device. This is another avenue where the maps can be spoofed before uploading. [52] discusses an experimental study on the security of unmanned aerial vehicles where emphasis is placed on GPS spoofing. Although the case study for this research alleviates the reliance on GPS navigation, the concept of spoofing attacks against drone systems remains. The attack scenario in [52] looks at spoofing attacks against the DJI phantom 4 Pro (P4P) and Parrot Bebop 2 drones. The severity and probability for these kinds of spoofing attacks are further considered in the FMEA in the next section.

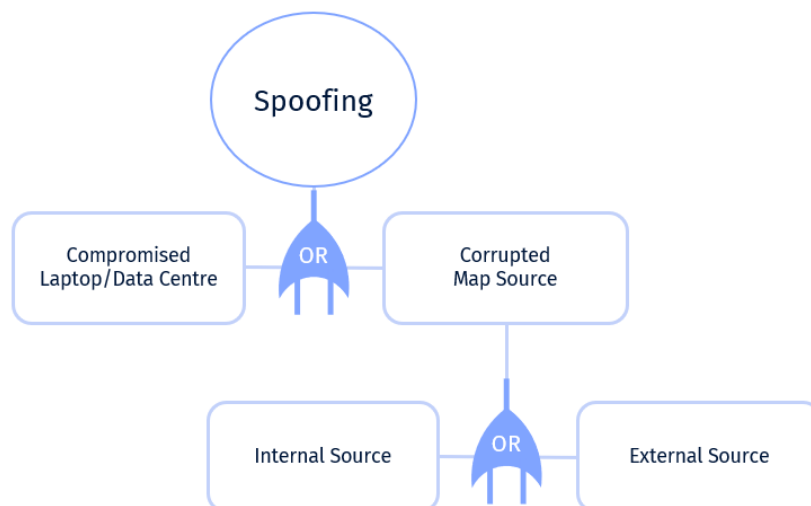


Figure 7 FTA diagram for Spoofing of the Drone Navigation Solution

4.1.2.b Tampering

Tampering is the malicious modification of components of a system. The drone system is basically made up of Hardware and Software components. All these incidents can compromise the drone system independently without correlation with each other. The hardware components which have the most vulnerable parts to be batteries, motors/propellers and the board can easily suffer damage. Intentional or unintentional initiation of physical sabotage can deprive the drone of power source, flying ability, electrical and data flow [53]. The firmware and controller OS are accessible for the purposes of this research, it is included in this analysis because of the security issues that comes along with open-source technology. The resources of nation state attackers and other malicious attackers to make do of zero-day attacks on firmware and OS makes it necessary to include these vectors in our threat analysis. The navigation solution as a web-based solution is open to tampering through the libraries it

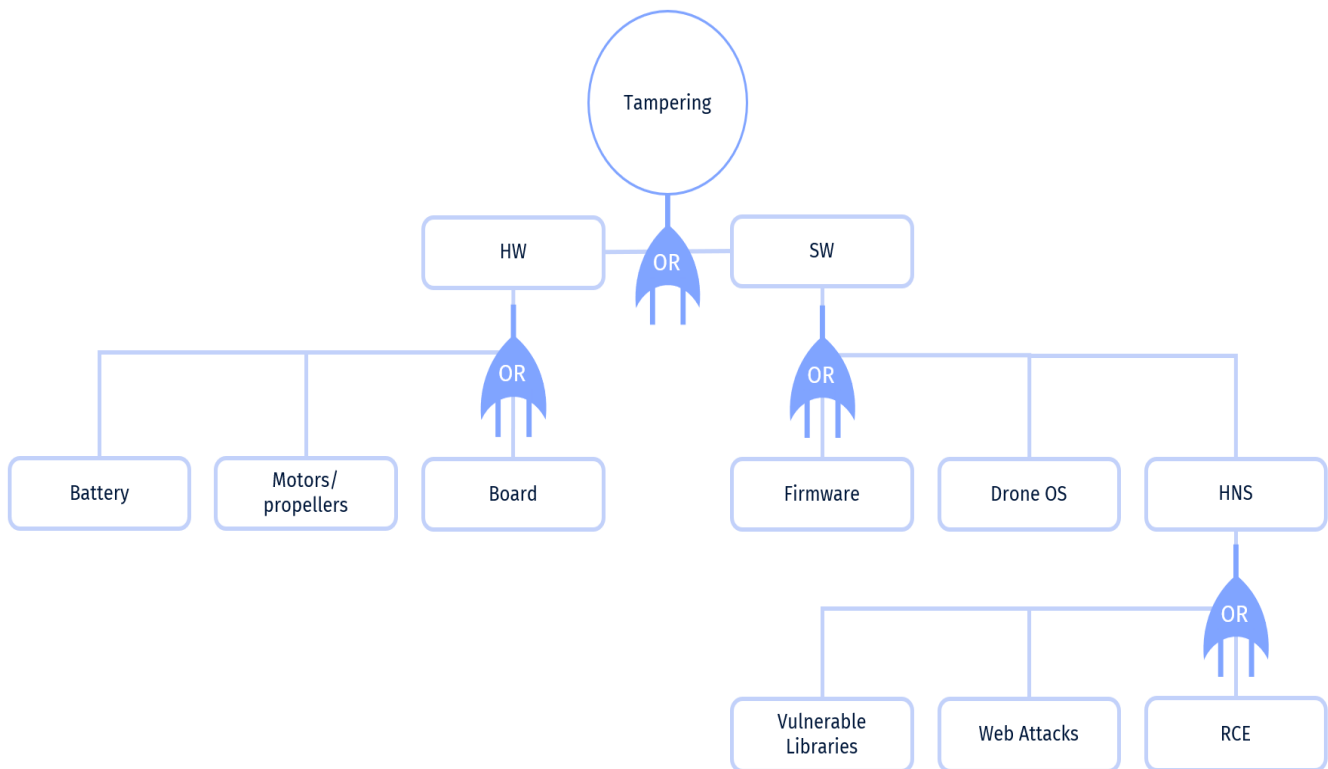


Figure 8 FTA diagram for Tampering of the Drone Navigation Solution

uses. Its packaging as a web platform has some inherent vulnerabilities. An attack scenario that depicts tampering attacks is an insecure data transmission vulnerability in the DJI Mimo mobile application. The mobile application does not employ basic data protection mechanisms making it possible for attackers to eavesdrop and modify data. The mobile

application also sends media data to a hosting site using AES 128-bit key encryption over unencrypted HTTP connection [54]. The consequences of such actions other than tampering of data are discussed in the next chapter.

4.1.2.c Repudiation

Repudiation is a technological concept where components of a system are not able to acknowledge responsibility for actions they effected. It is very important that components of the HNS and the network infrastructure are held liable for actions taken. This could be in terms of navigation solution where telemetry data and other spatial concerns need to be transmitted back to the controller and there will be no receipt or confirmation of such a transaction. The network component, depending on the drone system implementation or use case in play, could have components from another drone to a cell tower in the fly zone or a customer at the end of the system who needs to receive notifications from the drone flight. Non-repudiation is the security concept that poses the solution to this threat, and it is a quality that is required for every efficient system [55]. A real-life scenario for repudiation attacks is an FTPD zero-day vulnerability that existed on the busy box FTPD on Mavic, Spark and Inspire 2 drones. This vulnerability allowed attackers to modify stored files in the drone and unlock prohibited features such as height restrictions and no fly zones [56]. Non-repudiation in the drone OS supports file consistency and prevents flouting of drone operational policies.

