UNIVERSIDADE ESTADUAL DE MARINGÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Manna SafeloD: A Framework and Roadmap for Secure Design in the Internet of Drones

Luiz Henrique Custódio Mendes Marques

Tese de Doutorado do Programa de Pós-Graduação em Ciência da Computação (PCC–UEM)

Luiz Henrique Custódio Mendes Marques

Manna SafeIoD: A Framework and Roadmap for Secure Design in the Internet of Drones

Thesis submitted to the State University of Maringá (UEM) – in accordance with the requirements of the Computer Science Graduate Program, for the degree of Doctor in Computer Science. *FINAL VERSION*

Concentration Area: Computer Science

Advisor: Profa. Dra. Linnyer Beatrys Ruiz Aylon

UEM – Maringá
March 2026

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá - PR, Brasil)

Marques, Luiz Henrique Custódio Mendes

M357m Manna SafeIoD : a framework and roadmap for secure design in the internet of drones / Luiz Henrique Custódio Mendes Marques. -- Maringá, PR, 2026.
108 f. : il. color., figs., tabs.

Orientadora: Profa. Dra. Linnyer Beatrys Ruiz Aylon.
Tese (doutorado) - Universidade Estadual de Maringá, Centro de Tecnologia, Departamento de Informática, Programa de Pós-Graduação em Ciência da Computação, 2026.

1. Segurança em drones. 2. Design seguro. 3. Segurança da informação. I. Aylon, Linnyer Beatrys Ruiz , orient. II. Universidade Estadual de Maringá. Centro de Tecnologia. Departamento de Informática. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDD 23.ed. 004

Marinalva Aparecida Spolon Almeida - 9/1094

Luiz Henrique Custódio Mendes Marques

Manna SafeIoD: A Framework and Roadmap for Secure Design in the Internet of Drones

Tese apresentada à Universidade Estadual de Maringá (UEM), como parte dos requisitos para obtenção do título de Doutor em Ciência da Computação. *VERSÃO FINAL*

Área de Concentração: Ciência da Computação

Orientador: Profa. Dra. Linnyer Beatrys Ruiz Aylon

UEM – Maringá
Março de 2026

FOLHA DE APROVAÇÃO

Luiz Henrique Custódio Mendes Marques

Manna SafeIoD: A Framework and Roadmap for Secure Design in the Internet of Drones

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Departamento de Informática, do Centro de Tecnologia da Universidade Estadual de Maringá, como parte dos requisitos para obtenção do título de Doutor.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br LINNYER BEATRYS RUIZ AYLON
Data: 04/03/2026 21:32:45-0300
Verifique em https://validar.iti.gov.br

Profª. Drª.Linnyer Beatrys Ruiz Aylon
Universidade Estadual de Maringá – UEM (Orientadora-Presidente)

Documento assinado digitalmente
gov.br RODRIGO CALVO
Data: 20/03/2026 16:06:22-0300
Verifique em https://validar.iti.gov.br

Prof.Dr.Rodrigo Calvo
Universidade Estadual de Maringá – UEM (Membro Interno)

Documento assinado digitalmente
gov.br RODRIGO CLEMENTE THOM DE SOUZA
Data: 20/03/2026 16:31:15-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Rodrigo Clemente Thom de Souza
Universidade Estadual de Maringá – UEM (Membro Interno)

Documento assinado digitalmente
gov.br JULIANA VERGA SHIRABAYASHI
Data: 20/03/2026 15:36:59-0300
Verifique em https://validar.iti.gov.br

Profª. Drª. Juliana Verga Shirabayashi
Universidade Federal do Paraná(Membro Externo)

Documento assinado digitalmente
gov.br CHRISTIANE MARIE SCHWEITZER
Data: 04/03/2026 22:57:06-0300
Verifique em https://validar.iti.gov.br

Pro r
FEIS/UNESP(Membro Externo)

Aprovada em: 20 de fevereiro de 2026.
https://meet.google.com/nbn-fsxd-ppj

Este trabalho é dedicado às crianças adultas que,
quando pequenas, sonharam em se tornar cientistas.
Em especial, aos pesquisadores da Universidade
Estadual de Maringá e ao Manna_Team.

ACKNOWLEDGEMENTS

Eu ainda me lembro do dia em que peguei emprestado os últimos 100 reais do meu velho avô, o Seu João, para me inscrever no programa de mestrado. Naquele momento, eu não tinha um *"puto"* no bolso, mas tinha um sonho. E ali começava essa jornada.

Mestrado concluído, pensei: por que não um doutorado? Para muitos, uma escolha ousada; para um menino de família pobre, vindo de escola pública e com poucas perspectivas, talvez uma loucura. Mas segui.

Talvez, de fato, não houvesse muitas certezas no meu caminho. No entanto, lembro-me bem de uma professora do colégio que, ao ouvir meu sonho de entrar na UEM, disse com descrença: *"Você, Luiz? Eu duvido!"* Pois bem, professora, não só entrei, como agora me torno doutor por essa mesma instituição. Agradeço especialmente a você, porque às vezes o combustível da superação vem daquilo que tentam nos negar.

Dedico este trabalho à minha mãe, Sônia Maria Custódio. Mulher, guerreira, inspiração. Parafraseando os Racionais MC's:

"Daria um filme, uma negra e uma criança nos braços,
Solitária na floresta de concreto e aço."

Mãe, seu filho será **DOUTOR**. Então, por favor, grite comigo: *"Rick, você conseguiu!"* A senhora não tem ideia como é importante para mim, como foi meu esteio por tantas vezes. Eu sempre soube que, se desse tudo errado, você estaria ali para me ouvir, consolar, me dar o colo de mãe. Também, caso tudo desse certo, comemoraríamos juntos. Enfim, mãe, essa vitória também é sua. Cheguei, sou doutor, muito embora a senhora tenha concluído no máximo o segundo ano do ensino fundamental. Mas a sua sabedoria nunca precisou de diplomas para ser grandiosa. Obrigado por insistir na minha existência, por me fazer forte, por me fazer homem. Amo a senhora, mesmo do meu jeito estranho, que a senhora nunca reclamou. Assim, dedico todo este trabalho a seu esforço, à sua vida, Sônia Maria Custódio.

Ao meu avô, Seu João, que com 100 reais e um coração gigante ajudou a plantar essa semente. Mas dele também veio o maior ensinamento de todos — a fé. Foi ele quem me mostrou que a força verdadeira vem de dentro, e que a oração, quando sincera, move montanhas. *In memoriam*, vô. Obrigado por tudo. O seu gesto simples e cheio de amor foi o primeiro tijolo desta casa chamada doutorado. Onde quer que o senhor esteja, espero que esteja sorrindo. Esta vitória também é sua.

Agradeço também à mulher mais linda que já cruzou meu caminho, minha companheira de risos, conquistas e incertezas: Claudia Ananias. Pichuca, tu chegou como quem não queria nada, e de repente já era tudo. Obrigado por acreditar em mim, por ganhar de mim em todos os jogos, por segurar minha mão quando tudo parecia desabar, e por me lembrar todos os dias que eu posso — e devo — continuar.

Aos meus companheiros do Doutorado que fizeram parte dessa caminhada: Hugo Sanches, Jeffer, Tiago Madrigar — cada conversa, cada café, cada churrasco, cada meme compartilhado, cada apoio fizeram diferença. Obrigado por estarem comigo.

Agradeço, de forma especial, à minha orientadora, Profª Draª Linnyer. Uma mulher inspiradora, que me acolheu com alegria, confiança e uma energia contagiante. Professora, sua paixão pela pesquisa e sua forma humana de liderar me marcaram profundamente. Obrigado por abrir portas, por ensinar muito além da técnica — por mostrar que é possível ser referência e, ao mesmo tempo, ser leve, ser gente. O MannaTeam foi mais que um grupo de pesquisa; foi um lugar onde cresci como profissional e como ser humano.

Aos meus amigos Lucas Henrique, Matheus Augusto, Guilherme Volante — irmãos que eu não tive, e que Deus colocou no meu caminho. Obrigado pelo companheirismo, apoio e amizade incondicional. Amo vocês!

E, por fim — mas na verdade, acima de tudo —, agradeço a Deus. Porque em tantos momentos eu quis desistir. Em tantos outros, só me restava fechar os olhos e pedir forças. E sempre vinha. No silêncio da madrugada, no improvável que dava certo, no conforto que surgia quando tudo doía. Eu não seria nada sem essa fé que me sustentou quando as certezas acabavam. Obrigado, meu Deus, por não me abandonar. Por me lembrar que meu valor não está nos títulos, mas no amor com que compartilhamos com os irmãos.

Por fim, encerro com os versos de Negro Drama:
"Mais um filho pardo sem pai?
...
No meio de vocês ele é o mais esperto,
Ginga e fala gíria, gíria não, dialeto."

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES).

“Pele parda e ouço funk
E de onde vem os diamante? Da lama!
Valeu mãe, negro drama.”
(Racionais Mcs)

RESUMO

MARQUES. **Manna SafeIoD: A Framework and Roadmap for Secure Design in the Internet of Drones**. 2026. 108 p. Tese (Doutorado em Ciência da Computação) – Universidade Estadual de Maringá, Maringá – PR, 2026.

Com a crescente adoção de tecnologias avançadas de drones em diversos campos, a Internet de Drones (IoD) emergiu como um novo paradigma de mobilidade, particularmente aprimorando os Sistemas de Transporte Inteligentes (ITS) em ambientes urbanos. Apesar de seu potencial significativo, a IoD enfrenta desafios substanciais devido a restrições inerentes de recursos, como poder computacional limitado e capacidade energética reduzida, que dificultam a implementação de soluções robustas de cibersegurança. Essas limitações expõem as redes IoD a várias vulnerabilidades de segurança e ameaças à privacidade, necessitando uma análise exaustiva e compreensão desses riscos.

Neste sentido, apresentamos o SafeIoD, um framework de segurança abrangente projetado para estabelecer procedimentos padronizados para identificação proativa de riscos em dispositivos da Internet de Drones (IoD). Ele envolve etapas sequenciais para determinar a confiabilidade dos dispositivos submetidos a essa certificação. Portanto, o SafeIoD busca garantir um nível básico de segurança antes da implementação em um cenário real, onde os dispositivos de rede são avaliados em relação aos requisitos de segurança específicos. A validação por meio de testes experimentais com 15 participantes em quatro cenários de implantação de IoD e um caso de certificação militar demonstrou a eficácia do framework: a ferramenta alcançou uma taxa de satisfação do usuário de 73%, identificou com sucesso uma média de 3,0 requisitos de segurança por dispositivo e forneceu recomendações específicas de algoritmos criptográficos leves para 62,2% dos requisitos elicitados. Em uma simulação de cenário militar tático, o framework previu com precisão os padrões de propagação de risco, com simulações de rede COOJA confirmando que a implementação dos protocolos recomendados pelo framework reduziu a propagação bem-sucedida de ataques de 60% para menos de 5% da rede.

Palavras-chave: Internet dos Drones, segurança de UAV, certificação de ciber-segurança, Modelagem de ameaças.

ABSTRACT

MARQUES. **Manna SafeIoD: A Framework and Roadmap for Secure Design in the Internet of Drones**. 2026. 108 p. Tese (Doutorado em Ciência da Computação) – Universidade Estadual de Maringá, Maringá – PR, 2026.

With the increasing adoption of advanced drone technologies across diverse fields, the Internet of Drones (IoD) has emerged as a novel mobility paradigm, particularly enhancing Intelligent Transportation Systems (ITS) in urban environments. Despite its significant potential, the IoD faces substantial challenges due to inherent resource constraints such as limited computational power and energy capacity, which hinder the implementation of robust cybersecurity solutions. These limitations expose IoD networks to various security vulnerabilities and privacy threats, necessitating an exhaustive analysis and understanding of these risks. In this thesis we introduce SafeIoD, a comprehensive security framework designed to establish standardized procedures for proactive risk identification in Internet of Drones (IoD) devices. It involves sequential steps to determine the trustworthiness of devices subjected to this certification. Therefore, SafeIoD seeks to ensure a basic security level before implementation in a real scenario, where the network devices are evaluated in regards to the specific security requirements. Validation through experimental testing with 15 participants across four IoD deployment scenarios and one military certification case demonstrated the framework's effectiveness: the tool achieved 73% user satisfaction rating, successfully identified an average of 3.0 security requirements per device, and provided specific lightweight cryptographic algorithm recommendations for 62.2% of elicited requirements. In a tactical military scenario simulation, the framework accurately predicted risk propagation patterns, with COOJA network simulations confirming that implementation of framework-recommended protocols reduced successful attack propagation from 60% to below 5% of the network.

Keywords: Internet of Drones, UAV Security, Cybersecurity Certification, Threat Modeling, Blockchain Monitoring, Secure-by-Design.

LIST OF FIGURES

Figure 1 – Thesis Organization 21
Figure 2 – Certification Characteristics according to ENISA 31
Figure 3 – Threat Modeling IoD System 39
Figure 4 – Work-flow of the proposed methodology 43
Figure 5 – Maturity Levels 50
Figure 6 – Requirements Activities 52
Figure 7 – BPMN of the proposed framework 58
Figure 8 – High-level architecture of the SafeIoD. 59
Figure 9 – SafeIoD CLI 60
Figure 10 – Manna SafeIoD module interdependency graph. Solid lines indicate mandatory sequential flows; the dashed upper path represents the standalone requirements generation capability, while the lower dashed path illustrates the continuous monitoring feedback loop 71
Figure 11 – Military Case Study 74
Figure 12 – Attack Propagation Comparison 80
Figure 13 – Manna SafeIoD CLI Output - Phases 1-2: Context Establishment and Threat Identification for Drone-i military certification. 80
Figure 14 – Manna SafeIoD CLI Output - Security Requirements, Maturity Assessment, and COOJA Validation. 80

LIST OF TABLES

Table 1 – Comparative analysis of IoD attributes versus traditional mobile networks. (Adapted from Svaigen *et al.* (2023)) . . . 25
Table 2 – Comparative Analysis of Cybersecurity Certification Frameworks Against IoD Requirements . . . 35
Table 3 – Fundamental Entities in IoD Attack Vectors . . . 36
Table 4 – Threat Categories in IoD Systems . . . 38
Table 5 – Workflow Process for Security Requirements in IoD Systems . . . 54
Table 6 – Standard security requirements . . . 57
Table 7 – Mission Profile Input Schema . . . 61
Table 8 – Device Specification Input Schema . . . 62
Table 9 – Threat Entry Schema . . . 63
Table 10 – Sample Threat Database Entries . . . 64
Table 11 – Security Control Schema . . . 67
Table 12 – Sample Security Control Entries . . . 67
Table 13 – Module Configuration for Resource-Constrained Agricultural UAV . . . 69
Table 14 – Module Configuration for Urban Delivery Fleet . . . 70
Table 15 – Module Configuration for Military Tactical ISR . . . 70
Table 16 – Valid Module Configurations and Use Cases . . . 71
Table 17 – Performance evaluation form as completed by subjects. (Tests 1-4) . . . 75
Table 18 – Security Requirements and Algorithm Selection for IoD Devices (Tests 1-4) . . . 77
Table 19 – Security Requirements for Military Tactical ISR Deployment (Test 5) . . . 78
Table 20 – COOJA Simulation Parameters for Tactical Scenario . . . 79
Table 21 – Descriptive statistics for participant evaluation metrics ($n = 15$). . . . 81
Table 22 – Summary of inferential statistical tests ($n = 15$, $\alpha = 0.05$). . . . 82
Table 23 – Weight assignment rationale for IoD-weighted coverage index. . . . 84
Table 24 – Quantitative multi-criteria comparison of certification frameworks. . . . 84
Table 25 – Functional gap analysis: unsupported criteria per framework. . . . 85

CONTENTS

1 INTRODUCTION . . . 16
1.1 Problem Statement . . . 17
1.2 Goals and Contributions . . . 19
1.3 Justification . . . 20
1.4 Justification . . . 20
1.5 Thesis Organization . . . 20

2 BACKGROUND . . . 22
2.1 Drones . . . 22
2.2 Internet of Drones . . . 24
2.3 Domain-Specific Implementations and Market Trends . . . 27

3 RELATED WORK . . . 29
3.1 Security Certifications . . . 30
3.1.1 COMMON CRITERIA . . . *31*
3.1.2 ICSA Labs . . . *32*
3.1.3 ARMOUR . . . *32*
3.1.4 DSPSMA . . . *33*
3.1.5 SORA . . . *33*
3.1.6 GCACS-IoD . . . *34*
3.1.7 Other Certification Processes . . . *35*

4 IOD THREAT MODELLING . . . 36
4.1 Threat Actors . . . 37
4.2 Threat Classification . . . 37
4.3 Cyber Attack Taxonomy . . . 39

5 MANNA SAFEIOD . . . 42
5.1 Framework Definition . . . 43
5.1.1 Context Establishment . . . *44*
5.1.2 Risk Assessment . . . *45*
5.1.3 Maturity Report . . . *50*
5.1.4 Security Requirements . . . *52*
5.1.5 Certification Monitoring & review . . . *56*

5.2 Framework Implementation . . . 59
5.2.1 Establishing Context (User Interface) . . . *60*
5.2.2 Risk Calculator . . . *63*
5.2.3 Security Requirements Generator . . . *65*
5.2.4 Output interface . . . *68*
5.2.5 System components . . . *68*

6 EVALUATION . . . 72
6.1 Experimental Setup . . . 72
6.1.1 Software Implementation Test Scenario for Drone Firmware . . . *73*
6.1.2 Software Implementation Test Scenario for Cloud application based for ZSP integration . . . *73*
6.1.3 Hardware Implementation Test Scenario for UAV Security Modules *73*
6.1.4 Hardware Implementation Test Scenario for Reconfigurable UAV Hardware . . . *73*
6.1.5 Certification process Test Scenario with military application . . . *74*
6.2 Results Overview . . . 75
6.2.1 Statistical Analysis of Participant Evaluation . . . *81*
6.2.1.1 Descriptive Statistics . . . *81*
6.2.1.2 Confidence Intervals . . . *81*
6.2.1.3 Correlation Analysis . . . *81*
6.2.1.4 Summary of Statistical Findings . . . *82*
6.2.2 Multi-Criteria Comparative Analysis of Certification Frameworks . . *82*
6.2.2.1 Scoring Methodology . . . *82*
6.2.2.2 Coverage Results . . . *84*
6.2.2.3 Gap Analysis . . . *85*
6.3 Research Limitations . . . 86
6.3.1 Simulation and Experimental Validation Constraints . . . *86*
6.3.2 Participant Study . . . *86*
6.3.3 Comparative Analysis Constraints . . . *86*
6.3.4 Framework Scope Boundaries . . . *87*

7 FUTURE WORKS . . . 88
7.1 Simplicity of Use . . . 88
7.2 Decision Accuracy and Requirement Selection Validation . . . 89
7.3 Algorithm Database Limitations and Design Rationale . . . 90
7.4 Secure-by-design Process . . . 90
7.5 Privacy-by-design Issues . . . 91
7.6 Monitoring System . . . 91

8 CONCLUSION 93

BIBLIOGRAPHY 95

APPENDIX A ARTICLES 107

CHAPTER

1

INTRODUCTION

The rapid advancement of unmanned aerial vehicle (UAV) technology has facilitated the emergence of the Internet of Drones (IoD), a promising mobility paradigm significantly contributing to the advancement of Intelligent Transportation Systems (ITS), particularly within urban environments (GHARIBI; BOUTABA; WASLANDER, 2016a; OZMEN; BEHNIA; YAVUZ, 2019). The IoD constitutes a layered network architecture orchestrating drone operations in regulated airspace, integrating UAVs, Zone Service Providers (ZSPs), regulatory bodies, and wireless communication infrastructures (BATTH; NAYYAR; NAGPAL, 2018). This architecture supports critical drone-to-drone (D2D) and drone-to-infrastructure (D2I) communication, utilizing advanced communication technologies such as Automatic Dependent Surveillance—Broadcast (ADS-B), cellular networks, and specialized low-altitude air traffic management protocols.

The utilization of these platforms has experienced exponential growth annually, encompassing applications in transportation logistics, artistic and entertainment domains, surveillance operations, precision agriculture, and numerous other sectors. According to Gartner's market intelligence analysis, the commercial drone sector is projected to achieve revenues of $129 billion by 2026, underscoring the increasingly critical role of unmanned systems in the contemporary technological ecosystem.

Security is one of the significant challenges to be addressed in this unique scenario to avoid attacks from different sources (CHOUDHARY *et al.*, 2018a; GHARIBI; BOUTABA; WASLANDER, 2016b; LIN *et al.*, 2018a). Since civilian drones are in the airspace, a range of attack methods can be more harmful than grounded mobile networks, as extensively discussed in this work. For instance, drone vandalism can harm a person's life, where the damaged drone may fall on a person's head. In the same way, jamming can isolate a group of drones from the entire network, hindering an ITS service such as traffic monitoring. Furthermore, airspace is susceptible to novel attacks which are unprecedented on grounded networks.

The primary vulnerability vector in IoD architectures resides in wireless communication

infrastructure which, by nature, is inherently prone to transmission errors, communication losses, and service interruptions. These failure modes are extensively documented in the literature on MANETs (Mobile Ad-Hoc Networks) and FANETs (Flying Ad-Hoc Networks) (BOR-YALINIZ *et al.*, 2019). The high mobility characteristics of drone platforms, as emphasized by (LIN *et al.*, 2018b), significantly amplify scenario complexity, given that fleet coordination and data exchange must maintain extremely precise operational parameters. Additional critical considerations include energy consumption constraints and computational resource limitations. Drone platforms may lack sufficient computational resources to implement sophisticated cryptographic protocols, as demonstrated by studies such as (BHUNIA; SENGUPTA, 2017; ZHANG *et al.*, 2019).

Consequently, information security and IoD device protection can be considered the most valuable assets for organizations, highlighting the necessity for methodologies capable of ensuring the security of such assets, including user information, trajectory data, and sensitive organizational intelligence.

Concurrently, researchers and information security professionals have sought to develop techniques for detecting and mitigating various attack types. These techniques range across monitoring mechanisms, control policies, prevention methodologies, and detection systems. Within this context, the necessity emerges for developing a methodology for evaluation, certification, and monitoring of IoD architectural devices, capable of measuring, identifying, and analyzing the security posture of processes, controls, assets, systems, and networks. The Manna SafeIoD Framework seeks to address an existing gap in the real-world implementation of the IoD concept, specifically answering the fundamental question: “How can we ensure that devices possess the minimum security level required to operate within different domains without compromising human safety or the architectural integrity itself?” This response is essential for secure implementation. Along this research trajectory, the present work proposes a systematic methodology for device risk analysis as well as the criteria and necessary steps for implementing certification entities that seek to evaluate and authorize devices for real-world deployment.

1.1 Problem Statement

There exists widespread consensus within the academic community that cyberattacks constitute a serious threat to IoD architectural implementation, with numerous proposals addressing this challenge (YAHUZA *et al.*, 2021). However, it is not uncommon for evaluations of different threats to rely more heavily on inferential analysis rather than empirical validation of their severity, based on concrete evidence demonstrating actual damages and impacts. Typically, vulnerability assessment methodologies fail to consider the attack environment or adversarial perspectives. Consequently, obtained results are, at minimum, incomplete, necessitating more precise viewpoints for such evaluations.

The lack of methodological rigor in current literature-based methodologies can be ad-

dressed through the development of cybersecurity certifications for IoD systems. Certifications aim to define evaluation methods for information system components to establish criteria for measuring whether specific devices meet minimum security requirement sets for market deployment authorization. Additionally, these frameworks establish clear monitoring processes to guarantee compliance with established requirements based on certified scenarios and certification entities. Ref. The NIST SP 800-37 standard defines

cybersecurity certification as a comprehensive assessment of technical security operations and controls within an information system to determine correct implementation of security mechanisms meeting minimum requirements. An exemplary requirement includes ensuring that two devices can perform mutual authentication for message exchange (ERNST; MARTIN, 2010).

Although security standardization and certification are fundamental for guaranteeing IoD device protection, the current literature remains deficient in works addressing this specific thematic area. However, the utilization of certifications for IoT devices can serve as an initial reference framework. In recent years, IoT device security has been extensively explored, encompassing diverse technologies ranging from physical devices to Internet infrastructure. As defined by ISO/IEC 20924:2024, the IoT paradigm aims for connectivity among any physical objects that can be instrumented with sensors and actuators, connected primarily through wireless technologies.

The increasing utilization of IoT devices has led to a need to develop security certifications which promote a trustworthy digital ecosystem. The Security Compliance Framework (MOHAMED; HAMAD, 2020) provides best practices for device evaluation processes considering the complete data lifecycle. Similarly, the IoT Trust Framework (FAGAN *et al.*, 2020) describes principal strategic aspects for defining security levels associated with data in IoT devices. Beyond the cited works, governmental initiatives for creating methodologies and certifications can be identified: in the United States, the NIST (National Institute of Standards and Technology) (CYBERSECURITY, 2018) describes cybersecurity risk management processes. In the European Union, ENISA (European Union Agency for Network and Information Security) (KOHLER, 2020a) seeks to establish and coordinate the creation of cybersecurity certification frameworks. In Japan, JISEC (Japan Information Technology Security Evaluation and Certification Scheme) (BOX; HDD; EAL, 2010) aims to evaluate security system functionalities in general IT products.

Despite generic certifications such as JISEC and the IoT Trust Framework for IoT presenting high maturity levels, the presented methods and procedures fail to consider various particular aspects of IoD systems. Therefore, it becomes necessary to define specific certification frameworks tailored to this architectural paradigm.

1.2 Goals and Contributions

The need to define a secure design framework for the IoD ecosystem is crucial from both civilian and military points of view. Drones in an IoD network can operate in hostile environments and must therefore be protected from possible threats. Furthermore, devices need to be classified concerning the level of the security system, in order to operate in civil and military missions.

Given the context, motivations, and nature of the research problem, this study's main objective is to propose the development of a homogeneous and global framework for carrying out secure design processes, enabling the analysis and release of IoD devices for use in a real environment.

The Manna SafeIoD is a security framework designed to facilitate the development and implementation of secure IoD devices. This framework provides essential technical guidance to help industry stakeholders build robust and secure IoD environments. The proposed framework is organized into four core modules, each responsible for delivering a specific set of security functions:

1. A threat assessment methodology that accounts for operational context variability and environmental factors specific to IoD deployments.
2. A novel and clear definition of procedures for device risk analysis.
3. Security control establishment and certificate validation processes.
4. A CLI-based tool that provides a simple interface for interacting with the framework.

Beyond the framework implementation, this work provides the following scientific contributions:

- Mathematical Formalism and Threat Modeling: We introduce a formal mathematical representation of IoD attacks, clearly defining the entities involved, attack behaviors, and related security aspects. This approach establishes a general model applicable to various attack scenarios, supporting rigorous analysis concerning model correctness, computational complexity, and systematic vulnerability assessments.
- Integrated Taxonomy of Attacks: We propose a unified attack taxonomy based on three critical dimensions: the primary threat source, the attack behavior, and associated privacy and security issues. This taxonomy comprehensively categorizes threats into Communication Threats, Environment Threats, and Drone Threats, providing a foundational framework for future research and threat mitigation strategies.

To systematically evaluate the effectiveness of the proposed framework, this research addresses the following questions:

- **RQ1 (Security Requirements Elicitation):** Can the Manna SafeIoD framework effectively generate context-appropriate security requirements for heterogeneous IoD components, and to what extent can it recommend suitable lightweight implementations?
- **RQ2 (Risk Assessment Validity):** Does the risk propagation model accurately predict attack propagation patterns in IoD network topologies, and do the computed risk scores correlate with observed security outcomes?
- **RQ3 (Cross-Context Applicability):** Can the framework adapt its certification workflow to diverse operational contexts—spanning resource-constrained civilian devices to mission-critical military deployments—while maintaining acceptable usability for practitioners with varying security expertise?

1.3 Justification

1.4 Justification

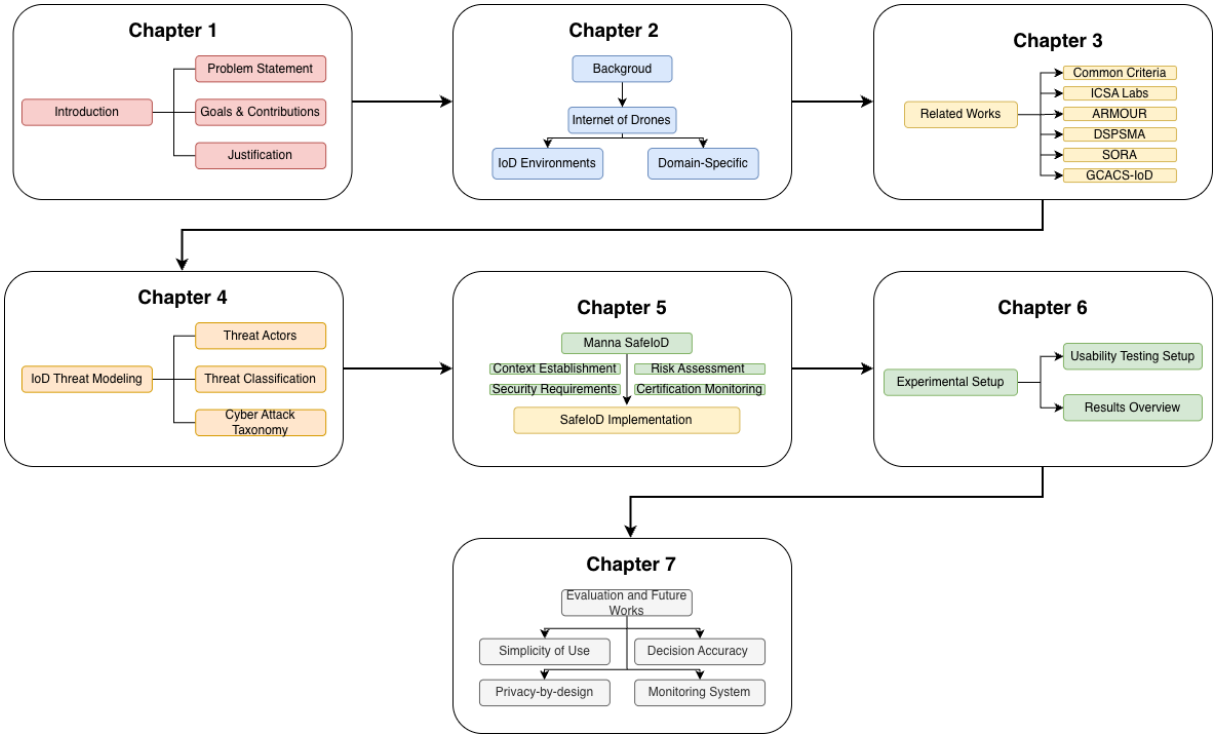
These resource constraints — already well-documented in the literature — have a direct certification implication: not all devices are equally capable of satisfying the same security requirements. Existing methodologies for penetration testing and vulnerability assessment fail to account for this heterogeneity, as they do not incorporate threat modeling, mission context evaluation, or security requirement elicitation as part of the certification workflow. Consequently, establishing methodologies and criteria for determining device reliability levels is essential, as such procedures are frequently neglected by available literature, rendering these approaches restrictive and incomplete — particularly given the specific architectural characteristics of `IoD` networks.

