Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A SOC-Innovative Intelligent Framework For UAVs CyberSecurity

Fadhila Tlili

fadhilatlili24@gmail.com

Université de Technologie de Troyes

Samiha Ayed

IMT Atlantique

Lamia Chaari Fourati

Digital Research Centre of Sfax

Research Article

Keywords: Unmanned Aerial Vehicles, Security operations center, Intrusion Detection System, Security, Attack detection

Posted Date: September 2nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10753956/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Soft Computing on October 17th, 2026.
See the published version at https://doi.org/10.1007/s00500-026-11455-z.

A SOC-Innovative Intelligent Framework For UAVs CyberSecurity

Fadhila Tlili[1,2,3*], Samiha Ayed[4] and Lamia CHAARI FOURATI[2,3]

[1*]LIST3N, University of Technology of Troyes, Troyes, France.
[2]Digital Research Center of Sfax (CRNS), Laboratory of Signals, systeMs, aRtificial Intelligence, neTworkS (SM@RTS), Sfax, Tunisia.
[3]National School of Electronics and Telecommunications of Sfax, University of Sfax, Sfax, Tunisia.
[4]Lab-STICC, IMT Atlantique, Brest, France.

*Corresponding author(s). E-mail(s): Fadhilatlili24@gmail.com;
Contributing authors: samiha.ayed@imt-atlantique.fr;
lamiachaari1@gmail.com;

Abstract

Unmanned Aerial Vehicles (UAVs) have increasingly emerged as critical assets in various civil and military applications, yet they remain highly vulnerable to a broad spectrum of cyber and physical security attacks. Such threats can compromise essential UAV functionalities, including communication links, navigation accuracy, and data integrity. While Security Operation Centers (SOCs) have been widely deployed to safeguard Internet of Things (IoT) infrastructures, their direct application to UAV environments remains largely unexplored. To address this research gap, this paper proposes the SOC-Innovative Intelligent Framework, an AI-driven architecture that extends SOC capabilities to cyber-physical aerial systems. The framework consolidates real-time anomaly detection, risk quantification, and autonomous mitigation within a closed operational feedback loop. replay-based evaluation further validate the framework's enhanced detection accuracy and reduced response latency under realistic mission conditions. This study positions SOC2I as a foundational step toward next-generation SOC architectures for UAV cybersecurity, effectively bridging the gap between conventional network SOCs and emerging aerial cyber-physical defense paradigms. Our proposed SOC2I explicitly adapts key SOC functions to UAV constraints by supporting threat-intelligence enrichment within SIEM correlation, a tiered analyst-supervised incident workflow, and safety-gated response actions suitable

for real-time aerial missions. This provides centralized situational awareness while preserving on-board resource budgets and mission safety.

Keywords: Unmanned Aerial Vehicles, Security operations center, Intrusion Detection System, Security, Attack detection.

1 Introduction

1.1 General Context

Within the last years, there has existed a notable paramount incorporation of Unmanned Aerial Vehicles (UAVs) [1] across multifarious sectors. These remotely piloted aircraft have laid the foundations of a field of transformative opportunities. In diverse applications, ranging from agriculture [2], logistics [3], surveillance and emergency response [4], UAVs went beyond traditional operational constraints. Recently, There has been a sociotechnical discussion about using UAVs as air taxis [5] to replace commercial helicopters due to their electric Vertical Takeoff and Landing (eVTOL) capabilities. By providing unrestrained access to remote and risky terrains [6], UAVs preceded in new frontiers of operational efficiency and facilitated the acquisition of data. The corresponding rise in security attacks and threats has accompanied the increasing prevalence of UAVs. These security risks expose the urgent necessity of an efficient solution for UAVs attacks countermeasures, detection, and security reports.

Despite their technological aptitude, UAVs remain susceptible to a wide sort of vulnerabilities. Alongside to a series of adversaries and attacks (e.g., jamming and spoofing attacks [7]). The harmful interventions made by these attacks prohibit and disable UAV communications, manipulate navigation systems, and expose data integrity to hard security challenges. Moreover, most attacks on different entries and surfaces paralyze the functionality of UAV operations. Traditional detection methods (e.g., Signature-based approaches and rule-based systems) struggled to keep up with the evolving nature and categories of UAV attacks. Arguably, some attacks are unstoppable, especially in cases where the system still does not recognize that its security has been compromised. Therefore, industry and research developers discovered ways to detect malfunctions, attacks, and misbehavior. They aim to develop different systems and frameworks using traditional and advanced methodologies. Traditional UAV security involves physical, communication, and data security. These methods address UAV security and privacy. They are effective in some cases, while they often fail to detect new attacks.

Meanwhile, the dynamic nature of UAVs requires proactive, adaptive, and intelligent solutions to detect and mitigate cyberattack impacts. Furthermore, the conventional methods of UAVs attacks detection have often proved inadequate in mitigating these multifaceted threats. As the sophistication of UAVs attack strategies increased, there is a pronounced demand for defense mechanisms. This needs the proposal to be proactive, adaptable, and powered by the outstanding application of artificial intelligence (AI). AI [8] solutions aim to safeguard these aerial platforms against attacks and

threats. Still, with the growth of cybersecurity incidents, UAV failure, vulnerabilities, and diverse attacks, AI-based models could not fulfill the bidirectional need for attack detection and mitigation. The ascendancy of UAV attacks and lack of efficient defensive and detective solutions led to the establishment of specialized Security Operation Centers (SOCs) [9]. They are designed to support and enhance UAVs security and response efforts. Through integrating SOC log analysis and swift incident response mechanisms, UAVs security measures are going to be reconfigured. However, despite the widespread usage of AI (Machine Learning (ML) and Deep Learning (DL)) [10] tools, the integration of SOC as a service will fortify UAVs security. AI's most common limitations include adversarial attacks, limited training data impacting the AI model's efficiency, and Bias in the training data. This could lead to false positives or false negatives, regular updates to evolving attacks, and operational countermeasures. These limitations lead to a security compromise. Owing to the gap in academic research studies that do not consider SOC for UAVs. Our contribution aims to propose and validate the integration of SOC with an intelligent framework for UAVs security. This work addresses the fundamental application of SOCs as a robust defense mechanism for UAVs.

To the best of our knowledge, limited research has investigated the integration of SOC principles within UAV cybersecurity environments. Motivated by this gap, this study explores and validates the potential integration of SOC capabilities into UAV security architectures through the proposed SOC2I framework.

Furthermore, given the potentially severe operational and safety consequences associated with UAV cyberattacks, this proposed study investigates UAVs attacks and their corresponding defenses based on an understanding of the vulnerabilities obtained through the usage of SOC.

1.2 Related Work and Research Gaps

A central issue within a major part of SOC literature is that it is very fragmented and widespread. At this point, a relatively small set of research has attempted to establish extensive architectural frameworks supporting SOC designs. While researchers generally concur on the essential capabilities, there is a lack of definitive agreement on the definition of a SOC. In addition, the majority of academic research concentrates on specific attributes of a SOC, occasionally neglecting the broader architectural and operational perspective. We found some research that is substantially relevant to our approach, as it aims to gain a more practical understanding of SOCs. A few researchers have proposed the integration of SOC in different IoT systems [11]. These efforts demonstrate the growing interest in extending SOC principles beyond traditional enterprise infrastructures toward distributed and cyber–physical environments. However, despite this progress, the literature remains largely SOC-centric and rarely considers the specific operational and security characteristics of UAV ecosystems, such as dynamic network topologies, airborne communication channels, and resource-constrained edge platforms. Authors in [12] describe the challenges and performance metrics for assessing the performance of SOC analysts. The paper emphasizes the importance of evaluating the effectiveness of SOC analysts in detecting, responding

to, and containing cybersecurity threats [13]. The authors conducted a study to identify the challenges faced by SOC analysts and provided a detailed analysis of these challenges. They also examined various quantitative performance metrics, such as Mean Time to Detect (MTTD), Mean Time to Acknowledge (MTTA), Mean Time to Respond (MTTR), Mean Time to Contain, and Cost of Incidents, used to assess the performance of SOC analysts. The study highlighted the interdependent nature of these challenges and performance metrics and identified factors that impact the accuracy of these metrics. The authors concluded that further research is needed to develop a universal model for assessing SOC and SOC analysts' performance. From an architectural perspective, however, this work primarily focuses on operational evaluation within existing SOC environments rather than proposing a concrete architectural framework for SOC deployment. Consequently, while it provides valuable insight into SOC performance assessment, it does not address how SOC infrastructures should be designed to support emerging distributed systems such as UAV networks. Authors in [14] explored the human factor capabilities in SOC and pointed out the challenges faced by SOC analysts. Additionally, the paper highlights the importance of understanding the interconnected and evolving nature of SOC systems. The study uses a two-phase research methodology involving a literature review as well as survey-based questionnaires and interviews with SOC analysts and experts. The results reveal several key challenges faced by SOC analysts, such as inadequate training and attack simulations and performance issues with hardware and software resources. Additionally, the study identifies a lack of suitable metrics for evaluating SOC analyst performance. Although the study contributes significantly to understanding the socio-technical dimensions of SOC environments, its primary emphasis remains on human and organizational aspects rather than on the technical architecture of SOC infrastructures. Therefore, the work does not explicitly address how SOC monitoring mechanisms or threat detection frameworks should be adapted for distributed cyber–physical systems such as UAV fleets. In [15], the study discusses the design of a SOC with successful development and implementation of a Cyber SOC. The authors focus on identifying the significant factors contributing to SOC framework efficiency. The study was conducted quantitatively and involved 63 respondents from 25 ministries and agencies in Malaysia. It was based on a questionnaire that assessed knowledge and understanding of the SOC framework, the success factors for SOC, and the involvement of humans, processes, and technology in SOC development and implementation. The findings agree with the general success factors for SOC and recognize the importance of SOC development and implementation. While this work contributes to the empirical understanding of the organizational factors influencing SOC success, the resulting framework mainly targets institutional and governmental SOC deployments. As a result, the architectural considerations of monitoring infrastructures, Threat Intelligence (TI) integration, and distributed telemetry collection are only partially addressed. Furthermore, the model does not explicitly consider the constraints and operational characteristics associated with UAV-based cyber–physical systems. In [16], the authors discuss the concept of integrating Network Operation Center (NOC) and SOC to counter cyber-security attacks and improve operational efficiency effectively. The authors conducted a systematic literature review to analyze the necessity and benefits of integrating NOC