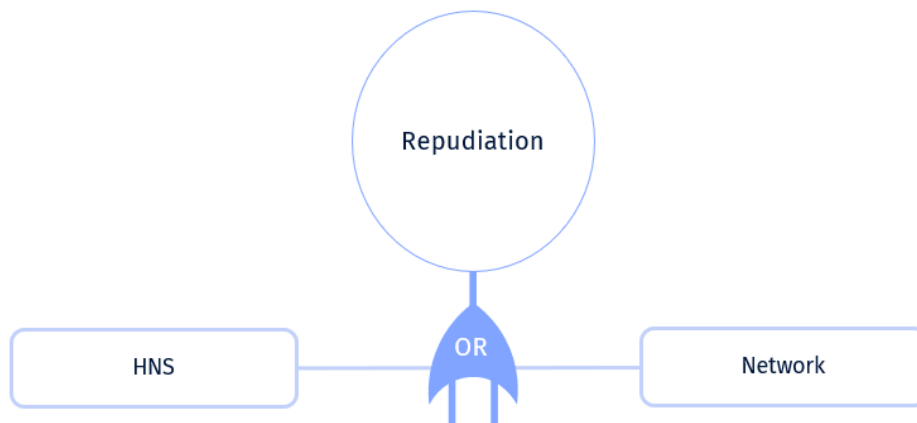


Figure 9 FTA diagram for Repudiation in the Drone Navigation Solution

4.1.2.d Information Disclosure

This is when information falls into the hands of unauthorized individuals. The most common causes are unsolicited human errors and concerted attacks on systems. Privacy breaches and data leaks are all forms of information disclosure that is considered in the purposes of drone

navigation in GNSS denied environments. Drones are extensions of network systems they are being managed from and consequentially making the kind of information they collect and handle very crucial. When this information tends to include various personal and sensitive data and not just images and videos of objects, it then extends to become subject to an array of legislations. Currently with the case study, the system makes use of a 5G connection for network communication, but it is only restricted to a communication between drone to laptop and not vice versa. Some of the messages that are sent from the drone to the laptop include

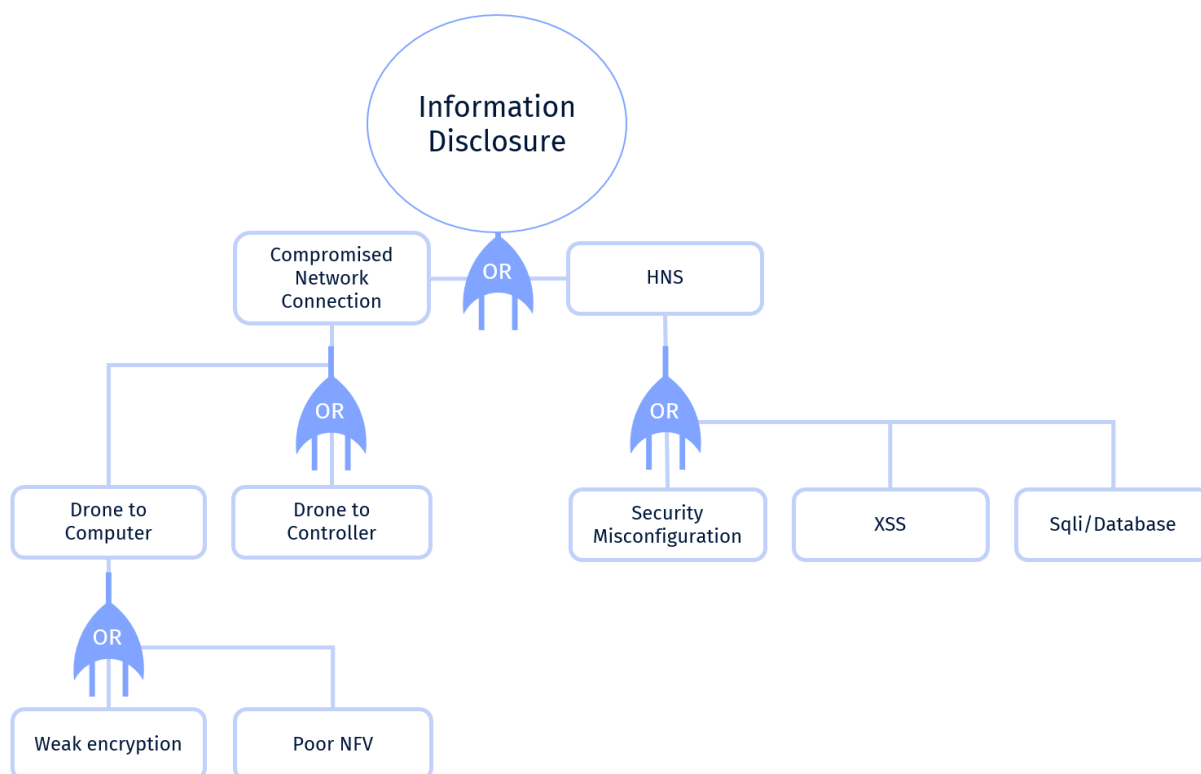


Figure 10 FTA diagram for Information disclosure in the Drone Navigation Solution

initialization messages, the position of the drones, longitude, altitude, and orientation [57]. Another attack scenario for information disclosure attacks was when hard-coded sensitive information like SSH private key and configuration files were hard-coded in DJI Phantom 3A's firmware [58]. A myriad of attacks exists against the web component for drones with an example from the FTA above being XSS and weak session management that allows attackers to steal session cookies making it possible for attackers to impersonate victims and take over their accounts. This XSS and weak session vulnerability also allows attackers to access victim's flight records and media files. Others forms of web attacks like CSRF, Broken

Authentication and XXE attacks are possible however, XSS was only used in the FTA as an example.

4.1.2.e Denial of Service

Denial of service attacks interrupts services and prevents legitimate users from accessing devices or systems. The drone has many components that can be attacked to deny access to the users. The hardware components are the easiest to attack. Any part that suffers physical damage will prevent the drone from flying. Hilla as the prime implementation of the navigation technology can be subject to ransomware attacks. The network communication link is another avenue that can be attacked. There are, various denial of service attacks that can be employed against the 5G network but the most likely will be de-authentication attacks and network slicing [59].