The proposed Manna SafeIoD framework addresses these limitations by implementing a holistic approach that integrates threat modeling, risk assessment, and continuous monitoring within a unified certification paradigm. This methodology ensures that security evaluation encompasses not only technical vulnerabilities but also operational context, environmental factors, and mission-specific requirements that are critical for IoD deployments.

1.5 Thesis Organization

This manuscript is organized as shown in Figure 1.

Figure 1 – Thesis Organization



Source: Elaborated by the author.

- Chapter 2 presents the background knowledge required to understand the IoD ecosystem, including drone architecture and comparative analysis with traditional mobile networks.
- Chapter 3 describes the related works of the main certification methods.
- Chapter 4 we develop our comprehensive threat modeling methodology, presenting the taxonomy of threat actors and detailed classifications of natural, physical, and cyber-threats.
- Chapter 5 we introduce the Manna SafeIoD framework definition, detailing its four core modules: context establishment, risk assessment, maturity reporting, and security requirements engineering. And describes the framework implementation, presenting the software architecture, command-line interface, risk calculator algorithm, and output interface.
- Chapter 6 presents our experimental validation, including usability testing with 15 participants across five IoD deployment scenarios, statistical analysis of evaluation metrics, multi-criteria comparative assessment of existing certification frameworks, and network simulation results.
- Chapter 7 we discuss the evaluation findings, identify limitations, and outline future research directions. We conclude the paper by summarizing our contributions to IoD security certification.

CHAPTER

2

BACKGROUND

The development of cybersecurity certification is intimately related to the architectural concepts of the target object, in this case, drones, as well as testing methodologies and existing attack types. Therefore, it is essential to comprehend the principal topics related to this domain for a complete understanding of this thesis project's proposal.

2.1 Drones

Unmanned Aerial Vehicles (UAVs), drones, and *Remotely Piloted Aircraft Systems* (RPAS) represent various nomenclatures for autonomous or remotely controlled aerial devices. In Brazil, the adopted terminology is Veículos Aéreos Não Tripulados (`VANTs`). There exists considerable diversity in drone types, applicable to both civilian and military spheres. Such devices can range from insect-sized platforms to aircraft as large as manned aviation systems (FLOREANO; WOOD, 2015). Typically, these devices are equipped with sensors, actuators, cameras, power units, processing units, and communication modules (MEKDAD *et al.*, 2023).

From an architectural perspective, the Internet of Drones paradigm has emerged as a critical evolution in UAV deployment, characterized by networked drone systems that operate collaboratively through centralized coordination frameworks (GHARIBI; BOUTABA; WASLANDER, 2016c). This paradigm shift necessitates enhanced security considerations, particularly in authentication mechanisms and data integrity protocols that govern inter-drone and drone-to-ground station communications (FOTOUHI *et al.*, 2019).

Drones are aerial devices equipped with diverse sensor arrays and represent complex cyber-physical systems that integrate multiple technological domains. The fundamental drone architecture consists of three principal elements: flight controller, ground control station, and data links (BATTH; NAYYAR; NAGPAL, 2018). Understanding these components is crucial for developing cybersecurity certification frameworks, as each element presents distinct attack

vectors and security requirements (MATHEU *et al.*, 2020).

- **Flight Controller**: This serves as the Central Processing Unit (CPU) of the drone system. It is responsible for receiving, processing, and interpreting data collected from sensors, including information regarding altitude, velocity, direction, and positional coordinates, among other parameters. Additionally, the flight controller receives commands from the ground control station and, based on this information, transmits signals to the drone's actuators, which control motor speeds and control surfaces to maintain stable flight and execute specific maneuvers (BATTH; NAYYAR; NAGPAL, 2018). From a cybersecurity perspective, the flight controller represents a critical asset requiring protection against firmware manipulation, sensor spoofing, and control signal injection attacks. The integrity of the flight control algorithms and their resistance to adversarial inputs constitute fundamental security requirements for certification frameworks.

- **Ground Control Station (GCS)**: This constitutes the operational nervous system, providing resources for human operators to control and/or monitor drones during their operations. It comprises a suite of electronic devices, including a central processing unit, display screen, joystick or other input devices, as well as flight control software and additional resources. The ground control station is responsible for processing data received from the drone's internal and external sensors (ALTAWY; YOUSSEF, 2016). The GCS represents a significant cybersecurity concern in IoD environments, as it serves as the primary interface for drone fleet management and must implement robust authentication mechanisms to prevent unauthorized access and command injection attacks (SRINIVAS *et al.*, 2019).

- **Data Links**: Data links constitute communication channels utilized for transmitting information and control commands to drones during their operations. These data links enable remote monitoring and control of drones through ground control systems. Information transmitted via these links may include drone location, remaining flight time, distance from GCS, target distance, and other relevant parameters. In most cases, data links employ radiofrequency (RF) technology for line of sight (LOS) missions, which occur when the operator maintains clear and unobstructed visual contact with the drone throughout the flight. For beyond line of sight (BVLOS) missions, where the drone may operate outside the operator's visual range, data links utilize satellite communications to enable remote drone control and relevant data transmission back to the operator (BOCCADORO; STRICCOLI; GRIECO, 2021a). The security of data links represents a paramount concern in IoD architectures, as these communication channels are susceptible to various attack vectors including eavesdropping, replay attacks, man-in-the-middle attacks, and jamming (OZMEN; BEHNIA; YAVUZ, 2019). Securing these communication channels requires implementation of robust encryption protocols, authentication mechanisms, and intrusion detection systems specifically designed for UAV operational environments.

2.2 Internet of Drones

The integration of drones into IoT networks is referred to as the Internet of Drones. This architecture was originally proposed by (GHARIBI; BOUTABA; WASLANDER, 2016c) and was designed with the intention of controlling and detecting the presence of drones in airspace. In general, IoD aims to ensure safety in airspace traffic through the control of where drones can be located and fly (MEHTA; GUPTA; TANWAR, 2020a).

Distinct from other mobile paradigms such as WSNs, UWSNs, or cellular networks (compared in Table 1), the IoD presents unique architectural challenges. Its primary differentiator is the unrestricted mobility of nodes, which navigate airspace at high speeds with variable altitudes. Coupled with the energy constraints inherent to battery-powered embedded systems, this environment creates a complex security landscape.

In the IoD architecture, drones are viewed as intelligent objects capable of executing tasks in groups in swarm formations or individually to perform missions such as monitoring, patrol, rescue, delivery, and other applications (BOCCADORO; STRICCOLI; GRIECO, 2021a). The conceptual foundation of IoD represents a paradigmatic shift from traditional UAV operations toward a coordinated, scalable network architecture that draws inspiration from three major large-scale networks: Air Traffic Control (ATC), cellular networks, and the Internet (GHARIBI; BOUTABA; WASLANDER, 2016c). This convergence enables the IoD to leverage the collision-free navigation capabilities of ATC, the deployment strategies of cellular networks, and the layered architectural principles of the Internet, creating a framework for coordinated airspace access. In general terms, within the IoD architecture, airspace is divided into: airways that consist of paths that drones can fly, with such paths having specific directions. The connection between two airways is accomplished through intersections, and finally, we have nodes that are free-flight spaces, i.e., spaces without defined airways.

Formally, Svaigen *et al.* (2023) defines that the IoD network can be represented by a graph $G = (V, E)$, where V is a set of three-dimensional points that drones must reach, based on their flight plans, and E is a set of aerial segments that connect two points of V, called waypoints. Thus, drone route planning can be viewed as a subgraph $G' = (V', E') \subset G$. This mathematical formalization provides the theoretical foundation for implementing security policies and access control mechanisms within the IoD framework, as it enables precise definition of authorized flight paths and restricted zones.

Table 1 – Comparative analysis of IoD attributes versus traditional mobile networks. (Adapted from Svaigen *et al.* (2023))

Characteristic	**IoD**	**Cellular**	**Vehicular (VANET)**	**WSN**	**UWSN**
Node Velocity	Rapid ($> 15m/s$)	Low mobility ($< 5m/s$)	Variable (Urban: $\approx 8m/s$; Highway: $> 20m/s$)	Quasi-static (Dependent on host)	Slow (Driven by water currents)
Mobility Pattern	Mission-dependent (3D)	Stochastic / Random	Constrained by road infrastructure	Mostly Random	Dictated by fluid dynamics
Verticality (Altitude)	Significant variation	Negligible	Negligible	Negligible	Significant variation
Topology Dynamism	High	High	High	Low	Low
Computational Capacity	Moderate	High	High	Limited	Limited
Power Limitations	Critical	Moderate	Relaxed	Critical	Critical

Gharibi, Boutaba and Waslander (2016c) proposes dividing airspace into zones, where each zone has its own airways, intersections, and nodes. For zone transitions, drones must mandatorily use entry and exit gates. For coordination of drones within zones, *Zone Service Providers* (ZSPs) are utilized, which are terrestrial control stations that perform communication and management of drones through a five-layer network architecture, comprising:

1. **Airspace Layer**: This layer refers to a collection of technologies, protocols, and systems that enable airspace management in which drones operate. This layer is responsible for collecting, processing, and providing essential information for drone flight planning, such as meteorological data, air traffic conditions, flight restrictions, information about landing and takeoff areas, among others. This layer is fundamental for enabling drones to operate safely and efficiently in an environment shared with other manned and unmanned aircraft (KHAN *et al.*, 2022). From a cybersecurity perspective, this layer must implement robust protocols for map representation, airspace broadcast and track capabilities, trajectory planning, airspace precise control, collision avoidance mechanisms, and weather condition integration. The security requirements include protection against GPS spoofing attacks, trajectory manipulation, and unauthorized airspace access attempts.

2. **Node-to-Node Layer**: This layer enables direct communication between network nodes (drones, ground stations, sensors, etc.) without the need for a centralized access point, such as a base station. This is particularly important in scenarios where communication infrastructure is limited or non-existent, such as in remote areas or search and rescue operations (HAIDER *et al.*, 2022). This layer seeks to maintain the zone updated with all drone metadata to provide a contingency path in case the drone cannot continue on its current path due to unexpected energy shortage or when emergency landing is necessary.

The security implications of this layer include securing peer-to-peer communications, implementing distributed trust mechanisms, and ensuring data integrity in ad-hoc network formations. Critical security features include zone graph maintenance, N2N broadcast and track capabilities, pathway planning and contingency protocols, refueling coordination, N2N precise control, emergency response mechanisms, and congestion notification systems.

3. **End-to-End Layer**: This layer is responsible for ensuring that information is encoded at the source, transmitted through one or more zones, and accurately decoded at the destination. This layer acts as a bridge between adjacent zones and intermediate gates, providing drones with all necessary information to enable `ZSP` changes. This layer can also assist in communication between different air traffic controllers and other drone management systems, ensuring that all parties involved in drone operation are synchronized and working together (GHARIBI; BOUTABA; WASLANDER, 2016c). The cybersecurity architecture of this layer must address interzone graph management, routing protocols between adjacent zones, handoff mechanisms for ZSP transitions, and explicit congestion notification systems. Security challenges include preventing man-in-the-middle attacks during zone transitions, ensuring secure handoff protocols, and maintaining communication integrity across multiple ZSP domains.

4. **Service Layer**: This layer is utilized for information transmission between drones and `ZSPs`. Its primary function is to provide a common platform where zone-related events can be transmitted to drones either individually or in swarm formations. The service layer implements zone broadcast capabilities that enable task distribution, service discovery, and coordination messages to be disseminated throughout the zone. From a security standpoint, this layer must implement secure broadcast mechanisms, message authentication protocols, and protection against broadcast storm attacks and message tampering.

5. **Application Layer**: This layer is intended for communication of future applications developed for the `IoD` architecture. (GHARIBI; BOUTABA; WASLANDER, 2016c) defines this layer as a free zone where private applications will be executed. Unlike other layers, there are no specific requirements for this layer. However, from a cybersecurity certification perspective, this layer represents both an opportunity and a challenge, as it must provide sufficient flexibility for innovation while maintaining security standards and preventing malicious applications from compromising the underlying IoD infrastructure.

Within each zone, there can be more than one `ZSP` providing different services; however, all must work together to ensure harmony in the network, avoiding potential accidents or service conflicts. This distributed management approach introduces complex security challenges related to ZSP authentication, service coordination protocols, and conflict resolution mechanisms. The IoD architecture's security implications are profound, as it transforms individual drone

security concerns into systemic network security challenges. The multi-layered approach requires security mechanisms that operate both within individual layers and across layer boundaries, implementing what (GHARIBI; BOUTABA; WASLANDER, 2016c) characterizes as "cross-cutting features" that include authentication of drones and ZSPs, protection against jamming of broadcast messages, prevention of airspace clogging attacks, and safeguarding against hacking of drones or ZSPs. These security requirements form the foundation for developing cybersecurity certification frameworks that can address the unique challenges of IoD environments while maintaining the operational flexibility necessary for diverse drone applications.

2.3 Domain-Specific Implementations and Market Trends

The academic and industrial communities have increasingly treated drone technology as a sophisticated, layered mobile network rather than merely isolated devices. This shift has accelerated the adoption of DaaS across diverse sectors, including the Internet of Things (IoT) and Smart Cities initiatives. Such integration promises to reshape both urban and rural landscapes, offering tangible benefits to social welfare. Comprehensive surveys (BOCCADORO; STRICCOLI; GRIECO, 2021b; ALSAMHI *et al.*, 2019a; ABUALIGAH *et al.*, 2021) have already cataloged the primary domains of DaaS. Below, we synthesize these domains focusing on their operational characteristics and data implications:

- **Disaster Management and Response:** UAVs are critical assets for public safety during crises like tsunamis, floods, or hostile attacks (SHAKHATREH *et al.*, 2019). In these scenarios, the primary function is the real-time transmission of high-bandwidth data (video feeds) to command centers to aid decision-making;
- **Environmental Sensing:** Functioning as airborne IoT nodes, drones extend the range of data acquisition networks. They are pivotal for tasks such as atmospheric pollution analysis and wildfire detection (JOŃCA *et al.*, 2022). These units typically carry specialized payloads, including LIDAR, scatterometers, and spectrometers, to aggregate data from ground sensors or perform direct measurements;
- **Infrastructure Integrity Assessment:** In sectors like civil engineering and industrial manufacturing, UAVs provide a safer alternative for inspecting physical assets. By utilizing directed video streams and sensor telemetry, they allow experts to monitor hazardous industrial zones or construction progress remotely (NOORALISHAHI *et al.*, 2021);
- **Intelligent Transportation Support:** Drones serve as a complementary layer to terrestrial traffic management (KHANPOUR *et al.*, 2025; ZHENG *et al.*, 2025). They assist in identifying congestion, accidents, and road hazards. Furthermore, through integration with Vehicular Ad Hoc Networks (VANETs), aerial nodes can broadcast alerts to drivers. This

application requires the handling of sensitive information, including license plates and driver behavior patterns;

- **Public Security and Crowd Control:** For civil surveillance, aerial units offer a vantage point for monitoring large gatherings or riots (FANG; SAVKIN, 2024). The architecture typically involves continuous video uplink to a central monitoring station to assess crowd dynamics;

- **Smart Farming:** Precision agriculture utilizes UAVs to optimize inputs and maximize yields, proving to be a time-efficient solution for modern farming (SHAKHATREH *et al.*, 2019). Similar to infrastructure monitoring, this domain relies heavily on visual and spectral sensors to assess crop health and soil conditions;

- **Last-Mile Logistics:** Although still facing regulatory hurdles, aerial delivery (e.g., Amazon Prime Air) represents a growing sector for transporting goods and medical supplies (SHASTRI; SHRIVASTAV, 2025). Security is paramount here, as the network must process precise geolocation data and customer details while ensuring safe path planning;

- **Aerial Network Extension:** A novel application involves using drones as flying base stations to enhance wireless coverage or throughput for ground users. In this configuration, the UAV becomes a critical infrastructure node, relaying massive amounts of user-generated traffic (CHANG *et al.*, 2023);

- **Renewable Energy Infrastructure:** IoD systems have become instrumental in the global energy transition, enabling efficient inspection and maintenance of solar farms, wind turbines, and power grid infrastructure (ABDELMABOUD, 2021). Equipped with thermal imaging and LiDAR sensors, drones can detect panel defects, blade cracks, and transmission line anomalies in real-time, reducing inspection time by up to 70% compared to manual methods while eliminating worker exposure to hazardous conditions (DJI Enterprise, 2024). The market for drones in power generation and distribution is projected to reach USD 4.4 billion by 2030, reflecting the sector's critical dependence on IoD for predictive maintenance and operational resilience (SkyQuest Technology, 2024);

CHAPTER

3

RELATED WORK

Despite the widespread adoption of drones, current hardware designs still exhibit vulnerabilities that may be exploited for data theft, route tracking, or denial-of-service purposes. Drones expose five primary attack surfaces that can be targeted by malicious actors: hardware, communication channels, control stations, pilots, and backend servers (KONG, 2021).

In recent years, the discussion surrounding security aspects has received substantial attention from both academia and industry. Wang *et al.* (2019) present a comprehensive survey on potential attacks targeting three core components of the IoD architecture: communication, computing power, and control subsystems. They also discuss the impact of such attacks on data security and privacy. Lin *et al.* (2018b) argue that recent literature on attacks clearly shows how relatively easy it will be to construct highly effective tools aimed at data degradation in smart city scenarios involving IoD systems.

The prevailing perception is that the consequences of security failures are even more critical in IoD environments, due either to the execution of critical operations by the devices, the vast volume of data exchanged over the network, or both (YAHUZA *et al.*, 2021). Attacks such as *jamming* (PIETRO; OLIGERI; TEDESCHI, 2019), *spoofing* (SATHYAMOORTHY *et al.*, 2020), and *hijacking* (KANG; JOE, 2018) are among the most studied in the literature, given their potential to exhaust or circumvent device and infrastructure resources, leading to service disruption and, therefore, system unavailability.

Considering the implementation of a secure IoD network in smart city contexts, Almulhem (2020) applied threat tree modeling to identify and classify known vulnerabilities in multi-drone systems. The author concludes that ensuring the security of IoD deployments requires accounting for device reliability across communication, mobility, and traceability dimensions.

Veerappan *et al.* (2021) introduced DRAT, an automated penetration testing framework for Wi-Fi-enabled drones. The tool integrates resources that allow for the orchestration of different testing levels. However, despite its technical capabilities, DRAT focuses solely on com-

mercial drones and does not address the unique requirements of IoD environments. Foundational works such as Arnold (2016) show that, since the early days of computing, systems have been subjected to various forms of testing to identify vulnerabilities. Nevertheless, more recent studies like McEnroe, Wang and Liyanage (2022) highlight the continuing challenges in standardizing security evaluations. These authors argue that current methodologies often provide ambiguous and inconsistent techniques for assessing security posture in computing devices.

Salamh, Karabiyik and Rogers (2021) proposed a risk analysis methodology for commercial drones based on the `STRIDE` model (KHAN *et al.*, 2017), enabling security evaluations across integrity, confidentiality, availability, and authorization dimensions. Their approach integrates penetration testing and digital forensic techniques. Although not exhaustive in its testing scope, its primary contribution lies in the definition of objective procedures and criteria to guide the scope and depth of testing. It is important to note, however, that the testing procedures presented in this work do not consider the broader context of the Internet of Drones.

3.1 Security Certifications

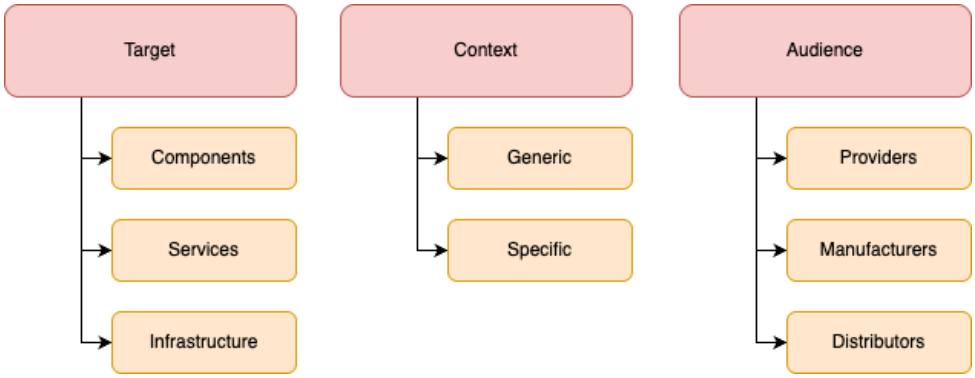
The specific characteristics of an IoD environment—such as the integration of monitoring tools and techniques, and the lifecycle complexity of devices—make the definition of a cybersecurity certification process particularly challenging. However, it is possible to identify essential elements within leading cybersecurity certification schemes that are applicable to the IoD domain. These include the establishment of clear security criteria, the execution of vulnerability assessments and testing, and ensuring the regular update of device software and hardware.

According to Górniak *et al.* (2019), any cybersecurity certification must address three fundamental characteristics: target, context, and audience. These dimensions are inspired by the ECSCF the European Cybersecurity Certification Framework—used to guide certification classification within the European Union.

Figure 2 presents the scope of each of these three characteristics. Broadly speaking, the Target refers to the product, component, or service being certified. In an IoD context, this may include drones, ZSPs, cloud systems, gateways, and other infrastructure. The Context concerns the environment in which the certification process is conducted, which should faithfully represent the operational conditions to which the device will be exposed. A precise definition of the context contributes to a detailed set of security requirements, ultimately leading to more robust devices. Finally, the Audience refers to the stakeholder—whether regulatory body, user, or integrator—for whom the certification serves as a statement of compliance with security standards.

The following subsections present four of the most prominent cybersecurity certification schemes currently used in the market. Two of these are industry-defined (NASSAR, 2012; ICSA, 2016), while the remaining two were designed within academic research initiatives (MATHEU; HERNANDEZ-RAMOS; SKARMETA, 2019; RODRIGUEZ *et al.*, 2020).

Figure 2 – Certification Characteristics according to ENISA



Source: Elaborated by the author.

3.1.1 COMMON CRITERIA

Common Criteria (CC) refers to the international standard ISO/IEC 15408 for cybersecurity certification (NASSAR, 2012). CC ensures that IT devices are specified and evaluated in a methodical, repeatable manner and at a level of assurance appropriate to their intended operational environment. Within this certification framework, assets—designated as *Target of Evaluation* (TOE)—are assessed based on a tailored set of security requirements that correspond to the implementation type (ERNST; MARTIN, 2010). Devices may be certified at one of seven *Evaluation Assurance Levels* (EAL), where Level 1 represents basic assurance and Level 7 denotes the highest degree of security validation.

The work by Kang and Kim (2017) explores the implementation of EAL2-level requirements on IoT devices, specifically smart TVs. The authors argue that while EAL1 is often recommended for IoT, its baseline requirements are insufficient to counteract the broad spectrum of existing threats, thus necessitating the adoption of EAL2. Their study emphasizes the importance of incorporating security throughout all layers of IoT device development in order to ensure adequate protection against evolving attack vectors.

Although CC is a well-established certification framework, its application to IoT systems is limited, as noted by Kaluvuri, Bezzi and Roudier (2014). The substantial documentation requirements and implementation overhead pose significant barriers in this domain, which is characterized by unique challenges when compared to conventional information systems. Additionally, CC certifies only a specific version of a product in a defined configuration. This implies that each update or reconfiguration may require a complete recertification process. This is especially problematic in the IoT context, where devices are frequently updated and modified, thereby demanding recurring certifications for each new version (KEBLAWI; SULLIVAN, 2006).

3.1.2 ICSA Labs

The *IoT Security Testing Framework*, defined by ICSA (2016), establishes a set of security testing requirements for IoT systems. These requirements encompass aspects such as encryption, communication, authentication, physical and cyber security, and real-time monitoring. A system that complies with all criteria is deemed suitable for deployment in real environments without compromising network functionality or security.

To address the constant evolution and updating of IoT devices, ICSA Labs incorporates frequent iterative updates into its certification process. This approach aims to tackle the inherent dynamism of the IoT landscape. To manage the device lifecycle effectively, ICSA Labs requires a contractual commitment from vendors, ensuring that device certifications are periodically reviewed and updated. Furthermore, random product assessments are conducted to enhance the robustness and credibility of the certification process.

According to Matheu, Hernandez-Ramos and Skarmeta (2019), after the evaluation phase, if a product fails to meet the certification criteria, the responsible entity is granted a short remediation window to address the identified issues. Should the product fail to achieve compliance within this timeframe, the ICSA Labs certification is revoked. The certification must be renewed annually, with the entire process repeated from scratch. It is important to note that this process is conducted solely by entities authorized by ICSA, and that both the evaluation approach and criteria are not standardized, potentially varying between laboratories.

3.1.3 ARMOUR

The ARMOUR certification framework emerged as part of a European Union initiative designed to fulfill the security requirements of IoT devices. It is structured as an automated testing framework that incorporates benchmarks and formal evaluation processes. As argued by Matheu, Hernandez-Ramos and Skarmeta (2019), its design adheres to the guidelines of the *European Cyber Security Organisation* (ECSO) and follows the standards set forth by the *EU Cyber Security Certification Framework* (ECSCF), which aim to harmonize certification practices across EU member states. In addition to the ECSO-prescribed components, ARMOUR introduces elements tailored to the specific security context of IoT devices.

The certification process consists of six phases, the final of which involves continuous device monitoring. It begins with a contextual assessment of the environment in which the device will operate, followed by a threat identification and modeling step based on the European Institute for Security Evaluation Standards' risk analysis methodology (DAVRI *et al.*, 2021). For each identified vulnerability, targeted tests and mitigation strategies are applied. Ultimately, the device enters a continuous monitoring phase, during which new evaluations are triggered under two conditions: the discovery of a new vulnerability or the release of a firmware update.

As noted by Flatt *et al.* (2016), one of the defining features of this certification scheme is

its labeling mechanism. A QR code is affixed to each certified device, linking to a webpage that displays the current certification status. This page may also provide context-specific results, such as assessments tailored to domestic deployment scenarios.

However, one limitation of the ARMOUR certification is that its vulnerability database is not publicly accessible. This lack of transparency raises concerns about the comprehensiveness and reliability of the evaluation procedures conducted during certification.

3.1.4 DSPSMA

In an effort to address the existing gaps found in the various cybersecurity certification schemes available on the market, Rodriguez *et al.* (2020) proposed the *Dynamic Security and Privacy Seal Model* (DSPSMA). This model introduces a real-time monitoring process to be used in conjunction with existing certification frameworks.

The authors present a two-phase audit process. The first phase involves certification, which is flexible and allows for the integration of multiple existing standards. The application of these standards is assessed in accordance with the European Union's regulatory landscape, including its electronic privacy directives such as the *General Data Protection Regulation* (GDPR). The integration of multiple normative standards helps minimize blind spots in certification, since each framework has its limitations and can complement the others when combined.

The second phase involves continuous monitoring, ensuring that the certification remains valid over time. If a device receives an update that introduces known vulnerabilities, a violation alert is sent to the vendor for remediation. Should the vulnerability remain unresolved, the certification is automatically revoked.

One of the most innovative aspects of this certification architecture is the use of blockchain technology for log storage. The blockchain preserves the historical records of each certification event and guarantees the authenticity and integrity of the data. As future work, the authors propose the development of custom certification metrics specific to this dynamic model.

3.1.5 SORA

Focused on UAVs, the article (DENNEY; PAI; JOHNSON, 2018) presents The Specific Operations Risk Assessment (SORA) is a risk assessment methodology developed by the Joint Authorities for Rulemaking on Unmanned Systems (JARUS). The European Union Aviation Safety Agency adopted this process.

The author proposes a methodology that employs a 10-step process to evaluate risks associated with drone operations in the Specific category—operations that fall between the low-risk Open category and the high-risk Certified category. SORA classifies risks into two primary dimensions: the Ground Risk Class (GRC), which evaluates the risk of a drone striking persons or property on the ground, and the Air Risk Class (ARC), which assesses the probability

of mid-air collisions with manned aircraft. The combination of GRC and ARC determines the Specific Assurance and Integrity Level (SAIL). Each SAIL level prescribes a set of Operational Safety Objectives (OSOs) that must be satisfied with appropriate levels of robustness—defined as the combination of integrity (safety gain) and assurance (demonstration method) (ASGHARI; IVAKI; MADEIRA, 2025).

One of SORA's notable strengths is its context-adaptive approach: the methodology requires operators to define a detailed Concept of Operations (ConOps) that specifies the operational environment, drone characteristics, crew qualifications, and emergency procedures. This contextual assessment enables tailored risk evaluation rather than one-size-fits-all certification.

However, despite its widespread adoption and methodological rigor, SORA presents significant limitations when considered for IoD cybersecurity certification. First, SORA is fundamentally oriented toward *operational safety* rather than *cybersecurity*; its risk dimensions (GRC and ARC) address physical hazards such as collisions and ground impact, but do not incorporate threat modeling for cyber attacks, including jamming, spoofing, or hijacking. Second, SORA does not provide mechanisms for security requirements engineering—deriving technical security controls from identified threats. Consequently, while SORA represents the most mature UAV-specific risk assessment framework currently available, it addresses concerns complementary to, but distinct from, the cybersecurity certification gap targeted by the present work.

