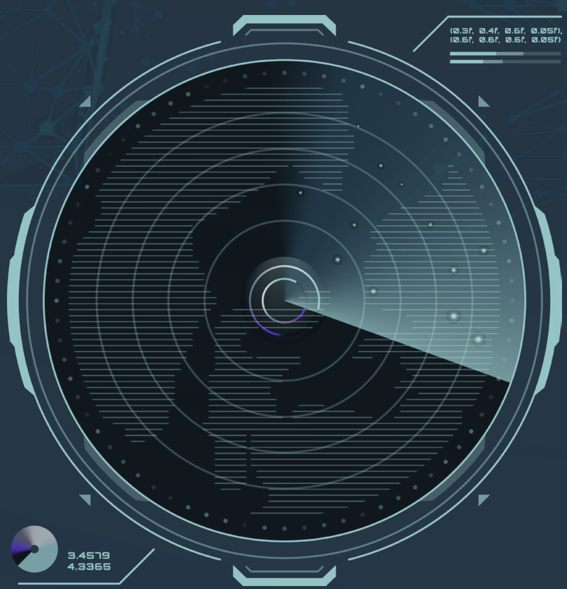
A FRAMEWORK FOR SAFER SKIES WITH SECURE UNMANNED AIRCRAFT TRAFFIC MANAGEMENT (UTM)

SUMMARY

Unmanned Traffic Management (UTM) strives to guarantee that autonomous aircraft can safely share airspace with all other flying objects: small drones, Remotely Piloted Aircraft Systems (RPAS), and manned aviation. Safety is the foundation of the aviation system. The advent of digital aviation, digital traffic management, and new kinds of vehicles requires a new framework to maintain, and even improve, safety and stakeholder trust. Given our increasingly digital aircraft and monitoring systems, any new safety regime must anticipate risks posed by digitally compromised aircraft.

Aviation systems put safety and security first. Drones and other vehicles must meet the same standards. To be widely adopted, security mechanisms must be robust, thoroughly tested, and well developed. Just as websites transitioned from HTTP to HTTPS for secure communication, the UTM ecosystem must transition to robust security measures—with the attendant new tools and standards. UTM implementations will need to address such security issues as reliable and trustworthy drone identification, tracking, communication security, and fleet management. Before they can ensure a secure and efficient Unmanned Aircraft (or Aerial) Systems (UASs) operational environment, developers must identify, analyze, and resolve multiple operational, technical, and regulatory issues.



The Technology Innovation Institute's (TII) Secure Systems Research Center (SSRC) is leading research on applying a zero-trust approach to secure interactions between Unmanned Aerial Vehicles (UAVs), Ground Control Stations (GCSs), and UTM services. SSRC is actively investigating a wide range of security measures to strengthen authentication, authorization, and non-repudiability—all to enhance resilience in the face of cybersecurity risks. Moreover, SSRC is collaborating with regulatory bodies and software communities like the Dronecode Foundation, the Global UTM Association (GUTMA), and the Internet Engineering Task Force (IETF) to standardize interfaces—all with the objective of defragmenting GCS-to-UTM interactions and facilitating a kind of HTTP-to-HTTPS security transition for the UTM ecosystem.

INTRODUCTION

Unmanned Aircraft Systems, often called drones, promise tremendous economic, societal, and security benefits. Regulators have traditionally required UAS operators to maintain visual control of operations, which has reduced their potential. Increasingly, though, regulators are working with scientists, engineers, and vendors to develop Unmanned Air Traffic Management systems [1]. These advancements, and their integration with conventional Airspace Traffic Management (ATM), can allow operations Beyond Visual Line of Sight (BVLOS, Fig 1). This collaborative effort aims to unlock the full potential of drone technology to operate in shared airspace, safely and efficiently.

UTM guarantees that drones will function effectively and avoid collisions with other aircraft and ground-based hazards. Like any complex system, however, UTM is susceptible to diverse security threats. These include cyberattacks, physical assaults, and human errors, among other factors.

Continuing UTM system development underscores the delicate balance between the priorities of safety and resilience. Therein lies the opportunity to build security into digital aviation's infrastructure from the outset, rather than bolting on patches to close vulnerabilities after breaches are made. We can leverage insights from other industries and integrate their best practices into aviation, elevating UTM to meet the standards of aviation-grade security. Constructing UTM services necessitates thorough security examinations as we define these new services and establish a federated model. This, inevitably, means significant work at every level.