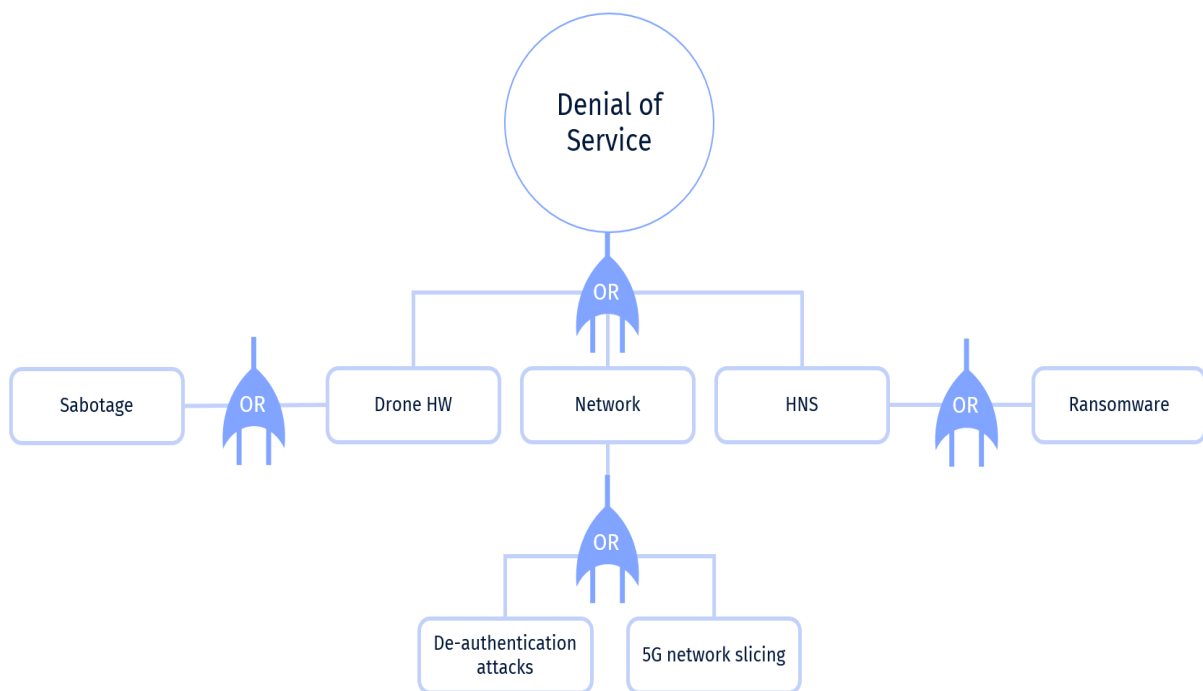


Figure 11 FTA diagram for Denial of Service in the Drone Navigation Solution

It was also discovered in this research that the other forms of attack in the STRIDE model could indirectly lead to Denial of service in the drone system. Spoofing prevents delivery of messages to targets in the systems and consequently prevents execution of commands. Tampering alters the state of a component of the drone system which can prevent it from functioning effectively. Repudiation can result in denial of service when the expected input gets altered or is not received from the expected source. Information Disclosure can leak credentials which grant access to a malicious user, thereby denying access to the legitimate user. Escalation of Privilege, lastly, can result in denial of service when a malicious user gains

the ability to manipulate user privileges. The legitimate user account can be simply deleted, or access credentials changed.

4.1.2.f Escalation of Privilege

The last base event for the FTA is privilege escalation. It is an attack that allows unauthorized privilege access to a system. The communication channel as a software defined network is susceptible to privilege escalation. The scalable data centre or powerful laptop in use can suffer misconfiguration which will allow the escalation of privilege of users. There are two types of privilege escalation: vertical and horizontal privilege escalation. Horizontal escalation involves getting access to accounts with similar access privileges as the initial compromised account and vertical escalation is when the standard user account is used to access accounts with higher privileges [60]. Same applies to the navigation solution where compromised account can be used to elevate privileges to delete or create malicious user accounts.

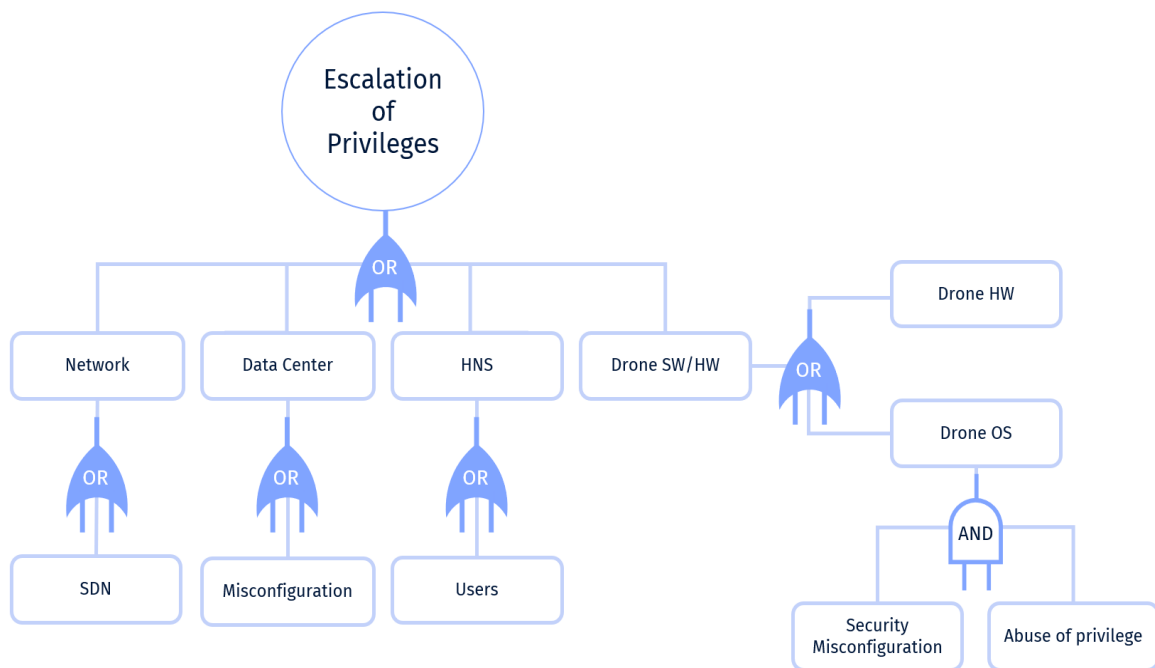


Figure 12 FTA diagram for Escalation of Privileges in the Drone Navigation Solution

An attack scenario that emulates privilege escalation is the DJI Assistant2 that is present in Wi-Fi manageable drones. It employs a weak authentication for a web-socket server that is vulnerable to a malicious take over. Due to hardcoded encryption keys, it is possible for attackers to change Wi-Fi password, become the drone owner and manipulate user accounts as they please. Countermeasures in such instances which includes restriction of web-socket server access, implementation of authorisation and strong encryption mechanism for web-

socket communications will become more evident as FMEA is applied as a complementary tool and the resulting solutions will be clearly defined in the standard recommendations.

The section 4.1.2 above answers the research question RQ1 and clearly shows the suitability of STRIDE as a threat model and its use as a model of examination of this use case. The parameters of the model were relevant as base events for the top to down iterative approach of the FTA. The next section discusses FMEA in a cybersecurity implementation.

4.2 FMEA ANALYSIS

Failure Mode and Effects Analysis also known as FMEA, is a methodology aimed at allowing research to anticipate failure during the design stage by identifying all the possible failures in a design or manufacturing process [16]. This method is meant to be complementary to the FTA in the sense that, after the analysis of threats that can be posed to the system, FMEA looks at the remainder of the various ways the system can fail. The method used here is similar to the risk assessment methods in IEC 62443-3-2:2020 which is mainly used for security assessment for industrial and automation control systems. The table, risk matrix and other relevant tools have been modified to suit this research work.