and SOC. They proposed a state-of-the-art architecture for integrated NOC and SOC, consisting of three layers: physical data source, Faults, Performance, Configuration, Administration, and Security (FCAPS) management [17], and overall situational management. Recently, authors in [18] proposed the Information Fusion for Secure Drone Operations (IFSDO) framework to enhance the security of autonomous drone missions through the integration of information fusion, cryptographic mechanisms, attribute-based access control, and ontology-driven policy enforcement. Their approach enables secure and autonomous management of access requests, dynamic spectrum allocation, and policy enforcement across different mission phases. The framework demonstrates the growing interest in integrating advanced security mechanisms into autonomous UAV operations. However, its primary focus remains on mission-level security management, access control, and secure information exchange between stakeholders and UAVs. In addition, [19] proposed a calibration framework for smart oblique capture to improve UAV-based pavement inspection and photogrammetric reconstruction quality. Their work demonstrates the growing adoption of UAVs in intelligent infrastructure monitoring and highlights the importance of data acquisition strategies for mission performance. However, the study focuses on imaging optimization and infrastructure assessment rather than cybersecurity monitoring, threat detection, or SOC-based security management. Consequently, while such approaches improve operational efficiency, they do not address the security and incident-response challenges targeted by SOC2I.

This approach improves operational visibility by combining network management and security monitoring capabilities. However, the proposed architecture primarily targets enterprise network infrastructures and assumes relatively stable communication environments. Consequently, it does not directly address the dynamic networking conditions, distributed telemetry sources, and mobility constraints typically encountered in UAV ecosystems. In parallel, recent research in UAV cybersecurity has explored mechanisms such as UAV-specific IDS, secure communication protocols, and distributed monitoring architectures for UAV fleets.

These studies typically focus on protecting UAV communication links, detecting anomalies in flight telemetry, or securing ground control stations. Although such mechanisms perform monitoring and detection functions conceptually similar to SOC operations, they are usually implemented as isolated security components rather than as part of a unified SOC-oriented architecture. Therefore, while UAV cybersecurity research addresses certain aspects of threat detection and system protection, it rarely integrates these capabilities into a comprehensive SOC framework capable of providing centralized situational awareness, coordinated incident response, and long-term TI analysis.

To provide a clearer analytical comparison of the reviewed works and to address the reviewer's concern regarding the lack of critical comparison, Table 1 summarizes the key characteristics of the most relevant studies. The comparison highlights the architectural scope, design assumptions, monitoring capabilities, and limitations of each work.

Furthermore, Table 1 has been expanded to include representative UAV cybersecurity approaches in addition to SOC-related studies. This enables a more balanced comparison and clarifies that the contribution of SOC2I is not the introduction of new

Table 1 Comparative analysis of representative SOC architectures

Reference	Primary Focus	Architectural Scope	Key Assumptions	Limitations / Contribution
[13]	SOC analyst performance metrics	Operational evaluation of SOC analysts	SOC efficiency depends on analyst detection and response performance	Provides valuable performance metrics (MTTD, MTTR, etc.), but does not propose an SOC architecture and does not address distributed cyber-physical systems such as UAV networks.
[14]	Human factors in SOC operations	Human and organizational SOC analysis	SOC effectiveness depends on analyst expertise and training	Focuses on socio-technical challenges in SOC environments; lacks architectural design for monitoring infrastructures and does not consider UAV-specific security requirements.
[15]	SOC implementation success factors	Organizational SOC deployment model	Effective SOC requires alignment of people, processes, and technologies	Provides an empirical model for SOC deployment but does not address monitoring architectures or cyber-physical infrastructures such as UAV ecosystems.
[16]	Integrated NOC–SOC architecture	Enterprise multi-layer monitoring framework	Integration of network management and security monitoring improves situational awareness	Designed for enterprise IT infrastructures with stable communication environments; not adapted to UAV mobility, distributed telemetry, or aerial network dynamics.
[18]	Secure autonomous drone operations through information fusion	Mission-level UAV security architecture	Secure UAV operations require information fusion, access control, cryptographic protection, and policy enforcement	Provides a comprehensive framework for secure autonomous drone operations and mission-level security management. However, it focuses on access control and secure information exchange rather than SOC functionalities such as SIEM correlation, threat intelligence integration, incident response orchestration, and centralized security operations.
[19]	UAV-based infrastructure monitoring and inspection	UAV data acquisition and photogrammetry framework	Accurate UAV inspections depend on optimized flight and imaging parameters	Provides a calibration framework for UAV-based infrastructure monitoring and smart oblique capture imaging. However, its focus is on data acquisition quality and photogrammetric reconstruction rather than UAV cybersecurity, threat detection, incident response, or SOC-oriented security operations.
Our Work (SOC2I)	UAV-oriented SOC framework with AI-based detection	Cyber-physical SOC architecture for UAV ecosystems	Centralized SOC analytics combined with distributed detection engines and AI-based anomaly detection	Extends traditional SOC concepts to UAV infrastructures by integrating UAV telemetry monitoring, IDS-based anomaly detection, and coordinated mitigation mechanisms within a unified SOC framework.

UAV security mechanisms, but rather their integration and operationalization within a SOC-oriented architecture.

However, none of the reviewed studies explicitly considers SOC deployment within UAV ecosystems or integrates UAV-specific cybersecurity mechanisms such as UAV IDS flight telemetry monitoring, or distributed aerial network security analytics.

Therefore, despite the progress made in SOC architecture research and UAV cybersecurity mechanisms, a clear research gap remains at the intersection of these two domains. Specifically, there is a lack of frameworks that integrate SOC operational capabilities with UAV-specific monitoring infrastructures and threat detection mechanisms.

Existing UAV security research primarily focuses on attack detection, communication protection, authentication, intrusion detection systems, physical-layer security, and mitigation techniques. In contrast, SOC2I focuses on the operational integration and coordination of these capabilities within a SOC-oriented architecture that incorporates SIEM-based event correlation, threat-intelligence support, risk-aware prioritization, analyst-supervised incident response, model-based mitigation, and resilient control mechanisms.

Consequently, while numerous UAV security solutions have been proposed, limited attention has been devoted to the development of operational frameworks that adapt SOC principles to UAV ecosystems. The proposed SOC2I framework represents an initial step toward addressing this gap by extending SOC concepts to UAV environments and enabling centralized monitoring, threat detection, incident response, and security orchestration across distributed UAV infrastructures.

1.3 Motivation and Paper Contribution

Given the multifaceted challenges posed by UAV security, this paper explores the integration of SOC principles within UAV cybersecurity environments. This approach envisions the seamless incorporation of an intelligent security framework into a SOC-oriented architecture. It highlights the increasing security challenges associated with the growing adoption of UAVs while proposing a framework designed to support their secure operation. The proposed framework combines proactive monitoring, adaptive response mechanisms, and advanced data analytics to strengthen threat detection, incident management, and operational resilience against evolving cyber threats.

The primary contributions of this paper are as follows:

- We highlight the key security issues associated with UAVs and the need for enhanced protective measures.
- We introduce the SOC-Innovative Intelligent Framework (SOC2I), which integrates SOC capabilities with AI-based models to provide robust security solutions.
- **Proactive and Adaptive Mechanisms**: We propose proactive surveillance and dynamic adaptive response mechanisms to anticipate and mitigate potential threats.
- We leverage advanced data analytics to improve threat detection and response strategies.

The rest of this paper is organized as follows. Section 2 provides an overview of UAV preliminaries, including their security concerns, AI detection techniques for attack detection, and the integration of SOC as a service for mitigation. Section 3 introduces our proposed SOC2I framework and the scheme design. Section 3.3 details the composition and processes of the framework. Section 4 presents the performance evaluation of our system model. Finally, Section 5 concludes the paper with remarks and potential future directions.

2 Background

2.1 UAVs General Overview

UAVs were substituted by Unmanned Aircraft System (UAS) [20]. It was proposed by the United States Department of Defense (DoD) [21] and the Federal Aviation Administration (FAA) in 2005. In general, UASs encompass UAVs, Ground Control Station (GCS), and the communication network [22] to exchange data.