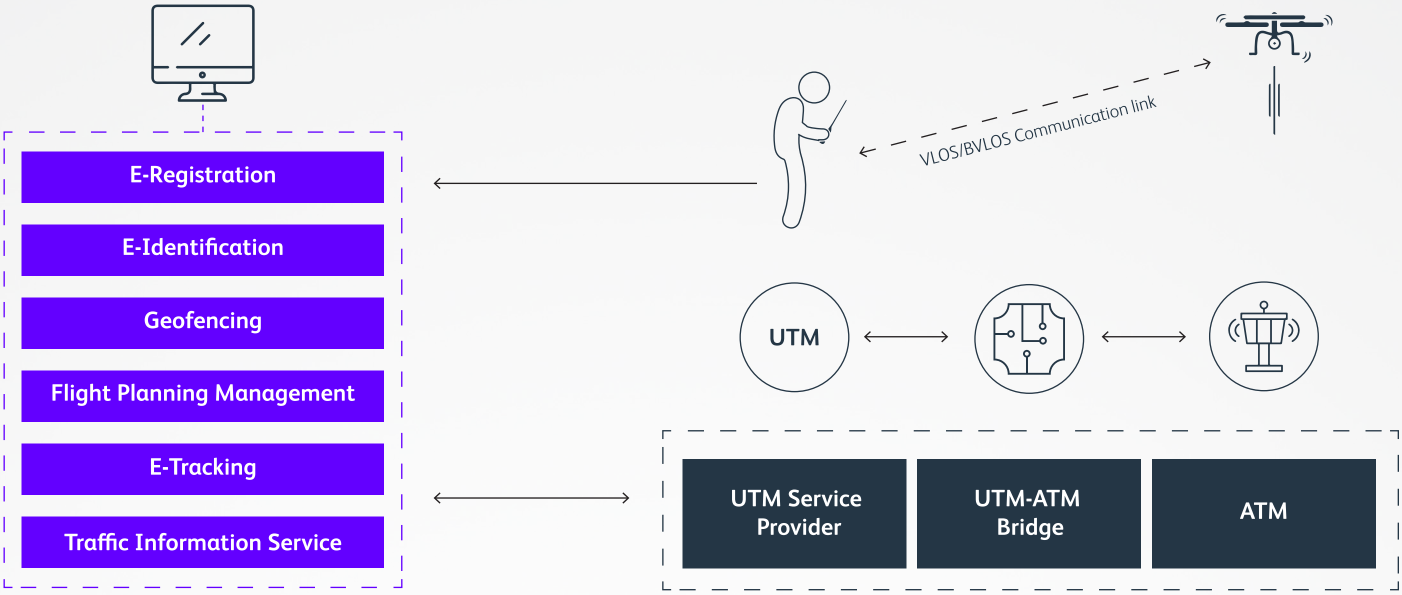
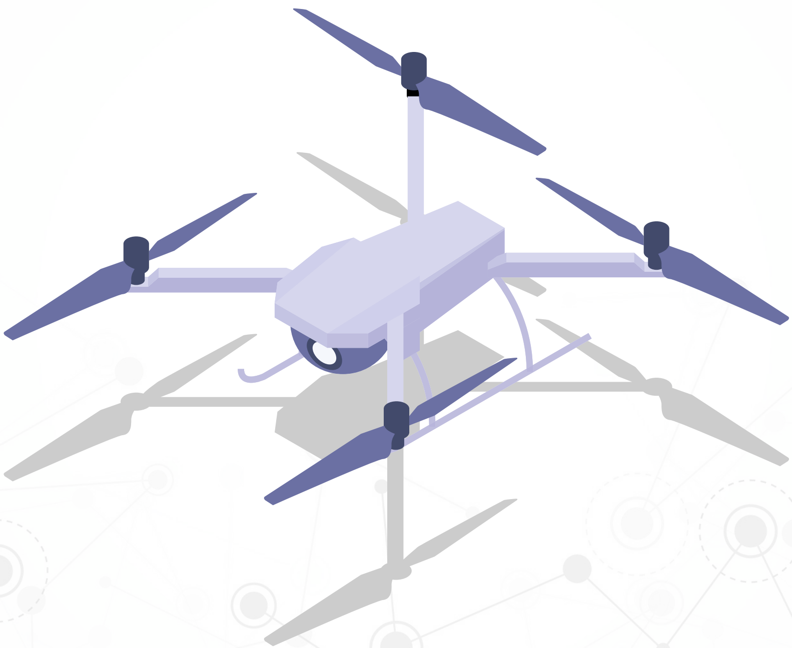


Fig 1: UTM framework



WHAT'S MISSING FROM TODAY'S UTM ECOSYSTEM?