3.1.6 GCACS-IoD

In the context of IoD-specific security solutions, (CHAUDHRY *et al.*, 2021) proposed GCACS-IoD, a certificate-based generic access control scheme designed to secure communication within IoD environments. The framework addresses two fundamental authentication scenarios: inter-drone (D2D) communication between UAVs operating in the same or adjacent flying zones, and drone-to-ground station (D2GSS) communication. GCACS-IoD employs Elliptic Curve Cryptography (ECC) to achieve computational efficiency suitable for resource-constrained drones while providing anonymity and resistance to replay, impersonation, and man-in-the-middle attacks.

However, subsequent cryptanalysis by (DAS *et al.*, 2021) revealed critical vulnerabilities in the original design, demonstrating that the private key of the trusted Control Room could be disclosed, enabling attackers to compromise the entire IoD network through malicious drone deployment and impersonation attacks. The authors proposed an improved version, iGCACS-IoD, which addresses these weaknesses through enhanced key management and formal verification. While GCACS-IoD and similar IoD authentication protocols represent important contributions to securing drone communication, they focus exclusively on specific security mechanisms—predominantly authentication and key agreement—rather than providing comprehensive methodologies for device certification, risk assessment, or security requirements engineering.

3.1.7 Other Certification Processes

In addition to the previously described certifications, some countries enforce specific regulatory processes for authorizing commercial use of IT and IoT devices. To ensure compliance with the General Data Protection Regulation (GDPR), the European Union issues a European Privacy Seal. This process involves manual audits conducted by certified experts (REGULATION, 2016).

In Singapore, the Security Accreditation Committee is responsible for issuing mandatory cybersecurity certifications for IT products supplied to government agencies. Similarly, in Germany, the ULD (Independent Centre for Privacy Protection) certifies IoT products as well as software, hardware, and services used by German authorities (MATHEU *et al.*, 2020).

In the United States, the *The Wireless Association* (CTIA) defines a certification process for devices operating with Wi-Fi LTE technology (ASSOCIATION *et al.*,). The certification evaluates compliance with requirements in several security categories, including authentication, encryption, update management, and threat monitoring.

Table 2 summarizes and compares the discussed certification schemes in terms of their adherence to key components proposed by this thesis, such as IoD Focus, risk assessment, vulnerability analysis, auditing, and public access.

Table 2 – Comparative Analysis of Cybersecurity Certification Frameworks Against IoD Requirements

Certification	IoD Specific	Context Adaptive	Risk Assess.	Risk Propag.	Threat Model	Sec. Req. Eng.	Maturity Levels	Lifecycle Coverage	Tool Support	Open Access
Common Criteria	–	–	○	–	◐	◐	●	○	–	●
ICSA Labs	–	–	●	–	◐	○	●	◐	–	–
ARMOUR	–	○	◐	–	◐	○	●	◐	◐	–
DSPSMA	–	○	◐	–	◐	–	○	◐	○	○
SORA	○	◐	◐	–	○	–	●	○	–	●
GCACS-IoD	●	–	◐	–	–	◐	–	–	–	○
Manna SafeIoD	●	●	●	●	●	●	●	●	●	●

Legend: ● = Fully Supported; ◐ = Partially Supported; ○ = Limited Support; – = Not Supported

CHAPTER

4

IOD THREAT MODELLING

Threat modeling (ALMULHEM, 2020) represents a systematic approach that encompasses identifying principal assets within a system and analyzing threats to these assets. According to (DERHAB *et al.*, 2022), an asset constitutes anything of value to an organization. Within the IoD context, examples of critical assets include drone platforms, Zone Service Providers (ZSPs), cloud infrastructure providers, communication channels, navigation systems, payload systems, and mission-critical data repositories.

For this analysis, we employ the attack tree methodology to represent the threat modeling of IoD architecture. This approach, originally proposed by (ALMULHEM, 2020) and subsequently refined for cyber-physical systems (PANDEY *et al.*, 2022), provides a structured framework for decomposing complex attack vector scenarios into manageable analytical components.

An attack vector within an IoD context consists of three fundamental entities: the malicious agent, the IoD device, and the actual target. This triadic relationship forms the foundation for understanding attack propagation in distributed drone networks as show Table 3.

Table 3 – Fundamental Entities in IoD Attack Vectors

Entity	**Description**
Malicious Agent	Adversarial actor seeking to identify exploitable vulnerabilities. Ranges from nation-state actors with electronic warfare capabilities to opportunistic criminals using readily available attack tools.
IoD Device	Most vulnerable component serving as entry point. Encompasses drones, communication links, ground control stations, and supporting infrastructure with inherent resource constraints.
Actual Target	Critical system or asset the attacker ultimately seeks to compromise, including critical infrastructure, sensitive data repositories, or command systems beyond the immediate drone network.

4.1 Threat Actors

An attack constitutes an offensive action with malicious intent, such as stealing, altering, disabling, or destroying information through unauthorized access to computer systems (AL-SAMHI *et al.*, 2019b). The interconnective capabilities present in the IoD architecture, combined with their inherent processing constraints and energetic limitations, provide sufficient conditions that enable numerous attack vectors against systems and services (MEHTA; GUPTA; TANWAR, 2020b).

To comprehensively evaluate threat landscapes in IoD environments, we categorize three distinct types of threat actors based on their capabilities, access levels, and operational constraints, as presented:

- **Privileged Insider:** Government officials, institutional personnel, maintenance technicians with direct physical access to drones/ZSPs. Can bypass technical controls through physical access and insider knowledge.
- **Proximate External:** Malicious hackers, unauthorized surveillance entities operating within service zone range. Enable RF attacks, signal interception, and electronic warfare techniques.
- **Unintentional:** Wildlife collisions, adverse weather, electromagnetic interference from legitimate sources. Non-malicious but can significantly impact operations and mask malicious activities.

4.2 Threat Classification

Drones and their associated IoD infrastructure are vulnerable to several categories of threats, which can be systematically classified into three primary types based on their origin, manifestation, and impact vectors:

- **Natural Threats**: Within the realm of IoD security, environmental vulnerabilities present pressing concerns that extend beyond traditional cybersecurity paradigms. Drones traversing airspace encounter various natural elements that can affect their operations, creating exploitable conditions for malicious actors. Environmental threats include meteorological phenomena such as wind shear, microbursts, electromagnetic storms, and atmospheric conditions that can disrupt navigation and communication systems. Neglecting these environmental factors provides attackers with opportunities to exploit adverse conditions, using weather patterns or aerial wildlife as cover for malicious activities, thereby disrupting IoD operations and compromising security postures (YAHUZA *et al.*, 2021).

Table 4 – Threat Categories in IoD Systems

Category	**Sub-category**	**Description**
Communication	Constrained-peer	D2D comms under energy/computational limits preventing robust security
	Non-constrained	Traditional vulnerabilities + mobile platforms/dynamic topology
Environment	Within-zone	Restricted movements; attackers exploit flight patterns/airspace constraints
	Inter-zone	Zone transitions via gates; vulnerabilities during handoff/boundary crossings
Provider	ZSP-related	Ground-based control system vulnerabilities
	Cloud-related	Targets: metadata, performance characteristics, operational parameters, ACL
Drone	Dual-role	Both attack victims and tools; compromised units attack other components

- **Physical Threats**: Drones are inherently susceptible to physical attacks stemming from human intervention and environmental obstacles. These attacks encompass vandalism through deliberate damage or destruction of drone platforms (ALSAMHI *et al.*, 2019b), theft involving unauthorized appropriation of drone assets (ALTAWY; YOUSSEF, 2016), and various forms of eavesdropping including ground-based signal interception and payload monitoring (DEY *et al.*, 2018). Physical threats pose substantial privacy and operational risks within the IoD ecosystem, causing direct harm to devices while exhibiting destructive behavior that can compromise mission integrity and data confidentiality.

- **Cyber Threats**: These threats exploit various network elements including drones, communication links (drone-to-drone and drone-to-infrastructure), cloud data storage systems, and ground control infrastructure. Cyber attacks often occur stealthily without causing immediate physical damage, making detection and attribution challenging. These threats are categorized into passive attacks such as automatic drone detection systems (RAMADAN *et al.*, 2021) and traffic analysis attacks (SCIANCALEPORE *et al.*, 2020), and active attacks including jamming techniques (FERNÁNDEZ-HERNÁNDEZ *et al.*, 2019), various spoofing methods (DAVIDSON *et al.*, 2016), hijacking attempts (KANG; JOE, 2018), and both software (BLAZY *et al.*, 2017) and hardware exploitation techniques (RODDAY; SCHMIDT; PRAS, 2016).

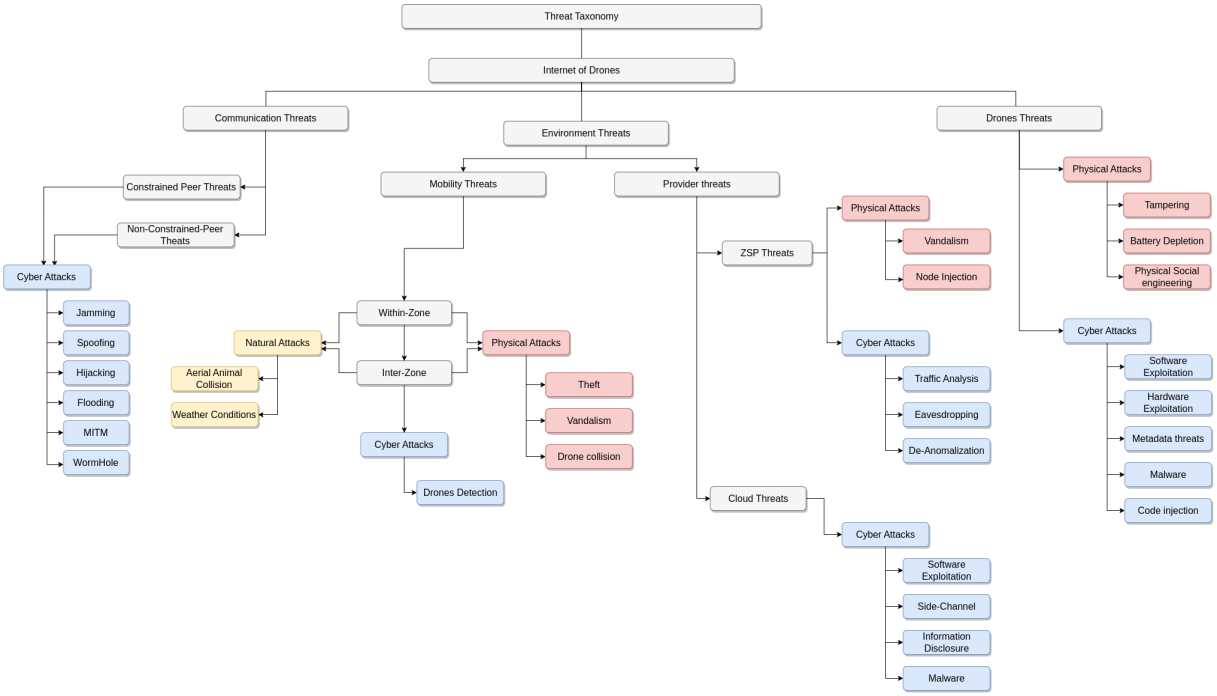
Figure 3 depicts the root of the attack tree, which serves as the focal point for all potential threats impacting an IoD system. These threats undergo iterative expansion, creating hierarchical subsets of threats represented as descendant nodes. To construct the tree, the attacks are subdivided into domains as described in Table 4.

4.3 Cyber Attack Taxonomy

Considering the unique characteristics of IoD environments, cyber attacks represent the most critical threat category due to their potential for causing catastrophic damage to individual drones or entire network infrastructures. The sophisticated nature of modern cyber attacks, combined with the increasing connectivity of IoD systems, creates attack surfaces that extend far beyond traditional network security perimeters.

These attacks can be systematically classified into six primary categories, each representing distinct attack methodologies with specific technical characteristics and mitigation requirements:

Figure 3 – Threat Modeling IoD System



Source: Elaborated by the author.

- **Jamming Attacks:** These constitute denial-of-service attacks targeting communication channels between drones and ground control systems or other network components. Jamming attacks disrupt radio frequency communications, making coordination between drones and ground control stations difficult or impossible. In such scenarios, affected drones lose situational awareness, navigation capabilities, and command reception, potentially resulting in mission failure or catastrophic incidents (PIETRO; OLIGERI; TEDESCHI, 2019). Advanced jamming techniques may employ frequency-hopping or adaptive algorithms to overcome anti-jamming countermeasures.

- **Spoofing Attacks:** These exploit vulnerabilities in data links between drones and ground control systems, enabling interception and manipulation of unencrypted or poorly protected

signals to mislead drone navigation systems. Spoofing attacks can target various systems including GPS receivers, altimeters, and communication protocols, potentially resulting in loss of accurate positional information, trajectory deviation, or complete drone theft (LIN *et al.*, 2018b). Sophisticated spoofing attacks may combine multiple signal sources to create convincing false environments that are difficult to detect.

- **Hijacking Attacks:** These involve transmission of unauthorized ground control signals designed to usurp legitimate control authority and force drones to respond to attacker commands. Hijacking attacks can result in complete loss of drone control, unauthorized mission redirection, or deliberate destruction through commands such as emergency shutdown during flight (ALSAMHI *et al.*, 2019b). Advanced hijacking techniques may exploit authentication weaknesses or session management vulnerabilities to establish persistent unauthorized control.

- **Flooding Attacks:** These attacks aim to overwhelm networks and individual services with massive volumes of data packets, preventing drones from accessing critical network services. Flooding attacks are categorized into Denial of Service (DoS) attacks targeting individual components (PU; ZHU, 2021) and Distributed Denial of Service (DDoS) attacks leveraging multiple attack sources to amplify impact (SALAMH *et al.*, 2019). In IoD contexts, flooding attacks may specifically target bandwidth-constrained communication links or resource-limited drone processing capabilities.

- **Wormhole Attacks:** These represent sophisticated routing-based attacks where malicious actors strategically position compromised drones or infrastructure components to create unauthorized communication tunnels. In wormhole attacks, two malicious nodes establish covert communication channels that bypass normal network routing protocols. Node A intercepts data packets in geographical area X and transmits them to Node B, which replays them in a different location, creating false proximity relationships and enabling various secondary attacks. Related attack variants include selective forwarding (LI *et al.*, 2021) and black-hole attacks (HASSIJA *et al.*, 2021) that share similar methodological foundations.

- **Hardware/Software Exploitation:** Both drone platforms and ground control systems are vulnerable to various forms of malicious software including malware (PLEBAN; BAND; CREUTZBURG, 2014), trojan horse programs (RODER; CHOO; LE-KHAC, 2018), keyloggers, and side-channel attacks (MARQUES; SILVA, 2021). These exploits may be embedded during manufacturing processes or introduced through subsequent software updates or maintenance procedures. In IoD environments, successful exploitation can result in complete loss of operational security, unauthorized access to confidential mission data, or persistent compromise of communication channels that enables long-term surveillance or sabotage activities.

The evolution of IoD technologies continues to introduce new attack vectors and amplify existing vulnerabilities. The integration of artificial intelligence, machine learning, and autonomous decision-making capabilities in modern drone systems creates additional attack surfaces that adversaries may exploit. Future threat modeling efforts must account for these emerging technologies and their associated security implications to ensure protection of IoD deployments.

CHAPTER

5

MANNA SAFEIOD

As discussed in (DERHAB *et al.*, 2022), research, the IoD constitutes a complex cyber-physical system (CPS) integrating heterogeneous hardware, software, and communication components. While methodologies for secure design exist for general CPS and embedded systems (PONSARD; MASSONET; DALLONS, 2016; SCHMITTNER; MA; SCHOITSCH, 2015; SOJKA; KREČ; HANZÁLEK, 2014), they fall short in addressing the contextual and environmental dynamism inherent to IoD deployments. This gap underscores the necessity for a tailored secure-by-design certification methodology specific to IoD.

The definition of an efficient IoD device evaluation framework must take into consideration three main aspects:

- **Standardization**: The utilization of drones is not confined to a specific region or country; therefore, certification should be standardized to provide a harmonized process across different contexts, domains, and countries.
- **Context**: For an effective certification process, it is necessary to take into consideration the context in which the device will be implemented. The context should encompass the purpose of the device, such as the type of target operation, the type of data manipulated, the operating environment, etc. This aspect is particularly challenging because the context of use may not be known a priori when the device is manufactured.
- **Environment**: IoD systems and devices operate in physical environments with variable conditions that can affect their level of security. Therefore, the maturity of a device may vary depending on the deployment aspects to which it may be exposed. At the end of the initial certification process, the device may be evaluated against a set of security requirements, but the initial tested configuration and maturity level may be affected due to software updates, changes in system configuration, or the need to be used in different operational contexts. Considering that software updates and patches are quite frequent due

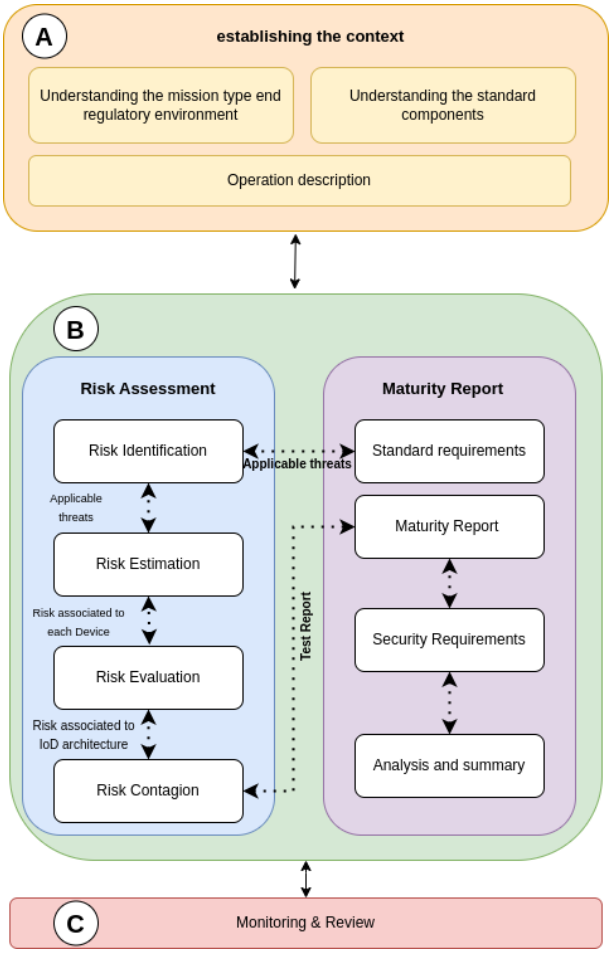
to the discovery of new vulnerabilities, it is necessary to define a lightweight recertification process design to reflect the changes introduced in the devices.

5.1 Framework Definition

Given the aforementioned characteristics, there is currently no suitable methodology tailored specifically for the IoD environment. This gap serves as one of our motivations to develop and introduce an evaluation security framework dedicated to this particular context. Figure 4 illustrates the diagram of the proposed evaluation methodology named Manna SafeIoD.

We have developed a straightforward methodology, the security assessment process represents the core of the methodology, integrating the context establishment, security risk assessment, security requirements and monitoring and review. These activities are described in more detail in the remainder of this section.

Figure 4 – Work-flow of the proposed methodology



Source: Elaborated by the author.

We have developed a straightforward methodology, the security assessment process represents the core of the methodology, integrating the context establishment, security risk

assessment, security requirements and monitoring & review. These activities are described in more detail in the remaining of this section.

5.1.1 Context Establishment

This step is intended to provide a understanding of the deployment conditions, limitations, and operational contexts in which the IoD component is utilized. This phase draws upon best practices in security requirements engineering for cyber-physical systems (DAS *et al.*, 2021) and governance frameworks (BOX; HDD; EAL, 2010), ensuring that the certification reflects real-world scenarios and evolving threat landscapes.

To accurately characterize the deployment and operational context, the following dimensions are analyzed:

1. **Deployment Environment:** Detailed characterization of the physical and geographical environment, including:
    - Type of setting: indoor/outdoor, urban/rural, controlled/uncontrolled airspace.
    - Physical constraints: signal interference, electromagnetic exposure, terrain.
    - Environmental factors: wind, precipitation, temperature extremes.
2. **Mission Operation Type:** Definition of the intended mission profile, including:
    - Purpose: surveillance, inspection, delivery, data collection.
    - Tasks: payload delivery, sensing operations, communication relays.
3. **Regulatory Environment:** Mapping of applicable legal and regulatory obligations:
    - National/international aviation regulations (e.g., FAA, EASA, ANAC).
    - Cybersecurity frameworks and data protection laws (e.g., GDPR, LGPD (Brazilian GRDP), ISO/IEC 27001.
    - Domain-specific standards for communication and safety.
4. **Deployment and Maintenance Processes:** Full lifecycle documentation:
    - Initial installation, configuration routines, and security onboarding.
    - Firmware updates, patch cycles, and preventive maintenance.
    - Roles and responsibilities of operational personnel.
5. **Contingency Procedures:** Preparedness for failure and emergencies:
    - Protocols for link loss, GNSS spoofing, battery depletion.
    - Emergency return, shutdown, or recovery protocols.

- Redundant communication mechanisms and fallback strategies.

Given that individual components possess unique architectural footprints and functional interfaces, they inevitably present different attack surfaces. Therefore, the characterization of the system must be performed through a multi-layered abstraction approach. This process involves collecting detailed metadata regarding the cybersecurity context of every entity, from the edge (drones) to the core infrastructure (ZSPs and gateways).

5.1.2 Risk Assessment

The primary objective of the security assessment phase is to derive a quantifiable metric that reflects the security posture of the device under analysis. This procedure is structured into three fundamental activities:

1. Threat Enumeration: This phase entails the systematic discovery of potential adverse events, mapping their origins and probable repercussions. The enumeration is data-driven, utilizing inputs such as device manufacturing specifications, operational mission profiles, and connectivity interfaces. This step is directly grounded in the IoD threat modeling previously established.

2. Risk Quantification: Following identification, this process assigns a magnitude to the risk associated with the Target of Evaluation (ToE). Recognizing that quantification often suffers from subjectivity, our approach mitigates imprecision by employing a specialized expert system to standardize the estimation using industry-standard metrics (CVSS).

3. Acceptability Analysis: The final stage involves benchmarking the calculated risk levels against pre-established security thresholds. This determines whether the residual risk falls within the tolerance levels defined by stakeholders or regulatory compliance frameworks.

To mathematically model the systemic risk within the Manna SafeIoD framework, we employ a graph-theoretic approach. While our logic draws inspiration from the propagation models by Li et al. (LI *et al.*, 2020), we adapt the dynamics to the specific volatility of ad hoc aerial networks. Rather than a biological infection metaphor, we formulate risk as a function of lateral movement potential within a directed graph $G(V,E)$, where V denotes the nodes (UAVs, ZSPs, Gateways) and E represents the active logical or physical links.

The IoD ecosystem is heterogeneous, comprising drones, ground stations, and cloud providers. The Manna SafeIoD indicators are engineered to be category-agnostic, obviating the need for distinct calculation engines for each hardware type. We classify threat sources into two vectors: (1) Physical vulnerabilities inherent to the hardware, and (2) Cyber threats residing in the firmware/software.

A critical concept in our model is the Risk Propagation Source. A module containing a threat capable of triggering a security incident endangers not only itself but its neighbors. In the mesh architecture, a directed path from node i to j is defined as a sequence of hops. If a route exists such that $i \to \mathrm{x} \to \mathrm{z} \cdots \to j$, we denote the connection relationship as $\lambda(i,j)$. The cumulative link relationship is the product of individual hops: $\lambda(i,j) = \lambda(i,x)\lambda(x,z)\ldots\lambda(s,j)$. The set of all valid paths from i to j is denoted by Λ. This assumption holds for the static topology snapshot during operation (MA; SELBY; ADIB, 2017).

Consequently, we introduce the Transmission Factor. This metric acknowledges that a threat on node i propagates through the network, threatening connected assets to varying degrees based on the strength and nature of the link. The assessment workflow is executed as follows:

- Phase 1 (Module Characterization): We treat every IoD entity as an abstract module. We define the multi-set of threat severity levels for a module as Θ (Equation (5.1)). To establish a baseline, we select the threat with the maximum CVSS score (μ_{score}) as the primary risk indicator (Equation (5.2)).

$$\Theta = \{\theta_0, \ldots, \theta_n\}, \text{where: } \theta_k \in [0.0, 10.0] \tag{5.1}$$

$$\mu_{score} = \max(\Theta) \tag{5.2}$$

  The baseline risk estimation ($\mathscr{E}_{risk}$) for a single module is derived using Equation (5.3), which functions as a ratio of the threat magnitude (ω) against the effectiveness of security controls.

$$\mathscr{E}_{risk} = \omega \times \frac{\mu_{score}}{\text{Security Controls}} \times \text{Impact} \tag{5.3}$$

  We map this numerical value to a qualitative severity scale:

$$\text{Risk}_{\text{Level}} = \begin{cases} \text{Negligible} & \mathscr{E}_{risk} = 0.0 \\ \text{Low} & 0.1 \leq \mathscr{E}_{risk} \leq 3.9 \\ \text{Moderate} & 4.0 \leq \mathscr{E}_{risk} \leq 6.9 \\ \text{High} & 7.0 \leq \mathscr{E}_{risk} \leq 8.9 \\ \text{Critical} & 9.0 \leq \mathscr{E}_{risk} \leq 10.0 \end{cases} \tag{5.4}$$

- Phase 2 (Adjacency Analysis): We calculate the transmission potential between direct neighbors. This yields the coefficient $\psi_{x \to y}$, representing the probability of risk propagating from module x to y. This is computed by weighting the estimated risk of the neighbor ($\mathscr{E}_{risk,y}$) against the specific threat relationship of the link.

- Phase 3 (Path Aggregation): We determine the Total Transmission Coefficient. This involves identifying all valid propagation paths Λ from a source i to any target j. The coefficient Ω_j is the aggregate of sequential transmission probabilities ($\psi_{x\to y}$) along these routes.
- Phase 4 (Event Probability): A threat θ detected on module i represents a probability, not a certainty. We calculate both the likelihood $\rho_i(\theta)$ and the potential impact $\mathscr{K}_i$ of the security event.
- Phase 5 (Systemic Integration): Finally, the global risk $\mathscr{R}_{sys}$ contributed by a source i is computed by integrating the local estimation, network transmission coefficients, and event probability.

Formalization of Systemic Propagation

To synthesize a complete network view, we must estimate how the risk from a specific target module cascades through the system. Let i be the potential source of compromise and j be any affected downstream node. The aggregated susceptibility coefficient for j is expressed as:

$$\Omega_j = \begin{cases} \sum_{\lambda\in\Lambda} \Psi_{\lambda(i,j)} & i \neq j \\ 1 & i = j \end{cases} \tag{5.5}$$

Here, Ω_j signifies the total susceptibility of module j, while $\Psi_{\lambda(i,j)}$ represents the coefficient for a specific path $\lambda_{(i,j)}$ within the set Λ. For a multi-hop path $\lambda(i,j) = \lambda(i,x)\lambda(x,y)\cdots\lambda(s,j)$, the path coefficient is the product of intermediate link coefficients: $\Psi_{\lambda(i,j)} = \psi_{i\to x}\cdot\psi_{x\to y}\cdots\psi_{s\to j}$. While precise node enumeration is challenging in dynamic operations, the Context Establishment phase provides the boundary conditions for this estimation.

We further refine the model by incorporating the probability $\rho_i(\theta)$ and the consequent kinetic or cyber effects $\mathscr{K}_i$ of threats exploiting specific vulnerabilities. The impact calculation is defined as:

$$\mathscr{K}_i = \sum_{k=1}^{T} [v_i(\theta_k)\cdot\rho_i(\theta_k)] = \sum_{k=1}^{T} \{v_i(\theta_k)\cdot[\gamma_1 + \gamma_2\Delta_i(\theta_k)]\} \tag{5.6}$$

In this formulation, $v_i(\theta_k)$ quantifies the inherent Asset Value impacted by threat θ_k on module i. This parameter is calibrated based on the mission criticality defined in the Context Establishment phase (ranging from 0.1 for auxiliary logging to 1.0 for flight control systems).

The probability function $\rho_i(\theta_k)$ is a composite metric derived from two dimensions:

1. Inherent Threat Severity ($\mathscr{T}_i$): Derived from the CVSS Base Score of the vulnerability.
2. Security Gap (Δ_i): Represents the residual vulnerability after applying controls, calculated as $\Delta_i(\theta_k) = 1 - \frac{\text{Implemented Controls}}{\text{Required Controls}}$.

The coefficients γ_1 and γ_2 act as weighting factors that calibrate the risk assessment strategy, where $\gamma_1 + \gamma_2 = 1$. The probability of the incident occurring, $\rho_i(\theta_k)$, is derived via:

$$\rho_i(\theta_k) = \gamma_1 \mathscr{T}_i(\theta_k) + \gamma_2 \Delta_i(\theta_k) \tag{5.7}$$

The selection of weights γ_1 and γ_2 is critical for the scientific validity of the model, as it determines the framework's sensitivity to unmitigated threats versus inherent vulnerability severity. The formulation $\rho_i(\theta_k) = \gamma_1 T_i(\theta_k) + \gamma_2 \Delta_i(\theta_k)$ represents a convex linear combination where $\gamma_1 + \gamma_2 = 1$, a mathematical construct widely adopted in multi-criteria risk assessment models to balance competing risk dimensions (FREUND; JONES, 2015). The calibration of these weights follows established principles from the cybersecurity risk assessment literature, where the relative emphasis between threat severity and control effectiveness is determined by the operational context and the assessment objectives (NADA, a).