The wireless channel model between the ground station and the UAV typically varies based on the flying altitude. Consequently, UAV networks consist of multiple UAVs with limited energy resources, functioning as Aerial Base Stations (ABS), relays, edge servers, or data collectors. These UAVs come in diverse types, each equipped with different specifications such as energy capacities, ranges, and configurations, and are commercially available. Their functionality extends across various applications facilitated by sensors, Global Positioning Systems (GPSs), cameras, stabilizers, and wireless interfaces. Positioned in proximity to the Internet of Things (IoT) environment, its primary responsibility is to receive substantial data volumes and provide outsourced data storage support to connected devices. Additionally, the system incorporates a computation module designed for conducting statistical analyses on the stored data and making informed decisions. The computation module is versatile, accommodating various applications executed by network-connected devices with computational tasks, thereby centralizing task processing. For UAVs to assist terrestrial networks effectively, diverse communication links are essential. In general, there exist various types of links, including UAV-to-UAV (U2U), UAV-to-GCS (U2G), and UAV-to-Infrastructure (U2I).

The inherent openness of wireless communication links exposes them to potential security threats. Successful impersonation of either the UAV or the GCS by an attacker could have severe consequences, particularly in military operations or applications intolerant to faults. In the field of civil aviation, an attack may lead to a UAV losing control or being manipulated with false control data, directing it into a restricted area and posing the risk of an aircraft incident. Consequently, it is imperative to implement mechanisms for data privacy.

Data privacy and safe information management have become major challenges due to the quick deployment of UAV systems in applications, including intelligent transportation and edge-enabled sensing infrastructures [23]. Sensitive data, such as user identities, biometric information [24], location trajectories, and operational telemetry, is regularly collected and processed by UAV platforms and needs to be shielded from misuse and illegal access. Recent research has proposed several mechanisms to strengthen UAV cybersecurity, including UAV IDS, federated learning–based detection architectures, hardware-assisted trust and attestation mechanisms, and swarm resilience algorithms designed to maintain coordination under adversarial conditions.

For instance, blockchain-based identity management [25, 26] has been suggested to enhance authentication and trust across UAV organizations via decentralized self-sovereign identity techniques. In addition, security architectures integrating edge computing [27] have been developed to protect communication channels and system operations. These technologies contribute to strengthening different security layers

in UAV ecosystems. While these approaches provide valuable capabilities for detecting anomalies or protecting specific components of UAV systems, they are typically designed as isolated security mechanisms targeting individual layers of the UAV architecture. As a result, they often lack a unified operational layer capable of correlating heterogeneous security events, aggregating telemetry and log data across distributed UAV nodes, and orchestrating coordinated incident response actions. In contrast, SOC paradigm provides centralized situational awareness, cross-layer monitoring, and coordinated mitigation through continuous log analysis and TI integration. Therefore, extending SOC principles to UAV ecosystems represents a fundamentally different operational approach, enabling system-wide visibility and coordinated defense that existing UAV-specific security mechanisms alone cannot provide.

2.2 Attack Models

The vulnerability of UAVs to various cyber threats necessitates a comprehensive understanding and proactive defense against adversarial attacks. There are distinct attack models that pose challenges for UAVs.

Through an exploration of these attack models, the subsequent assessment aims to provide insights into the multifaceted strategies and mathematical formulations employed to detect and mitigate attacks such as spoofing and jamming attacks on UAVs.

Spoofing attacks pose a significant risk to UAVs by targeting their sensors and navigation systems with deceptive information. In these attacks, false data is presented to mislead the UAV, compromising its ability to perceive its surroundings accurately. Spoofing techniques may include the falsification of GPS signals or the manipulation of sensor readings, introducing potential hazards to UAV operations. A fundamental challenge in spoofing attacks lies in the detection of deviations between expected and received signals. Quantifying the extent of misinformation introduced becomes crucial to safeguard UAV sensors against deceptive practices. To address this challenge, a mathematical model M is employed, defined as $M = |Deviation|$, representing the absolute deviation (D) between expected and received signals. The dynamic setting of the detection threshold τ based on historical data enables the identification of abnormal deviations indicative of a potential spoofing attack.

For jamming attacks, they target the communication systems of UAVs, aiming to disrupt the transmission and reception of critical data. In these attacks, deliberate interference saturates communication channels with noise, causing a decrease in the signal-to-noise ratio (SNR) and hindering effective communication between the UAV and its control center. The jamming attack's main issue revolves around detecting abrupt decreases in the signal-to-noise ratio, signaling potential interference with communication signals. The calculation of the signal-to-noise ratio (SNR) ($SNR = \frac{S}{N}$), where S represents signal power and N represents noise power, becomes crucial. An abrupt decrease in SNR below a dynamically defined threshold σ indicates the presence of jamming, prompting further investigation and the implementation of counteractive measures.

Beyond spoofing and jamming, UAV systems are also exposed to link hijacking attacks in which adversaries take over or manipulate the command-and-control (C2)

channel between the UAV and the GCS. Such attacks typically manifest as abnormal command sequences, unexpected control mode transitions, or inconsistencies between commanded and executed maneuvers. UAV onboard computing units may be compromised by malware, leading to unauthorized mission logic changes, payload data exfiltration, or resource exhaustion. Practical indicators include abnormal CPU/memory usage, unexpected process activity, firmware integrity violations, or irregular telemetry reporting behavior. Insider threats or stolen credentials may enable unauthorized access to the GCS, mission plan manipulation, or malicious configuration updates. This can be reflected in anomalous authentication patterns, unusual privilege usage, and unexpected configuration or mission upload events. In SOC2I, these attack classes are treated as sources of measurable *deviation* in monitored telemetry and logs, which can be captured by statistical and behavioral indicators used in the anomaly detection module.

2.3 Security Operation Centers (SOCs)

SOCs play an essential role in the prevention, detection, and mitigation of cyberattacks, and their importance has steadily increased with the growing complexity of modern networked systems. In this work, we adopt the SOC paradigm as an operational model for continuous monitoring, correlation, and incident response; however, we explicitly situate this paradigm within UAV cybersecurity, where the protected system is not a conventional enterprise network but a cyber-physical ecosystem composed of airborne platforms, ground control stations (GCS), mission payloads, and heterogeneous air-ground communication links.

Unlike traditional SOC settings, UAV security architectures typically incorporate (i) resource-constrained embedded components on-board the UAV, (ii) dynamic and intermittently connected communication topologies (U2U, U2G, and U2I), and (iii) mission- and safety-critical constraints that couple cyber incidents with physical consequences. Accordingly, the integration of SOC capabilities within UAV infrastructures represents a critical advancement in cybersecurity, enabling proactive monitoring and adaptive incident response across interconnected aerial platforms. Moreover, several existing UAV security architectures already implement *SOC-like* functions such as centralized logging at the GCS, anomaly detection over flight telemetry, and coordinated response workflows but these functions are often realized as isolated modules (e.g., IDS-only components) rather than as a unified SOC-oriented operational architecture.

An SOC functions as a centralized (or logically centralized) operational unit that monitors, analyzes, and responds to security events in real time. Leveraging advanced analytical and automation tools, it correlates multiple data sources to identify anomalies and initiate appropriate mitigation actions. Through continuous observation and correlation, an SOC enhances system resilience, reduces response latency, and provides a unified defense layer against attacks such as spoofing and jamming. Within UAV ecosystems, this integration strengthens trust, coordination, and mission assurance across multiple nodes and communication channels, including both airborne and ground segments.

The SOC architecture may vary depending on operational scale and security requirements, but it typically comprises several interdependent components. In UAV-oriented deployments, these components must explicitly ingest UAV telemetry streams (navigation, control, sensor payload), communication traces (link quality, packet/flow metadata), and mission-context signals (flight phase, geofencing status), in addition to conventional logs:

- **Network Perimeter:** Composed of routers, firewalls, secure gateways, and (where applicable) UAV communication controllers that manage and secure traffic between UAV nodes, GCS, and supporting infrastructure.
- **Log Collection:** Aggregates telemetry, system logs, and air-ground communication logs from distributed UAV nodes and ground assets to support centralized correlation and forensic analysis.
- **Security Information and Event Management (SIEM):** Correlates multi-source UAV events (telemetry anomalies, link anomalies, access violations) to detect patterns and early indicators of compromise.
- **Threat Intelligence:** Integrates external and internal intelligence feeds (vulnerabilities, IOCs, attacker TTPs) to contextualize alerts; in UAV systems, this also includes UAV-specific threat patterns (e.g., GNSS spoofing signatures, RF jamming profiles).
- **Endpoint Protection:** Deploys distributed protection mechanisms such as IDS and Endpoint Detection and Response (EDR) tools across UAV and ground assets, subject to on-board compute and energy constraints.
- **IDS (UAV-oriented):** Monitors both cyber and cyber-physical indicators, including deviations in flight telemetry consistency, abnormal control-command sequences, and anomalies in U2U/U2G/U2I communications; alerts can trigger containment or safe-mode behaviors.
- **Data Loss Prevention (DLP):** Monitors and controls mission data flows (e.g., imagery, sensor payload) to prevent leakage or unauthorized exfiltration, particularly during relay or backhaul to ground infrastructure.