Secure UTM involves factors beyond the UTM services themselves. UTM development demands detailed knowledge of the fast-moving airborne UASs and the fixed GCSs. A holistic approach that brings in regulators, standards organizations, vendors, and researchers is essential.

Unfortunately, current efforts still fall short in seven essential areas.

Regulatory harmonization: Regulators globally are crafting diverse technical and regulatory frameworks for UTM to manage burgeoning drone fleets. So far, regulators in each jurisdiction approach these jobs piecemeal; harmonization is essential to preserve safety and security for traffic that moves above municipal, regional, and national borders. Shared standards and protocols for data exchange, interfaces, and service parameters are vital for averting chaos. To attain them, to ensure safety and security in the air for all stakeholders, we must have a common regulatory framework and develop new concepts and new tools and embody them in practical implementations.

Currently, major standards like ASTM F3411, (Remote ID and Tracking) and ASTM F3548-21, (UTM/UAS Service Supplier (USS) Interoperability) focus on assuring interoperability and efficient data exchanges between UTM Service Providers (UTMSPs). Yet these standards do not clearly define interfaces between UTM services and UAS operators' Ground Control Systems. The resultant ambiguity has fragmented efforts to integrate drone systems with UTMSPs. Consider two UTM Service Providers, Alpha and Beta. They may use the same UTM specifications, or they may use UTM specifications from different regulations. In either case, off-the-shelf UTM programs that comply with existing standards along with interoperability may communicate with each other very well as they hand off control over UAVs moving from one airspace to the other. But UTM software makers provide digital interfaces to GCS clients for flight and mission operations. When data from these extensions is added to the UTM data stream, what makes sense to UTM Alpha may look like nonsense to UTM Beta.

The result is confusion. The systems are disjointed, and properly unified security interfaces are virtually impossible. (Fig 2)

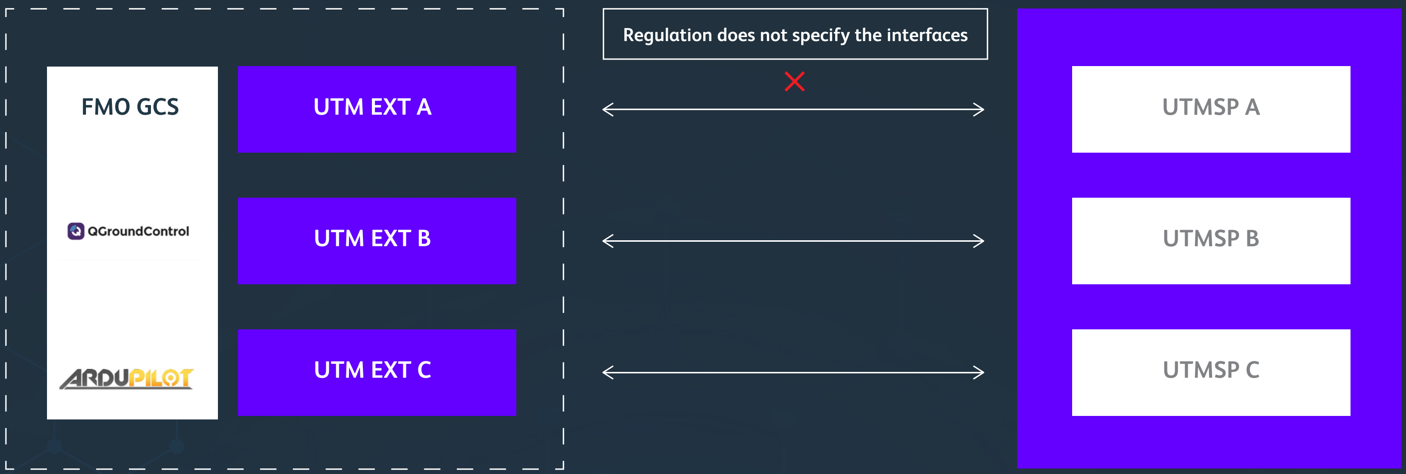


Fig 2: UTM interface implementation fragmentation

End-to-end Secure communications: There are security gaps in end-to-end communications links between drones, GCSs, and UTMSPs. Unless these gaps are closed, malicious actors can exploit these links' vulnerabilities. For example, hackers could spy on drones and seize control of their communications or even operations. The consequences could be severe, and successful hacks might overshadow drone use cases and delay deployment for many years.