Rather than adopting arbitrary values, the calibration profiles are grounded in principles derived from established risk assessment standards and the domain-specific characteristics of IoD environments. We define three standard calibration profiles:

- **Balanced Profile** ($\gamma_1 = 0.5, \gamma_2 = 0.5$): Assigns equal importance to the inherent threat severity (derived from the CVSS Base Score) and the security control gap. This default configuration follows the principle established by the OWASP Risk Rating Methodology, which assumes equal weighting of all risk factors as its baseline model, recommending subsequent customization based on organizational context (OWASP Foundation, 2023). The NIST SP 800-30 framework similarly treats threat likelihood and impact magnitude with equivalent importance in its standard risk-level matrix, defining risk as a function of both dimensions without inherent prioritization (NADA, a). ISO/IEC 27005:2022 further advocates a balanced consideration of threats, vulnerabilities, and existing controls in its general risk analysis approach, employing both event-based and asset-based identification without privileging one over the other (International Organization for Standardization, 2022b). This profile serves as the default setting for general IoD certification where no specific operational bias is warranted, representing the most conservative and broadly applicable configuration.
- **Threat-Centric Profile** ($\gamma_1 = 0.8, \gamma_2 = 0.2$): Prioritizes the inherent severity of vulnerabilities over the presence of mitigating controls. This configuration is grounded in the

MIL-STD-882E system safety standard, which mandates that hazards classified as catastrophic or critical in severity require immediate risk acceptance authority action regardless of existing partial mitigations (Department of Defense, 2012). The FAIR (Factor Analysis of Information Risk) model further supports this approach by demonstrating that in scenarios where Threat Capability (TCap) significantly exceeds Control Strength (CS), the vulnerability function is dominated by the threat dimension (FREUND; JONES, 2015). In the specific context of military UAV operations, Hartmann and Steup (HARTMANN; STEUP, 2013) demonstrate that adversarial capabilities—including GPS spoofing, command link interception, and electronic warfare—represent existential threats whose severity dominates risk assessment independently of partial mitigations. The 80/20 weighting ratio reflects the established practice in dynamic risk assessment of applying constant weighting factors that ensure threats with higher severity always produce proportionally higher risk impacts, as documented in quantitative risk models for computing infrastructures (AWAN; BURNAP; RANA, 2013). This profile is designated for high-threat environments (e.g., military ISR zones, contested airspace) where the mere presence of a high-severity vulnerability (high CVSS score) drives the risk score regardless of partial controls.

- **Control-Centric Profile** ($\gamma_1 = 0.2, \gamma_2 = 0.8$): Emphasizes the security control gap (Δ_i) as the primary risk driver. This configuration is informed by compliance-driven certification frameworks where the absence of mandatory controls constitutes the dominant risk factor. The NIST SP 800-30 explicitly identifies "the adequacy of planned or existing security controls for reducing or eliminating risk" as a deterministic factor in its risk determination methodology (NADA, a). In compliance-oriented environments, the ISACA risk assessment model prioritizes control gap analysis—measuring the difference between implemented and required controls—as the primary mechanism for driving remediation decisions (ISACA, 2017). The European Cybersecurity Certification Framework (ECSCF) structures its assurance levels fundamentally around the verifiable implementation of security controls rather than threat-level assessments (KOHLER, 2020b), making this profile appropriate for controlled environments where regulatory compliance is the primary certification objective. ISO/IEC 27001:2022 reinforces this approach by requiring that all controls within an ISMS be risk-based, with control implementation status serving as the primary indicator of security posture (International Organization for Standardization, 2022a). This profile is used in regulated civilian environments (e.g., urban delivery fleets under GDPR/LGPD compliance) where risk is primarily driven by the absence of mandatory controls rather than by external threat severity.

The rationale for selecting $\gamma_1 = 0.8$ and $\gamma_2 = 0.2$ (and its inverse) rather than more extreme ratios (e.g., 0.9/0.1) is twofold: (1) no dimension should be rendered negligible, as even in threat-dominated environments the control posture retains diagnostic value, and in compliance-driven environments, the emergence of novel high-severity threats must still be

captured; and (2) the 80/20 distribution provides sufficient discriminatory power between profiles while maintaining sensitivity to both risk dimensions, consistent with established multi-criteria decision analysis practices in cybersecurity (AWAN; BURNAP; RANA, 2013; NADA, a).

The selection of the appropriate profile is determined during the Context Establishment phase (Stage A) based on mission type classification, regulatory requirements, and the operational threat environment, as detailed in Section 5.1.1.

The final derivation aggregates the estimated risk $\mathscr{E}_{risk}$ across all modules to present the total systemic risk $\mathscr{R}_{sys}$:

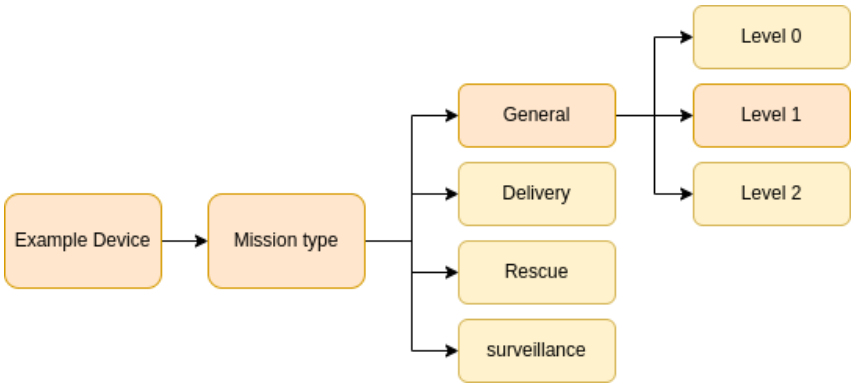
$$\mathscr{R}_{sys} = \sum_{j=1}^{J} \mathscr{K}_i \cdot \mathscr{E}_{risk,j} \cdot \Omega_j = \mathscr{K}_i \sum_{j=1}^{J} \mathscr{E}_{risk,j} \cdot \Omega_j \tag{5.8}$$

5.1.3 Maturity Report

As specified by ECSCF (KOHLER, 2020a), devising a security certification must consider the unique structure of each use case and designate an appropriate category for each assurance level, referred to herein as maturity.

Manna SafeIoD will grant certification based on the overall risk assessment of the device. This certification will indicate the security level of the tested device and its suitability for the designated mission type. The device's security level will be determined using a security maturity scale, which categorizes devices into distinct levels across various domains, as illustrated in Figure 5.

Figure 5 – Maturity Levels



Source: Elaborated by the author.

- Level 0 (Do not fly) —Denotes the complete absence of security safeguards. Devices in this category face extreme exposure to threats and fail to comply with the essential security standards necessary for safe deployment.
- Level 1 (Operational necessity only) —Denotes that the device incorporates basic security protocols and meets minimum operational requirements, rendering it eligible for certifi-

cation. However, additional security measures identified during modeling threat must be implemented within the stipulated timeframe to maintain certification.

- Level 2 (Safe to fly) —Indicates advanced security protocols and full compliance with basic and critical mission requirements. The evaluation process reveals no critical threats to the target system.

The certifying entity will establish the minimum overall risk threshold for each mission type. This study aims to establish an open-source methodology, granting each entity the autonomy to define criteria. However, as a general model, we suggest the following classification:

$$\mathrm{R}isk_{\mathrm{Maturity}} = \begin{cases} \text{Level 0} & 90 \leq Risk_{\mathrm{overall}} \leq 100 \\ \text{Level 1} & 70 \leq Risk_{\mathrm{overall}} \leq 89 \\ \text{Level 2} & 00 \leq Risk_{\mathrm{overall}} \leq 69 \end{cases} \tag{5.9}$$

Device certification hinges on its maturity adequacy. Failure to meet this requirement will result in denial of certification. Nonetheless, the assessment report will outline the indispensable security prerequisites for achieving the minimum required security level for the specified operation.

For devices meeting the minimum acceptable standards, issuance of a preliminary flight authorization report is recommended. This report will detail the requirements for achieving a higher security level.

As a result of the security evaluation process, a cybersecurity label is generated. It's important to emphasize that this labeling approach must consider the specific context of the scenario being assessed and the certification procedure itself. Bases from the Common Criteria (CC) methodology, three primary factors are taken into consideration for inclusion in the designation:

- Target of Evaluation (TOE): Within the framework of CC, a TOE encompasses a collection of software, firmware, and/or hardware, potentially accompanied by associated guidance. In our context, the TOE also encompasses the protocol under examination and the testing environment.
- Protection Profiles (Levels of Security):In this case designated as levels 0, 1, 2 these profiles delineate the level of security corresponding to the risk posed by the scenario being evaluated.
- Certification entity: consists of the device's certification authority

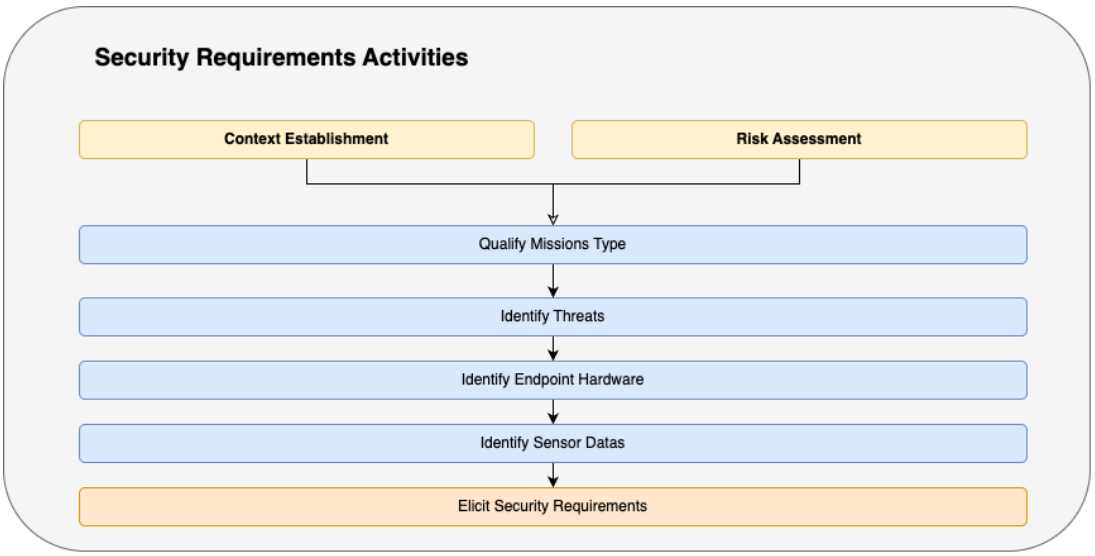
This label could include a digital representation (e.g., NFC tag or a QR code) to ease the access to the latest version of the certificate.

5.1.4 Security Requirements

The purpose of this step is define the method to certifying entity identify security requirements satisfactorily. As mentioned previously, there is currently no comprehensive security requirements engineering framework available for IoD environments (CHOUDHARY *et al.*, 2018b), since the nature of IoD is quite different from classical software systems due to the heterogeneity and adaptability characteristics of the IoD that result from the addition of the physical layer.

We extend on the basis of Requirements Engineering (RE) methodologies by integrating key security elements such as asset identification, security goals definition, threat modeling, and risk assessment each adapted to reflect the unique operational context of IoD, including layered control, autonomous coordination, and decentralized zone management. Central to this process is the adoption of the misuse case technique, as introduced by (SINDRE; OPDAHL, 2005), which complements traditional use case modeling by capturing scenarios that intentionally violate expected system behaviors. Our proposal is based on five activities, as presented in detail in Figure 6.

Figure 6 – Requirements Activities



Source: Elaborated by the author.

- Qualify Mission Type: This initial phase consolidates information derived from the Context Establishment and Risk Assessment phases. This classification informs subsequent security decisions by aligning them with the level of exposure, autonomy, and communication dependencies inherent to the mission.
- Identify Threats: In this activity, we systematically identify threats applicable to the IoD system. Threats are categorized into three primary domains: Communication Threats, Environment Threats, Drone-Specific Threats. Each identified threat contributes to shaping

the security posture required. Threat categorization should be performed based on the context presented in Chapter 4

- Identify Endpoint Hardware: IoD systems depend on various physical endpoints, including base stations, routers, embedded controllers, and smart gateways. This phase focuses on cataloging and validating the hardware components within the IoD infrastructure, emphasizing the use of authenticated and certified components to reduce supply chain attacks and physical compromise.
- Identify Sensor Data: Given that drones interact with the physical world primarily through sensors and actuators, this activity identifies the characteristics of all sensing components (e.g., cameras, altimeters, LIDARs, GPS receivers).
- Elicit Security Requirements: The final activity synthesizes all prior analyses to elicit formalized security requirements.

Table 5 illustrates the way in which the proposed process is applied to the IoD, which explains the input, technique, output and name of the activity. Each activity contributes to a collective whole, and its results can be used for both the preceding and succeeding activities. Where applicable, it is also recommended to follow the security standards (e.g. ISO/IEC 27000, ISO/IEC 27001) . The certifying entity needs to review each activity and may propose changes if and where required. Having completed the sequence of prescribed activities, the entity will be able to obtain a set of the desired security requirements.

Table 5 – Workflow Process for Security Requirements in IoD Systems

Activity	**Input**	**Technique**	**Output**
Qualify Mission Type	Operational profile, context model, mission objectives	Classification heuristics, risk correlation	Categorized list of IoD mission types and associated critical assets
Identify Threats	Mission types, preliminary asset list	Misuse cases, threat modeling	Structured list of threats (communication, environment, drone-specific)
Identify Endpoint Hardware	Drone architecture, control station infrastructure, vendor documentation	Device profiling, authentication validation	Verified list of hardware endpoints and trusted vendors
Identify Sensors data	Types of onboard sensors, communication channels (e.g., RF, LTE, 5G)	Protocol analysis, communication stack mapping	List of sensor types and their associated transmission protocols
Elicit Security Requirements	Output of all preceding activities A1 to A4	Structured analysis based on mandatory categories	Finalized list of security requirements

Considering the complexity of the IoD architecture, our proposal is based on eight categories of security requirements, as shown in Table 6, which must be implemented to obtain certification. The level of complexity in each category may vary depending on the type of mission to which the module will be subjected, therefore, based on threat modeling, it is up to the certified entity to define the specific requirements for each module. The mandatory categories are detailed below.

- **Authentication**: In the domain of the IoD, the security requirements for authentication and integrity are paramount, given the context of communication between different devices at different layers and protocols. Specifically in the context of UAVs, due to resource constraints as described by (LI *et al.*, 2021), authentication schemes must be extremely lightweight to minimize computational overhead and data transfer requirements, ensuring efficient and secure communication between drones, ZSPs and other systems (LEI *et al.*, 2021). The verification of data integrity and authenticity is equally critical, ensuring that critical information, such as configuration files or flight plans, has not been tampered with by unauthorized parties (ALLADI *et al.*, 2020).

- **Access Control**: The majority of IoD applications is real-time-based, and IoD customers generally expect to receive real-time data from drones that are part of a specific flight area. However, this could lead to a serious security vulnerability if users are permitted to have

direct access to real-time data from flying drones. Data collected in different applications requires protection to meet the access control requirement of the IoD. If not, any corrupted unit could render the whole IoD susceptible. In this context access control protocols is necessary in a wide variety of situations; for example, when a device allows for diferents modes/permissions of interaction, one for end-to-end layer behavior and one for service layer, a rudimentary form of access control is needed. (DAS *et al.*, 2021).

- **Network Security**: The IoD ecosystem being large and densely connected, requires proper network connection mechanisms to maximize the positive impact of the technology. If the network fails, all other security measures are compromised, affecting the entire IoD ecosystem. As highlighted (YANG *et al.*, 2022), unsecured internet connections, particularly over WiFi and wireless networks, are frequently used for communication within the UAV network. Several works highlight the use of 5g (IRSHAD *et al.*, 2021) and 6g (RAJA *et al.*, 2022) mobile networks for the efficient implementation of IoD networks. In this context is necessary to think about encompassing the drone's behavior in adverse situations, the confidentiality of communication between network nodes, and privacy. For instance, in a critical application, drones equipped with sensors collect data, which is then transmitted to a central server for analysis. Ensuring the security of this wireless communication is crucial to prevent unauthorized access to sensitive data, thereby safeguarding intellectual property and operational secrets.

- **Data security**: In traditional industrial environments, availability and integrity are often prioritized over confidentiality due to their measurable economic impacts. However, this perspective is not sustainable in the context of smart cities, where the challenges of data security are more complex and multifaceted. The challenges in this domain relate to three colliding factors: Firstly, due to the heterogeneity of devices, data security mechanisms need to be able to operate with extremely few resources. Secondly, due to the criticality of some IoD devices especially the drones, the data security requirements are very high. With the high data transmission rate generated, data privacy is called into question, for example it becomes possible to create detailed profiles of users, putting their privacy at risk (SOLANGI *et al.*, 2018). In such scenarios, employing data anomalization strategies becomes crucial to protect sensitive information while still allowing for the efficient operation of IoD systems.

- **Resilience**: In IoD, ensuring resilience is crucial for maintaining system operations even when parts of the system are compromised. This involves employing security technologies should provide the capability to continue normal system operations if parts of the system are considered compromised. For instance, if a drone's communication module is compromised, the system should be able to reroute tasks to other components or employ alternative communication channels to ensure uninterrupted service. This resilience can be achieved through three key strategies identified by Laszka et al (LASZKA *et al.*, 2020).: redundancy,

diversity, and hardening. Redundancy involves deploying additional components to absorb failures, diversity ensures that different components or communication methods are used to minimize shared vulnerabilities, and hardening strengthens individual components against potential threats.

- **Monitoring**: Dynamic monitoring of behavior in a system is an effective way to detect and respond to malicious activity, and systems that provide these capabilities are commonly known as Intrusion Detection Systems (IDSs). In IoD domain, two key security requirements stand out: the capability to monitor infrastructure and the ability to respond to both known and unknown threats as they arise. This emphasis on security is particularly important in the IoD context due to the integration with older, less secure devices into the network. These devices may not always be updated with the latest security patches to protect against known vulnerabilities, necessitating continuous monitoring to safeguard against potential threats.

- **Physical Security**: Hardware is more difficult and more costly to compromise and subvert than software. Therefore hardware security can provide a robust foundation for embedded device security. On the other hand, hardware that contains backdoors or undocumented debug features can completely compromise the security of the entire device.

- **Regulation and standard**: In order to protect the security and privacy of citizens, each country establishes a series of regulations and laws on how devices should be operated. In this context, the device under analysis must comply with the recommendations on Cybersecurity of 5G Networks, the General Data Protection Regulation (GDPR), the NIS Directive (involves the aviation sector), the Electronic Communications Code and Security Laws Cyber (involves cybersecurity certification of devices and applications) covering different aspects of security and privacy, all directly or indirectly connected to aspects of the drone Internet architecture.

5.1.5 Certification Monitoring & review

The proposed certification methodology encompasses the entire operational lifespan of an IoD node.

- **Manufacturing** The certificate's lifecycle and the system's composed by different stages. The device's lifecycle begins with the manufacturing phase, in which the device is produced, programmed, and configured so it can be later used in a IoD enviroment. This phase our framework can be used to certification process in which the device is evaluated and certified based on principle secure-by-design. According (SEQUEIROS *et al.*, 2020) the Security-by-Design paradigm, security should be monitored and optimized at all phases of the SDLC, and particularly during the Requirements, Design, implementation, and Testing

Table 6 – Standard security requirements

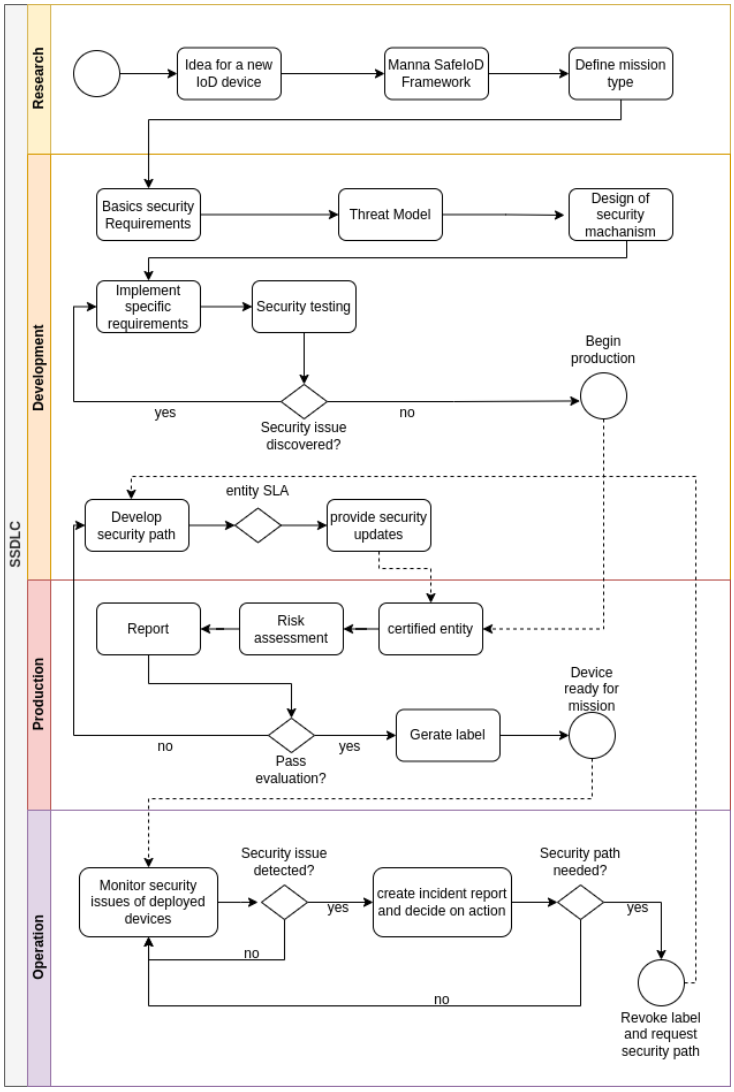
	Requirement	Refs
Authentication	Lightweight Authentication Schemes	(LEI *et al.*, 2021)
	Data Integrity and Authenticity	(SUN *et al.*, 2020)
	Key Distribution and Management	(JAN; ABBASI; ALGARNI, 2021)
	Mutual Authentication	(JAN; ABBASI; ALGARNI, 2022)
	Non-Repudiation	(RIOS; JUNG; JOHNSON, 2022)
Access Control	Fine-grained	(ZHUO; ZHANG, 2023)
	Privacy-preserving	(CHEN *et al.*, 2020)
	Environment transparency	(BERA; DAS; SUTRALA, 2021)
	Secure Certificate	(KHAN *et al.*, 2021)
Network Security	Network isolation	(GORREPATI; GUNTUR, 2021)
	Timeliness	(WANG *et al.*, 2020)
	Availability (jamming, DoS, etc)	(GHELANI; GHARIA; EL-OCLA, 2024)
	Overhead minimization	(TANVEER *et al.*, 2023)
	Mobile transmission security	(IRSHAD *et al.*, 2021)
	Security policy enforcement	(CRACKNELL, 2017)
	Blockchain approach	(RAJA *et al.*, 2022)
Data Security	Anomalization techniques	(USMAN *et al.*, 2019)
	Data flow control	(SINGHAL; RAHUL, 2019)
	Secure external data storage	(ULLAH *et al.*, 2022)
	Data loss mitigation	(ZHUO; ZHANG, 2023)
	Data encryption	(OZMEN; BEHNIA; YAVUZ, 2019)
Resilience	Continuous operation	(SINCHE *et al.*, 2018)
	Operation intermittent	(SINCHE *et al.*, 2018)
Monitoring	Threat detection and response	(GARG *et al.*, 2018)
	Handle heterogeneous sources	(WANG *et al.*, 2017)
	Infrastructure monitoring	(FESENKO *et al.*, 2022)
Physical Security	Side-Channel detection	(PRATES *et al.*, 2020)
	Fault injection detection	(GANGOLLI; MAHMOUD; AZIM, 2022)
	Encryption Engines	(SAMANTH; KV; BALACHANDRA, 2023)
	Firmware Protection	(TSAUR; CHANG; CHEN, 2022)
	Hardware-Based Roots of Trust	(EHRET *et al.*, 2020)
Regulation	Security policy enforcement	(CRACKNELL, 2017)
	Protection legislation compliance	(CHO, 2013)
	Standard compliance	(CRACKNELL, 2017)

phases. Figure 7 illustrates the recommended application of the framework in the IoD device design process.

After the manufacturing the bootstrapping phase usually includes a set of processes by which an IoD device joins a network in a specific domain e.g., surveillace (MCNEAL, 2016), rescue (KARACA *et al.*, 2018), delivery (PUGLIESE; GUERRIERO; MACRINA, 2020). During this phase, the device is configured for a specific context and the context information should be embedded label (which should be up-to-date).

- **Operation** During the operation phase, the device delivers its intended functionality in the target environment. In this stage, continuous monitoring is essential to detect threats that may not have been identified during the initial certification—particularly emerging

Figure 7 – BPMN of the proposed framework



Source: Elaborated by the author.

threats such as zero-day vulnerabilities. The Manna SafeIoD framework does not prescribe a specific mechanism for active vulnerability detection; rather, it is the responsibility of the certifying authority to define and implement appropriate monitoring procedures. These procedures must be explicitly stated on the certification label and transparently communicated to the IoD device's manufacturer or supplier. Upon detection of a new threat, the manufacturer may determine that a software or hardware update is required. If such updates introduce substantial changes—particularly those affecting the device's security posture—the device may be required to undergo a new certification cycle, and its existing security level or label may be suspended or revoked. To ensure compliance with operational security requirements, the device shall be subject to active runtime monitoring via the Manna SafeIoD governance architecture, detailed in the following section.

- **Decommissioning** Occurs when the IoD device is no longer needed by the consumer or

reaches the end of its life cycle and is no longer supported by the provider, a series of processes must be executed. These include revoking certification for the device model, securely erasing all consumer and product-related files, both from the device and the certifying servers, revoking any cryptographic materials, and disassociating the device from consumer accounts, if the consumer still maintains an account with the provider.

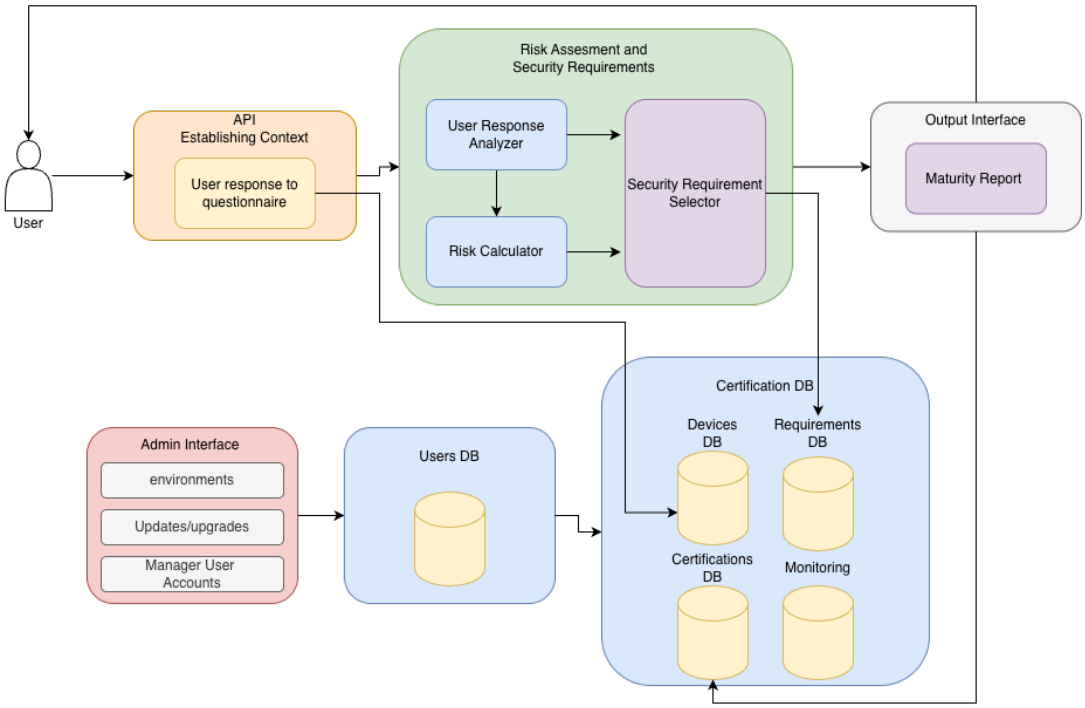
5.2 Framework Implementation

Aligned with the theoretical foundations discussed earlier, this section introduces the process used to develop a minimum viable prototype (MVP) of the framework, enabling the design and implementation of secure IoD devices and smart applications, as outlined in Chapter 2.

The sections that follow provide an overview of the framework's structure and describe the modules contained within each SafeIoD component. We also summarize the implementation of the command-line tool that supports user interaction with the framework.

Figure 8 presents the high-level software architecture of the proposed system. The annotated elements correspond to the conceptual stages defined previously in Figure 4, establishing a clear relationship between the theoretical model and its practical realization.

Figure 8 – High-level architecture of the SafeIoD.



Source: Elaborated by the author.

The proposed architecture consists of five functional modules: (1) the Establishing

Context module, which provides the user interface for data acquisition through questionnaires; (2) the Risk Assessment and Security Requirements module, responsible for analyzing user responses, calculating risk levels, and selecting appropriate security requirements; (3) the Certification Database, which manages persistent storage of devices, requirements, certifications, and monitoring data; (4) the Administrative Interface, enabling system configuration, environment management, updates, and user account administration; and (5) the Output Interface, which generates comprehensive maturity reports based on the assessment results.

5.2.1 Establishing Context (User Interface)

The Establishing Context module represents the initial step of the Manna SafeIoD certification workflow, guiding users through the systematic characterization of deployment conditions and operational requirements. As illustrated in Figure 9, this module is implemented through a Command-Line Interface (CLI) that structures the context elicitation process into a hierarchical questionnaire system.