In a UAV-oriented context, these entities operate in a tightly coupled manner. The network perimeter governs communication control through traffic filtering and access enforcement. In addition, log collection provides the foundational telemetry and traces for analysis, and the SIEM correlates and prioritizes security events across air and ground segments. TI enriches these correlations with UAV-relevant context, while Endpoint Protection and IDS provide localized anomaly detection and containment. Importantly, UAV constraints motivate a hybrid operational model: lightweight detection at the edge (on-board or near-edge) combined with centralized correlation and incident coordination at the SOC/GCS layer, which is consistent with how several UAV security architectures already separate on-board monitoring from ground-based decision-making.

SOC analytics may be partially automated, with human analysts supervising alerts, or increasingly automated through AI-driven decision support for real-time responsiveness. In UAV environments, the response process must extend beyond detection

to the orchestration of coordinated mitigation actions that preserve safety and mission continuity. Depending on severity, responses may range from generating alerts and re-authentication of control links to notifying the GCS, triggering geofencing constraints, isolating compromised nodes within a fleet, or executing automated containment protocols (e.g., safe landing/return-to-home policies) when cyber indicators suggest elevated operational risk.

Ultimately, an effective SOC architecture for UAV systems relies on the integration of these functional components within a unified operational workflow that is explicitly grounded in UAV cybersecurity architectures and IDS practices. Such integration supports continuous threat assessment, adaptive defense mechanisms, and informed decision-making, essential requirements for maintaining the security, reliability, and mission continuity of UAV networks.

3 Proposed Solution: Novel SOC2I Framework

3.1 SOC2I Framework Scheme Design

The SOC2I framework extends contemporary SOC–AI integrations by adapting them to the cyber-physical and operational constraints of UAVs. The overall architecture of the proposed SOC2I framework is illustrated in Figure 1, which summarizes the system's main components and their interactions. The figure presents the logical architecture of SOC2I. The operational implementation of the framework is further detailed through the Attacks Resilient Control (ARC) module, the Model-based Attack Mitigation (MaM) layer, the Distributed Detection Grid, and the workflow described in Algorithm 1. These components collectively define telemetry acquisition, anomaly detection, threat correlation, incident prioritization, and response orchestration within realistic UAV cyber–physical environments.

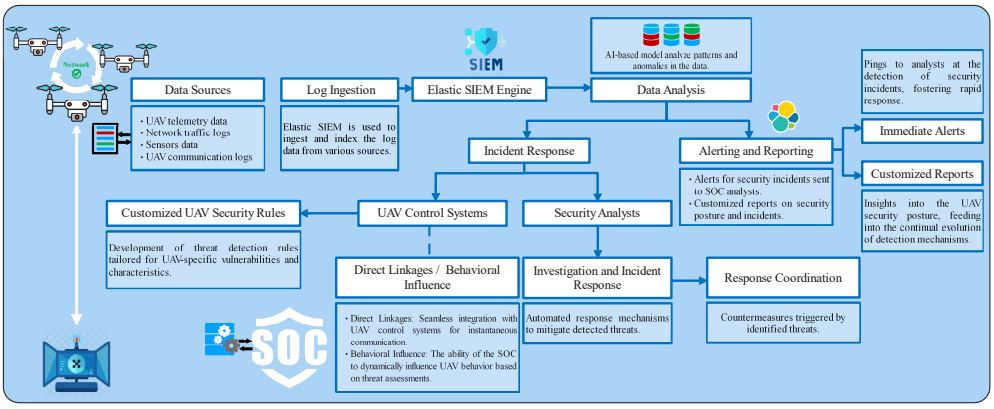

Fig. 1 SOC2I Proposed Scheme Design.

At its core is a context-aware fusion layer that correlates aeronautical telemetry, flight dynamics, and communication traces with Elastic SIEM analytics. This fusion

enables timely anomaly detection and adaptive response while preserving on-board and network resource budgets.

We adopt the classical Z-score statistic,

$$Z = \frac{X - \mu}{\sigma}, \tag{1}$$

for rapid, single-variable deviation detection. The justification for this choice is threefold. First, Z-scores are computationally trivial and therefore suitable for real-time, resource-constrained environments such as edge nodes or embedded SOC connectors. Secondly, thresholded alerting and downstream risk scoring can easily incorporate the Z-score, which offers a normalized deviation metric that is directly interpretable. Third, when telemetry variables are approximately Gaussian after simple normalization, Z-scores yield near-optimal detection of mean shifts. Important limitations are acknowledged. Z-scores are suboptimal for heavy-tailed or multimodal distributions and are insensitive to small multivariate shifts. Where such conditions are expected, we recommend (and implement as fallbacks) robust univariate statistics (e.g., median absolute deviation), exponentially weighted moving averages for concept drift, or multivariate alternatives such as the Mahalanobis distance or multivariate change detection. The SOC2I design defaults to Z-score for initial screening and escalates to more sophisticated detectors when distributional assumptions fail or when correlated anomalies are observed.

The SOC real-time prioritization is implemented with a linear risk score,

$$\text{Risk_Score} = \alpha \cdot I + \beta \cdot L, \tag{2}$$

where I denotes estimated impact and L denotes estimated likelihood. We select a linear combination for three reasons: transparency, ease of calibration by analysts, and smooth integration with thresholded automation. Alternatives such as multiplicative risk models, Bayesian risk fusion, or utility-based decision functions can capture nonlinear interactions between impact and likelihood. When interactions are expected to be significant, we recommend extending the linear form to a generalized additive model or employing a Bayesian network to quantify epistemic uncertainty. In practice, the linear form is used for baseline prioritization; more sophisticated fusion is engaged for high-value incidents or persistent threats.

Autonomy in UAV response is achieved via a parameterized decision policy denoted

$$\text{UAV_Behavior} = f(\text{TL}, \text{CB}), \tag{3}$$

where TL is the threat level and CB are contextual behavioral priors. We deliberately design f as a hybrid policy: a safety-first rule layer for immediate, verifiable mitigations, followed by a lightweight, interpretable policy learner (for example, a shallow decision tree or a parameterized policy with constrained action set). This design balances the need for provable safety and operational explainability against the potential performance gains of unconstrained reinforcement learning. Pure deep reinforcement learning is avoided at the autonomous control layer because it complicates

verification, increases sample complexity, and reduces interpretability in safety critical UAV operations. Where RL is used experimentally, it remains confined to simulation environments and is gated by formal verification before any field deployment.

It is important to emphasize that SOC2I is proposed as a SOC-oriented UAV cybersecurity architecture rather than as a standalone anomaly detection algorithm. The contribution of SOC2I does not reside in the novelty of Z-score normalization, LOF scoring, or linear risk prioritization considered individually. Instead, SOC2I integrates these lightweight and interpretable mechanisms within a unified operational workflow combining distributed detection, SIEM-based correlation, risk-aware prioritization, analyst-supervised incident response, model-based mitigation, and resilient control adapted to UAV cyber-physical constraints.

The subsequent subsections present the principal SOC2I components and the rationale for algorithmic choices.

3.2 Attacks Resilient Control

The Attacks Resilient Control (ARC) module forms the SOC2I defensive control plane. ARC performs rapid behavioral deviation detection, containment, and graceful degradation so that mission objectives are preserved under adversarial influence. ARC uses a combination of model-based estimators for nominal dynamics, residual generation for fault and attack detection, and a parametric controller reconfiguration strategy to preserve stability and safety. Model-based control is favored over purely heuristic fallback rules because it permits provable bounds on deviation, enables predictive mitigation, and facilitates more accurate root cause attribution. When model uncertainty is high, ARC relaxes to conservative, certified safe behaviors until confidence is restored. To operationalize attack-aware control, ARC continuously compares the observed UAV telemetry with the expected system behavior predicted by a nominal dynamics model. The resulting residual signal is defined as

$$r_t = x_t - \hat{x}_t \tag{4}$$

where (x_t) denotes the observed telemetry vector and $(\hat{x}_t)$ represents the corresponding state estimate generated by the nominal system model. The residual signal serves as an indicator of deviations from expected operational behavior. A potential attack or abnormal operating condition is identified when the residual magnitude exceeds a predefined threshold:

$$|r_t|_2 > \tau_r \tag{5}$$

where (τ_r) denotes the residual detection threshold. This mechanism enables ARC to distinguish normal mission variations from significant behavioral deviations potentially associated with cyberattacks, communication disturbances, or system faults. When the threshold condition is satisfied, ARC initiates a safety-preserving control strategy that transitions the UAV toward a protected operational mode (u_t^{safe}). The objective of this mode is to maintain flight stability, preserve communication integrity, and ensure mission continuity while limiting the propagation of potentially compromised control decisions. Depending on the estimated threat severity and operational context, the

response may include safe-hold operation, return procedures, communication-link protection measures, mission reconfiguration, or escalation to the SOC incident-response workflow. Furthermore, the behavioral policy ($f(TL, CB)$) is implemented as a safety-gated decision function that combines the current threat level (TL) with contextual behavioral information (CB), including mission phase, communication-link quality, telemetry consistency, and operational safety constraints. Rather than relying on an unconstrained black-box controller, the policy maps these inputs to a bounded set of validated response actions. This design preserves interpretability, facilitates analyst supervision, and ensures that autonomous responses remain aligned with UAV safety requirements and mission objectives.