Security interoperability: In the context of UTM systems, security interoperability extends beyond individual components to include seamless communication and collaboration between different UTM Service Suppliers (USSs). UTM hardware, software, and service suppliers are building cooperation; gaps remain. Establishing standardized protocols for data exchange, authentication, and encryption between different USSs is essential to ensure secure interoperability and effective coordination at scale. Although the open-source community (InterUSS) has been making some progress, there are as yet no definitions of end-to-end security.

Drone Identification and Authentication: While various initiatives aim to establish drone identification protocols, existing UTM frameworks lack robust, zero-trust mechanisms for uniquely identifying UAVs. This gap could give adversaries an opening to impersonate a recognized drone, alter drone IDs, and hijack communications [2].

Secure Runtime Assurance: The industry lacks mechanisms for integrating security, runtime assurance [3] , and artificial intelligence/machine learning (AI/ML) into UTM infrastructure and communications. Secure Runtime Assurance will be vital in reducing the risk and/or "blast radius" (total impact) of drone malfunctions and communication failures.

Swarm Support: Current UTM systems are designed to communicate with individual drones. Swarm support will be required to improve collaboration, safety, efficiency, and airspace optimization for UAVs operating in coordinated groups. Lack of standardization hampers effective coordination. And it raises security concerns: without clear protocols, drone fleets are susceptible to unauthorized access, data breaches, and other security threats.

Hostile drones: Current UTM systems are designed for friendly drones operating as intended. In security-focused geographical areas, additional infrastructure and capabilities will be required to detect, track, and disable hostile drones (or friendly drones that have been compromised) to reduce the risk of property damage, unauthorized surveillance, or unsafe interference with friendly UAVs.

CURRENT UTM LANDSCAPE

Unmanned Traffic Management systems are designed to facilitate safe and efficient drone operations in low-altitude airspaces. Regulators worldwide are developing their own varied technical and regulatory frameworks for UTM to address the challenges of escalating drone traffic. The U.N.'s International Civil Aviation Organization (ICAO), other organizations like the Global UTM Association (GUTMA), and standards development organizations (e.g. ASTM International, IEEE) are leading efforts to harmonize UTM regulations, processes, and technologies worldwide [4].

Aviation regulators and government agencies are also developing various regional frameworks. (Fig 4) In the European Union, the European Aviation Safety Agency (EASA) is stewarding collaboration on the U-Space Framework to support safe, efficient access to airspace for large numbers of drones [5]. The U-Space process began in 2019 and is scheduled to enter the third of four phases in 2025, reaching full deployment after 2030. (Fig 5)

In the U.S., the Federal Aviation Administration (FAA) [6] [7] and NASA are leading and overseeing work on an adaptive UTM design capable of integrating new technologies and facilitating advanced forms of digital information exchange.

The American UTM Pilot Program (UPP) [8], led by the FAA, has undergone two phases. Phase One demonstrated critical UTM services, including flight-intent exchange and UAS Volume Reservations, in collaboration with FAA UAS test sites. Phase Two, under the FAA Reauthorization Act of 2018, focused on testing remote-identification technologies in complex environments, with progress documented in reports and demonstration videos. The program aims to establish essential capabilities for managing small drones within the U.S. National Airspace System.