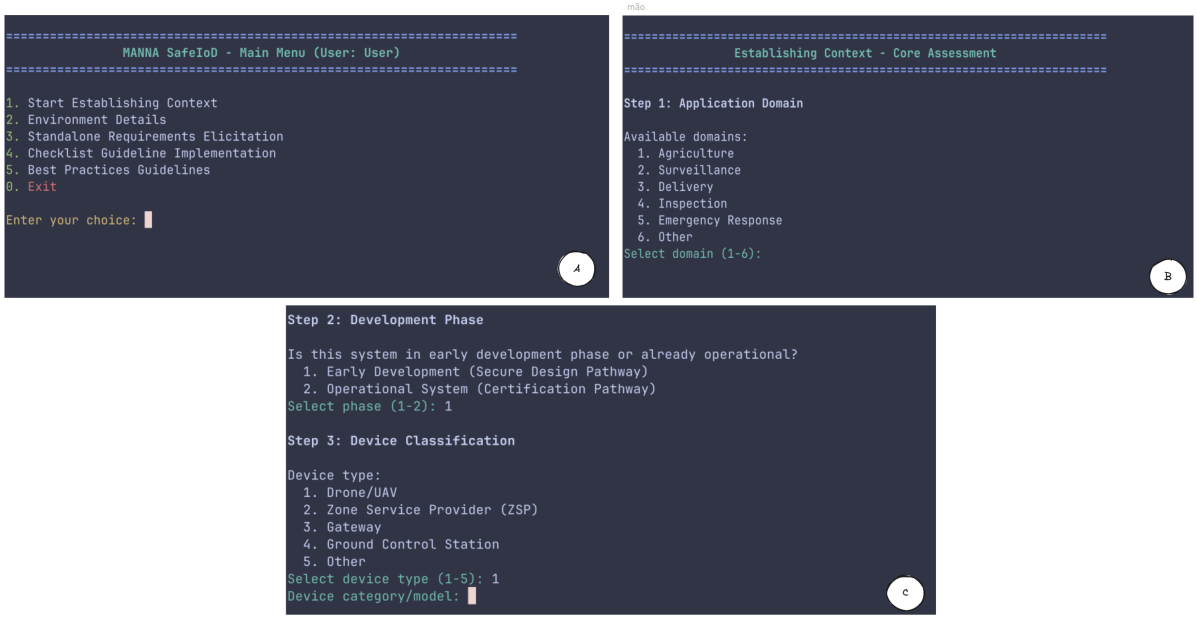


Figure 9 – SafeIoD CLI

Upon successful authentication, users are presented with a main menu offering five primary functionalities: (1) Start Establishing Context — initiating the core secure design or certification process; (2) Environment Details — managing deployment environment configurations; (3) Standalone Requirements Elicitation — enabling manual selection of security requirements for advanced users; (4) Checklist Guideline Implementation — providing requirement checklists based on previous assessments; and (5) Best Practices Guidelines — offering domain-specific security recommendations. The context establishment workflow follows a structured interrogation methodology. Initially, users must specify the application domain and declare whether the

IoD system is in its early development phase (secure design pathway) or represents an existing operational system (certification pathway). This distinction enables the tool to adaptively tailor the subsequent questioning sequence and assessment criteria. The questionnaire employs a conditional branching logic to optimize information gathering while minimizing user burden. Core questions systematically address the following dimensions:

- Device Classification: Type and category of IoD component under evaluation (drone, ZSP, gateway, ground control station).
- Mission Profile: Target operation type and criticality level.
- Data Handling Characteristics: Information storage requirements, data sensitivity classification (normal, sensitive, critical), and cloud integration dependencies.
- Network Topology: Type and frequency of interactions with Zone Service Providers (ZSPs) and other network entities.
- Regulatory Context: Applicable regulatory frameworks and compliance requirements (e.g., ANAC, FAA, EASA, GDPR, LGPD).
- Threat Exposure: Physical and cyber threat landscape, including potential adversarial access scenarios

Below are tables with the formal definition of the type of each of the data captured in this phase.

The mission profile captures operational context through a structured questionnaire. Table 7 defines the complete input schema with valid ranges and data types.

Table 7 – Mission Profile Input Schema

Field	**Type**	**Valid Values**	**Description**
`domain`	Enum	{Agriculture, Surveillance, Delivery, Inspection, Emergency, Military, Other}	Application domain
`phase`	Enum	{Development, Operational}	System lifecycle phase
`device_type`	Enum	{Drone, ZSP, Gateway, GCS, Cloud}	IoD component category
`mission_criticality`	Integer	[1–5]	1=Low, 5=Critical
`data_sensitivity`	Enum	{Non-Sensitive, PII, Critical}	Data classification level
`stores_data`	Boolean	{true, false}	Local data storage capability
`cloud_integration`	Boolean	{true, false}	Cloud service dependency
`zsp_interaction`	Enum	{None, Periodic, Continuous}	ZSP communication frequency
`regulatory_framework`	List[Enum]	{FAA, EASA, ANAC, GDPR, LGPD, ISO27001, MIL-STD}	Applicable regulations
`environment`	Enum	{Indoor, Urban, Rural, Maritime, Military}	Deployment environment
`airspace_class`	Enum	{Controlled, Uncontrolled, Restricted}	Airspace classification

Each IoD component is characterized by technical attributes that influence threat applicability and security control feasibility. Table 8 defines the device specification structure.

Table 8 – Device Specification Input Schema

Field	Type	Valid Values	Description
`device_id`	String	UUID format	Unique device identifier
`manufacturer`	String	Free text	Device manufacturer
`model`	String	Free text	Device model designation
`firmware_version`	String	Semantic versioning	Current firmware version
`comm_protocols`	List[Enum]	{WiFi, LTE, 5G, LoRa, ADS-B, MAVLink}	Supported protocols
`sensors`	List[Enum]	{GPS, Camera, LIDAR, Altimeter, IMU, Thermal}	Onboard sensors
`compute_class`	Enum	{Constrained, Moderate, High}	Computational capability
`has_tpm`	Boolean	{true, false}	Hardware security module presence
`has_secure_boot`	Boolean	{true, false}	Secure boot capability
`encryption_support`	List[Enum]	{AES-128, AES-256, ChaCha20, ECC, RSA}	Supported cryptographic algorithms

The IoD network is represented as a directed graph $G(V,E)$ with the following JSON structure:

Algorithm 2 – Network Topology JSON Schema.

```
{
  "topology_id": "string (UUID)",
  "nodes": [
    {
      "node_id": "string (UUID)",
      "device_spec": "<Device Specification Object>",
      "mission_profile": "<Mission Profile Object>"
    }
  ],
  "edges": [
    {
      "source": "string (node_id)",
      "target": "string (node_id)",
      "protocol": "enum (WiFi|LTE|5G|LoRa|Wired)",
      "encrypted": "boolean",
      "bidirectional": "boolean",
      "trust_level": "float [0.0-1.0]"
    }
  ]
}
```

The questionnaire implements intelligent filtering mechanisms whereby subsequent questions are conditionally presented based on prior responses. For instance, if a user indicates that the device will not store information, data-related questions are automatically bypassed, streamlining the assessment process. All user inputs are processed by the Input Generator component, which performs data extraction, normalization, and validation. The extracted context parameters are then persisted in the system database, enabling session continuity and allowing users to resume incomplete assessments. Simultaneously, this structured context data feeds directly into the Risk Assessment module, where it informs threat modeling, risk calculation, and security requirement selection processes as defined in Section 5.

5.2.2 Risk Calculator

The Risk Assessment and Security Requirements module constitutes the analytical core of the Manna SafeIoD framework, operationalizing the theoretical risk assessment methodology detailed in Section 5.1.2. This module receives structured context data from the Establishing Context module and executes a multi-stage risk calculation process that culminates in the selection of appropriate security requirements and the determination of device maturity levels.

The module comprises two primary sub-components: (1) the **User Response Analyzer**, which processes and normalizes input data from the context questionnaire, extracting relevant security parameters such as mission criticality, data sensitivity classification, deployment environment characteristics, and regulatory constraints; and (2) the **Risk Calculator**, which implements the mathematical risk propagation model to compute device-level and system-level risk metrics.

The Risk Calculator implements a graph-based risk propagation algorithm that treats the IoD ecosystem as a directed graph $G = (V, E)$, where vertices V represent IoD modules (drones, ZSPs, gateways, cloud services) and edges E represent communication or dependency relationships between modules. Algorithm 3 presents the core risk assessment procedure.

The algorithm operates in five distinct phases, corresponding to the theoretical steps outlined in Section 5.1.2:

Phase 1: Module-level risk estimation. For each IoD component, the algorithm identifies applicable threats from the threat database $\mathscr{T}$ based on device type, firmware characteristics, and operational context. The maximum CVSS score is extracted and combined with the count of implemented security controls and the calculated impact value to produce the estimated risk R_i for module i according to Equation (3).

Each threat entry follows the structure defined in Table 9.

Table 9 – Threat Entry Schema

Field	**Type**	**Description**
`threat_id`	String	Unique threat identifier (e.g., `IOD-COMM-001`)
`category`	Enum	{Communication, Environment, Drone, Provider, Physical, Cyber}
`subcategory`	String	Specific threat classification (e.g., `Jamming`, `Spoofing`)
`cvss_base`	Float [0.0–10.0]	CVSS v3.1 Base Score
`cvss_vector`	String	CVSS vector string (e.g., `L/PR:N/UI:N/S:U/C:H/I:H/A:H`)
`applicable_devices`	List[Enum]	Device types vulnerable to this threat
`applicable_protocols`	List[Enum]	Protocols through which threat manifests
`mitigating_controls`	List[String]	Security control identifiers that mitigate this threat
`propagation_factor`	Float [0.0–1.0]	Likelihood of lateral propagation (ψ coefficient base)

Table 10 illustrates representative entries from the threat database.

Table 10 – Sample Threat Database Entries

Threat ID	Category	Subcategory	CVSS	Applicable Devices	Mitigating Controls	Prop. Factor
IOD-COMM-001	Communication	GPS Spoofing	8.1	Drone, GCS	SC-AUTH-003, SC-NET-007	0.3
IOD-CYBER-003	Cyber	Firmware Tampering	9.0	Drone, ZSP, Gateway	SC-PHY-004, SC-PHY-005	0.7
IOD-PHYS-002	Physical	Deauthentication Attack	7.5	Drone, GCS	SC-NET-002, SC-NET-006	0.5

Phase 2: Inter-module contagion coefficient calculation. For each communication or dependency edge in the topology graph, the algorithm computes the threat transmission coefficient $C_{i \to j}$, representing the degree to which a compromised module i can propagate risk to its neighbor j. This calculation considers the overlap between threat vectors, protocol vulnerabilities, and access control mechanisms at the interface boundary.

Phase 3: Total infection coefficient computation. Using Dijkstra-based path enumeration (LEVNER; TSADIKOVICH, 2024), the algorithm identifies all directed paths from potential risk sources to each module in the system (ARAT; AKLEYLEK, 2023). The total infection coefficient C_j for module j is computed by summing the products of contagion coefficients along each path, as formalized in Equation (5).

Phase 4: Impact and probability estimation. For each module, the algorithm calculates the cumulative impact factor F_i by aggregating the weighted probabilities of security events across all identified threats. The probability $P_i(t)$ incorporates both the intrinsic exploitability of threat t and the effectiveness of existing security measures, as defined in Equations (6) and (7).

Phase 5: System-level risk aggregation and requirement selection. The overall system risk R_{system} is computed by integrating module risks, impact factors, and infection coefficients according to Equation (8). Subsequently, each module's risk classification (None, Low, Medium, High, Critical) determines the set of mandatory security requirements $\mathscr{SR}_i$ from the eight categories defined in Table 6. The union of all module-specific requirements forms the comprehensive security requirement set for the entire IoD deployment.

The Risk Calculator module persists all computed metrics to the Certification Database, enabling traceability and supporting the subsequent generation of maturity reports and compliance documentation. The selected security requirements are forwarded to the Security Requirement Selector component, which structures them according to the stakeholder-specific format and regulatory framework identified during context establishment.

Algorithm 3 – IoD Risk Assessment and Propagation

Require: Context parameters C, IoD topology graph $G(V,E)$, threat database $\mathscr{T}$
Ensure: Overall system risk R_{system}, module risk vector $\mathbf{R}$, security requirements $\mathscr{SR}$

$\mathbf{R} \leftarrow \emptyset$
$\mathscr{SR} \leftarrow \emptyset$
for each module $i \in V$ **do**
  $DT_i \leftarrow \text{IdentifyThreats}(i, C, \mathscr{T})$
  $\max_{cvss} \leftarrow \max(\{cvss(t) : t \in DT_i\})$
  $SC_i \leftarrow \text{CountSecurityControls}(i, C)$
  $I_i \leftarrow \text{CalculateImpact}(i, C)$
  $mt_i \leftarrow \text{GetModuleType}(i)$
  $R_i \leftarrow mt_i \times \frac{\max_{cvss}}{SC_i} \times I_i$
  $\mathbf{R}[i] \leftarrow R_i$
end for
$\mathbf{C} \leftarrow \text{InitializeContagionMatrix}(|V|)$
for each edge $(i, j) \in E$ **do**
  $C_{i \to j} \leftarrow \text{CalculateThreatCoefficient}(i, j, DT_i, DT_j)$
  $\mathbf{C}[i][j] \leftarrow C_{i \to j}$
end for
for each module $j \in V$ **do**
  $\mathscr{L}_j \leftarrow \text{FindAllPaths}(G, V, j)$
  $C_j \leftarrow 0$
  for each path $l \in \mathscr{L}_j$ **do**
    $C_l \leftarrow 1$
    for each edge $(u, v) \in l$ **do**
      $C_l \leftarrow C_l \times \mathbf{C}[u][v]$
    end for
    $C_j \leftarrow C_j + C_l$
  end for
end for
for each module $i \in V$ **do**
  $F_i \leftarrow 0$
  for each threat $t \in DT_i$ **do**
    $th_i(t) \leftarrow \text{GetThreatValue}(t, i)$
    $S_i(t) \leftarrow \text{CalculateNonCorrelation}(t, i, SC_i)$
    $P_i(t) \leftarrow w_1 \cdot T_i(t) + w_2 \cdot S_i(t)$
    $F_i \leftarrow F_i + th_i(t) \cdot P_i(t)$
  end for
end for
$R_{system} \leftarrow \sum_{j \in V} F_j \cdot \mathbf{R}[j] \cdot C_j$
for each module $i \in V$ **do**
  $category \leftarrow \text{ClassifyRisk}(\mathbf{R}[i])$
  $\mathscr{SR}_i \leftarrow \text{SelectRequirements}(category, C, DT_i)$
  $\mathscr{SR} \leftarrow \mathscr{SR} \cup \mathscr{SR}_i$
end for
return R_{system}, $\mathbf{R}$, $\mathscr{SR}$

5.2.3 Security Requirements Generator

The Security Requirements Generator module implements the elicitation approach described in Section 5.1.4. For background and an in-depth discussion of IoD security requirements, refer to (SALILI *et al.*, 2024; SEZGIN; BOYACI, 2024; YAHUZA *et al.*, 2021). This module takes as input the normalized context attributes and the risk indicators produced by the Risk Assessment module, and translates them into concrete security requirements derived from the eight

mandatory categories described in Table 6. Its internal design is composed of three cooperating subcomponents that together execute the full requirement selection and consolidation workflow.

- **User Response Analyzer:** This component performs multi-level analysis on user responses, distinguishing between binary indicators (yes/no answers), categorical classifications (e.g., mission type: surveillance, delivery, inspection), and sensitivity gradations (e.g., data classification: normal, sensitive, critical). The analyzer implements a rule-based inference engine that correlates user inputs with the five security requirement elicitation activities presented in Figure 6. The extracted parameters are normalized and encapsulated in a structured requirements context object $RC = \{mission, threat\_exp, hardware, data, architecture\}$, which serves as input to the Security Requirements Selector component.

- **Security Requirements Selector** implements a constraint-based mapping algorithm that systematically selects appropriate security requirements from a curated repository aligned with the eight mandatory categories: Authentication, Access Control, Network Security, Data Security, Resilience, Monitoring, Physical Security, and Regulation (as defined in Table 6).

  Algorithm 4 formalizes the selection procedure. The algorithm iterates through the eight security categories, applying context-aware filters and risk-based prioritization to construct a tailored requirement set $\mathscr{SR}_i$ for each module i in the IoD ecosystem.

Algorithm 4 – Security Requirements Selection

Require: Requirements context RC, module risk vector $\mathbf{R}$, threat set DT, requirement database $\mathscr{RDB}$
Ensure: Module-specific security requirements $\mathscr{SR}$

$\mathscr{SR} \leftarrow \emptyset$
$categories \leftarrow$ {Auth, Access, Network, Data, Resilience, Monitor, Physical, Regulation}
for each module i in IoD topology **do**
  $risk\_class_i \leftarrow$ ClassifyRisk($\mathbf{R}[i]$)
  $\mathscr{SR}_i \leftarrow \emptyset$
  for each category $cat \in categories$ **do**
    $base\_reqs \leftarrow$ GetBaseRequirements($cat, \mathscr{RDB}$)
    $filtered\_reqs \leftarrow$ ApplyContextFilters($base\_reqs, RC, i$)
    $prioritized\_reqs \leftarrow$ PrioritizeByRisk($filtered\_reqs, risk\_class_i$)
    $threat\_reqs \leftarrow$ MapThreatsToRequirements($DT_i, cat, \mathscr{RDB}$)
    $regulatory\_reqs \leftarrow$ GetRegulatoryRequirements($RC.jurisdiction, cat$)
    $merged\_reqs \leftarrow prioritized\_reqs \cup threat\_reqs \cup regulatory\_reqs$
    $\mathscr{SR}_i \leftarrow \mathscr{SR}_i \cup$ RemoveDuplicates($merged\_reqs$)
  end for
  $\mathscr{SR}_i \leftarrow$ ValidateCompleteness($\mathscr{SR}_i, risk\_class_i$)
  $\mathscr{SR} \leftarrow \mathscr{SR} \cup \{(i, \mathscr{SR}_i)\}$
end for
return $\mathscr{SR}$

The requirement database $\mathscr{RDB}$ maintains a structured repository of security requirements sourced from established standards (ISO/IEC 27001, NIST Cybersecurity Framework), domain-specific best practices (CRACKNELL, 2017), and peer-reviewed IoD security

research (as cataloged in Table 6). Each requirement entry includes metadata specifying applicable IoD component types (drone, ZSP, gateway, cloud service), implementation complexity ratings, and interdependencies with other requirements.

- **Requirements Aggregator:** consolidates individual module requirements into a comprehensive, system-level security specification. When multiple modules generate overlapping requirements (e.g., mutual authentication between drone and ZSP appears in requirements for both components), the aggregator merges them into unified, bidirectional requirements while preserving module-specific implementation details. he aggregator identifies cross-module dependencies using a directed acyclic graph (DAG) representation (LIANG *et al.*, 2023). For instance, if Module A requires encrypted communication channels and Module B mandates key management infrastructure, the aggregator ensures both requirements are present and properly sequenced in the implementation roadmap. The aggregator also persists the complete requirement provenance chain—linking each requirement to its originating threat, risk score, context parameter, and applicable security standard—enabling full traceability throughout the certification lifecycle.

Security controls are defined in a structured repository $\mathscr{SC}$ that maps to the eight requirement categories from Table 6. Each control entry specifies implementation characteristics and effectiveness metrics.

Table 11 – Security Control Schema

Field	**Type**	**Description**
`control_id`	String	Unique identifier (e.g., `SC-AUTH-001`)
`category`	Enum	One of eight security categories from Table 6
`name`	String	Human-readable control name
`description`	String	Implementation description
`effectiveness`	Float [0.0–1.0]	Normalized mitigation effectiveness
`compute_overhead`	Enum	{Low, Medium, High} — resource requirements
`applicable_devices`	List[Enum]	Compatible device types
`mitigates_threats`	List[String]	Threat IDs this control addresses
`implementation_alg`	String	Recommended algorithm (e.g., `AES-256-GCM`)

Table 12 presents representative security control definitions.

Table 12 – Sample Security Control Entries

Control ID	**Category**	**Name**	**Eff.**	**Overhead**	**Mitigates**	**Algorithm**
SC-AUTH-001	Authentication	Lightweight Mutual Auth.	0.85	Low	IOD-COMM-001, IOD-CYBER-001	ECDH-Curve25519
SC-NET-002	Network Security	Encrypted C2 Channel	0.90	Medium	IOD-PHYS-002, IOD-COMM-003	AES-256-GCM
SC-PHY-004	Physical Security	Secure Boot	0.95	Low	IOD-CYBER-003, IOD-CYBER-004	RSA-2048 + SHA-256

5.2.4 Output interface

The Output Interface module constitutes the presentation layer of the Manna SafeIoD framework, responsible for synthesizing assessment results into stakeholder-appropriate deliverables that support the complete device lifecycle from manufacturing through decommissioning.

For IoD systems undergoing secure-by-design evaluation during the manufacturing phase, the Output Interface generates comprehensive security specification documents structured to guide implementation teams throughout the Software Development Life Cycle (SDLC). These deliverables provide a roadmap to security requirements implementation. Guideline to monitoring and active quality The secure design output additionally includes mission-type-specific cryptographic protocol recommendations, encompassing key exchange mechanisms for point-to-point drone-ZSP communication, digital signature schemes for firmware integrity verification, and secure boot architecture guidelines aligned with hardware capabilities extracted during context establishment. Visual representations of secure communication flows, trust boundary delineations, and defense-in-depth layering strategies tailored to the identified IoD topology complete the specification package, embodying the Security-by-Design paradigm illustrated in the BPMN workflow of Figure 7.

For operational IoD devices or systems undergoing certification evaluation, the Output Interface produces formal maturity reports aligned with the three-level classification scheme detailed in Section 5.1.3. The certification report opens with a compliance assessment summary that comprehensively evaluates the device's conformity with security requirements for the specified mission type, documenting all satisfied, partially satisfied, and unsatisfied requirements with supporting evidence traced back through the risk assessment phase.

For devices achieving suboptimal maturity levels, the report includes a prioritized gap analysis enumerating specific deficiencies that prevent higher certification, along with a remediation roadmap specifying required security enhancements ordered by criticality and implementation complexity.

5.2.5 System components

The CLI is implemented in GoLang and supports cross-platform execution on Windows and Linux operating systems. The modular architecture enables parameter customization to optimize performance and facilitates feature extensibility, such as integration of additional risk metrics or alternative threat modeling databases. A PostgreSQL database maintains all framework data, including user credentials, assessment requests, and computed security metrics.

A fundamental design principle of the Manna SafeIoD framework is its modular architecture, which enables flexible deployment across heterogeneous IoD certification scenarios.

The framework decomposes the certification process into four independently deployable modules: Context Establishment (Module A), Risk Assessment (Module B), Security Require-

ments Engineering (Module C), and Certification Monitoring & Review (Module D). This decomposition yields three primary advantages:

Certifying entities can instantiate only the modules required for their specific use case. For lightweight pre-deployment assessments, a minimal configuration comprising Modules A and B suffices to generate preliminary risk scores without full security requirements elicitation. Conversely, comprehensive certification for mission-critical military applications activates all four modules with enhanced parameter configurations.

Each module maintains well-defined interfaces and can be updated independently without affecting adjacent components. When new threat categories emerge (e.g., novel GPS spoofing variants), only Module B's threat database requires modification. Similarly, regulatory framework updates (e.g., new EASA directives) propagate exclusively through Module C's requirements repository. This isolation minimizes regression testing scope and accelerates patch deployment cycles—critical for maintaining certification validity in rapidly evolving threat landscapes.

The framework supports both scaling dimensions. Horizontal scalability enables parallel processing of multiple certification requests by instantiating additional module replicas behind a load balancer—essential for certification authorities managing large device fleets.

To illustrate modular adaptability, we present three representative deployment configurations aligned with distinct operational conditions.

Configuration 1: Resource-Constrained Civilian Drone (Agricultural Monitoring). For a single agricultural monitoring UAV operating in rural, uncontrolled airspace with minimal data sensitivity, the certifying entity deploys a streamlined configuration as shown in Table 13.

Table 13 – Module Configuration for Resource-Constrained Agricultural UAV

Module	**Status**	**Configuration Parameters**
A (Context)	Active	Simplified questionnaire (12 questions); single-device topology
B (Risk Assessment)	Active	Threat database subset (environmental + basic cyber); $\gamma_1 = 0.5$, $\gamma_2 = 0.5$ (balanced profile)
C (Requirements)	Partial	Categories limited to: Authentication, Network Security, Resilience
D (Monitoring)	Inactive	Deferred to operational phase

This configuration completes certification in approximately 15 minutes with minimal computational resources, producing a focused requirement set of 8–12 security controls appropriate for the constrained platform.

Configuration 2: Multi-Drone Urban Delivery Fleet. For a commercial delivery operator deploying 50 drones across urban zones with PII-handling capabilities and continuous ZSP interaction, the configuration expands as detailed in Table 14.

Table 14 – Module Configuration for Urban Delivery Fleet

Module	**Status**	**Configuration Parameters**
A (Context)	Active	Full questionnaire; multi-node topology graph (50 UAVs + 3 ZSPs + 2 gateways)
B (Risk Assessment)	Active	Complete threat database; network propagation analysis enabled; $\gamma_1 = 0.3$, $\gamma_2 = 0.7$ (control-centric profile)
C (Requirements)	Full	All eight categories active; GDPR/LGPD regulatory mapping enabled
D (Monitoring)	Active	Continuous vulnerability tracking; 90-day recertification cycle

This configuration requires approximately 1 hour for initial certification but provides comprehensive coverage including systemic risk propagation analysis across the fleet topology.

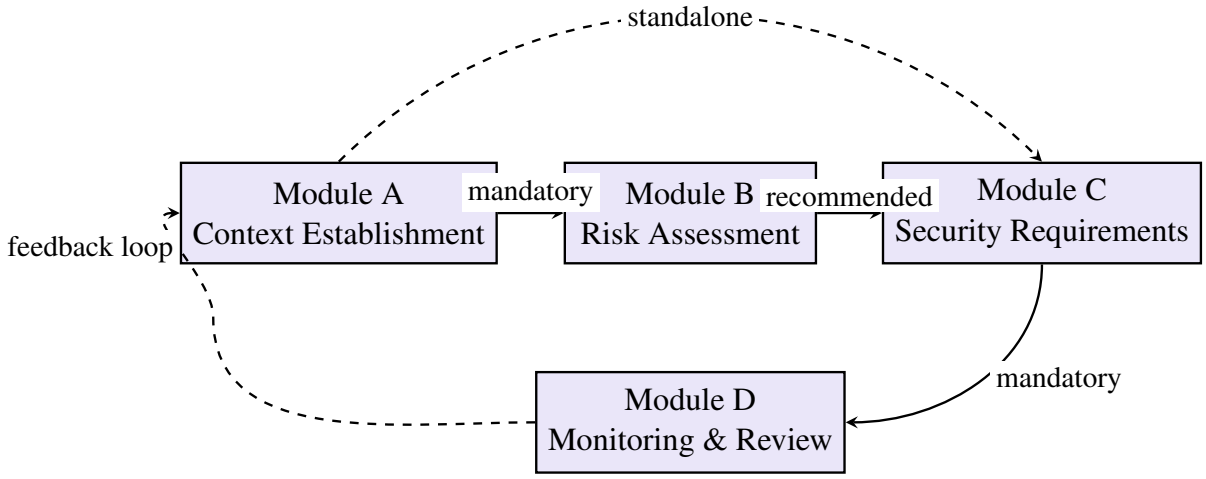
Configuration 3: Military Tactical ISR Deployment. For the tactical scenario described in Section 6.1.5, maximum security assurance necessitates full module activation with enhanced parameters as specified in Table 15.

Table 15 – Module Configuration for Military Tactical ISR

Module	**Status**	**Configuration Parameters**
A (Context)	Active	Extended questionnaire including adversarial capability assessment; classified mission profile
B (Risk Assessment)	Active	Military threat extensions; $\gamma_1 = 0.8$, $\gamma_2 = 0.2$ (threat-centric profile); mandatory propagation simulation
C (Requirements)	Full	All categories + MIL-STD-882E mapping; mandatory hardware roots of trust
D (Monitoring)	Active	Real-time threat intelligence integration; 30-day recertification cycle; incident response protocols

While modules operate with defined interfaces, certain interdependencies govern valid configurations. Module B (Risk Assessment) requires prior completion of Module A (Context Establishment) to obtain topology and mission parameters. Module C (Security Requirements) can operate in standalone mode for manual requirement selection but produces optimized outputs when fed risk indicators from Module B. Module D (Monitoring) presupposes successful completion of the initial certification cycle (Modules A$\rightarrow$B$\rightarrow$C) to establish baseline security postures against which deviations are detected.

Figure 10 – Manna SafeIoD module interdependency graph. Solid lines indicate mandatory sequential flows; the dashed upper path represents the standalone requirements generation capability, while the lower dashed path illustrates the continuous monitoring feedback loop



Source: Elaborated by the author.

These dependencies are enforced through the framework's orchestration layer, which validates configuration coherence before execution and provides diagnostic feedback when invalid module combinations are requested. The orchestration layer implements a finite state machine that tracks certification progress and ensures compliance with the workflow constraints illustrated in Figure 4.

Table 16 summarizes the valid module configurations and their corresponding use cases.

Table 16 – Valid Module Configurations and Use Cases

Module A	**Module B**	**Module C**	**Module D**	**Configuration Type**	**Primary Use Case**
●	●	–	–	Minimal Assessment	Preliminary risk screening
●	●	●	–	Standard Certification	Initial device certification
●	●	●	●	Full Lifecycle	Production deployment with monitoring
–	–	●	–	Standalone Requirements	Manual security requirements selection
●	●	–	●	Continuous Assessment	Runtime monitoring without full recertification

The modular architecture thus provides certifying entities with the flexibility to balance certification rigor against resource constraints, adapting the framework's analytical depth to match the specific requirements of each IoD deployment scenario.

CHAPTER

6

EVALUATION

To assess the practical applicability of the Manna SafeIoD framework, we designed a series of usability-oriented experiments focused on validating whether the implemented components behave consistently with the conceptual methodology introduced in Chapter 5. The overall structure of the evaluation was inspired by the experimental procedures adopted in prior works on IoT and UAS security assessment, particularly the test design strategies presented by Samaila et al. (SAMAILA *et al.*, 2020) and the operational task modeling described by Santiago (SANTIAGO, 2019). While these studies target different domains, their methodological insights provided a foundation for shaping our own evaluation protocol.

In our setup, we formulated representative usage tasks that simulate common operational scenarios in which users would interact with the SafeIoD tool. These tasks were constructed to mirror realistic decision-making processes and to enable assessment of the framework's ability to generate consistent outputs under varied contextual conditions. After completing the scenarios, the outputs and tool behavior were analyzed using three performance metrics described in the following subsections. These metrics allowed us to examine the internal coherence of the framework, the usability of the generated requirements, and the responsiveness of the implemented modules.