3.3 Distributed Detection Grid

Elastic SIEM integration orchestrates a *Distributed Detection Grid* consisting of multiple lightweight Detection Engines deployed at strategic network nodes and on selected UAVs. The grid decentralizes initial detection to reduce latency and bandwidth usage while preserving centralized correlation and forensic capability. This distributed architecture is chosen because UAV operations are inherently geographically dispersed, have intermittent connectivity, and benefit from local, near-real-time detection.

Detection Engines perform local preprocessing, feature extraction, and preliminary anomaly scoring. Aggregated outputs are reported to the Centralized SOC, which performs cross-engine correlation, long-term profiling, and coordinated mitigation. This hybrid decentralization yields the low latency of edge detection and the global situation awareness of a central SOC.

3.4 Anomaly Detection

The Detection Engine within the SOC2I framework serves for the detection process. These analyses ensure a swift and targeted response to potential threats through advanced and adaptive mechanisms. Therefore, the detection engine operates based on a highly accurate algorithm based on the local outlier factor (LOF) technique. The LOF method is explicitly designed for variable density regions. UAV telemetry often exhibits heterogeneous sampling densities due to maneuvering, differing mission phases, and environmental changes. LOF adapts to such variability by comparing local densities rather than relying on global thresholds. Moreover, LOF yields a continuous, interpretable anomaly score rather than a binary label. This raw score enables tiered escalation policies and analyst review without repeated scoring. Alternative unsupervised detectors were considered. Isolation Forests provide fast, scalable detection but assume anomalies are easier to isolate than normal points and do not naturally adapt to local density variations. One-class SVMs can be effective but are sensitive to hyperparameters and scale poorly with data volume. For multivariate temporal anomalies, sequence models (autoencoders or recurrent models) can capture dynamics more precisely but require substantially more labeled or synthetic training data and higher computational cost. Consequently, SOC2I adopts LOF as the default density-aware detector.

Formally, LOF computes a relative density score by comparing the reachability density of a point with that of its k nearest neighbors. Denoting reachability density by $\mathrm{rd}(\cdot)$, the LOF score for a point x is higher.

$$\mathrm{LOF}(x) = \frac{\frac{1}{|N_k(x)|}\sum_{y \in N_k(x)} \mathrm{rd}(y)}{\mathrm{rd}(x)}. \tag{6}$$

LOF values indicate greater outlierness. The neighborhood size k is treated as a tunable parameter; SOC2I selects it k using cross-validation on benign mission data and revalidates periodically to account for concept drift. For example, UAVs spoofing and jamming attack strategies and mitigation baselines are formulated as follows:

1. **Spoofing Attack**: GPS spoofing involves transmitting false GPS signals to the UAV and provides it with inaccurate position data. We can model this problem using the following mathematical formulation: declaring $P = [p_1, p_2, p_3]$ the true positions of a UAV GPS receiver in R^3 with $S = [s_1, s_2, s_3]$ the position that the GPS receiver is deceived with due to the GPS spoofing. Hence, a function $f : R \leftarrow R^3$, such that $f(P) = S$ and f are consistent with the actual GPS signals. For each $i = [1, 2, 3]$, there exists a function $g_i : R^3 \leftarrow R$ that relates the spoofed GPS signal s_i to the actual GPS signal a_i, and the function f satisfies $f_i(P) = g_i(f(P))$ for all i. Therefore, a GPS spoofing attack can then be formulated to minimize the distance between the true position P and the spoofed position S.
2. **Jamming Attack**: Let S_t be the genuine signal on UAVs wireless communication channel at a time t and let N_t be the noise signal at a time t. The total signal at a time t is given by $T_t = S_t + N_t$. The jamming attack occurs when an attacker transmits a jammed signal J_t with the same frequency f of the target channel, which allows the performance of a jamming attack A_j. Therefore, the total signal at a particular time t that corresponds with the jamming attack time is given by: $X_t = S_t + J_t + N_t$. This will disturb the normal operation of the communication channel, quantified by a disruption function $F(X)$, which measures the degree to which the jamming attack has disturbed the signal at a time t. Therefore, the attacker seeks to maximize $F(X_t)$ to maximize the disruption. The counter function established by the UAV user aims to defend itself by minimizing $F(X_t)$. This could be directed at a single target or could be of a broad nature to affect largely. The extent of the attack is quantified using a QF function applied on $QF(X_t)$, which measures the area over which the jamming attack is effective.

The deviations caused by spoofing, jamming, or other like link hijacking, malware activity, or insider compromise are reflected in the monitored feature vector x_t (telemetry, link-quality indicators, command/control traces, and security logs). SOC2I quantifies feature-wise deviations through Z-score normalization $z_{t,i} = (x_{t,i} - \mu_i)/\sigma_i$, while LOF captures abnormal multivariate operating regimes when the joint behavior of UAV telemetry and communication traces departs from nominal mission profiles.

3.5 Model-Based Attack Mitigation (MaM)

MaM is a strategic layer within the SOC2I framework that enhances the overall resilience of UAV security by leveraging advanced modeling techniques. The proactive identification and mitigation of potential attacks are essential components of SOC2I as a robust defense strategy. MaM provides a predictive, adaptive layer to preempt and mitigate attacks before they fully manifest. This predictive capability enhances the overall agility of the SOC2I framework. MaM uses parametric or low-order state-space models to forecast nominal telemetry and to estimate residuals attributable to attacks. The motivation for model-based mitigation is twofold. First, predictive models enable early action when residuals show consistent divergence from forecasts. Second, models support the synthesis of minimally invasive mitigations that preserve mission goals. For a given telemetry observation (x_t), the model (M) represents a predictive approximation of nominal UAV behavior and generates an expected system state ($\hat{x}_t$). The deviation between observed and predicted behavior is quantified through the residual error

$$e_t = x_t - \hat{x}_t \tag{7}$$

where (e_t) denotes the discrepancy between the current telemetry and the nominal operating conditions estimated by (M). Persistent or significant residual deviations indicate potential attack activity, abnormal system behavior, or unexpected environmental disturbances. Based on the magnitude and persistence of these residuals, MaM generates mitigation recommendations while minimizing disruption to the ongoing mission. Such minimally invasive mitigations may include increased monitoring, communication-link re-authentication, isolation of suspicious communication channels, transition to conservative operating modes, or escalation to SOC analysts when automated mitigation cannot be safely applied. MaM-Based approach is particularly beneficial in scenarios where attacks exhibit unique characteristics or are previously unseen. Traditional rule-based systems may struggle with novel attack patterns, whereas models can adapt and learn from new data, making them more powerful at countering sophisticated threats. This adaptability is crucial in the context of UAV security, where attackers may employ evolving tactics to exploit vulnerabilities. Additionally, MaM contributes to the continuous learning loop within the SOC2I framework. The models are updated based on the feedback loop from the incidents and responses.

Algorithm 1 gives the SOC2I sequential flow. The pseudocode provides clear interfaces between detection, scoring, response, learning, and control integration.

Table 2 provides the formal definitions of all symbols, parameters, and variables used throughout Algorithm 1, linking the procedural flow to its underlying mathematical formulation.

Algorithm 1: SOC2I Sequential Flow

Input : Telemetry vector $x_t \in \mathbb{R}^d$, logs $\mathcal{L}$, communication traces, and distributed grid reports $\mathcal{R}_t$

Output: Detected anomalies $\mathcal{A}$, risk scores Risk(e), and response actions

Initialize $\mathsf{Buf}_{\Delta t}$ and parameters $\{\mu, \sigma, k, w_z, w_\ell, \tau_a, \alpha, \beta, \tau_1, \tau_2, \lambda\}$

for *each observation time* t **do**

  for $i \leftarrow 1$ **to** d **do**

    $z_{t,i} \leftarrow (x_{t,i} - \mu_i)/\sigma_i$

  Compute $\mathrm{LOF}_k(x_t)$

  $s_t^{\mathrm{local}} \leftarrow w_z \|z_t\|_\infty + w_\ell \max(0, \mathrm{LOF}_k(x_t) - 1)$

  $s_t^{\mathrm{grid}} \leftarrow \dfrac{\sum_{j=1}^{N_d} c_t^{(j)} s_t^{(j)}}{\sum_{j=1}^{N_d} c_t^{(j)} + \varepsilon}$

  $s_t \leftarrow \max(s_t^{\mathrm{local}}, s_t^{\mathrm{grid}})$

  if $s_t > \tau_a$ **then**

    Append $e_t = (t, x_t, z_t, \mathrm{LOF}_k(x_t), s_t, \mathcal{R}_t)$ to $\mathcal{A}$

  Push s_t into $\mathsf{Buf}_{\Delta t}$

  for *each* $e \in \mathcal{A}$ **do**

    $L(e) \leftarrow \mathrm{norm}(\mathbf{1}[\exists j : s_t^{(j)} > \tau_a], \mathrm{runlength}(e), \mathrm{QoS_drift}(e))$

    $I(e) \leftarrow \sum_{m \in \mathrm{affected}} w_m \, \mathrm{degradation}_m(e)$ with $\sum_m w_m = 1$