4.2.1 The FMEA Process

The risk analysis diagram in the standard quoted above, is quite complicated but adapted for use for this research. It is mainly an iterative process that allows the analyst to adjust the parameters used for analysis. The point of examination where a rhetorical question is asked about the suitability of the residual risk, helps make this method exhaustive. A summary of the steps is listed below.

1. Identification of the system.

At this stage, the analyst gets familiar with the system, components, and architecture. It might also be relevant to consider regulations or guidelines already in place. The analyst must also consider how the systems relate to external services or how it affects other systems at large.

2. Initial cyber risk assessment.

This is when the benchmark gets set for the analysis. It is necessary to make a list of known vulnerabilities and threats that affect the system. Notice of the assessment results and the system as it is, should be taken into consideration. Grades are set for the results of this

analysis. An ancillary question can further be asked as how the initial cyber risk assessment should be done. The foundational requirements used in IEC 62443-1-1:2009, Network and System Security- Terminology, concepts, and models, can be used as a basis of classification in setting the initial grades for the system. The foundational requirements are listed below:

FR 1 - Identification and authentication

FR 2 - Use Control

FR 3 - System Integrity

FR 4 - Data confidentiality

FR 5 - Restricted data flow

FR 6 - Timely response to events

FR 7 - Resource Availability

3. Partitioning the system.

The system can be divided into zones and conduits at this stage. This can be done in terms of how similar or dissimilar some components are like communication channels, criticality of assets, operational functions, logical locations or required access.

4. Tolerable risk and further risk assessment.

The process at the stage, poses a question of initial exceeding tolerable risk. If the answer to that question is yes, there is a need for the process to repeat till a tolerable level of the risk is achieved but if the answer is no, the analyst can move to the next step.

5. Document and asset owner approval.

The role of the asset owner varies on a use case basis. It varies from the analyst to an individual to oversees the evaluated system. If the results are satisfactory, the entire process and results can then be certified in accordance with regulations, standards and polices that apply in that context.

4.2.2 The FMEA Table

The table below summarizes the process and gives a description of an as-is and a to-be state of the system.

1	Failure Mode	Failure Effects	Causes	Probability	Severity	Detection	Risk Index	Actions Recommended	Probability	Severity	Detection	Risk Index
2	Inability to start	1. Inability of drone to takeoff 2. Bad response timing	1. System Firmware 2. Spoofing Reporting Message	3	2	2	12	1. Code signing 2. Network allowlists 3. Static network configuration	2	2	2	8
3	Deviation from route	1. Accidents 2. Loss of drone	1. Exploitation of remote services 2. External Remote Services 3. Internet Accessible	3	3	2	18	1. Application isolation 2. Vulnerability scanning 3. Threat intelligence program 4. MFA	2	3	2	12
4	Drone Hijacking	1. Use of drone as a pivot to attack the rest of the system. 2. Loss of information	1. Commonly used port 2. Data Manipulation 3. Spoofing Reporting Message	3	3	3	27	1. Disable or remove feature or program 2. Network intrusion prevention 3. Network segmentation	2	2	2	8
5	Compromised drone data	1. Inaccurate navigation by navigation solution.	1. Drone feed leakage 2. Data from Information Repositories	2	3	2	12	1. Audit 2. Restrict file and directory permissions	1	3	2	6
6	Compromised drone user accounts	1. Increased privilege in network	1. Valid Accounts(Compromised Accounts) 2. Domain takeover	3	3	2	18	1. Account use policies 2. Privileged account management 3. User account management	1	3	2	6

Table 5 FMEA table for drone operation in a GNSS denied environment.

4.2.3 Risk matrix and parameter definitions

This section defines the terminology used in the table as well as the risk matrix included in the FMEA implementation.

Failure Mode - description of failure being analysed.

Severity (SEV) - An assessment of the seriousness of the effect of the potential failure mode upon the customer.

Occurrence (OCC) - Description of how frequently the specific failure cause is expected to occur, ranked on a scale of 1 to 3 as per the table below.

Detection (DET) - An assessment of the probability that the current controls will detect the potential cause, or the subsequent failure mode.

Risk Index (RI) - The product of the Severity, Occurrence, and Detection Rankings i.e. $RI = SEV * OCC * DET$.

The matrix used below is adapted from IEC 62443-3-2:2020 Annex B and is not fixed and can be adapted or modified to suit the context of the analysis.

Index	Probability	Description
1	Improbable	Conceivably possible, but very unlikely to occur.
2	Somewhat Improbable	Quite possible or not unusual to occur.
3	Highly probable	Certain to occur.

Table 6 Probability table showing parameters used for determining likelihood in risk assessment.

Index	Severity	Description
1	Minor	Little to no impact to human lives, drones, and other assets in the environment.
2	Moderate	Bearable financial losses and minimal damage to equipment with some warning.
3	Extreme	Fatal injuries, substantial financial loss and equipment damage without warning.

Table 7 Severity table showing parameters used for degree of impact in risk assessment.

Index	Detection	Description
1	Low	Easily detected by mere observation with the physical eye.
2	Medium	Detection may be possible with the help of some observational tools.
3	High	Almost impossible to detect.

Table 8 Detection table showing parameters used for how easily risks are identified in risk assessment.

Risk Index	Category	Description
1 to 7	acceptable	risk level minimal enough to be accepted.
8 to 17	tolerable	presence of risk but moderate enough to be tolerated.
18 to 27	inacceptable	risk levels are inordinate and are intolerable.

Table 9 Risk Index table adapted from IEC 62443-3-2:2020 Annex B

The section above answers the rest of the research question RQ2. The FMEA and FTA has given an avenue to evaluate the threats that exists against the drone system and the risk of them occurring. The results of these analysis are used to develop a framework for secure drone operations in GNSS denied environments.

5 Framework

The last of the objectives of this research has been geared towards this chapter. The application of risk-based models and the various analysis used in this research has been done with the motive of finding the most vulnerable parts of the drone system to recommend procedures and controls to improve security.

5.1 Development of Framework

The results of the analysis that were used for the input were found to be consistent with the foundational requirements used in IEC 62443-1-1:2009 and some system requirements in IEC 62443-3-3:2019, Network and System security requirements and security levels. The foundational requirements from IEC 62443-1-1 were used as the basis of the categorization for this framework.

5.1.1 Identification and Authentication

Identification is the security phenomenon that allows systems to uniquely identify users [61] while authentication allows the system to prove the user to be who they genuinely claim to be. Users are essential components of the drone system, but other parts need to be subjected to vigorous identification and authentication mechanisms to ensure the optimum security posture. Authentication and authorization mechanisms can be in the form of inbuilt features in the operating system and firmware or come externally as biometric input plugins. The need for users to be identified and authenticated cannot be emphasized enough as compromised drone user accounts can be used somewhere else in the technology infrastructure of the user. Map sources, firmware updates, application libraries and other drone system components need to be authenticated to alleviate repudiation.