6.1 Experimental Setup

To evaluate both the functionality of the tool's modules and the usability of the overall workflow, we developed five test scenarios inspired by methodological approaches found in the literature, particularly in (SAMAILA *et al.*, 2020). Two scenarios targeted software-based implementations in order to validate the core operations of Manna SafeIoD and assess its ability to recommend secure coding practices. Two additional scenarios focused on hardware-oriented configurations, simulating typical industrial setups used in UAV device development. The final scenario examined a combined hardware–software configuration to evaluate the end-to-end

certification process.

These scenarios were designed to reflect diverse operational conditions: resource-constrained platforms, where the number of security requirements must be carefully minimized, and mission-critical environments—such as military applications—where broader and more stringent requirements are expected. A group of participants executed the scenarios, allowing us to observe tool behavior under realistic usage conditions. The subsections that follow describe each scenario in detail.

6.1.1 Software Implementation Test Scenario for Drone Firmware

This scenario considers a developer responsible for implementing firmware or onboard applications on a constrained UAV platform who must select suitable lightweight security algorithms. The goal is to ensure that the chosen controls comply with mission-specific security requirements and the characteristics of the operating environment.

6.1.2 Software Implementation Test Scenario for Cloud application based for ZSP integration

This scenario represents another software-oriented request, where a developer is implementing a cloud-based traffic-analysis service that integrates with the ZSPs. The application, which is designed to operate in the service layer of the IoD architecture, runs on a single-board computer or on an edge-computing platform. In this context, the developer queries the framework to obtain the security requirements applicable to this IoD service.

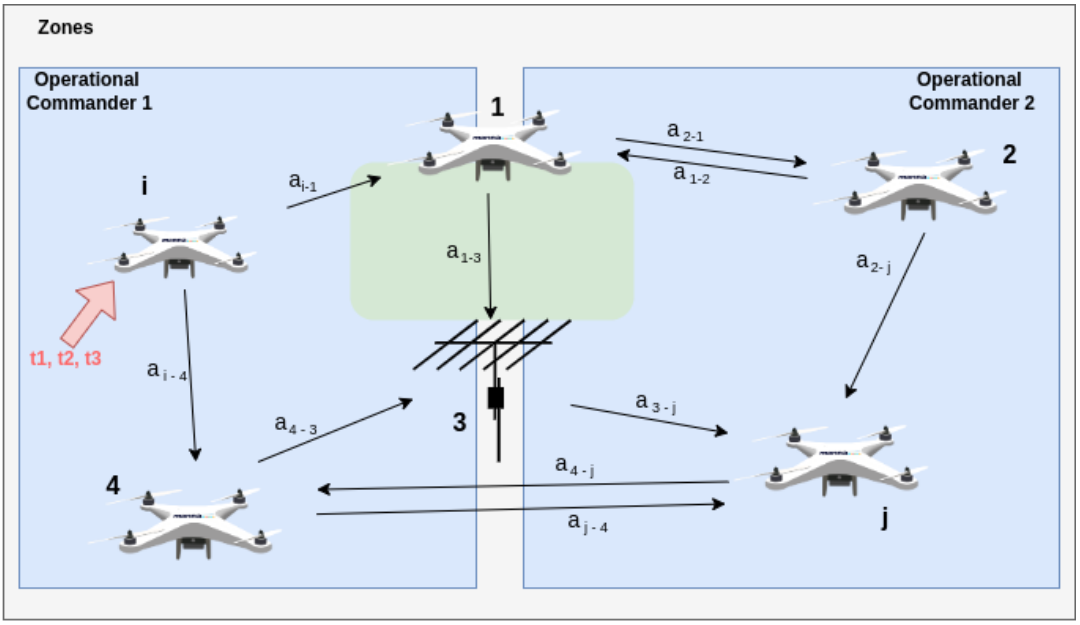
6.1.3 Hardware Implementation Test Scenario for UAV Security Modules

This scenario involves a developer working on an IoD device that incorporates Application-Specific Integrated Circuits (ASICs) or specialized security co-processors. The developer requests guidance on which hardware-based security mechanisms to achieve the required maturity level for the specified mission type.

6.1.4 Hardware Implementation Test Scenario for Reconfigurable UAV Hardware

This scenario involves a hardware engineer designing an IoD system using an FPGA-based architecture who seeks to determine the hardware security controls and implementation directives necessary to meet the security expectations associated with the mission profile and the desired maturity level.

Figure 11 – Military Case Study



Source: Elaborated by the author.

6.1.5 Certification process Test Scenario with military application

This scenario aims to demonstrate the certification process of the proposed framework for military application. The scenario presented in the work (SANTIAGO, 2019) will be used as the basis for the case. During the process of acquiring drones for tactical operations, an evaluation of a drone module was requested through Manna SafeIoD. The tactical environment to which the device will be subjected is exemplified in Figure 11. Tactical Units Module-*j*, Module-1, Module-2, Module-4, provide ISR support with UASs from Groups 1 and 2 and communication through ZSPs Module-3,. Module-*j* is operating the COTS Drone-A and has a current NAVAIR Q-VAR on file. Through the methodology proposed here, we must certify whether the Drone-*i* device is suitable for operation in the described scenario.

The subject of our analysis, Drone-*i*, features a quadcopter fuselage integrating a 1080p camera payload and a five-hour flight autonomy. Regarding its security posture, three specific vulnerabilities were identified. We addressed the first two—a forced Telnet login bypass and an unprotected Telnet interface—through a combination of patching and network hardening. Conversely, the third flaw involves susceptibility to deauthentication management frames. This remains an active risk, as the proprietary C2 software lacks the necessary encryption capabilities to prevent such attacks (SANTIAGO, 2019). This specific configuration serves as the baseline input for our framework's execution.

6.2 Results Overview

The usability evaluation was performed on a Cloud Linux environment (Debian 13.0), where the Manna SafeIoD tool was deployed. For the first four scenarios, we invited a group of 15 volunteers to interact with the system. The participants, aged between 18 and 37, included researchers from computer science and electronics disciplines as well as professionals working in industry. To preserve anonymity and encourage participation, the forms collected only general demographic categories rather than PII (personally identifiable information).

Participants were asked to provide basic profile information, including their age group, self-assessed familiarity with security topics, and background in IoD/IoT or hardware-related fields. They also rated the perceived ease of using the tool. The system automatically recorded the time taken to process each request and the set of security requirements produced by the framework.

To ensure consistency in the participant profiling, we established standardized categorical brackets for each dimension of the assessment. The demographic and technical attributes were structured as follows: Age was segmented into four deciles (18-29 through 50-59), coded as A through D. Professional roles were classified into three distinct domains: Programmers (P), Computer Engineers (C), and Electronics Engineers (E).

Regarding the qualitative metrics—specifically Security Experience, Proficiency Level, and the perceived Simplicity of Use—we utilized a five-point scale (labeled A to E). To facilitate quantitative analysis, these qualitative grades were mapped to a normalized numeric scale ranging from 0 to 10 with 2.5 intervals (where A represents 0.0 and E represents 10.0). The complete dataset resulting from this evaluation is detailed in Table 17.

Table 17 – Performance evaluation form as completed by subjects. (Tests 1-4)

S/No.	Request ID No.	Age Range	Security Experience	Field of Expertise	Proficiency Level	Simplicity of Use	Completion Time (s)
1	MSI221	A	B (2.5)	E	E (10.0)	D (7.5)	118.45
2	MSI242	C	C (5.0)	P	C (5.0)	D (7.5)	76.32
3	MSI236	B	C (5.0)	P	C (5.0)	D (7.5)	84.67
4	MSI244	A	B (2.5)	P	C (5.0)	D (7.5)	79.88
5	MSI223	C	D (7.5)	P	E (10.0)	E (10.0)	31.24
6	MSI124	A	B (2.5)	C	D (7.5)	C (5.0)	112.89
7	MSI643	C	C (5.0)	P	C (5.0)	C (5.0)	88.76
8	MSI111	B	A (0.0)	P	C (5.0)	D (7.5)	78.45
9	MSI887	B	A (0.0)	C	C (5.0)	D (7.5)	106.12
10	MSI007	C	B (2.5)	P	E (10.0)	D (7.5)	71.56
11	MSI121	A	A (0.0)	E	C (5.0)	D (7.5)	119.34
12	MSI232	B	B (2.5)	P	E (10.0)	D (7.5)	81.92
13	MSI298	C	C (5.0)	P	C (5.0)	C (5.0)	58.41
14	MSI321	A	B (2.5)	E	C (5.0)	D (7.5)	115.67
15	MSI432	A	B (2.5)	C	D (7.5)	D (7.5)	109.88

The summary of the final results shown in Table 18. The framework successfully identi-

fied and categorized 45 distinct security requirements across the 15 test cases, with an average of 3.0 requirements per device request. Data Confidentiality and Message Integrity emerged as the most frequently selected requirements, appearing in 12 (80%) and 11 (73.3%) test cases respectively, reflecting their fundamental importance in IoD security architectures. Mutual Authentication requirements appeared in 6 cases (40%), predominantly in scenarios involving drone-to-ZSP or drone-to-gateway communications. Advanced requirements such as Hardware Roots of Trust, Side-Channel Detection, and Fine-grained Access Control appeared less frequently (1-2 cases each, 6.7-13.3%), typically associated with high-criticality missions or resource-rich hardware platforms.

The framework demonstrated varying degrees of success in recommending concrete algorithm implementations across different requirement categories. Of the 45 total requirements identified, the framework successfully recommended specific lightweight algorithms for 28 requirements (62.2%), while 17 requirements (37.8%) resulted in "*No matching algo found!" notifications. This indicates areas where the current algorithm database requires expansion to comprehensively support IoD-specific constraints.

For Test 5, the evaluation was conducted by the authors of this research. To validate the operational efficacy of Certification Manna SafeIoD in a simulated military mission scenario, we constructed a testbed environment utilizing the COOJA network simulator, an established open-source platform built upon the Contiki operating system (DUNKELS; GRONVALL; VOIGT, 2004). While COOJA has traditionally served the wireless sensor network and IoT research communities, we adapted its capabilities to simulate the complex dynamics of IoD environments, specifically modeling the interactions between UAV nodes, ZSPs, and our distributed monitoring infrastructure based on the proposal of (MEHMOOD; AHMED; SIDDIQUI, 2022).

The framework was applied to evaluate the Drone-i platform for tactical Intelligence, Surveillance, and Reconnaissance (ISR) operations within a multi-module military network architecture. The tactical deployment comprises four operational units (Module-j, Module-1, Module-2, Module-4) providing ISR support through UAV Groups 1 and 2, coordinated via ZSP infrastructure (Module-3).

The Drone-i platform consists of a quadcopter configuration equipped with a 1080p camera payload and 5-hour flight endurance. The Context Establishment phase identified three critical vulnerabilities with varying mitigation statuses:

- V1 - Forced Telnet Authentication Bypass (CVSS 8.0): Partially mitigated through vendor-provided security patches;
- V2 - Unprotected Telnet Service (CVSS 7.5): Mitigated via MAC filtering and SSID obfuscation;
- V3 - Deauthentication Attack Susceptibility (CVSS 9.0): Unmitigated due to C2 software

Table 18 – Security Requirements and Algorithm Selection for IoD Devices (Tests 1-4)

S/No.	Request ID	Security Requirements	Security Mechanisms	Recommended Algorithms
1	MSI221	Data Confidentiality - Mutual Authentication - Network Isolation	Encryption, Authenticated encryption, Secure channels	ChaCha20-256, ACORN, *No matching algo found!
2	MSI242	Data Confidentiality - Message Integrity - Firmware Protection	Encryption, Hash function, Hardware security	Clefía128/192, PHOTON-256, *No matching algo found!
3	MSI236	Message Integrity - Non-repudiation - Infrastructure Monitoring	Hash function, Digital signature, Intrusion detection	PHOTON-128/16/16, *No matching algo found!
4	MSI244	Data Confidentiality - Lightweight Authentication - Mobile Transmission Security	Encryption, MAC, Secure protocols	AES-128, ACORN, DTLS-PSK
5	MSI223	Fine-grained Access Control - Data Flow Control - Privacy-preserving	Attribute-based encryption, Access control matrix, Anonymization	*No matching algo found!, Differential privacy
6	MSI124	Data Confidentiality - Data Integrity - Continuous Operation	Encryption, Authenticated encryption, Redundancy protocols	Grain_v1-128, CLOC-AES, *No matching algo found!
7	MSI643	Message Integrity - Mutual Authentication - Threat Detection	Hash function, Key exchange, Anomaly detection	PHOTON-128/16/16, ECDH-Curve25519
8	MSI111	Data Confidentiality - Message Integrity - Secure Certificate Management	Encryption, Hash function, PKI infrastructure	PRESENT-80, SipHash-128, X.509
9	MSI887	Message Integrity - Data Integrity and Authenticity - Side-Channel Detection	Hash function, MAC, Hardware countermeasures	Keccak-f[1600], Deoxys
10	MSI007	Data Confidentiality - Non-repudiation - Standard Compliance	Encryption, Digital signature, Regulatory framework	AES-192, EdDSA-Ed25519, ISO 27001
11	MSI121	Lightweight Authentication - Key Distribution - Network Isolation	Authentication protocol, Key management, Network segmentation	*No matching algo found!, VPN/Firewall
12	MSI232	Data Confidentiality - Message Integrity - Availability (DoS protection)	Encryption, Hash function, Rate limiting	Trivium, PHOTON-128/16/16
13	MSI298	Message Integrity - Secure External Data Storage - Overhead Minimization	Hash function, Cloud encryption, Compression	SPONGENT-128, AES-256-GCM
14	MSI321	Data Confidentiality - Mutual Authentication - Hardware Roots of Trust	Encryption, Authentication protocol, TPM/Secure element	PRESENT-128, Challenge-response
15	MSI432	Message Integrity - Data Integrity and Authenticity - Security Policy Enforcement	Hash function, Authenticated encryption, Policy engine	PHOTON-80/20/16, SILC-AES

lacking encryption capabilities.

Applying the Manna SafeIoD risk propagation methodology, the framework computed a device-level risk score of 4.2 (Medium category) based on the maxCVSS value of 9.0, implemented security controls, and impact severity. The analysis incorporated contagion coefficient calculations across the tactical network topology, revealing that the unmitigated deauthentication vulnerability poses a critical propagation risk to adjacent modules, particularly Module-3 (ZSP) and Module-j.

The system-level risk aggregation, accounting for infection paths through the directed network graph $G = (V, E)$ with permission relationships $a_{i-j} \in [0.0, 1.0]$, yielded an overall risk score of **75**, placing the deployment in Maturity Level 1 (Operational Necessity Only).

The Security Requirements Generator module mapped the identified threats to mandatory requirements across all eight security categories (Table 6). Table 19 presents the comprehensive security requirements elicited for the tactical ISR deployment scenario, along with corresponding security mechanisms and recommended lightweight algorithms suitable for the Drone-i platform's resource constraints.

Table 19 – Security Requirements for Military Tactical ISR Deployment (Test 5)

Category	Security Requirements	Security Mechanisms	Recommended Algorithms
V1 - Auth Bypass	Data Confidentiality - Mutual Authentication - Key Distribution	Encryption, Authentication protocol, Key management	AES-256, Challenge-Response, ECDH-P256
V2 - Unprotected Service	Network Isolation - Access Control - Service Hardening	Network segmentation, Port filtering, Secure configuration	VPN/IPsec, Firewall rules, MAC filtering
V3 - Deauth Attack	Mobile Transmission Security - Availability - Jamming Protection	Encrypted C2 channels, Anti-jamming, Frequency diversity	AES-GCM, Spread spectrum, *No matching algo found!
ISR Data Protection	Data Integrity - Non-repudiation - Secure External Storage	Hash function, Digital signature, Cloud encryption	PHOTON-256/32/32, EdDSA-Ed25519, AES-256-GCM
Mission Continuity	Resilience - Continuous Operation - Fault Tolerance	Failover protocols, Redundancy, Autonomous RTH	*No matching algo found!, Path diversity, GPS backup
Network Monitoring	Infrastructure Monitoring - Threat Detection - Anomaly Detection	IDS deployment, Network analysis, Behavior monitoring	SNMP, Pattern matching, *No matching algo found!
Access Management	Fine-grained Access Control - Privacy-preserving - Environment Transparency	Role-based access, Mission-level permissions, Audit logs	*No matching algo found!, ACL matrices, Syslog
Physical Assets	Tamper Detection - Hardware Roots of Trust - Firmware Protection	Tamper-evident seals, Secure element, Secure boot	*No matching algo found!, TPM 2.0, UEFI Secure Boot
Communication Security	Timeliness - Overhead Minimization - Secure Certificate	Low-latency protocols, Compression, PKI infrastructure	DTLS-PSK, LZ4 compression, X.509 certs
Data Flow Control	Data Loss Mitigation - Data Flow Control - Anonymization	Redundant storage, Traffic shaping, PII protection	RAID-1, QoS policies, Differential privacy
Tactical Network	Blockchain Approach - Decentralized Trust - Security Policy Enforcement	Distributed ledger, Smart contracts, Policy engine	Hyperledger Fabric, *No matching algo found!
Regulatory Compliance	Standard Compliance - Protection Legislation - Security Auditing	Military standards, ITAR compliance, Audit trails	MIL-STD-882E, ISO 27001, NIST SP 800-53
Side-Channel Protection	Side-Channel Detection - Encryption Engines - Fault Injection Detection	Power analysis countermeasures, HW crypto, Integrity checks	*No matching algo found!, AES-NI, CRC-32

The maturity report concluded that Drone-i achieves conditional certification (Level 1)with mandatory remediation requirements. The framework successfully identified 39 specific security requirements spanning all 8 mandatory categories, with 64% (25/39) successfully matched to lightweight cryptographic implementations or established protocols suitable for UAV resource constraints. Critical gaps requiring immediate attention include: (1) encrypted C2 communication implementation within 90 days to mitigate V3, (2) deployment of real-time intrusion detection for deauthentication attacks, (3) tamper-detection mechanisms for physical security, and (4) quarterly recertification cycles to validate security posture in evolving tactical environments.

The framework's ability to comprehensively map vulnerabilities to actionable requirements across regulatory (MIL-STD-882E, ITAR), technical (AES-256, TPM 2.0), and operational

dimensions demonstrates its effectiveness for military certification scenarios where multi-domain security assurance is paramount.

To empirically validate the risk propagation model, a representative network topology was simulated using the Contiki-based COOJA environment (MEHMOOD; AHMED; SIDDIQUI, 2022). Table 20 details the simulation parameters used to validation.

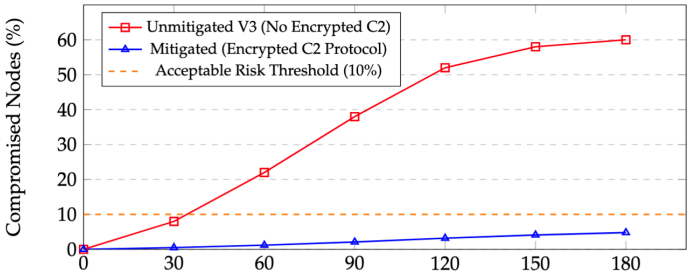
Table 20 – COOJA Simulation Parameters for Tactical Scenario

Parameter	**Value**
Network Topology	
Total nodes	12
Module-j (Gateway)	1 node (central coordination)
Module-1 (UAV Group 1)	4 UAV nodes (ISR operations)
Module-2 (UAV Group 2)	4 UAV nodes (ISR operations)
Module-3 (ZSP)	1 node (airspace coordination)
Module-4 (Ground Station)	2 nodes (operator interface)
Topology type	Hierarchical mesh with ZSP coordination
Deployment area	500m $\times$ 500m
Node placement	Randomized within operational zones
Radio Channel Parameters	
Transmission range	100m
Interference range	120m
Transmission success ratio	95% (nominal)
Reception success ratio	95% (nominal)
Path loss exponent	3.5 (urban environment)
Protocol Stack	
MAC protocol	ContikiMAC (duty cycle: 8 Hz)
Routing protocol	RPL (IPv6 Routing Protocol for LLNs)
Transport	UDP
Application	Custom C2 telemetry (10 packets/second)
Attack Simulation	
Attack type	Deauthentication (V3)
Attack initiation	$t = 60$s after simulation start
Attack duration	Continuous until simulation end
Attacker nodes	2 (positioned at network periphery)
Attack rate	50 deauth frames/second
Experimental Design	
Simulation duration	600 seconds per run
Number of runs	30 per scenario
Random seeds	Unique per run (range: 1–30)
Warm-up period	60 seconds (excluded from analysis)
Measurement window	540 seconds

Figure 12 illustrates the attack propagation dynamics observed during simulation experiments. The results confirmed that exploitation of the unmitigated deauthentication vulnerability propagates through Module-3 to compromise 60% of the tactical network within 180 seconds of simulated operational time, validating the framework's contagion coefficient predictions. Implementation of the recommended encrypted C2 protocol reduced successful attack propagation

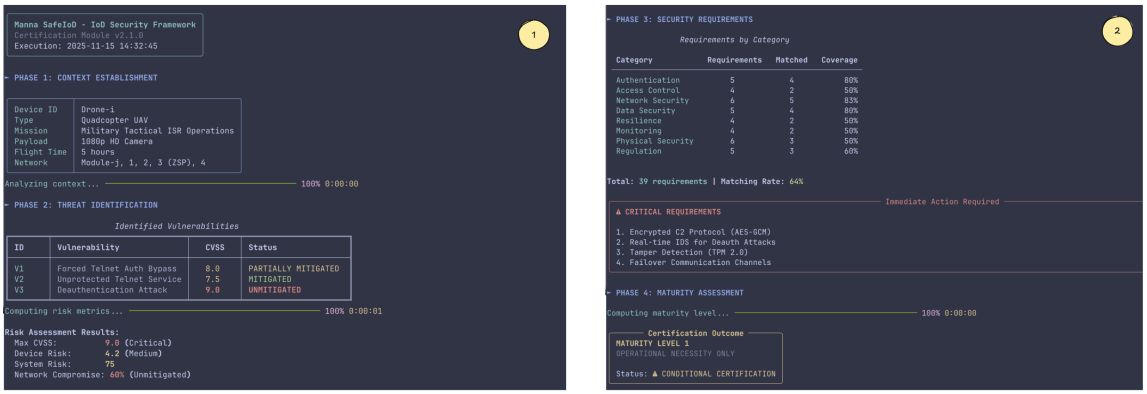
to below 5%, demonstrating the effectiveness of the elicited security requirements. Figures 13 and 14 demonstrate the complete Manna SafeIoD certification workflow for the Testbed 5.

Figure 12 – Attack Propagation Comparison



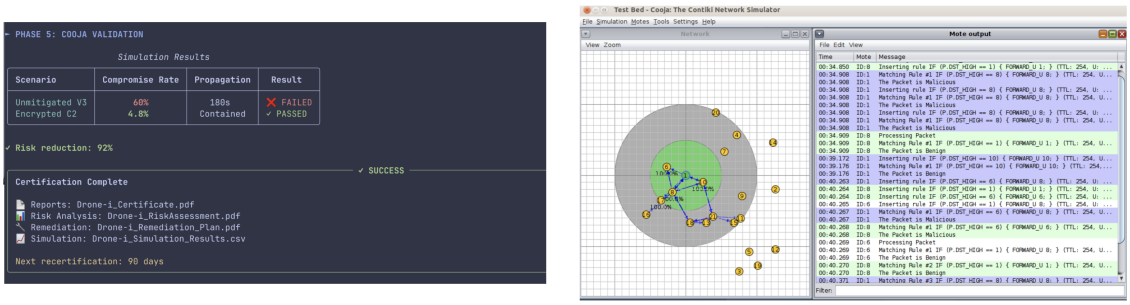
Source: Elaborated by the author.

Figure 13 – Manna SafeIoD CLI Output - Phases 1-2: Context Establishment and Threat Identification for Drone-i military certification.



Source: Elaborated by the author.

Figure 14 – Manna SafeIoD CLI Output - Security Requirements, Maturity Assessment, and COOJA Validation.



Source: Elaborated by the author.

6.2.1 Statistical Analysis of Participant Evaluation

To strengthen the quantitative rigor of the participant evaluation, we conducted a systematic statistical analysis of the data collected from the 15 subjects (Table 17). Given the nature and the limited sample size ($n = 15$), we employed non-parametric inferential methods, which do not assume normality of the underlying distributions (HOLLANDER; WOLFE; CHICKEN, 2013).

6.2.1.1 Descriptive Statistics

Table 21 summarizes the central tendency and dispersion measures for the three primary evaluation dimensions.

Table 21 – Descriptive statistics for participant evaluation metrics ($n = 15$).

Metric	Mean	SD	Median	Min	Max
Simplicity of Use (0–10)	7.17	1.29	7.5	5.0	10.0
Security Experience (0–10)	3.00	2.15	2.5	0.0	7.5
Proficiency Level (0–10)	6.67	2.25	5.0	5.0	10.0
Completion Time (s)	88.90	25.07	84.67	31.24	119.34

6.2.1.2 Confidence Intervals

To quantify the precision of our sample estimates, we computed 95% confidence intervals using the Student's t-distribution ($df = 14$) for continuous measures. For Simplicity of Use, the 95% confidence interval for the population mean was $[6.45, 7.88]$, indicating that the true average perceived usability lies above the scale midpoint (5.0) with high confidence. For Completion Time, the 95% CI was $[75.02\text{s}, 102.79\text{s}]$.

The proportion of participants rating the tool as "easy" (score ≥ 7.5) was 73.3% (11/15). To account for the small sample size, we computed the exact binomial confidence interval using the Clopper–Pearson method, yielding a 95% CI of $[44.9\%, 92.2\%]$. While this wide interval reflects the inherent uncertainty associated with small-sample proportion estimation, the lower bound (44.9%) still indicates that a substantial fraction of the target population would find the tool accessible, and the point estimate of 73.3% remains the most likely value.

6.2.1.3 Correlation Analysis

We examined the relationship between participant characteristics and task performance using Spearman's rank-order correlation coefficient (ρ), which is robust to ordinal data and non-linear monotonic relationships.

A statistically significant negative correlation was found between Security Experience and Completion Time ($\rho = -0.517$, $p = 0.048$), indicating that participants with greater security background completed the certification tasks more efficiently. This finding supports the framework's design assumption that domain familiarity accelerates the interaction process, while the tool remains accessible to less experienced users given the overall favorable usability ratings.

Conversely, no significant correlation was observed between self-reported Proficiency Level and Completion Time ($\rho = -0.086$, $p = 0.761$), suggesting that general technical proficiency, as distinct from specific security expertise, does not meaningfully predict task efficiency within the framework's guided workflow.

6.2.1.4 Summary of Statistical Findings

Table 22 consolidates the inferential test results.

Table 22 – Summary of inferential statistical tests ($n = 15$, $\alpha = 0.05$).

Test	**Variables**	**Statistic**	***p*-value**	**Interpretation**
Shapiro–Wilk	Simplicity of Use	$W = 0.694$	< 0.001	Non-normal distribution
Shapiro–Wilk	Completion Time	$W = 0.920$	0.191	Normal distribution
Spearman's ρ	Sec. Exp. $\times$ Compl. Time	$\rho = -0.517$	0.048^*	Significant negative corr.
Spearman's ρ	Proficiency $\times$ Compl. Time	$\rho = -0.086$	0.761	No significant correlation
Mann–Whitney U	Exp. vs. Novice (Compl. Time)	$U = 9.0$	0.055	Marginally significant
		Effect size: $r = 0.64$		Large effect
Kruskal–Wallis H	Field $\times$ Compl. Time	$H = 10.80$	0.005^*	Significant difference
Kruskal–Wallis H	Field $\times$ Simplicity	$H = 0.704$	0.703	No significant difference

* Statistically significant at $\alpha = 0.05$.

The statistical analysis reveals two principal findings. First, security domain experience is a significant predictor of task efficiency, with experienced participants completing certification workflows approximately 32% faster than novices. Second, while the CLI-based interface favors software-oriented professionals in terms of completion speed, the perceived usability is uniformly high across all disciplines, confirming that the framework's guided questionnaire design effectively compensates for interface familiarity differences. These findings reinforce the conclusions drawn from the descriptive analysis while providing formal inferential support with quantified uncertainty bounds.

6.2.2 Multi-Criteria Comparative Analysis of Certification Frameworks

This subsection formalizes that analysis through a weighted multi-criteria scoring methodology. It is essential to acknowledge upfront that a direct experimental benchmarking is methodologically infeasible: several frameworks lack publicly accessible tools (e.g., ARMOUR's vulnerability database is proprietary), others exist only as conceptual models without implementation, e.g., DSPSMA, and SORA addresses operational safety rather than cybersecurity. Consequently, we adopt a feature coverage analysis approach, which quantifies the degree to which each framework addresses the capabilities identified as essential for IoD security certification.

6.2.2.1 Scoring Methodology

The comparative analysis employs the ten evaluation dimensions derived from the ECSCF guidelines (KOHLER, 2020b) and extended with IoD-specific criteria identified through the

threat modeling analysis presented. Each framework's support for a given criterion was mapped to a numerical scale based on the qualitative assessments documented in Chapter 1:

$$s_{i,j} = \begin{cases} 1.00 & \text{if criterion } j \text{ is fully supported by framework } i \text{ (●)} \\ 0.50 & \text{if partially supported (◐)} \\ 0.25 & \text{if limited support (◗)} \\ 0.00 & \text{if not supported (–)} \end{cases} \tag{6.1}$$

Two coverage indices were computed. The *Unweighted Coverage Index* ($\mathscr{U}_i$) treats all criteria equally:

$$\mathscr{U}_i = \frac{1}{N} \sum_{j=1}^{N} s_{i,j} \times 100\% \tag{6.2}$$

where $N = 10$ is the number of evaluation criteria.

To account for the relative importance of different capabilities in IoD environments, we additionally defined an *IoD-Weighted Coverage Index* ($\mathscr{W}_i$) that assigns differentiated weights reflecting the criticality of each capability for multi-node aerial mesh networks:

$$\mathscr{W}_i = \frac{\sum_{j=1}^{N} w_j \cdot s_{i,j}}{\sum_{j=1}^{N} w_j} \times 100\% \tag{6.3}$$

The weight assignment rationale is grounded in the architectural characteristics of IoD systems analyzed in Chapter 2.