    $\mathrm{Risk}(e) \leftarrow \alpha I(e) + \beta L(e)$

  $\overline{s}_{t,\Delta t} \leftarrow \mathrm{mean}(\mathsf{Buf}_{\Delta t})$

  $\widehat{r}_t \leftarrow \lambda \widehat{r}_{t-1} + (1 - \lambda)\overline{s}_{t,\Delta t}$

  if $\widehat{r}_t \le \tau_1$ **then**

    Threat Level $\leftarrow$ Low

  else if $\widehat{r}_t \le \tau_2$ **then**

    Threat Level $\leftarrow$ Moderate

  else

    Threat Level $\leftarrow$ High

  if *Threat Level is Low* **then**

    Execute automatic low-severity response

  else if *Threat Level is Moderate* **then**

    Evaluate $\mathcal{U}_t \leftarrow \mathrm{MaM_evaluate}(\mathsf{M}, x_t, \mathcal{L})$

    Apply $\mathcal{U}_t$ if safe

  else

    Alert SOC analysts

    Apply safe-hold behavior through ARC

    Evaluate and apply vetted mitigation actions

  Log detected anomalies, risk scores, and response actions

3.6 Operational Integration of SOC2I in UAV Systems

SOC2I adapts core SOC operational functions to the cyber–physical characteristics of UAV systems. Unlike conventional enterprise infrastructures, UAV environments involve dynamic network topologies, intermittent air–ground communication links,

Table 2 Mathematical Symbols Used in Algorithm

Symbol	Definition
k	Number of nearest neighbors used by the LOF algorithm.
λ	Exponential smoothing coefficient used in threat-level estimation.
Δt	Time window used for anomaly score aggregation and buffering.
$x_t \in \mathbb{R}^d$	Multivariate UAV telemetry feature vector at time t containing d monitored parameters (navigation, communication, and system metrics).
μ_i, σ_i	Mean and standard deviation of telemetry feature i used for Z-score normalization.
$z_{t,i}$	Standardized Z-score of feature i, computed as $z_{t,i} = (x_{t,i} - \mu_i)/\sigma_i$.
$\mathrm{LOF}_k(x_t)$	Local Outlier Factor computed for telemetry vector x_t using k nearest neighbors.
w_z, w_ℓ	Weight coefficients for Z-score and LOF contributions to the anomaly score.
s_t^{local}	Local anomaly score combining statistical and density-based indicators.
$s_t^{(j)}$	Anomaly score generated by distributed detection engine j.
$c_t^{(j)}$	Confidence weight associated with detection engine j, reflecting reliability of its observation.
N_d	Number of distributed detection engines participating in anomaly detection.
ε	Small constant used to stabilize distributed anomaly score aggregation.
s_t^{grid}	Aggregated anomaly score obtained from distributed detection engines.
s_t	Final anomaly score used for threshold comparison.
τ_a	Anomaly detection threshold.
$\mathsf{Buf}_{\Delta t}$	Sliding buffer storing anomaly scores over time window Δt.
$\widehat{r}_t$	Exponentially smoothed anomaly evidence used for threat level estimation.
τ_1, τ_2	Thresholds for classifying threat levels (Low, Moderate, High).
$I(e)$	Estimated impact of anomaly event e.
$L(e)$	Estimated likelihood of event e based on persistence and corroboration.
$\mathrm{Risk}(e)$	Risk score combining impact and likelihood.
$\mathcal{U}_t$	Set of mitigation actions proposed by the Model-based Attack Mitigation (MaM) module.
$f(\mathrm{TL}, \mathrm{CB})$	Behavioral policy mapping threat level and contextual behavior to UAV control actions.

and strict real-time safety constraints. To handle these situations, SOC2I merges quick detection of problems at the edge with centralized SOC analysis and managed response methods. Within this architecture, TI is used primarily as a contextual enrichment layer during SIEM correlation. Alerts created from unusual data or communication issues are enhanced with important information related to UAVs, like signs of GNSS spoofing or jamming, strange radio frequency patterns (like changes in SNR/RSSI), and tags based on mission rules or known attack methods. These contextual details help prioritize alerts better and connect information from UAV telemetry, ground control station logs, and network events without needing a separate external threat intelligence platform. SOC2I also incorporates a tiered analyst-in-the-loop workflow consistent with SOC operational practices. Low-severity events cause automated handling and logging, while moderate-severity incidents cause semi-automatic procedures with stricter safety checks. SOC analysts receive high-severity threats and enforce safety-preserving UAV behaviors like safe-hold or mission-safe fallback modes.

This approach focuses human supervision on the most safety-critical situations and maintains rapid automated responses for routine anomalies. Playbook-like response procedures are integrated within the incident response stage of SOC2I. These procedures include control-link re-authentication when command-channel anomalies are detected, isolation of compromised communication nodes, and activation of safety mechanisms through the Attacks Resilient Control module. In parallel, the MaM component proposes mitigation actions derived from system models, which are executed only when verified as safe for the current operational context. Finally, SOC2I aligns these SOC mechanisms with UAV system constraints. The Distributed Detection Grid allows UAV nodes or edge gateways to spot problems locally while still keeping a central connection for SOC analysis. Lightweight statistical indicators support resource-constrained environments, whereas safety-gated responses ensure that mitigation actions preserve mission continuity and flight safety. Together, these adaptations position SOC2I as a SOC-oriented operational workflow tailored to the specific requirements of UAV cyber–physical systems. The deployment model assumes lightweight detection capabilities operating at UAV or edge-gateway level, while centralized SIEM analytics and incident coordination are executed at the SOC layer.

4 SOC2I Experimental Setup and Replay-Based Validation

4.1 Replay environment

For UAV flight log analysis, the selection and setup of an appropriate simulation tool are of paramount importance to ensure accurate data analysis and insights. The specific requirements of our research, which include the need for flexibility, scalability, and seamless integration with AI models, have driven our choice of simulation tool. Among the various options considered, the Elastic SIEM (ELK Stack) has emerged as a compelling candidate for our research objectives.

The ELK Stack offers exceptional flexibility, with the ability to efficiently ingest, parse, and transform CSV flight logs. Logstash, the data processing component, is designed to handle data in CSV format seamlessly, ensuring that our UAV flight log data is compatible with the tool. Furthermore, the ELK Stack's exceptional scalability makes it ideal for managing large volumes of data generated by UAVs, allowing for comprehensive analysis.

4.2 Evaluation and Validation

To conduct SOC2I validation and evaluations for attack detection, we applied a structured flow. The development paradigm is composed of four major stages. They are described as follows:

1. **Data Visualization and Assimilation**: This is the first established step. It involves the ingestion of CSV data [28] that emulates jamming and spoofing attack scenarios into the ELK Stack platform. This phase necessitates the creation of log

entries formatted to align with ELK Stack's data processing standards. The experiments utilize the publicly available UAV Attack Dataset from IEEE DataPort, which provides multivariate UAV telemetry collected during normal flight operations as well as under GPS spoofing and RF jamming attacks. The dataset offers realistic attack traces and operational measurements suitable for evaluating UAV cybersecurity monitoring, anomaly detection, and incident response frameworks.

2. **Rule Creation**: Subsequently, the formulation of detection rules and queries within ELK Stack is imperative. These rules serve the purpose of identifying patterns and anomalies present within the CSV data, signifying the occurrence of jamming or spoofing attacks. Custom Logstash filters and Kibana dashboards are developed as integral elements to visualize and oversee the data, facilitating effective monitoring. SOC2I integrated two rules for both attacks. These rules follow two queries of detection for jamming and spoofing detection, respectively.
3. **Testing and Evaluation**: The testing phase involves the dataset-driven validation within the CSV dataset, closely monitoring ELK Stack for the activation of predefined detection rules, job performance. This active monitoring enables the identification and comprehensive investigation of potential incidents based on predefined patterns and anomalies.
4. **Refinement**: Based on the insights gained from the testing and evaluation phase, a critical refinement step is undertaken. This process involves making changes to the detection rules to make them better.

Following testing and evaluation, the system monitors for alerts and notifications triggered by predefined detection rules. This allows for the identification and investigation of potential incidents based on patterns and anomalies. The results of the testing phase inform the refinement of detection rules and procedures. This iterative process aims to optimize the efficiency of the detection process, ultimately leading to enhanced security for UAV operations.

In summary, the approach presented ensures a systematic and methodical means of simulating, testing, and refining the detection of jamming and spoofing attacks within the ELK Stack environment.

After using the Detect Outlier operator, the outlier is appended to the resulting dataset. Figures 2 and Figure 3 show the result of some features of the dataset with outlier scores represented as red data points for jamming and spoofing. In the results, the outlier score is observed with accurate results of the SOC2I detection. The outliers in plot features indicate that the spectrum of anomalies is expected to be regular data points.

These points are closer to the anomalies, therefore, they are expected to be outliers. If an additional boolean flag is required to signify whether a data point is an outlier, a numeric-to-binary operator may be introduced into the resulting dataset. This operator converts the external numeric result into a true or false binary value, taking into account the threshold specified in the operator parameter and the output from the LOF operator.

To further assess the validation of SOC2I framework, there are three metrics used for performance evaluation. They are described as follows:

1. **Mean Time to Detect (MTD)**: MTD is the statistical measure representing the average duration required to identify and detect a security event. This statistic is utilized to monitor and assess the performance of SOC analytics, as well as to evaluate the overall detection capabilities of the SOC as a service.
2. **Mean Time to Acknowledge (MTA)**: The MTA measures the duration between the generation of an alert on the SIEM or monitored dashboard and the initiation of an inquiry and resolution of the issue by the SOC framework. The main focus is on the time needed to identify and initiate problem-solving. This statistic is valuable for monitoring the responsiveness and the alert effectiveness. Furthermore, this statistic is valuable for monitoring the efficiency of incident response and the occurrence of alert exhaustion. It is determined by summing the duration between alarm and acknowledgment and then dividing it by the total number of events.
3. **Detection Rate**: The detection rate (alternatively known as sensitivity, recall), is a metric that is employed in analyses to assess the effectiveness of the simulation in accurately identifying all pertinent occurrences of a particular group of items.