5.1.2 Use Control

Authentication and authorization to a drone system requires a need for use control consistently. The manner of manipulation of data needs to be regulated in accordance with privileges given with access. There are various states of data throughout the drone system and the requirements for the control of use varies accordingly. This was salient during the FTA, use control was identified to be necessary to prevent denial of service. The assets that are deemed critical should be properly allocated to prevent situations where they are unavailable

when needed. It was similar when evaluating escalation of privilege. Use control levels assigned to users need to be implemented efficiently to prevent the abuse of use. It was also discovered in the FMEA that use control as a cybersecurity phenomenon was abused in the failure mode, deviation from route as exploitation of external and remote services. This has made it necessary for the system to not only manage access privileges but also terminate connections after a stipulated period of inactivity. The language of programming and conventions used in development of the drone system should be agreed upon by stakeholders to enable easy recognition of malicious activities. For example, the existence of a VBScript code in a heavily cooked python and JavaScript environment is easy to flag.

5.1.3 System Integrity

This is a section of the framework that is primarily concerned with repudiation and tampering in the drone system. There are matters concerning both hardware and software components of the drone system. System integrity is required throughout the drone system considering data at rest and data in motion, hardware in a ground station or for navigation assistance and even a network component in the system at large. The 5G network is the connection type proposed in the case study for this network. The heavy use of SDN in 5G network implementation makes it easy for individual network components to be attacked. It is also necessary to consider the authenticity of broadcast control signals, fake requests, and data traffic from many devices. Devices are known to connect to the strongest node with the highest signal-to-interference-plus-noise ratio (SINR) in 5G connections and it is recommended to include randomness in the (SINR) to prevent determining the location of the drone in the network should malicious actors gain entry. Depending on the network adopted for the implementation of this drone system it is needful to evaluate it in isolation before the incorporation of drones in its operations. Another portion of the drone system that is susceptible to repudiation and needs measures for system integrity is the HNS. Most drone systems have web interfaces which make use of various dependencies and web application technologies [62]. Web security standards like OWASP top ten can be adopted to further harden the web interface and other web technologies used in the drone system. Code used for the development of the navigation software and other components of the drone system should follow secure development procedures. Lastly, it is imperative for the drone system to correctly timestamp events and transactions. This is helpful for auditing in the case of an incident and certifying the integrity of requests in the system.

5.1.4 Data Confidentiality

The type of data moving through the drone system must be classified and the severity of the impact of its disclosure must be determined. Data confidentiality measures should then be assigned equally. Backups need to be considered in the encryption process as it is an extension of the data that needs to be protected. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution, and encryption key backup in accordance with defined standards that are more specific with encryption and cryptographic implementations. Generally accepted practices and recommendations can be found in documents from NIST, ISO and IEEE [63] [64].

5.1.5 Restricted Data Flow

From the FMEA, drone feed leakage and data from information repositories were identified as some of the causes of compromised drone data. Not only restriction of file and directory permission but a restriction on data flow as well is required. The advent of SDN simplifies configuration of networks now. There is an improved use of access lists and other regulatory tools in networks where there is added allowance of wholesale and onetime push. The FTA also reveals the different components in the drone system that shows the various states of data flow. Depending on the drone system implementation, further specialized regulatory tools should be placed at vantage points of the connection to monitor and filter data flow. Firewalls, IDS and IPS systems, depending on how they are placed in the line, can be used effectively to restrict data flow. Other than the use of regulatory devices, the principle of restricting data flow can also be applied in the drone system's network architecture. The network should be divided into logical segments and the exposure for various parts evaluated accordingly. This especially addresses security threats like exploitation of remote services, external remote services and internet accessible resources that were identified in the FMEA to cause the drones to deviate from route or a total hijack. Another advantage that comes with network segmentation and restriction of data flow is efficiency of network monitoring as it becomes easier to tell what normal levels of traffic in the network system is and able to identify breach in the network when there is unusual activity. Large flow of traffic where there isn't supposed to be is an easy way of identifying intrusion.

5.1.6 Timely Response to Events

Some recommendations of timely response to events are indirectly linked to restricted data flow, system integrity and the identification and authentication segments of this framework. An ability to respond timely to a breach stem basically from the fact that it was identified early enough. This factor comes into play when placing restrictions on data flow as there are incorporations of data monitoring and filtering in play there. Measures that help in collecting and investigating evidence come under this section. When a drone is being tampered with, there should be clear channels of communication that informs the user of attempts to attack the drone. This could come in many ways from simple alerts on the controller's phone or workstation to beeps from the drone itself to indicate attempts at tampering. It is also necessary to keep accurate time in the drone system to help audit logs and investigate events. A use of an NTP server in the network or an intentional attachment as a peripheral time module to the drone could remediate the efforts of attacks in wiping tracks as they will have to get physical access to the drones and not just the network before they can alter time logs.

5.1.7 Resource Availability

The last part of the framework responds to issues that causes the drone system or some components of it to become inaccessible. The FTA identified denial of service as the main method attack method. This could be done through ransomware attacks where all system resources are encrypted, and a decryption key is released only until a ransom has been paid. There are anti-ransomware protection tools available for use in networks, but they mostly operate by creating isolated backups and snapshots of the system. Drone system data, logs and any relevant info should be backed up periodically unto an isolated system to enable a rebuild should there be a ransomware attack. The evaluation for the frequency and scope of data backed up, should be done in consideration of the logistics and resources available for the backup. Another component that was found vulnerable to DoS attacks and could be caused by voluntary and involuntary action is the drone network. The network could become unavailable for use when it becomes congested and loaded with traffic beyond the optimum bandwidth. The requirements for the kind of data to be transmitted needs to be resourced with the corresponding network bandwidth to prevent unintended network denial of service. Physical protections must be put in place to prevent sabotage of drones and other components of the drone system, primarily on the ground when the drone is not in flight and is stored in an easily

accessible space. Some protections such as locks or security screws along as making the drone packaging airtight makes it difficult for tampering.

5.2 Standards Recommendation

This section summarizes the framework details written above and lists the security recommendations as bullet points. The third research question RQ3, is answered below.

5.2.1 Identification and Authentication

- Use of MFA in identification and authentication in the drone system.
- Map sources from authorized sources only.
- Firmware updates should be signed and acquired from developer sources only for drones and peripherals.
- Application dependencies should be audited before implementation.
- Restrict number of logins attempt for drone system interfaces.
- Enforced periodic change of user account credentials for drone system.
- Prevention of password sharing and reuse in the drone system.
- Ensure password selection strength.

5.2.2 Use Control

- Assign user roles in the drone system on a need to access base only.
- Remote session connections to the drone system over encrypted channels only.
- Remote connections to the drone system should not be in perpetuity but should be terminated after a stipulated period.
- Force users to change default passwords.

5.2.3 System Integrity

- The use of tampering safe locks if a physical time module is used in the drone operation.

- An NTP server should be on a separate network if used to protect time source integrity.
- Timestamps should be checked periodically to enforce synchronization throughout the drone system.
- Communication between drone system and external networks should be over encrypted channels.
- Employ network monitoring and logging tools during drone operation.
- Back up of drone system logs on separate network.
- The developers of the system should agree on a naming convention for the development of the drone system.
- Dependencies for the web interface implementation of the navigation solution should be audited periodically.
- Input for the web interface should be validated.
- Use of bootloader solutions for secure boot.
- No hard coding of credentials in drone system.