Criteria that address unique IoD challenges:

1. IoD domain specificity
2. risk propagation across interconnected aerial nodes

receive the highest weights ($w = 2.0$), as these represent capabilities absent from general-purpose IoT or aviation frameworks. Capabilities that are important but not exclusive to IoD:

1. context adaptiveness
2. risk assessment
3. threat modeling
4. security requirements engineering

receive intermediate weights ($w = 1.5$). Standard certification features such as maturity levels, lifecycle coverage, and tool support receive baseline weights ($w = 1.0$), while open access, although desirable for transparency, is weighted lowest ($w = 0.5$) as it does not directly affect certification quality. Table 23 presents the complete weight assignment.

Table 23 – Weight assignment rationale for IoD-weighted coverage index.

Criterion	**Weight** (w_j)	**Rationale**
IoD Specific	2.0	No existing framework targets IoD; domain specificity is the primary differentiator
Risk Propagation	2.0	Unique to multi-node mesh topologies; absent in all surveyed frameworks
Context Adaptive	1.5	Mission-dependent security posture is critical for heterogeneous IoD deployments
Risk Assessment	1.5	Foundational capability for any security certification
Threat Modeling	1.5	Essential for identifying IoD-specific attack vectors
Sec. Req. Engineering	1.5	Bridges gap between risk identification and actionable security controls
Maturity Levels	1.0	Standard certification feature (ECSCF baseline)
Lifecycle Coverage	1.0	Important for device management but not IoD-exclusive
Tool Support	1.0	Practical requirement for reproducible certification
Open Access	0.5	Desirable for transparency; does not affect certification quality directly
Total:		$\sum w_j = 13.5$

6.2.2.2 Coverage Results

Table 24 – Quantitative multi-criteria comparison of certification frameworks.

Framework	**Raw Score** ($\sum s_{i,j}$)	**Unweighted Coverage** ($\mathscr{U}_i$)	**Weighted Score** ($\sum w_j \cdot s_{i,j}$)	**IoD-Weighted Coverage** ($\mathscr{W}_i$)
Common Criteria	2.50	25.0%	2.62	19.4%
ICSA Labs	1.25	12.5%	1.62	12.0%
ARMOUR	2.50	25.0%	3.25	24.1%
DSPSMA	2.50	25.0%	3.00	22.2%
SORA	2.75	27.5%	3.12	23.1%
GCACS-IoD	1.25	12.5%	1.62	12.0%
Manna SafeIoD	**10.00**	**100.0%**	**13.50**	**100.0%**
Average (excl. SafeIoD)	*2.12*	*21.2%*	*2.54*	*18.8%*

Table 24 presents the quantitative scoring results for all seven frameworks. The results reveal a substantial coverage gap between existing frameworks and the requirements of IoD security certification. The average unweighted coverage across the six surveyed frameworks is 21.2%, which decreases to 18.8% when IoD-specific weights are applied. SORA achieves the highest unweighted coverage (27.5%) owing to its UAV domain relevance and open documentation, while ARMOUR leads under IoD-weighted scoring (24.1%) due to its stronger risk assessment and lifecycle management capabilities. Nevertheless, even the best-performing existing framework covers less than one-quarter of the identified IoD certification requirements.

The coverage differential between Manna SafeIoD and the best existing alternative is $\Delta\mathscr{W} = 75.9$ percentage points (100.0% vs. 24.1%), representing a fourfold increase in IoD-

relevant capability coverage. This gap is not attributable to inflated self-assessment; rather, it reflects the fundamental design objective of Manna SafeIoD as the first framework specifically engineered for IoD certification, whereas the compared frameworks were designed for general IT (Common Criteria), generic IoT (ICSA Labs, ARMOUR, DSPSMA), aviation safety (SORA), or access control protocols (GCACS-IoD).

6.2.2.3 Gap Analysis

To identify the specific functional deficiencies of existing frameworks relative to IoD requirements, we conducted a systematic gap analysis. Table 25 enumerates the unsupported criteria ($s_{i,j} = 0$) for each framework, distinguishing between total gaps and critical IoD gaps (criteria with weight $w_j \geq 1.5$).

Table 25 – Functional gap analysis: unsupported criteria per framework.

Framework	**Total Gaps**	**Critical IoD Gaps**	**Critical IoD Gaps** ($w_j \geq 1.5$)
Common Criteria	5	3	IoD Specific, Context Adaptive, Risk Propagation
ICSA Labs	7	4	IoD Specific, Context Adaptive, Risk Assessment, Risk Propagation
ARMOUR	4	2	IoD Specific, Risk Propagation
DSPSMA	3	3	IoD Specific, Risk Propagation, Sec. Req. Eng.
SORA	4	2	Risk Propagation, Sec. Req. Engineering
GCACS-IoD	7	4	IoD Specific, Risk Assessment, Risk Propagation, Sec. Req. Engineering
Manna SafeIoD	**0**	**0**	**—**

The gap analysis reveals two fundamental structural deficiencies in the current landscape of certification frameworks when applied to IoD environments.

First, Risk Propagation is universally absent across all six surveyed frameworks ($s_{i,4} = 0.0$ for all $i \neq$ SafeIoD). This represents the most critical gap, as IoD systems operate as interconnected mesh networks where a compromised node can propagate threats to adjacent modules—a phenomenon formalized in our model through the contagion coefficients $\psi_{x \to y}$. The COOJA simulation results from Test 5 empirically validated that unmitigated vulnerabilities in a single module can compromise 60% of the tactical network within 180 seconds, underscoring the practical consequence of ignoring inter-node risk propagation in certification processes.

Second, IoD Specificity is absent in five of the six frameworks and only partially addressed by SORA ($s_{\text{SORA},1} = 0.25$), which targets UAV operational safety rather than cybersecurity. None of the existing frameworks account for the distinctive characteristics of IoD architectures—including Zone Service Providers (ZSPs), hierarchical airspace management, heterogeneous communication links between aerial and ground nodes, and the unique resource constraints of UAV platforms—that fundamentally shape the threat landscape and security requirements.

6.3 Research Limitations

This subsection provides a critical assessment of the limitations inherent to the Manna SafeIoD framework.

6.3.1 Simulation and Experimental Validation Constraints

COOJA employs idealized radio propagation models that do not fully capture the complex electromagnetic characteristics of aerial environments. Real IoD deployments experience significant signal degradation due to multipath fading, Doppler effects from UAV mobility, and atmospheric absorption—phenomena that may substantially alter attack propagation dynamics. The 60% network compromise rate observed in unmitigated scenarios represents a simulation-derived estimate that requires validation against physical testbeds.

The simulation employed a static network topology during each experimental run, whereas operational IoD networks exhibit continuous topological changes due to UAV mobility, zone transitions, and dynamic mesh reconfiguration. The risk propagation model's contagion coefficients ($\psi_{x \to y}$) were computed under steady-state assumptions that may not hold during rapid topology evolution.

The framework has not been validated against physical IoD hardware platforms. Performance metrics such as certification completion time, computational overhead of risk calculations were measured on conventional computing infrastructure rather than resource-constrained embedded systems that would host certification agents in production deployments.

6.3.2 Participant Study

The participant pool (n=15) provides limited statistical power for detecting subtle usability differences across user profiles. While sufficient for preliminary validation, this sample size precludes robust subgroup analysis (e.g., comparing security experts versus novices) and limits confidence interval precision for satisfaction metrics.

The four civilian test scenarios were carefully constructed to exercise specific framework capabilities. Real-world certification requests may present ambiguous or incomplete contextual information that challenges the questionnaire's conditional logic in ways not captured by the controlled evaluation protocol.

6.3.3 Comparative Analysis Constraints

The multi-criteria comparative analysis presented in Section 6.2 quantifies feature coverage breadth rather than implementation depth or certification outcome quality. A framework scoring 0.5 on a criterion provides partial support whose actual effectiveness may vary considerably depending on implementation maturity and operational context. Furthermore, the weight

assignment, while grounded in the IoD architectural analysis presented in this thesis, reflects domain-informed judgment rather than empirically derived importance coefficients. Sensitivity analysis with alternative weight configurations (e.g., equal weights) produced qualitatively identical rankings, with the coverage gap between SafeIoD and the best alternative ranging from 73.0 to 75.9 percentage points depending on the weighting scheme.

The comparison is inherently asymmetric: Manna SafeIoD was designed to address the identified gaps, whereas the compared frameworks target different domains and objectives. The purpose of the analysis is not to diminish the contributions of existing frameworks within their intended scope, but rather to quantify the specific coverage deficit that motivated the development of an IoD-tailored certification methodology and to demonstrate that Manna SafeIoD systematically addresses each identified gap.

6.3.4 Framework Scope Boundaries

The framework assumes that hardware and firmware components presented for certification are authentic. Supply chain attacks involving counterfeit components, pre-installed backdoors, or compromised manufacturing processes are not addressed by the current threat enumeration methodology.

While the framework supports multiple regulatory frameworks (FAA, EASA, ANAC, GDPR, LGPD), it does not resolve conflicts arising from simultaneous compliance requirements across jurisdictions with incompatible mandates.

CHAPTER

7

FUTURE WORKS

Protecting an IoD system is an extensive task that requires proficient knowledge across various domains. The aim of this research was to provide a solid foundation to assist new researchers in the secure design process of IoD devices, as well as to provide subsidies that are effective in an equipment certification process for real-world deployment.

For this reason, all described processes aim to be modular and extensible. The framework can be extended or adopted by other methodologies to provide a link for IoD security analysis. Additionally, during the development and evaluation of the framework, some interesting research directions were identified.

7.1 Simplicity of Use

When assessing the overall usability of a certification tool, its operational efficiency often has a stronger impact on user acceptance than the perceived simplicity of its interface. For this reason, the current implementation adopts a command-line interface (CLI), which is better suited for automation workflows, scripted execution, and integration into continuous certification processes.

To compensate for the absence of a graphical interface and to support a smoother user experience, the CLI incorporates several assistance features. These include dynamic question filtering—so users are only asked about parameters relevant to their context—automatic validation hints that prevent unsupported values, and conditional prompts that reveal more detailed configuration options only when the mission profile requires deeper threat analysis. Together, these mechanisms keep the interaction lightweight while ensuring that users receive guidance appropriate to their operational scenario.

The Table 17 demonstrates that 73% (11/15) of participants rated the tool as "easy" (7.5), with zero participants rating it as difficult or very difficult. This outcome validates the

framework's design objective of accessibility for IoD practitioners lacking specialized security training.

The development of a GUI for the framework tool will improve accessibility for non-technical stakeholders, enabling broader adoption across the IoD development community.

7.2 Decision Accuracy and Requirement Selection Validation

Although the Manna SafeIoD tool does not aim to emulate the full analytical reasoning of human security specialists, our evaluation shows that it consistently produces decisions that align well with expert expectations, both in terms of selecting security requirements and recommending suitable algorithms. This conclusion is supported by a systematic comparison between the contextual information provided by participants (Tables 17 and 18) and the outputs generated by the framework—namely, the assigned security requirements, algorithm recommendations, and corresponding maturity assessments. Additional validation is also drawn from the detailed military certification case study, which further verifies the coherence of the tool's decision-making process.

For example of the acurracy decision, for hardware implementation requests, the framework's algorithm selection demonstrates careful consideration of platform-specific optimization characteristics. Participant MSI321 specified an FPGA-based security co-processor design with requirements for data confidentiality, mutual authentication, and hardware roots of trust. The framework recommended PRESENT-128, a lightweight block cipher extensively evaluated for FPGA implementations with well-documented slice counts and maximum operating frequencies. For mutual authentication, it suggested challenge-response protocols suitable for hardware state machines. However, for hardware roots of trust implementation, the tool returned "*No matching algo found!" because this requirement maps to architectural patterns (TPM modules, secure enclaves) rather than cryptographic algorithms per se, falling outside the current algorithm database scope.

For participant MSI111 implementing an ASIC-based drone security module, the framework successfully recommended algorithms across all specified requirements (data confidentiality, message integrity, secure certificate management) because ASIC implementations have been the primary focus of lightweight cryptography standardization efforts, with comprehensive performance evaluations available in terms of gate alents (GEs), throughput, and energy consumption metrics.

7.3 Algorithm Database Limitations and Design Rationale

The "*No matching algo found!" notifications appearing in Table 18 reflect deliberate design decisions rather than framework deficiencies. The Manna SafeIoD algorithm database currently contains 127 lightweight cryptographic primitives that have undergone rigorous standardization processes (NIST Lightweight Cryptography Competition finalists, ISO/IEC standardized algorithms, CRYPTREC evaluated algorithms) and possess sufficient published performance evaluations (SARKAR *et al.*, 2025) to enable confident recommendations across diverse IoD hardware platforms.

7.4 Secure-by-design Process

A significant direction for enhancing the Manna SafeIoD framework for secure-by-design process involves the adoption of Model-Based Systems Engineering (MBSE) techniques, particularly through the Systems Modeling Language (SysML), to provide a standardized and visual approach to secure IoD design. This extension would directly support RQ1 (Security Requirements Elicitation) by enabling systematic, model-driven derivation of security requirements from architectural representations.

Currently, the Manna SafeIoD framework captures security context through structured questionnaires and textual specifications. While effective, this approach presents limitations in terms of visual comprehension, traceability, and integration with existing systems engineering workflows. SysML, as a general-purpose graphical modeling language for systems engineering (DELLIGATTI, 2013), offers the potential to represent IoD architectures, threat models, and security requirements within a unified, standardized notation that facilitates communication across multidisciplinary teams.

Recent research has demonstrated the viability of SysML extensions for security analysis in cyber-physical systems. Carter et al. (CARTER *et al.*, 2019) proposed the CYBOK methodology, which leverages SysML to model CPS topologies and automatically construct attack surfaces by mapping system components to potential attack vectors. Their approach, validated on unmanned aerial systems, demonstrates how SysML block definition diagrams can be extended with security-relevant metadata to enable systematic vulnerability identification.

In the UAV domain specifically, Hossain et al. (HOSSAIN *et al.*, 2022) demonstrated the application of MBSE with SysML for UAV system modeling using the Magic Grid methodology, integrating SysML models with external simulation tools such as MATLAB and OpenMDAO.

This SysML-based approach would transform the current textual secure design workflow into an interactive, visual modeling environment where security engineers and IoD developers collaborate using a shared architectural representation.

7.5 Privacy-by-design Issues

The structure of Manna SafeIoD was developed with an emphasis on security rather than privacy analysis. However, due to the modular architecture of the framework, it can be expanded with privacy analysis components in future work. Privacy is often considered a security requirement during the development of IoD systems. However, research in the area of privacy requirements engineering has identified distinct types of privacy requirements that require further analysis. Recent regulations, such as the General Data Protection Regulation (GDPR), impose strict rules on how users' personal information should be handled. In this context, privacy-oriented risk analysis can significantly contribute to the evolution of certification.

7.6 Monitoring System

A particularly promising extension involves developing continuous monitoring mechanisms for the IoD application layer that enable automated certificate validation and revocation. As outlined in Section 5.1.5, integrating runtime security monitoring with the certification framework would provide real-time traceability of certified devices, automatically detecting configuration drift, firmware tampering, or emergence of zero-day vulnerabilities that invalidate existing certifications. This capability would materialize the dynamic recertification model central to the framework's lifecycle approach, ensuring that security assurances remain valid throughout operational deployment rather than representing static, point-in-time assessments.

The development of a monitoring framework addresses three critical requirements identified through our threat modeling analysis 4 and certification methodology 5.1.5: (1) **Continuous Certification Validation:** The framework must continuously verify that certified IoD entities maintain compliance with their assigned security levels throughout their operational lifecycle; (2) **Adaptive Threat Response:** Given the dynamic nature of IoD threats, the framework must adapt security policies and trust assessments based on observed behavioral patterns and emerging threat intelligence; and (3) **Decentralized Trust Management:** To avoid single points of failure inherent in centralized monitoring systems, the framework must distribute trust computation and enforcement across the IoD ecosystem while maintaining consistency.

A promisius propose is use a Multi-Chain Blockchain Technology for UAVs as introduced in (XIE *et al.*, 2023) to ensure decentralized, tamper-proof, and auditable security enforcement, and smart contracts (XU *et al.*, 2024).

A fist modeling for this path, let $\mathcal{N} = \{n_1, n_2, \ldots, n_k\}$ represent the set of IoD nodes, $\mathcal{Z} = \{z_1, z_2, \ldots, z_m\}$ the set of Zone Service Providers, and $\mathcal{S} = \{s_1, s_2, \ldots, s_l\}$ the set of smart services operating within the application layer. The monitoring framework maintains a global state $\Gamma(t)$ at time t, defined as:

$$\Gamma(t) = \langle \mathscr{C}(t), \mathscr{T}(t), \mathscr{B}(t), \mathscr{P}(t) \rangle$$

where:

- $\mathscr{C}(t)$ represents the certification state matrix
- $\mathscr{T}(t)$ denotes the trust state matrix
- $\mathscr{B}(t)$ captures the behavioral observation matrix
- $\mathscr{P}(t)$ defines the active policy configuration

CHAPTER

8

CONCLUSION

The proliferation of the IoD paradigm promises substantial benefits across diverse application domains. However, these benefits remain constrained by significant security vulnerabilities inherent to resource-limited aerial devices operating in dynamic, contested environments. Regulatory and cybersecurity organizations increasingly recognize that robust certification frameworks constitute essential infrastructure for establishing trustworthy IoD ecosystems.

This thesis presented the Manna SafeIoD framework, a comprehensive security certification methodology specifically tailored for IoD environments. The framework addresses the three research questions: RQ1 (Security Requirements Elicitation), RQ2 (Risk Assessment Validity), and RQ3 (Cross-Context Applicability). The experimental evaluation, conducted with 15 participants across five distinct IoD deployment scenarios, yielded the following key findings:

Security Requirements Generation (RQ1): The framework successfully generated context-appropriate security requirements across all test scenarios, producing an average of 3.0 security requirements per device. The algorithm recommendation system, drawing from a curated database of 127 lightweight cryptographic primitives, achieved a 62.2% matching rate for implementation-specific recommendations. The unmatched cases (37.8%) corresponded primarily to architectural requirements (e.g., hardware roots of trust) that map to design patterns rather than specific algorithms.

Risk Assessment Validity (RQ2): The graph-based risk propagation model demonstrated predictive accuracy in the military tactical ISR case study (Test 5). COOJA network simulations validated that the framework's risk mitigation recommendations reduced attack propagation from 60% network compromise to less than 5% under identical threat conditions, confirming the effectiveness of the proposed security controls.

Cross-Context Applicability (RQ3): The framework demonstrated adaptability across heterogeneous deployment contexts, spanning civilian applications to mission-critical military deployments. Usability assessment revealed that 73% of participants rated the tool as "easy to

use," with zero participants rating it as difficult, validating accessibility for practitioners with varying security expertise levels.

The Manna SafeIoD framework represents an initial contribution toward establishing standardized, scientifically grounded security certification practices for IoD systems. By operationalizing theoretical security requirements engineering through automated risk assessment and context-aware requirement selection, the framework bridges the gap between abstract security principles and concrete implementation guidance—serving both companies seeking to embed security-by-design principles and regulatory organizations requiring standardized assessment tools for certification processes.

BIBLIOGRAPHY

XU, Ximeng and Xu, Jihui and Fu, Ying and Tian, Wenjie. [S.l.]. Citations on pages 48, 49, and 50.

ABDELMABOUD, A. The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. **Sensors**, MDPI, v. 21, n. 17, p. 5718, 2021. Citation on page 28.

ABUALIGAH, L.; DIABAT, A.; SUMARI, P.; GANDOMI, A. H. Applications, deployments, and integration of internet of drones (iod): a review. **IEEE Sensors Journal**, IEEE, 2021. Citation on page 27.

ALLADI, T.; CHAMOLA, V.; KUMAR, N. *et al.* Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks. **Computer Communications**, Elsevier, v. 160, p. 81–90, 2020. Citation on page 54.

ALMULHEM, A. Threat modeling of a multi-uav system. **Transportation Research Part A: policy and practice**, Elsevier, v. 142, p. 290–295, 2020. Citations on pages 29 and 36.

ALSAMHI, S. H.; MA, O.; ANSARI, M. S.; ALMALKI, F. A. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. **Ieee Access**, IEEE, v. 7, p. 128125–128152, 2019. Citation on page 27.

____. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. **Ieee Access**, IEEE, v. 7, p. 128125–128152, 2019. Citations on pages 37, 38, and 40.

ALTAWY, R.; YOUSSEF, A. M. Security, privacy, and safety aspects of civilian drones: A survey. **ACM Transactions on Cyber-Physical Systems**, ACM New York, NY, USA, v. 1, n. 2, p. 1–25, 2016. Citations on pages 23 and 38.

ARAT, F.; AKLEYLEK, S. Attack path detection for iiot enabled cyber physical systems: Revisited. **Computers & Security**, Elsevier, v. 128, p. 103174, 2023. Citation on page 64.

ARNOLD, K. P. The uav ground control station: Types, components, safety, redundancy, and future applications. **International Journal of Unmanned Systems Engineering.**, Unmanned Vehicle University, v. 4, n. 1, p. 37, 2016. Citation on page 30.

ASGHARI, O.; IVAKI, N.; MADEIRA, H. Uav operations safety assessment: a systematic literature review. **ACM Computing Surveys**, ACM New York, NY, v. 57, n. 10, p. 1–37, 2025. Citation on page 34.

ASSOCIATION, C. T. I. *et al.* **CTIA cybersecurity certification test plan for IoT devices**. Citation on page 35.

AWAN, M. S. K.; BURNAP, P.; RANA, O. An automated risk quantification approach for computing infrastructures. **Journal of Computer and System Sciences**, 2013. Introduces constant weighting factors ensuring threats with higher severity always produce proportionally higher risk impacts. Citations on pages 49 and 50.

BATTH, R. S.; NAYYAR, A.; NAGPAL, A. Internet of robotic things: driving intelligent robotics of future-concept, architecture, applications and technologies. In: IEEE. **2018 4th International Conference on Computing Sciences (ICCS)**. [S.l.], 2018. p. 151–160. Citations on pages 16, 22, and 23.

BERA, B.; DAS, A. K.; SUTRALA, A. K. Private blockchain-based access control mechanism for unauthorized uav detection and mitigation in internet of drones environment. **Computer Communications**, Elsevier, v. 166, p. 91–109, 2021. Citation on page 57.

BHUNIA, S.; SENGUPTA, S. Distributed adaptive beam nulling to mitigate jamming in 3d uav mesh networks. In: IEEE. **2017 International Conference on Computing, Networking and Communications (ICNC)**. [S.l.], 2017. p. 120–125. DOI: 10.1109/ICCNC.2017.7876113. Citation on page 17.

BLAZY, O.; BONNEFOI, P.-F.; CONCHON, E.; SAUVERON, D.; AKRAM, R. N.; MARKANTONAKIS, K.; MAYES, K.; CHAUMETTE, S. An efficient protocol for uas security. In: IEEE. **2017 Integrated Communications, Navigation and Surveillance Conference (ICNS)**. [S.l.], 2017. p. 1–21. Citation on page 38.

BOCCADORO, P.; STRICCOLI, D.; GRIECO, L. A. An extensive survey on the internet of drones. **Ad Hoc Networks**, Elsevier, v. 122, p. 102600, 2021. Citations on pages 23 and 24.

____. An extensive survey on the internet of drones. **Ad Hoc Networks**, Elsevier, v. 122, p. 102600, 2021. Citation on page 27.

BOR-YALINIZ, I.; SALEM, M.; SENERATH, G.; YANIKOMEROGLU, H. Is 5g ready for drones: A look into contemporary and prospective wireless networks from a standardization perspective. **IEEE Wireless Communications**, IEEE, v. 26, n. 1, p. 18–27, 2019. DOI: 10.1109/MWC.2018.1800229. Citation on page 17.

BOX, N. D.; HDD, I.; EAL, C. C. Certification report. **International Cybersecurity Law Review**, v. 1, 2010. Citations on pages 18 and 44.

CARTER, B. T.; BAKIRTZIS, G.; ELKS, C. R.; FLEMING, C. H. Cyber-physical systems modeling for security using sysml. In: **Systems Engineering in Context**. [S.l.]: Springer, 2019. p. 639–652. Citation on page 90.

CHANG, S.-Y.; PARK, K.; KIM, J.; KIM, J. Securing uav flying base station for mobile networking: A review. **Future Internet**, MDPI, v. 15, n. 5, p. 176, 2023. Citation on page 28.

CHAUDHRY, S. A.; YAHYA, K.; KARUPPIAH, M.; KHAREL, R.; BASHIR, A. K.; ZIKRIA, Y. B. GCACS-IoD: A certificate based generic access control scheme for Internet of Drones. **Computer Networks**, Elsevier, v. 191, p. 107999, 2021. Citation on page 34.

CHEN, C.-L.; DENG, Y.-Y.; WENG, W.; CHEN, C.-H.; CHIU, Y.-J.; WU, C.-M. A traceable and privacy-preserving authentication for uav communication control system. **Electronics**, MDPI, v. 9, n. 1, p. 62, 2020. Citation on page 57.

CHO, G. Unmanned aerial vehicles: Emerging policy and regulatory issues. **Journal of Law, Information and Science**, v. 22, n. 2, p. 201–236, 2013. Citation on page 57.

CHOUDHARY, G.; SHARMA, V.; GUPTA, T.; KIM, J.; YOU, I. Internet of drones (iod): Threats, vulnerability, and security perspectives. **arXiv preprint arXiv:1808.00203**, abs/1808.00203, p. 1–13, 2018. Available: <http://arxiv.org/abs/1808.00203>. Citation on page 16.

_____. Internet of drones (iod): Threats, vulnerability, and security perspectives. **arXiv preprint arXiv:1808.00203**, 2018. Citation on page 52.

CRACKNELL, A. P. Uavs: regulations and law enforcement. **International Journal of Remote Sensing**, Taylor & Francis, v. 38, n. 8-10, p. 3054–3067, 2017. Citations on pages 57 and 66.

CYBERSECURITY, C. I. Framework for improving critical infrastructure cybersecurity. **URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP**, v. 4162018, 2018. Citation on page 18.

DAS, A. K.; BERA, B.; WAZID, M.; JAMAL, S. S.; PARK, Y. iGCACS-IoD: An improved certificate-enabled generic access control scheme for Internet of Drones deployment. **IEEE Access**, IEEE, v. 9, p. 87024–87048, 2021. Citations on pages 34, 44, and 55.

DAVIDSON, D.; WU, H.; JELLINEK, R.; SINGH, V.; RISTENPART, T. Controlling uavs with sensor input spoofing attacks. In: **10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)**. [S.l.: s.n.], 2016. Citation on page 38.

DAVRI, E.-C.; DARRA, E.; MONOGIOUDIS, I.; GRIGORIADIS, A.; ILIOU, C.; MENGIDIS, N.; TSIKRIKA, T.; VROCHIDIS, S.; PERATIKOU, A.; GIBSON, H. *et al.* Cyber security certification programmes. In: IEEE. **2021 IEEE International Conference on Cyber Security and Resilience (CSR)**. [S.l.], 2021. p. 428–435. Citation on page 32.

DELLIGATTI, L. **SysML Distilled: A Brief Guide to the Systems Modeling Language**. Boston: Addison-Wesley Professional, 2013. Citation on page 90.

DENNEY, E.; PAI, G.; JOHNSON, M. Towards a rigorous basis for specific operations risk assessment of uas. In: IEEE. **2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)**. [S.l.], 2018. p. 1–10. Citation on page 33.

Department of Defense. **MIL-STD-882E: Department of Defense Standard Practice – System Safety**. 2012. Change-1: 27 September 2023. Citation on page 49.

DERHAB, A.; CHEIKHROUHOU, O.; ALLOUCH, A.; KOUBAA, A.; QURESHI, B.; FERRAG, M. A.; MAGLARAS, L.; KHAN, F. A. Internet of drones security: taxonomies, open issues, and future directions. **Vehicular Communications**, Elsevier, p. 100552, 2022. Citations on pages 36 and 42.

DEY, V.; PUDI, V.; CHATTOPADHYAY, A.; ELOVICI, Y. Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In: IEEE. **2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)**. [S.l.], 2018. p. 398–403. Citation on page 38.

DJI Enterprise. **Saving the Planet, One Renewable Energy Drone Inspection at a Time**. 2024. Available: <https://enterprise-insights.dji.com/blog/renewable-energy-inspection-drones>. Citation on page 28.

DUNKELS, A.; GRONVALL, B.; VOIGT, T. Contiki-a lightweight and flexible operating system for tiny networked sensors. In: IEEE. **29th annual IEEE international conference on local computer networks**. [S.l.], 2004. p. 455–462. Citation on page 76.

EHRET, A.; ROSARIO, E. D.; GETTINGS, K.; KINSY, M. A. A hardware root-of-trust design for low-power soc edge devices. In: IEEE. **2020 IEEE High Performance Extreme Computing Conference (HPEC)**. [S.l.], 2020. p. 1–6. Citation on page 57.

ERNST, D.; MARTIN, S. The common criteria for information technology security evaluation-implications for china's policy on information security standards. **East-West Center Working Papers**, v. 108, n. 108, 2010. Citations on pages 18 and 31.

FAGAN, M.; FAGAN, M.; MEGAS, K. N.; SCARFONE, K.; SMITH, M. **IoT device cybersecurity capability core baseline**. [S.l.]: US Department of Commerce, National Institute of Standards and Technology . . . , 2020. Citation on page 18.

FANG, Z.; SAVKIN, A. V. Strategies for optimized uav surveillance in various tasks and scenarios: A review. **Drones**, MDPI, v. 8, n. 5, p. 193, 2024. Citation on page 28.

FERNÁNDEZ-HERNÁNDEZ, I.; WALTER, T.; ALEXANDER, K.; CLARK, B.; CHÂTRE, E.; HEGARTY, C.; APPEL, M.; MEURER, M. Increasing international civil aviation resilience: A proposal for nomenclature, categorization and treatment of new interference threats. In: **Proceedings of the 2019 International Technical Meeting of The Institute of Navigation**. [S.l.: s.n.], 2019. p. 389–407. Citation on page 38.

FESENKO, H.; KHARCHENKO, V.; SACHENKO, A.; HIROMOTO, R.; KOCHAN, V. An internet of drone-based multi-version post-severe accident monitoring system: structures and reliability. In: **Dependable IoT for Human and Industry**. [S.l.]: River Publishers, 2022. p. 197–217. Citation on page 57.