4.3 SOC2I Performance Analysis and Results

Table 3 for SOC2I rules replay-based evaluation provides a comprehensive overview of the applied AI solution methods and their corresponding outcomes in a log-replay experimentation. The table encompasses three distinct rules: SOC2I-Jamming Rule, SOC2I-Spoofing Rule, and SOC2I Overall Rule. Each rule is associated with an applied LOF method and showcases the average duration of the simulation. The Responses State / Ratio shows the success state of the simulation. The given SOC2I value indicates the success of the established rules. For instance, the SOC2I-Jamming Rule took an average duration of 167 milliseconds to process and was marked as Succeeded in the response state, with a total of 1372 responses and 57 reported alerts of jamming attacks.

Similarly, the SOC2I-Spoofing Rule had an average duration of 170 milliseconds, denoted as Succeeded, with an equivalent total of 1372 responses and 38 reported spoofing alerts. The SOC2I Overall Rule, which aggregates the outcomes of all rules, is represented in the table with relevant response statistics. These results serve as a valuable reference for understanding the performance and effectiveness of the applied AI methods in simulating SOC2I rules. Table 4 presents the SOC2I Job Performance

Table 3 SOC2I Rules simulation

Rule	Average duration	Response Number	Reported Alerts
SOC2I-Jamming Rule	167ms	1372	57
SOC2I-Spoofing Rule	170ms	1372	38
SOC2I Overall Rule	-	2864	95

Metrics and Results that provide a detailed analysis of key performance metrics and outcomes related to specific SOC2I jobs. The table describes the essential information for two distinct jobs, SOC2I-Specific-Jamming and SOC2I-Specific-Spoofing. Each job

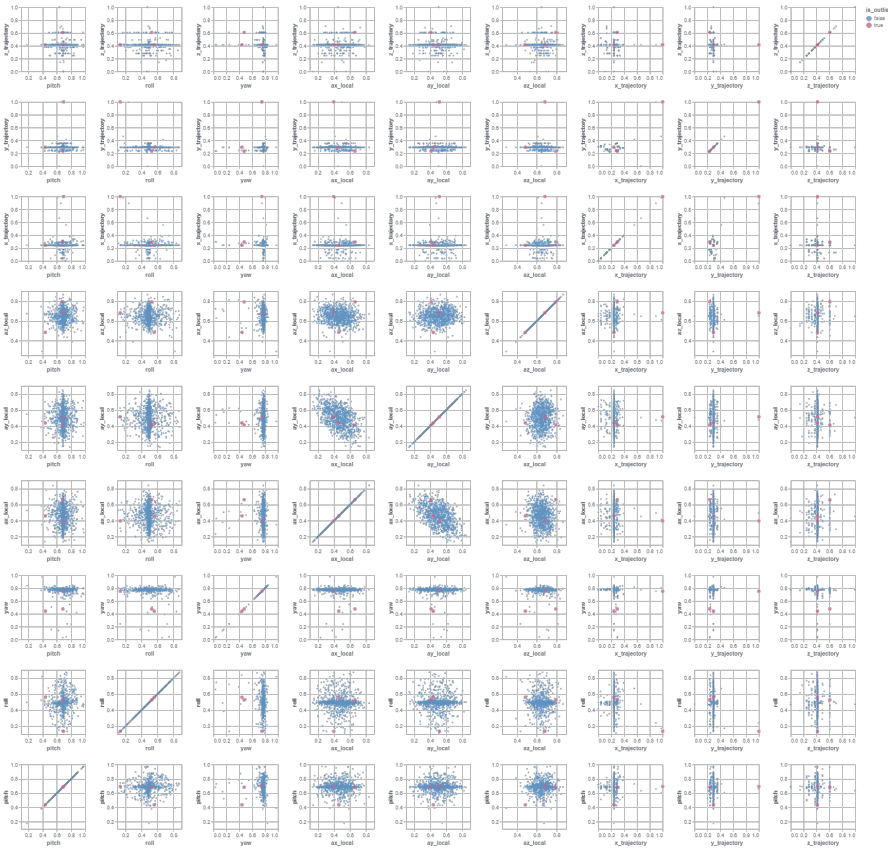

Fig. 2 SOC2I Patterns Results for Jamming Attack Detection

Table 4 SOC2I Job Performance Metrics and Results

Job ID	Mean Time to Detect	Mean Time to Acknowledge	Detection Rate
SOC2I-Specific-Jamming	632.8ms	268ms	0.97
SOC2I-Specific-Spoofing	552.8ms	272ms	0.82

ID is associated with essential performance metrics, including MTD, MTA, and the detection rate.

For the SOC2I-Specific-Jamming job, the MTD is reported as 632.8 milliseconds, indicating the average time taken to identify an event. The MTA for this job is 268 milliseconds, representing the average time taken to acknowledge the identified event. The corresponding detection rate is exceptionally high at 0.97, reflecting the effectiveness of the system in promptly and accurately detecting jamming incidents. Similarly, for the SOC2I-Specific-Spoofing job, the MTD is recorded as 552.8 milliseconds, showcasing a swift identification process. The MTA is reported as 272 milliseconds, indicating a prompt acknowledgment of identified spoofing events. The detection rate for this job is 0.82, signifying a strong capability to identify and respond to spoofing incidents.

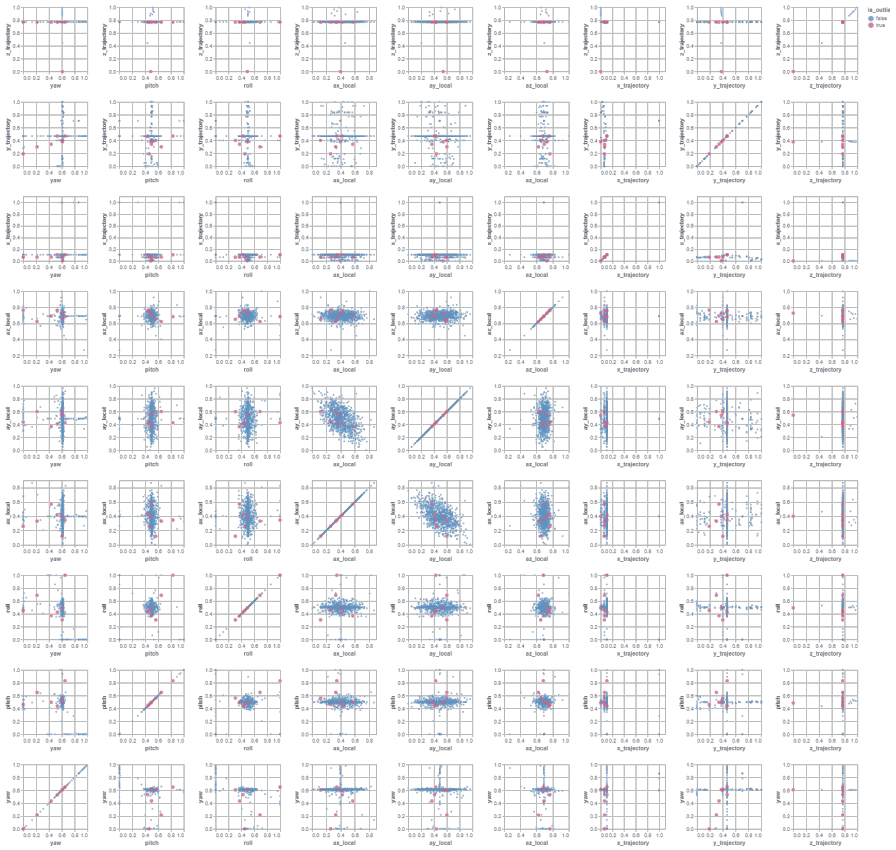

Fig. 3 SOC2I Patterns Results for Spoofing Attack Detection

These results are a comprehensive reference for evaluating the performance and efficiency of specific SOC2I jobs. They provide insights into the system's ability to detect and respond to jamming and spoofing events based on critical metrics.

The objective of the evaluation is to assess the ability of the proposed architecture to detect, correlate, and respond to UAV security events within a SOC-oriented operational environment.