5.2.4 Data Confidentiality

- Exception handlers should not disclose information to users of drone system.
- Error messages on user interface should not disclose details of events to users.
- The authenticating entity shouldn't provide any hint as to the reason of for the authentication failure, e.g., inadequate password characters, unknown user.
- Data collected during flight should be encrypted.
- Data should be encrypted during transmission from the drone to other points of the system.
- Cryptographic architecture for the drone system should be standardised (e.g., strong key algorithm, asymmetric encryption to enforce authentications between app, drone, and server).
- Sensitive data should be encrypted in storage.

5.2.5 Restricted Data Flow

- Privileged access management for users of the drone system.

- Network and application segregation for architecture of drone system.
- Implementation of IPS, IDS and other network regulatory tools to filter data in drone system network.
- Shutdown of unused services and network ports in the drone system.
- Regulation of types of allowed data or connections from remote point to drone network system.
- Reflex restriction mechanism for sensitive data flow should there be a network breach.

5.2.6 Timely Response to Events

- Monitoring of drone system network traffic.
- Effective notification system for drone system events.
- Notification for tampering effects on drone.

5.2.7 Resource Availability

- Redundant network architecture.
- Use of anti-ransomware solutions in the drone system network.
- Periodic backing up of drone system data.
- Network bandwidth optimization for drone system operations.
- Principle of least functionality for protocols and services in the drone network.
- Concurrent session controls per interface.

In the table below, the requirements from the standard have been grouped with attack vectors from the STRIDE model they remediate. The acronyms used represent each of the attack vectors in the STRIDE model as indicated below:

- S – Spoofing
- T – Tampering
- R – Repudiation
- I – Information Disclosure
- D – Denial of Service
- E – Escalation of Privilege.

The fourth column contains reference to similar controls from the IEC 62443-3-3 to enable further reading if there be any interest.

Ref.	Standard	STRIDE	IEC 62443-3-3 Reference
5.2.1	Identification and Authentication		
5.2.1.1	Use of MFA in identification and authentication in the drone system.	TRE	SR 1.1 RE 3
5.2.1.2	Map sources from authorized sources only.	STR	
5.2.1.3	Firmware updates should be signed and acquired from developer sources only for drones and peripherals.	STR	
5.2.1.4	Application dependencies should be audited before implementation.	TR	
5.2.1.5	Restrict number of logins attempt for drone system interfaces.	D	SR 1.11
5.2.1.6	Enforced periodic change of user account credentials for drone system.	TRID	
5.2.1.7	Prevention of password sharing and reuse in the drone system.	SRIDE	
5.2.1.8	Ensure password selection strength.	T	SR 1.7
5.2.2	Use Control		
5.2.2.1	Assign user roles in the drone system on a need to access base only.	SIE	SR 2.1 RE 2
5.2.2.2	Remote session connections to the drone system over encrypted channels only.	STRIE	
5.2.2.3	Remote connections to the drone system should not be in perpetuity but should be terminated after a stipulated period.	SRID	SR 2.6
5.2.2.4	Force users to change default passwords.	TRIE	
5.2.3	System Integrity		
5.2.3.1	The use of tampering safe locks if a physical time module is used in the drone operation.	TD	
5.2.3.2	An NTP server should be on a separate network if used to protect time source integrity.	STRD	
5.2.3.3	Timestamps should be checked periodically to enforce synchronization throughout the drone system.	STRD	
5.2.3.4	Communication between drone system and external networks should be over encrypted channels.	STRID	SR 3.1
5.2.3.5	Employ network monitoring and logging tools	STRD	

	during drone operation.		
5.2.3.6	Back up of drone system logs on separate network.	STR	
5.2.3.7	The developers of the system should agree on a naming convention for the development of the drone system.	SR	
5.2.3.8	Dependencies for the web interface implementation of the navigation solution should be audited periodically.	TR	SR 3.4
5.2.3.9	Input for the web interface should be validated.	TRIDE	SR 3.5
5.2.3.10	Use of bootloader solutions for secure boot.	TRDE	
5.2.3.11	No hard coding of credentials in drone system.	RIE	
5.2.4	Data Confidentiality		
5.2.4.1	Exception handlers should not disclose information to users of drone system.	I	SR 3.7
5.2.4.2	Error messages on user interface should not disclose details of events to users.	RI	SR 3.7
5.2.4.3	The authenticating entity shouldn't provide any hint as to the reason of for the authentication failure, e.g., inadequate password characters, unknown user.	RI	SR 3.7
5.2.4.4	Data collected during flight should be encrypted.	TRI	
5.2.4.5	Data should be encrypted during transmission from the drone to other points of the system.	STRI	SR 4.3
5.2.4.6	Cryptographic architecture for the drone system should be standardised (e.g., strong key algorithm, asymmetric encryption to enforce authentications between app, drone, and server).	STRI	
5.2.4.7	Sensitive data should be encrypted in storage.	TRI	
5.2.5	Restricted Data Flow		
5.2.5.1	Privileged access management for users of the drone system.	TRIDE	
5.2.5.2	Network and application segregation for architecture of drone system.	TRIDE	SR 5.1
5.2.5.3	Implementation of IPS, IDS and other network regulatory tools to filter data in drone system network.	STRIDE	
5.2.5.4	Shutdown of unused services and network ports in the drone system.	RIDE	
5.2.5.5	Regulation of types of allowed data or connections from remote point to drone network	STRID	SR 5.3

	system.		
5.2.5.6	Reflex restriction mechanism for sensitive data flow should there be a network breach in the drone system.	TRE	SR 5.2
5.2.6	Timely Response to Events		
5.2.6.1	Monitoring of drone system network traffic.	TR	SR 6.2
5.2.6.2	Effective notification system for drone system events.	TR	
5.2.6.3	Notification for tampering effects on drone.	TRD	
5.2.7	Resource Availability		
5.2.7.1	Redundant network architecture.	D	
5.2.7.2	Use of anti-ransomware solutions in the drone system network.	TD	SR 7.1
5.2.7.3	Periodic backing up of drone system data.	TD	SR 7.3
5.2.7.4	Network bandwidth optimization for drone system operations.	TD	SR 7.1 RE 1
5.2.7.5	Principle of least functionality for protocols and services in the drone network.	TRDE	SR 7.7
5.2.7.6	Concurrent session controls per interface in the drone system.	TRDE	

Table 10 Cybersecurity framework for drone operation in GNSS denied environment.

6 Conclusion and Further Research

This research has achieved the objectives that were declared in chapter 1 which were:

- To identify a risk/threat analysis model to be implemented for drone operation in GNSS-denied environments.
- Development and assessment of a Failure Mode and Effects Analysis and Fault Tree Analysis template for the research.
- To identify security standards and requirements that can be used for drone operation in GNSS-denied environments.

This chapter is about the conclusion of the research and avenues for further research where the ever-evolving nature of threats and attacks requires continuous innovation from academia and the cybersecurity industry.