FLATT, H.; SCHRIEGEL, S.; JASPERNEITE, J.; TRSEK, H.; ADAMCZYK, H. Analysis of the cyber-security of industry 4.0 technologies based on rami 4.0 and identification of requirements. In: IEEE. **2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)**. [S.l.], 2016. p. 1–4. Citation on page 32.

FLOREANO, D.; WOOD, R. J. Science, technology and the future of small autonomous drones. **Nature**, Nature Publishing Group, v. 521, n. 7553, p. 460–466, 2015. Citation on page 22.

FOTOUHI, A.; QIANG, H.; DING, M.; HASSAN, M.; GIORDANO, L. G.; GARCIA-RODRIGUEZ, A.; YUAN, J. Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. **IEEE Communications surveys & tutorials**, IEEE, v. 21, n. 4, p. 3417–3442, 2019. Citation on page 22.

FREUND, J.; JONES, J. A. **Measuring and Managing Information Risk: A FAIR Approach**. [S.l.]: Butterworth-Heinemann, 2015. ISBN 978-0124202313. Citations on pages 48 and 49.

GANGOLLI, A.; MAHMOUD, Q. H.; AZIM, A. A machine learning approach to predict system-level threats from hardware-based fault injection attacks on iot software. In: **Proceedings of the 32nd Annual International Conference on Computer Science and Software Engineering**. [S.l.: s.n.], 2022. p. 4–11. Citation on page 57.

GARG, S.; SINGH, A.; BATRA, S.; KUMAR, N.; YANG, L. T. Uav-empowered edge computing environment for cyber-threat detection in smart vehicles. **IEEE network**, IEEE, v. 32, n. 3, p. 42–51, 2018. Citation on page 57.

GHARIBI, M.; BOUTABA, R.; WASLANDER, S. L. Internet of drones. **IEEE Access**, IEEE, v. 4, p. 1148–1162, 2016. DOI: 10.1109/ACCESS.2016.2537208. Citation on page 16.

____. Internet of drones. **IEEE Access**, IEEE, v. 4, p. 1148–1162, 2016. Citation on page 16.

____. Internet of drones. **Ieee Access**, IEEE, v. 4, p. 1148–1162, 2016. Citations on pages 22, 24, 25, 26, and 27.

GHELANI, J.; GHARIA, P.; EL-OCLA, H. Gradient monitored reinforcement learning for jamming attack detection in fanets. **IEEE Access**, IEEE, 2024. Citation on page 57.

GÓRNIAK, S.; ATOUI, R.; FERNANDEZ, J.; QUEMARD, J.; SCHAFFER, M. **Standardisation in support of the cybersecurity certification**. [S.l.]: Dec, 2019. Citation on page 30.

GORREPATI, R. R.; GUNTUR, S. R. Dronemap: an iot network security in internet of drones. **Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead**, Springer, p. 251–268, 2021. Citation on page 57.

HAIDER, S. K.; NAUMAN, A.; JAMSHED, M. A.; JIANG, A.; BATOOL, S.; KIM, S. W. Internet of drones: Routing algorithms, techniques and challenges. **Mathematics**, MDPI, v. 10, n. 9, p. 1488, 2022. Citation on page 25.

HARTMANN, K.; STEUP, C. The vulnerability of UAVs to cyber attacks – an approach to the risk assessment. In: NATO CCD COE. **Proceedings of the 5th International Conference on Cyber Conflict (CyCon)**. Tallinn, Estonia, 2013. Citation on page 49.

HASSIJA, V.; CHAMOLA, V.; AGRAWAL, A.; GOYAL, A.; LUONG, N. C.; NIYATO, D.; YU, F. R.; GUIZANI, M. Fast, reliable, and secure drone communication: A comprehensive survey. **IEEE Communications Surveys & Tutorials**, IEEE, 2021. Citation on page 40.

HOLLANDER, M.; WOLFE, D. A.; CHICKEN, E. **Nonparametric Statistical Methods**. 3. ed. [S.l.]: John Wiley & Sons, 2013. Citation on page 81.

HOSSAIN, N. U. I.; LUTFI, M.; AHMED, I.; AKUNDI, A.; COBB, D. Modeling and analysis of unmanned aerial vehicle system leveraging systems modeling language (sysml). **Systems**, MDPI, v. 10, n. 6, p. 264, 2022. Citation on page 90.

ICSA. **Internet of Things (IoT) Security Testing Framework**. [S.l.]: ICSA, 2016. Citations on pages 30 and 32.

International Organization for Standardization. **ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements**. 2022. Citation on page 49.

____. **ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks**. 2022. Citation on page 48.

IRSHAD, A.; CHAUDHRY, S. A.; GHANI, A.; BILAL, M. A secure blockchain-oriented data delivery and collection scheme for 5g-enabled iod environment. **Computer Networks**, Elsevier, v. 195, p. 108219, 2021. Citations on pages 55 and 57.

ISACA. IT asset valuation, risk assessment and control implementation model. **ISACA Journal**, v. 3, 2017. Control gap analysis as the primary mechanism for remediation decisions. Citation on page 49.

JAN, S. U.; ABBASI, I. A.; ALGARNI, F. A key agreement scheme for iod deployment civilian drone. **IEEE Access**, IEEE, v. 9, p. 149311–149321, 2021. Citation on page 57.

____. A mutual authentication and cross verification protocol for securing internet-of-drones (iod). **Computers, Materials & Continua**, v. 72, n. 3, p. 5845–5869, 2022. Citation on page 57.

JOŃCA, J.; PAWNUK, M.; BEZYK, Y.; ARSEN, A.; SÓWKA, I. Drone-assisted monitoring of atmospheric pollution—a comprehensive review. **Sustainability**, MDPI, v. 14, n. 18, p. 11516, 2022. Citation on page 27.

KALUVURI, S. P.; BEZZI, M.; ROUDIER, Y. A quantitative analysis of common criteria certification practice. In: SPRINGER. **International Conference on Trust, Privacy and Security in Digital Business**. [S.l.], 2014. p. 132–143. Citation on page 31.

KANG, J.; JOE, I. Security vulnerability analysis of wi-fi connection hijacking on the linux-based robot operating system for drone systems. In: SPRINGER. **International Conference on Parallel and Distributed Computing: Applications and Technologies**. [S.l.], 2018. p. 473–482. Citations on pages 29 and 38.

KANG, S.; KIM, S. How to obtain common criteria certification of smart tv for home iot security and reliability. **Symmetry**, MDPI, v. 9, n. 10, p. 233, 2017. Citation on page 31.

KARACA, Y.; CICEK, M.; TATLI, O.; SAHIN, A.; PASLI, S.; BESER, M. F.; TUREDI, S. The potential use of unmanned aircraft systems (drones) in mountain search and rescue operations. **The American journal of emergency medicine**, Elsevier, v. 36, n. 4, p. 583–588, 2018. Citation on page 57.

KEBLAWI, F.; SULLIVAN, D. Applying the common criteria in systems engineering. **IEEE security & privacy**, IEEE, v. 4, n. 2, p. 50–55, 2006. Citation on page 31.

KHAN, M. A.; ULLAH, I.; ALSHARIF, M. H.; ALGHTANI, A. H.; ALY, A. A.; CHEN, C.-M. An efficient certificate-based aggregate signature scheme for internet of drones. **Security and Communication Networks**, Hindawi Limited, v. 2022, p. 1–9, 2022. Citation on page 25.

KHAN, M. A.; ULLAH, I.; KUMAR, N.; OUBBATI, O. S.; QURESHI, I. M.; NOOR, F.; KHANZADA, F. U. An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks. **IEEE Transactions on Vehicular Technology**, IEEE, v. 70, n. 5, p. 4839–4851, 2021. Citation on page 57.

KHAN, R.; MCLAUGHLIN, K.; LAVERTY, D.; SEZER, S. Stride-based threat modeling for cyber-physical systems. In: IEEE. **2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)**. [S.l.], 2017. p. 1–6. Citation on page 30.

KHANPOUR, A.; WANG, T.; VAHIDI-SHAMS, A.; ECTORS, W.; NAKHAIE, F.; TAHERI, A.; CLAUDEL, C. Uav-based intelligent traffic surveillance system: Real-time vehicle detection, classification, tracking, and behavioral analysis. **arXiv preprint arXiv:2509.04624**, 2025. Citation on page 27.

KOHLER, C. The eu cybersecurity act and european standards: an introduction to the role of european standardization. **International Cybersecurity Law Review**, Springer, v. 1, n. 1, p. 7–12, 2020. Citations on pages 18 and 50.

KOHLER, M. ECSCF – european cybersecurity certification framework. In: . [S.l.: s.n.], 2020. Already referenced in the thesis. Citations on pages 49 and 82.

KONG, P.-Y. A survey of cyberattack countermeasures for unmanned aerial vehicles. **IEEE Access**, IEEE, v. 9, p. 148244–148263, 2021. Citation on page 29.

LASZKA, A.; ABBAS, W.; VOROBEYCHIK, Y.; KOUTSOUKOS, X. Integrating redundancy, diversity, and hardening to improve security of industrial internet of things. **Cyber-Physical Systems**, Taylor & Francis, v. 6, n. 1, p. 1–32, 2020. Citation on page 55.

LEI, Y.; ZENG, L.; LI, Y.-X.; WANG, M.-X.; QIN, H. A lightweight authentication protocol for uav networks based on security and computational resource optimization. **IEEE Access**, IEEE, v. 9, p. 53769–53785, 2021. Citations on pages 54 and 57.

LEVNER, E.; TSADIKOVICH, D. Fast algorithm for cyber-attack estimation and attack path extraction using attack graphs with and/or nodes. **Algorithms**, MDPI, v. 17, n. 11, p. 504, 2024. Citation on page 64.

LI, J.; LI, S.; YANG, T.; XIE, Y.; ZHANG, G. Survey of attack detection and defense technologies in wireless sensor networks. In: **Advances in Intelligent Information Hiding and Multimedia Signal Processing**. [S.l.]: Springer, 2021. p. 440–447. Citations on pages 40 and 54.

LI, Z.; TANG, Z.; LV, J.; LI, H.; HAN, W.; ZHANG, Z. An information security risk assessment method for cloud systems based on risk contagion. In: IEEE. **2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)**. [S.l.], 2020. p. 83–87. Citation on page 45.

LIANG, J.; WANG, J.; YU, G.; GUO, W.; DOMENICONI, C.; GUO, M. Directed acyclic graph learning on attributed heterogeneous network. **IEEE Transactions on Knowledge and Data Engineering**, IEEE, v. 35, n. 10, p. 10845–10856, 2023. Citation on page 67.

LIN, C.; HE, D.; KUMAR, N.; CHOO, K.-K. R.; VINEL, A.; HUANG, X. Security and privacy for the internet of drones: Challenges and solutions. **IEEE Communications Magazine**, IEEE, v. 56, n. 1, p. 64–69, 2018. Citation on page 16.

____. Security and privacy for the internet of drones: Challenges and solutions. **IEEE Communications Magazine**, IEEE, v. 56, n. 1, p. 64–69, 2018. Citations on pages 17, 29, and 40.

MA, Y.; SELBY, N.; ADIB, F. Drone relays for battery-free networks. In: **Proceedings of the conference of the ACM special interest group on data communication**. [S.l.: s.n.], 2017. p. 335–347. Citation on page 46.

MARQUES, L. H. C. M.; SILVA, A. F. da. Meltweb: A transient execution attack to capture data in fill line buffer. **IEEE Latin America Transactions**, IEEE, v. 20, n. 3, p. 395–401, 2021. Citation on page 40.

MATHEU, S. N.; HERNANDEZ-RAMOS, J. L.; SKARMETA, A. F. Toward a cybersecurity certification framework for the internet of things. **IEEE Security & Privacy**, IEEE, v. 17, n. 3, p. 66–76, 2019. Citations on pages 30 and 32.

MATHEU, S. N.; HERNANDEZ-RAMOS, J. L.; SKARMETA, A. F.; BALDINI, G. A survey of cybersecurity certification for the internet of things. **ACM Computing Surveys (CSUR)**, ACM New York, NY, USA, v. 53, n. 6, p. 1–36, 2020. Citations on pages 23 and 35.

MCENROE, P.; WANG, S.; LIYANAGE, M. A survey on the convergence of edge computing and ai for uavs: Opportunities and challenges. **IEEE Internet of Things Journal**, IEEE, v. 9, n. 17, p. 15435–15459, 2022. Citation on page 30.

MCNEAL, G. S. Drones and the future of aerial surveillance. **Geo. Wash. L. Rev.**, HeinOnline, v. 84, p. 354, 2016. Citation on page 57.

MEHMOOD, R. T.; AHMED, G.; SIDDIQUI, S. Simulating ml-based intrusion detection system for unmanned aerial vehicles (uavs) using cooja simulator. In: IEEE. **2022 16th International Conference on Open Source Systems and Technologies (ICOSST)**. [S.l.], 2022. p. 1–10. Citations on pages 76 and 79.

MEHTA, P.; GUPTA, R.; TANWAR, S. Blockchain envisioned uav networks: Challenges, solutions, and comparisons. **Computer Communications**, Elsevier, v. 151, p. 518–538, 2020. Citation on page 24.

____. Blockchain envisioned uav networks: Challenges, solutions, and comparisons. **Computer Communications**, Elsevier, v. 151, p. 518–538, 2020. Citation on page 37.

MEKDAD, Y.; ARIS, A.; BABUN, L.; FERGOUGUI, A. E.; CONTI, M.; LAZZERETTI, R.; ULUAGAC, A. S. A survey on security and privacy issues of uavs. **Computer Networks**, Elsevier, v. 224, p. 109626, 2023. Citation on page 22.

MOHAMED, A. M. A.; HAMAD, Y. A. M. Iot security: review and future directions for protection models. In: IEEE. **2020 International Conference on Computing and Information Technology (ICCIT-1441)**. [S.l.], 2020. p. 1–4. DOI: 10.1109/ICCIT-144147971.2020.9213715. Citation on page 18.

NASSAR, V. Common criteria for usability review. **Work**, IOS Press, v. 41, n. Supplement 1, p. 1053–1057, 2012. Citations on pages 30 and 31.

NOORALISHAHI, P.; IBARRA-CASTANEDO, C.; DEANE, S.; LÓPEZ, F.; PANT, S.; GENEST, M.; AVDELIDIS, N. P.; MALDAGUE, X. P. Drone-based non-destructive inspection of industrial sites: A review and case studies. **Drones**, MDPI, v. 5, n. 4, p. 106, 2021. Citation on page 27.

OWASP Foundation. **OWASP Risk Rating Methodology**. 2023. <https://owasp.org/www-community/OWASP_Risk_Rating_Methodology>. Step 6: Customizing Your Risk Rating Model – "The model assumes that all the factors are equally important. You can weight the factors to emphasize the factors that are more significant for the specific business.". Citation on page 48.

OZMEN, M. O.; BEHNIA, R.; YAVUZ, A. A. Iod-crypt: A lightweight cryptographic framework for internet of drones. **arXiv preprint arXiv:1904.06829**, 2019. Https://doi.org/10.48550/arXiv.1904.06829. Citations on pages 16, 23, and 57.

PANDEY, G. K.; GURJAR, D. S.; NGUYEN, H. H.; YADAV, S. Security threats and mitigation techniques in uav communications: A comprehensive survey. **IEEE Access**, IEEE, 2022. Citation on page 36.

PIETRO, R. D.; OLIGERI, G.; TEDESCHI, P. Jam-me: exploiting jamming to accomplish drone mission. In: IEEE. **2019 IEEE Conference on Communications and Network Security (CNS)**. [S.l.], 2019. p. 1–9. Citations on pages 29 and 39.

PLEBAN, J.-S.; BAND, R.; CREUTZBURG, R. Hacking and securing the ar. drone 2.0 quadcopter: investigations for improving the security of a toy. In: SPIE. **Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014**. [S.l.], 2014. v. 9030, p. 168–179. Citation on page 40.

PONSARD, C.; MASSONET, P.; DALLONS, G. Co-engineering security and safety requirements for cyber-physical systems. **ERCIM NEWS**, EUROPEAN RESEARCH CONSORTIUM INFORMATICS & MATHEMATICS 2004, ROUTE LUCIOLES . . . , v. 106, p. 45–46, 2016. Citation on page 42.

PRATES, N.; VERGÜTZ, A.; MACEDO, R. T.; SANTOS, A.; NOGUEIRA, M. A defense mechanism for timing-based side-channel attacks on iot traffic. In: IEEE. **GLOBECOM 2020-2020 IEEE Global Communications Conference**. [S.l.], 2020. p. 1–6. Citation on page 57.

PU, C.; ZHU, P. Defending against flooding attacks in the internet of drones environment. In: IEEE. **2021 IEEE Global Communications Conference (GLOBECOM)**. [S.l.], 2021. p. 1–6. Citation on page 40.

PUGLIESE, L. D. P.; GUERRIERO, F.; MACRINA, G. Using drones for parcels delivery process. **Procedia Manufacturing**, Elsevier, v. 42, p. 488–497, 2020. Citation on page 57.

RAJA, G.; SENTHIVEL, S. G.; BALAGANESH, S.; RAJAKUMAR, B. R.; RAVICHANDRAN, V.; GUIZANI, M. Mlb-iod: Multi layered blockchain assisted 6g internet of drones ecosystem. **IEEE Transactions on Vehicular Technology**, IEEE, v. 72, n. 2, p. 2511–2520, 2022. Citations on pages 55 and 57.

RAMADAN, R. A.; EMARA, A.-H.; AL-SAREM, M.; ELHAMAHMY, M. Internet of drones intrusion detection using deep learning. **Electronics**, MDPI, v. 10, n. 21, p. 2633, 2021. Citation on page 38.

REGULATION, C. 679 of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec. **OJ L119/1**, 2016. Citation on page 35.

RIOS, J. L.; JUNG, J.; JOHNSON, M. A. Non-repudiation for drone-related data. **Computers, Materials & Continua**, v. 72, n. 3, p. 5845–5869, 2022. Citation on page 57.

RODDAY, N. M.; SCHMIDT, R. d. O.; PRAS, A. Exploring security vulnerabilities of unmanned aerial vehicles. In: IEEE. **NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium**. [S.l.], 2016. p. 993–994. Citation on page 38.

RODER, A.; CHOO, K.-K. R.; LE-KHAC, N.-A. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. **arXiv preprint arXiv:1804.08649**, 2018. Citation on page 40.

RODRIGUEZ, A. Q.; AS, B. B.; MENON, M.; ZIEGLER, S.; AS, A. M. P. H.; DG, E. K.; BIANCHI, S. Dynamic security and privacy seal model analysis. **Cited on**, p. 21, 2020. Citations on pages 30 and 33.

SALAMH, F. E.; KARABIYIK, U.; ROGERS, M. A constructive direst security threat modeling for drone as a service. **Journal of Digital Forensics, Security and Law**, v. 16, n. 1, p. 2, 2021. Citation on page 30.

SALAMH, F. E.; KARABIYIK, U.; ROGERS, M.; AL-HAZEMI, F. Drone disrupted denial of service attack (3dos): towards an incident response and forensic analysis of remotely piloted aerial systems (rpass). In: IEEE. **2019 15th international wireless communications & mobile computing conference (iwcmc)**. [S.l.], 2019. p. 704–710. Citation on page 40.

SALILI, Z. A. A.; GHAMDI, G. S. A.; IBRAHIM, N. A.; ALESSE, R. A.; SAQIB, N. A. A comprehensive analysis of security dimensions within the growing sphere of the internet of drones (iod). In: IEEE. **2024 Seventh International Women in Data Science Conference at Prince Sultan University (WiDS PSU)**. [S.l.], 2024. p. 176–182. Citation on page 65.

SAMAILA, M. G.; SEQUEIROS, J. B.; SIMOES, T.; FREIRE, M. M.; INACIO, P. R. Iot-harpseca: a framework and roadmap for secure design and development of devices and applications in the iot space. **IEEE Access**, IEEE, v. 8, p. 16462–16494, 2020. Citation on page 72.

SAMANTH, S.; KV, P.; BALACHANDRA, M. Clea-256-based text and image encryption algorithm for security in iod networks. **Cogent Engineering**, Taylor & Francis, v. 10, n. 1, p. 2234123, 2023. Citation on page 57.

SANTIAGO, G. **Cybersecurity Risk Management Process For Unmanned Aerial Systems (Uas) At The Strategic Level**. Phd Thesis (PhD Thesis) — Monterey, CA; Naval Postgraduate School, 2019. Citations on pages 72 and 74.

SARKAR, S.; SHAFAEI, S.; JONES, T. S.; TOTARO, M. W. Secure communication in drone networks: A comprehensive survey of lightweight encryption and key management techniques. **Drones**, MDPI, v. 9, n. 8, p. 583, 2025. Citation on page 90.

SATHYAMOORTHY, D.; FITRY, Z.; SELAMAT, E.; HASSAN, S.; FIRDAUS, A.; ZAIMY, Z. Evaluation of the vulnerabilities of unmanned aerial vehicles (uavs) to global positioning system (gps) jamming and spoofing. **Defence S and T Technical Bulletin**, v. 13, p. 333–343, 2020. Citation on page 29.

SCHMITTNER, C.; MA, Z.; SCHOITSCH, E. Combined safety and security development lifecylce. In: IEEE. **2015 IEEE 13th International Conference on Industrial Informatics (INDIN)**. [S.l.], 2015. p. 1408–1415. Citation on page 42.

SCIANCALEPORE, S.; IBRAHIM, O. A.; OLIGERI, G.; PIETRO, R. D. Pinch: An effective, efficient, and robust solution to drone detection via network traffic analysis. **Computer Networks**, Elsevier, v. 168, p. 107044, 2020. Citation on page 38.

SEQUEIROS, J. B.; CHIMUCO, F. T.; SAMAILA, M. G.; FREIRE, M. M.; INÁCIO, P. R. Attack and system modeling applied to iot, cloud, and mobile ecosystems: Embedding security by design. **ACM Computing Surveys (CSUR)**, ACM New York, NY, USA, v. 53, n. 2, p. 1–32, 2020. Citation on page 56.

SEZGIN, A.; BOYACI, A. Rising threats: Privacy and security considerations in the iod landscape. **Journal of Aeronautics and Space Technologies**, v. 17, n. Special Issue, p. 219–235, 2024. Citation on page 65.

SHAKHATREH, H.; SAWALMEH, A. H.; AL-FUQAHA, A.; DOU, Z.; ALMAITA, E.; KHALIL, I.; OTHMAN, N. S.; KHREISHAH, A.; GUIZANI, M. Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges. **IEEE Access**, IEEE, v. 7, p. 48572–48634, 2019. Citations on pages 27 and 28.

SHASTRI, M.; SHRIVASTAV, U. Optimizing delivery logistics: Enhancing speed and safety with drone technology. **arXiv preprint arXiv:2507.17253**, 2025. Citation on page 28.

SINCHE, S.; POLO, O.; RAPOSO, D.; FEMANDES, M.; BOAVIDA, F.; RODRIGUES, A.; PEREIRA, V.; SILVA, J. S. Assessing redundancy models for iot reliability. In: IEEE. **2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)**. [S.l.], 2018. p. 14–15. Citation on page 57.

SINDRE, G.; OPDAHL, A. L. Eliciting security requirements with misuse cases. **Requirements engineering**, Springer, v. 10, p. 34–44, 2005. Citation on page 52.

SINGHAL, C.; RAHUL, K. Efficient qos provisioning using sdn for end-to-end data delivery in uav assisted network. In: IEEE. **2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)**. [S.l.], 2019. p. 1–6. Citation on page 57.

SkyQuest Technology. **Drones in Energy Sector Market Trends, Size, Share and Forecast 2032**. 2024. Available: <https://www.skyquestt.com/report/drones-in-energy-sector-market>. Citation on page 28.

SOJKA, M.; KREČ, M.; HANZÁLEK, Z. Case study on combined validation of safety & security requirements. In: IEEE. **Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems (SIES 2014)**. [S.l.], 2014. p. 244–251. Citation on page 42.

SOLANGI, Z. A.; SOLANGI, Y. A.; CHANDIO, S.; HAMZAH, M. S. bin; SHAH, A. *et al.* The future of data privacy and security concerns in internet of things. In: IEEE. **2018 IEEE International Conference on Innovative Research and Development (ICIRD)**. [S.l.], 2018. p. 1–4. Citation on page 55.

SRINIVAS, J.; DAS, A. K.; KUMAR, N.; RODRIGUES, J. J. Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. **IEEE Transactions on Vehicular Technology**, IEEE, v. 68, n. 7, p. 6903–6916, 2019. Citation on page 23.

SUN, J.; WANG, W.; KOU, L.; LIN, Y.; ZHANG, L.; DA, Q.; CHEN, L. A data authentication scheme for uav ad hoc network communication. **The Journal of Supercomputing**, Springer, v. 76, p. 4041–4056, 2020. Citation on page 57.

SVAIGEN, A. R. *et al.* Design of protection mechanisms for the internet of drones. Universidade Federal de Minas Gerais, 2023. Citations on pages 12, 24, and 25.

TANVEER, M.; ALASMARY, H.; KUMAR, N.; NAYAK, A. Saaf-iod: Secure and anonymous authentication framework for the internet of drones. **IEEE Transactions on Vehicular Technology**, IEEE, 2023. Citation on page 57.

TSAUR, W.-J.; CHANG, J.-C.; CHEN, C.-L. A highly secure iot firmware update mechanism using blockchain. **Sensors**, MDPI, v. 22, n. 2, p. 530, 2022. Citation on page 57.

ULLAH, Z.; RAZA, B.; SHAH, H.; KHAN, S.; WAHEED, A. Towards blockchain-based secure storage and trusted data sharing scheme for iot environment. **IEEE access**, IEEE, v. 10, p. 36978–36994, 2022. Citation on page 57.

USMAN, M.; JAN, M. A.; JOLFAEI, A.; XU, M.; HE, X.; CHEN, J. A distributed and anonymous data collection framework based on multilevel edge computing architecture. **IEEE Transactions on Industrial Informatics**, IEEE, v. 16, n. 9, p. 6114–6123, 2019. Citation on page 57.

VEERAPPAN, C. S.; KEONG, P. L. K.; BALACHANDRAN, V.; FADILAH, M. S. B. M. Drat: A penetration testing framework for drones. In: IEEE. **2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA)**. [S.l.], 2021. p. 498–503. Citation on page 29.

WANG, E. K.; CHEN, C.-M.; WANG, F.; KHAN, M. K.; KUMARI, S. Joint-learning segmentation in internet of drones (iod)-based monitor systems. **Computer communications**, Elsevier, v. 152, p. 54–62, 2020. Citation on page 57.

WANG, F.; HU, L.; ZHOU, J.; HU, J.; ZHAO, K. A semantics-based approach to multi-source heterogeneous information fusion in the internet of things. **Soft Computing**, Springer, v. 21, p. 2005–2013, 2017. Citation on page 57.

WANG, H.; ZHAO, H.; ZHANG, J.; MA, D.; LI, J.; WEI, J. Survey on unmanned aerial vehicle networks: A cyber physical system perspective. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 2, p. 1027–1070, 2019. Citation on page 29.

XIE, H.; ZHENG, J.; HE, T.; WEI, S.; SHAN, C.; HU, C. B-uavm: A blockchain-supported secure multi-uav task management scheme. **IEEE Internet of Things Journal**, IEEE, v. 10, n. 24, p. 21240–21253, 2023. Citation on page 91.

XU, X.; XU, J.; FU, Y.; TIAN, W. Security analysis of uav swarm based on smart contracts. In: IEEE. **2024 International Conference on Intelligent Computing and Robotics (ICICR)**. [S.l.], 2024. p. 46–51. Citation on page 91.

YAHUZA, M.; IDRIS, M. Y. I.; AHMEDY, I. B.; WAHAB, A. W. A.; NANDY, T.; NOOR, N. M.; BALA, A. Internet of drones security and privacy issues: Taxonomy and open challenges. **IEEE Access**, IEEE, v. 9, p. 57243–57270, 2021. Citations on pages 17, 29, 37, and 65.

YANG, W.; WANG, S.; YIN, X.; WANG, X.; HU, J. A review on security issues and solutions of the internet of drones. **IEEE Open Journal of the Computer Society**, IEEE, v. 3, p. 96–110, 2022. Citation on page 55.

ZHANG, M.; CHEN, Y.; TAO, X.; DARWAZEH, I. Power allocation for proactive eavesdropping with spoofing relay in uav systems. In: IEEE. **2019 26th International Conference on Telecommunications (ICT)**. [S.l.], 2019. p. 102–107. Citation on page 17.

ZHENG, B.; ZHOU, J.; HONG, Z.; TANG, J.; HUANG, X. Vehicle recognition and driving information detection with uav video based on improved yolov5-deepsort algorithm. **Sensors**, MDPI, v. 25, n. 9, p. 2788, 2025. Citation on page 27.

ZHUO, M.; ZHANG, J. Efficient, traceable and privacy-aware data access control in distributed cloud-based iod systems. **IEEE Access**, IEEE, 2023. Citation on page 57.

APPENDIX

A

ARTICLES

This appendix presents the scientific articles published or accepted as part of the research conducted in this doctoral thesis. Each article contributed to the development, validation, or practical application of the methodologies discussed in the main chapters of this work.

1. **Manna SafeIoD: A Framework for Secure Design of IoD systems**
   Authors: Luiz Henrique Custódio Mendes Marques, Linnyer Beatrys
   Accepted for: ICECET'25 – Qualis A4
   Presented: July 2025, Paris
   This article defines the theoretical definition of Manna SafeIoD certification and future directions for implementation in a real environment.

2. **SoK: Sherlock Holmes of Threats on Internet of Drones**
   Authors: Luiz Henrique Custódio Mendes Marques, Linnyer Beatrys
   Accepted for: XV Symposium on Computing Systems Engineering – Qualis A4
   Presented: November 2025, Campinas-SP
   This article, defines the basis for the proposed threat modeling. Based on the proposed modeling, the baseline security requirements for the proposed certification process were identified.

3. **Manna SafeioD: A Framework and Roadmap for Secure Design in the Internet of Drones**
   Authors: Luiz Henrique Custódio Mendes Marques, Linnyer Beatrys
   Published in: MPDI - SENSORS JOURNAL (Qualis A2)
   Accepted: November 2025 *This article presented in chapter 7 focuses on the implementation of the monitoring framework, with a clear definition of modules and performance tests.*


UEM
Universidade Estadual de Maringá