4.4 Discussion

SOC integration within UAV systems represents an emerging and rapidly evolving domain in cybersecurity. While the SOC2I framework demonstrated enhanced detection capability and operational resilience, its deployment revealed important challenges regarding scalability, resource consumption, and cost optimization. From an operational perspective, the SOC2I architecture was designed to reduce resource pressure on UAV nodes by separating lightweight monitoring from centralized SOC analytics. Statistical deviation checks such as Z-score normalization and LOF-based anomaly

scoring are applied on processed telemetry windows, enabling anomaly detection without requiring continuous high-cost computation on airborne platforms. Meanwhile, the Distributed Detection Grid allows preliminary detection signals to be generated close to the data sources while the SIEM layer performs centralized correlation and response coordination. The SOC2I simulation incurred a total cost of 131.29 $ for a 48-hour deployment. This amount reflects cloud-based compute and data processing expenses under a moderate telemetry workload. A detailed cost decomposition shows that approximately 54% of the total was attributed to Elastic SIEM and log ingestion, 28% to machine learning inference and containerized AI services, and 18% to data storage and network transfer. These proportions indicate that SOC2I is currently optimized for analytical depth rather than cost efficiency. The objective of this analysis is not to estimate the operational cost of large UAV swarms but rather to provide an initial indication of the computational and analytical resources required by the SOC2I framework. From a scalability perspective, the resource footprint grows almost linearly with the number of UAV nodes when full telemetry streaming is enabled. For large swarms, this could translate into considerable cloud resource demand unless distributed edge aggregation is introduced. Similarly, real-time inference and alert correlation increase CPU and memory utilization at the SOC layer. These trade-offs highlight the importance of hybrid architectures that balance centralized SOC analytics with lightweight edge monitoring. Overall, the cost analysis indicates that SOC2I, while technically effective, currently favors performance and analytical coverage over economic scalability. Future optimization should target adaptive telemetry sampling, edge-side preprocessing, and dynamic resource allocation to reduce redundant data transfer and processing overhead. These improvements would support a more sustainable integration of SOC capabilities into UAV networks operating under diverse mission constraints.

The current evaluation should be interpreted as a proof-of-concept validation of the proposed SOC2I architecture rather than as a comparative benchmark of anomaly detection algorithms. The experimental analysis focuses on replay-based processing of UAV telemetry logs containing jamming and spoofing attacks and does not include comparisons with alternative intrusion detection systems or anomaly detection methods. Furthermore, the evaluation currently reports operational SOC metrics and detection rates without providing precision, specificity, false-positive rates, or F1-scores. Future work will extend the evaluation to additional UAV attack classes and perform comparative benchmarking against established UAV intrusion detection approaches.

5 Conclusion and Future Work

This paper presented the SOC2I framework, integrating AI within SOCs to enhance UAV cybersecurity. SOC2I enables proactive surveillance, adaptive response, and context-aware analytics for detecting and mitigating attacks.

The framework establishes a continuous monitoring and feedback loop linking detection, risk assessment, and mitigation. Experimental results show improved anomaly detection and situational awareness under representative UAV conditions.

However, several limitations remain, including scalability in large UAV swarms, vulnerability to adversarial ML manipulation, and real-world deployment constraints related to latency, resource limitations, and regulatory factors.

Future work will address these issues by improving scalability, enhancing adversarial robustness, and validating SOC2I in operational UAV networks. Further efforts will also focus on cost-efficient implementations and SOC standardization to support interoperable and secure UAV ecosystems. Although the proposed framework demonstrates promising results, the current evaluation remains limited to replay-based experiments involving jamming and spoofing attacks. Future work will include comparative benchmarking against existing UAV intrusion detection systems, additional attack categories, and more comprehensive performance metrics, including precision, F1-score, specificity, and false-positive rates.

conflict of interest

The authors declare no competing interests.

Funding

No funding was received for the preparation of this manuscript.

References

[1] F. Tlili, L. C. Fourati, S. Ayed, and B. Ouni, "Investigation on vulnerabilities, threats and attacks prohibiting uavs charging and depleting uavs batteries: Assessments & countermeasures," *Ad Hoc Networks*, p. 102805, 2022.

[2] A. D. Boursianis, M. S. Papadopoulou, P. Diamantoulakis, A. Liopa-Tsakalidi, P. Barouchas, G. Salahas, G. Karagiannidis, S. Wan, and S. K. Goudos, "Internet of things (iot) and agricultural unmanned aerial vehicles (uavs) in smart farming: A comprehensive review," *Internet of Things*, vol. 18, p. 100187, 2022.

[3] Y. Li, M. Liu, and D. Jiang, "Application of unmanned aerial vehicles in logistics: a literature review," *Sustainability*, vol. 14, no. 21, p. 14473, 2022.

[4] M. Stampa, A. Sutorma, U. Jahn, F. Willich, S. Pratzler-Wanczura, J. Thiem, C. Röhrig, and C. Wolff, "A scenario for a multi-uav mapping and surveillance system in emergency response applications," in *2020 IEEE 5th international symposium on smart and wireless systems within the conferences on intelligent data acquisition and advanced computing systems (IDAACS-SWS)*, pp. 1–6, IEEE, 2020.

[5] A. Tiseira, R. Novella, L. Garcia-Cuevas, and M. Lopez-Juarez, "Concept design and energy balance optimization of a hydrogen fuel cell helicopter for unmanned aerial vehicle and aerotaxi applications," *Energy Conversion and Management*, vol. 288, p. 117101, 2023.

[6] M. Kucharczyk and C. H. Hugenholtz, "Remote sensing of natural hazard-related disasters with small drones: Global trends, biases, and research opportunities," *Remote Sensing of Environment*, vol. 264, p. 112577, 2021.

[7] F. Tlili, S. Ayed, L. Chaari, and B. Ouni, "Artificial intelligence based approach for fault and anomaly detection within uavs," in *International Conference on Advanced Information Networking and Applications*, pp. 297–308, Springer, 2022.

[8] A. Haddaji, S. Ayed, and L. C. Fourati, "Artificial intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey," *Computers and Electrical Engineering*, vol. 104, p. 108460, 2022.

[9] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020.

[10] M. Soori, "Artificial intelligent in optimization of steel moment frame structures a review," *International Journal of Structural and Construction Engineering*, 2024.

[11] S. K. Das, F. Benkhelifa, Y. Sun, H. Abumarshoud, Q. H. Abbasi, M. A. Imran, and L. Mohjazi, "Comprehensive review on ml-based ris-enhanced iot systems: basics, research progress and future challenges," *Computer Networks*, vol. 224, p. 109581, 2023.

[12] Y. M. Samir Achraf Chamkar and N. Gherabi, "Soc analyst performance metrics: Towards an optimal performance model," *EDPACS*, vol. 68, no. 3, pp. 16–29, 2023.

[13] S. N. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, and T. Finin, "Early detection of cybersecurity threats using collaborative cognition," in *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*, pp. 354–363, IEEE, 2018.

[14] S. A. Chamkar, Y. Maleh, and N. Gherabi, "The human factor capabilities in security operation center (soc)," *EDPACS*, vol. 66, no. 1, pp. 1–14, 2022.

[15] M. A. Majid and K. A. Z. Ariffin, "Model for successful development and implementation of cyber security operations centre (soc)," *PLOS ONE*, vol. 16, no. 11, pp. 1–24, 2021.

[16] D. Shahjee and N. Ware, "Integrated network and security operation center: A systematic analysis," *IEEE Access*, vol. 10, pp. 27881–27898, 2022.

[17] D. Shahjee and N. Ware, "Designing a framework of an integrated network and security operation center: A convergence approach," in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, pp. 1–4, IEEE, 2022.

[18] T. Kacem, S. Gayatri Annamreddy, M. D. Silvius, P. Costa, T. Martin, and E. Blasch, "Information fusion for secure autonomous drone operations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 8, pp. 11564–11573, 2025.

[19] J. Liu, J. Lemus-Romani, E. J. Rueda, E. González-Rauter, and M. Becerra-Rozas, "Optimizing uav flight parameters for linear infrastructure pathology detection: Assessing smart oblique capture," *Drones*, vol. 10, no. 5, 2026.

[20] A. Hamissi and A. Dhraief, "A survey on the unmanned aircraft system traffic management," *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–37, 2023.

[21] L. Suchman, "Imaginaries of omniscience: Automating intelligence in the us department of defense," *Social Studies of Science*, vol. 53, no. 5, pp. 761–786, 2023.

[22] A. I. Hentati and L. C. Fourati, "Comprehensive survey of uavs communication networks," *Computer Standards & Interfaces*, p. 103451, 2020.

[23] A. Yao, S. Pal, X. Li, Z. Zhang, C. Dong, F. Jiang, and X. Liu, "A privacy-preserving location data collection framework for intelligent systems in edge computing," *Ad Hoc Networks*, vol. 161, p. 103532, 2024.

[24] A. Yao, S. Pal, C. Dong, X. Li, and X. Liu, "A framework for user biometric privacy protection in uav delivery systems with edge computing," in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pp. 631–636, IEEE, 2024.

[25] C. Dong, F. Jiang, X. Li, A. Yao, G. Li, and X. Liu, "A blockchain-aided self-sovereign identity framework for edge-based uav delivery system," in *2021 IEEE/ACM 21st international symposium on cluster, cloud and internet computing (CCGrid)*, pp. 622–624, IEEE, 2021.

[26] C. Dong, S. Pal, S. Chen, F. Jiang, and X. Liu, "A privacy-aware task distribution architecture for uav communications system using blockchain," *IEEE Internet of Things Journal*, vol. 12, no. 9, pp. 11233–11243, 2025.

[27] K. Fang, J. Deng, C. Dong, U. Naseem, T. Liu, H. Feng, and W. Wang, "Mocfl: mobile cluster federated learning framework for highly dynamic network," in *Proceedings of the ACM on Web Conference 2025*, pp. 5065–5074, 2025.

[28] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Uav attack dataset," 2020.