6.1 Conclusion

After some comparative analysis, the STRIDE model was chosen as the most suitable threat analysis model that could be used to evaluate a drone system among other models like PASTA, DREAD and VAST. The consideration of other factors that comes into play for this peculiar drone system, other than the conventional system where GNSS is the main form of navigation, made the STRIDE model the most viable framework for the threat analysis. The drone system was successfully divided into units with the basis of classification being the similarity in architecture and function. This enables it to be used as a template as other types of drones may have different components but consequently perform similar functions. The division of the drone system considers the navigation solution holistically with the template being capable of use for drone systems that makes use of other navigation methods. FTA proved to be a useful tool for threat analysis where the various threats and vulnerabilities that exist against the drone system were examined. The FMEA allowed for risk analysis where a complementary evaluation of the risks posed by the threats permitted us to see the likelihood and occurrence of those threats. IEC standards 62443-3-2:2020, security risk assessment for system design, 62443-1-1:2009, Network and System Security- Terminology, concepts, and models, and 62443-3-3:2019, Network and System security requirements and security levels were found to be the most relevant standards and requirements that could be adapted for the development and evaluation of a cybersecurity framework for drone operation. The 62443-3-2 standard recommended methods for risk analysis of the drone system which was used to

analyse the system further. The conventional safety faults that are identified usually in FMEA for systems were adapted to seek out cybersecurity vulnerabilities rather. IEC 62443-1-1 provided guidelines for the initial cybersecurity risk assessment which can be used as parameters or criteria for the evaluation. As a proof of essence of the research work, the framework that was recommended for drone operation was very much in line with the classification that were recommended by 62443-1-1 for the initial risk assessment and some of the requirements of the framework developed from this research were also similar to some requirements in 62443-3-3.

6.2 Further Research

This research work is not the conclusive work for cybersecurity operations in the drone sector and thus, there is room for further research. There are other forms of navigation solutions for drones which makes use of other technologies beyond satellite based and AI assisted navigations which will require further research work beyond this framework. Furthermore, the drone industry is very agile, and this sees rapid development in the technologies used in this sector. It takes more than a year for a standard to be developed and adopted by an international standardization body and this could effectively render the standard useless or inapplicable as the modules they are intended to address could be out of use, the security issue resolved, or a new technology developed with its own ensuing cybersecurity vulnerabilities by the time the standard is published. This research work is not only relevant for UAVs but can also serve as a foundation for other forms of cybersecurity research on autonomous based navigation systems link self-driving cars and under water drones.

References

- [1] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, “Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments,” *Information Technology and Law Series*, pp. 21–45, 2016, doi: https://doi.org/10.1007/978-94-6265-132-6_2.
- [2] A. R. Hall and C. J. Coyne, “The political economy of drones,” *Defence and Peace Economics*, vol. 25, no. 5, pp. 445–460, Aug. 2013, doi: <https://doi.org/10.1080/10242694.2013.833369>.
- [3] S. P. Arteaga, L. A. M. Hernandez, G. S. Perez, A. L. S. Orozco, and L. J. G. Villalba, “Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo,” *IEEE Access*, vol. 7, pp. 51782–51789, 2019, doi: <https://doi.org/10.1109/access.2019.2911526>
- [4] “Huld’s Platform for GNSS-Free Visual Navigation,” Huld, Aug. 25, 2021. <https://huld.io/news/hulds-platform-for-gnss-free-visual-navigation/>
- [5] N. M. Rodday, R. de O. Schmidt, and A. Pras, “Exploring security vulnerabilities of unmanned aerial vehicles,” *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2016, doi: <https://doi.org/10.1109/noms.2016.7502939>.
- [6] A. K. Abed and A. Anupam, “Review of security issues in Internet of Things and artificial intelligence-driven solutions,” *SECURITY AND PRIVACY*, Nov. 2022, doi: <https://doi.org/10.1002/spy2.285>.
- [7] “Standard Specification for Design and Construction of a Small Unmanned Aircraft System (sUAS),” www.astm.org. <https://www.astm.org/Standards/F2910.htm> (accessed Oct. 1, 2022).
- [8] “Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS),” www.astm.org. <https://www.astm.org/Standards/F3002.htm> (accessed Oct. 1, 2022).
- [9] “Standard Specification for Design and Construction of a Small Unmanned Aircraft System (sUAS),” www.astm.org. <https://www.astm.org/Standards/F2910.htm> (accessed Oct. 1, 2022).
- [10] “Laadullinen tutkimus — Jyväskylän yliopiston Koppa,” koppa.jyu.fi. <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus>

- [11] P. Järvinen and A. Järvinen, “Tutkimustyön metodeista,” pp.103, Tampere: Tampereen Yliopistopaino Oy, 2004
- [12] K. Peffers et al., “The Design Science Research Process: A Model for Producing and Presenting Information Systems Research,” pp. 83–106, Jan. 2006.
- [13] P. Satia, “Drones: A History from the British Middle East,” *Humanity: An International Journal of Human Rights, Humanitarianism, and Development*, vol. 5, no. 1, pp. 1–31, 2014, doi: <https://doi.org/10.1353/hum.2014.0002>.
- [14] B. Custers, “Drones Here, There and Everywhere Introduction and Overview,” *Information Technology and Law Series*, pp. 3–20, 2016, doi: https://doi.org/10.1007/978-94-6265-132-6_1
- [15] S. Kabir, “An overview of fault tree analysis and its application in model-based dependability analysis,” *Expert Systems with Applications*, vol. 77, pp. 114–135, Jul. 2017, doi: <https://doi.org/10.1016/j.eswa.2017.01.058>.
- [16] S. Ierace, “The basics of FMEA, by Robin E. McDermott, Raymond J. Mikulak and Michael R. Beauregard,” *Production Planning & Control*, vol. 21, no. 1, pp. 99–99, Jan. 2010, doi: <https://doi.org/10.1080/09537280903372119>.
- [17] M. P. Ananda, Harris Conan Bernstein, K. E. Cunningham, W. A. Feess, and E. G. Stroud, “Global Positioning System (GPS) autonomous navigation,” Mar. 1990, doi: <https://doi.org/10.1109/plans.1990.66220>.
- [18] P J G Teunissen, O. Montenbruck, and G. W. Hein, *Springer handbook of global navigation satellite systems*. Cham, Switzerland: Springer, 2017.
- [19] A. Santra, S. Mahato, S. Dan, and A. Bose, “Precision of satellite-based navigation position solution: A review using NavIC data,” *Journal of Information and Optimization Sciences*, vol. 40, no. 8, pp. 1683–1691, Nov. 2019, doi: <https://doi.org/10.1080/02522667.2019.1703264>.
- [20] M. Kishimoto et al., “QZSS System Design and its Performance,” pp. 405–410, Jan. 2007.
- [21] Jens Leitloff and F. M. Riese, “Examples for CNN training and classification on Sentinel-2 data,” Jan. 2018, doi: <https://doi.org/10.5281/zenodo.3268451>.
- [22] R. Klette, *Concise Computer Vision*. 2014. doi: <https://doi.org/10.1007/978-1-4471-6320-6>.
- [23] Iso.org, 2023. <https://www.iso.org/obp/ui/#iso:std:iso:21384:-3:ed-1:v1:en>. (accessed Jan. 5, 2023).

- [24] J. Valente and A. A. Cardenas, "Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family," Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Nov. 2017, doi: <https://doi.org/10.1145/3139937.3139943>.
- [25] G. Choudhary, V. Sharma, T. Gupta, Ji Yoon Kim, and I. You, "Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives," Aug. 2018, doi: <https://doi.org/10.48550/arxiv.1808.00203>.
- [26] R. Majeed, N. A. Abdullah, M. F. Mushtaq, and R. Kazmi, "Drone Security: Issues and Challenges," International Journal of Advanced Computer Science and Applications, vol. 12, no. 5, 2021, doi: <https://doi.org/10.14569/ijacsa.2021.0120584>.
- [27] R. Altawy and A. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones," ACM Transactions on Cyber-Physical Systems, vol. 1, no. 2, pp. 1–25, Nov. 2016, doi: <https://doi.org/10.1145/3001836>.
- [28] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," Ad Hoc Networks, vol. 133, p. 102894, Aug. 2022, doi: <https://doi.org/10.1016/j.adhoc.2022.102894>.
- [29] J. Ni, X. Lin, K. Zhang, and X. Shen, "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Sep. 2016, doi: <https://doi.org/10.1109/vtcfall.2016.7881177>.
- [30] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 6903–6916, Jul. 2019, doi: <https://doi.org/10.1109/tvt.2019.2911672>.
- [31] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles," IEEE Access, vol. 8, pp. 43711–43724, 2020, doi: <https://doi.org/10.1109/access.2020.2977817>.
- [32] M. P. Arthur, "Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS," 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Aug. 2019, doi: <https://doi.org/10.1109/cits.2019.8862148>.

- [33] Helka-Liina Maattanen, “3GPP Standardization for Cellular-Supported UAVs,” Dec. 2020, doi: <https://doi.org/10.1002/9781119575795.ch6>.
- [34] 3gpp.org, 2017.
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3234> (accessed Jan. 22, 2023).
- [35] 3gpp.org, 2018.
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3527> (accessed Jan. 22, 2023).
- [36] 3gpp.org, 2018.
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3575> (accessed Jan. 22, 2023).
- [37] “Committee F38 Scope,” www.astm.org.
<https://www.astm.org/COMMIT/SCOPES/F38.htm> (accessed Feb. 13, 2023)..
- [38] “Committee F38 Subcommittees,” www.astm.org.
<https://www.astm.org/COMMIT/SUBCOMMIT/F3801.htm>. (accessed Feb. 13, 2023).
- [39] “Standard Practice for UAS Registration and Marking (Excluding Small Unmanned Aircraft Systems),” www.astm.org.
<https://www.astm.org/Standards/F2851.htm> (accessed Feb. 13, 2023).
- [40] “Standard Specification for Design and Construction of a Small Unmanned Aircraft System (sUAS),” www.astm.org. <https://www.astm.org/Standards/F2910.htm>.
- [41] “Standard Specification for Design, Construction, and Verification of Lightweight Unmanned Aircraft Systems (UAS),” www.astm.org.
<https://www.astm.org/Standards/F3298.htm> (accessed Feb. 13, 2023).
- [42] “Standard Specification for Design of the Command-and-Control System for Small Unmanned Aircraft Systems (sUAS),” www.astm.org.
<https://www.astm.org/Standards/F3002.htm>
- [43] “WK62669 New Test Method for Detect and Avoid,” www.astm.org.
<https://www.astm.org/DATABASE.CART/WORKITEMS/WK62669.htm> (accessed Feb. 13, 2023).
- [44] “ISO/TC 20/SC 16 - Unmanned aircraft systems,” ISO.
<https://www.iso.org/committee/5336224.html>.
- [45] Iso.org, 2023. <https://www.iso.org/obp/ui/#iso:std:iso:21384:-4:ed-1:v1:en>. (accessed Feb. 13, 2023).

- [46] Iso.org, 2023. <https://www.iso.org/obp/ui/#iso:std:iso:21895:ed-1:v1:en>. (accessed Feb. 13, 2023).
- [47] Iso.org, 2023. <https://www.iso.org/obp/ui/#iso:std:iso:tr:23629:-1:ed-1:v1:en> (accessed Feb. 13, 2023).
- [48] Iso.org, 2023. <https://www.iso.org/obp/ui/#iso:std:iso:23665:ed-1:v1:en> (accessed Feb. 13, 2023)
- [49] “Proving operations of drones with initial UAS traffic management (PODIUM),” www.eurocontrol.int. <https://www.eurocontrol.int/project/proving-operations-drones-initial-uas-traffic-management> (accessed Feb. 13, 2023).
- [50] “Unmanned aircraft systems,” www.eurocontrol.int, Apr. 19, 2023. <https://www.eurocontrol.int/unmanned-aircraft-systems> (accessed Feb. 13, 2023)..
- [51] Z. Renyu, S. C. Kiat, W. Kai, and Z. Heng, “Spoofing Attack of Drone,” 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Dec. 2018, doi: <https://doi.org/10.1109/compcomm.2018.8780865>
- [52] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, “Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study,” 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Jan. 2018, doi: <https://doi.org/10.1109/vlsid.2018.97>.
- [53] F. Salamh, U. Karabiyik, and M. Rogers, “A Constructive DIREST Security Threat Modeling for Drone as a Service,” *The Journal of Digital Forensics, Security and Law*, 2021, doi: <https://doi.org/10.15394/jdfsl.2021.1695>.
- [54] R. L. Security, “Analyzing Data Use by the DJI Mimo App,” *River Loop Security*, May 12, 2020. https://www.riverloopsecurity.com/blog/2020/05/dji_mimo/ (accessed Mar. 13, 2023).
- [55] J. I. Rios, J. Jung, and M. A. Johnson, “Non-Repudiation for Drone-Related Data,” *NASA STI Program Report Series*, Nov. 2022.
- [56] I. Astaburuaga, A. Lombardi, Brian La Torre, C. Hughes, and S. Sengupta, “Vulnerability Analysis of AR.Drone 2.0, an Embedded Linux System,” Jan. 2019, doi: <https://doi.org/10.1109/ccwc.2019.8666464>.
- [57] Jong Ho Won, S.-H. Seo, and E. Bertino, “A Secure Communication Protocol for Drones and Smart Objects,” *Computer and Communications Security*, Apr. 2015, doi: <https://doi.org/10.1145/2714576.2714616>).

- [58] D. Eugenio, "DJI Drone Vulnerability," Check Point Research, Nov. 08, 2018. <https://research.checkpoint.com/2018/dji-drone-vulnerability> (accessed Apr. 13, 2023).
- [59] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," IEEE Xplore, Jun. 01, 2019. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8802852> (accessed Jan. 15, 2023).
- [60] Fekadu Yihunie, A. Singh, and S. Bhatia, "Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles," pp. 701–710, Oct. 2019, doi: https://doi.org/10.1007/978-981-13-8406-6_66
- [61] C. J. Brooks, C. Grow, P. Craig, and D. Short, *Cybersecurity Essentials*. John Wiley & Sons, 2018.
- [62] N. Yang, L. Wang, G. Geraci, M. ElKashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015, doi: <https://doi.org/10.1109/mcom.2015.7081071>.
- [63] R. M. Aria and Yogi Andriawan, "Implementation of Cryptography Module Security Certification Based on SNI ISO/IEC 19790:2012 - Security Requirements for Cryptography Module," Aug. 2019, doi: <https://doi.org/10.1109/isitia.2019.8937280>
- [64] N.I.S.T., "Security Requirements for Cryptographic Modules," csrc.nist.gov, Dec. 03, 2002. <https://csrc.nist.gov/publications/detail/fips/140/2/final> (accessed Apr. 13, 2023)