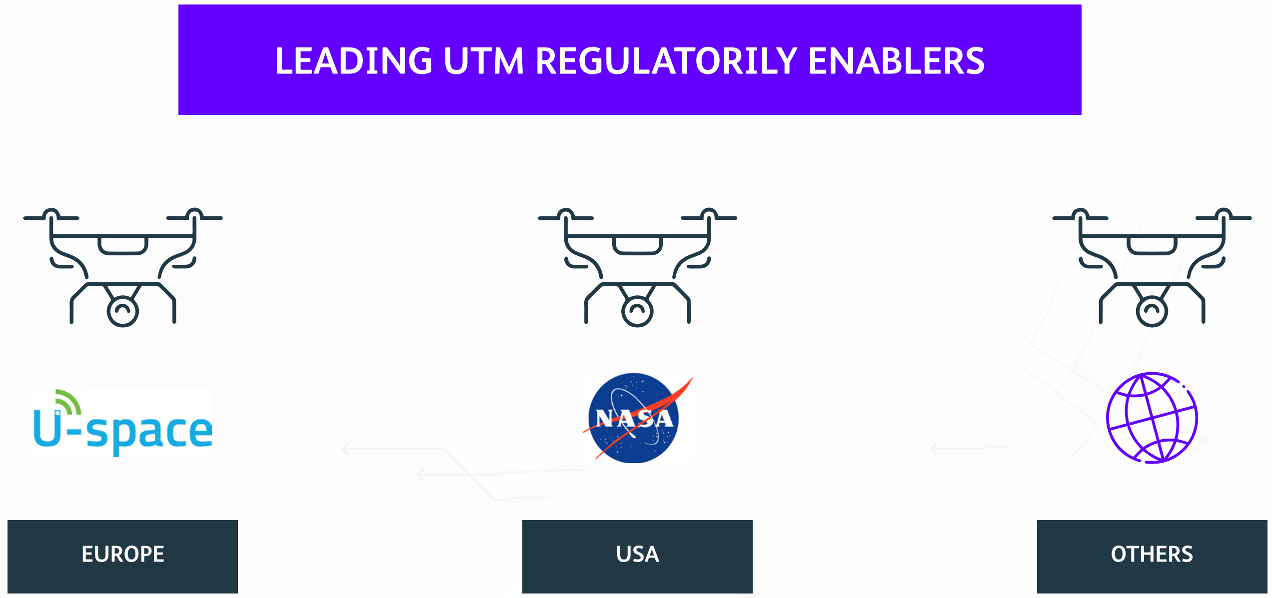


Fig 4: Leading Regulators

Other regional regulators are developing various UTM frameworks at smaller scales. These are all important for progress and broader drone adoption. As drone activity expands, these UTM frameworks will need to evolve to address heightened security risks and ensure the continuity of safe airspace operations. This will require a combination of better automation, more transparent connectivity, improving security, and ever-stronger countermeasures.

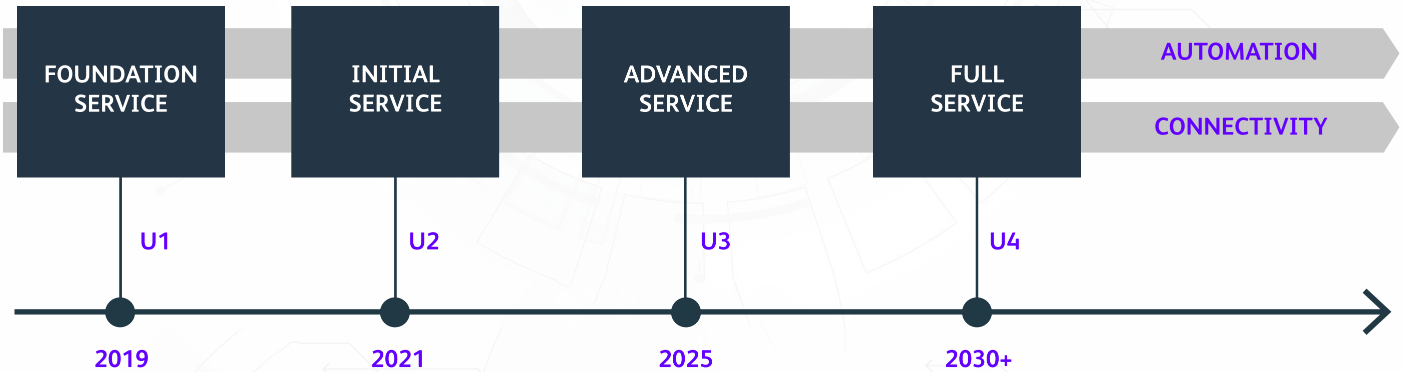


Fig 5: UTM U-SPACE service deployment timeline

The secure-communication landscape is complex and incorporates multiple radio technologies. Despite this complexity, it is crucial to ensure the integrity and security of communications between drones and UTM services. (Fig 3) The radio-communication technology landscape includes systems for Command and Control (C2), cellular networks, Dedicated Short-Range Communication (DSRC), Wi-Fi, Bluetooth, and Satellite Communication (SATCOM). UTM Service Providers communicate through Flight Information Management Systems (FIMS) to facilitate airspace management. Rapid communication between UTMSPs provides real-time discovery and synchronization.

In the absence of secure end-to-end communication, malicious actors may exploit vulnerabilities in any of these links. Again, the consequences could be severe. Impersonation and tampering could compromise critical elements like flight plans and network remote ID; even without direct interference, extortion and threats to these systems could disrupt operations. Malicious attacks on drone registration systems could disrupt tracking and security systems. Denial-of-Service (DoS) attacks could disrupt communications. Exploits of Trusted Discovery and Synchronization Service (DSS) vulnerabilities jeopardize data integrity for UTM Service Providers (UTMSPs). Addressing these issues is imperative to safeguard the integrity and security of the entire UTM infrastructure.

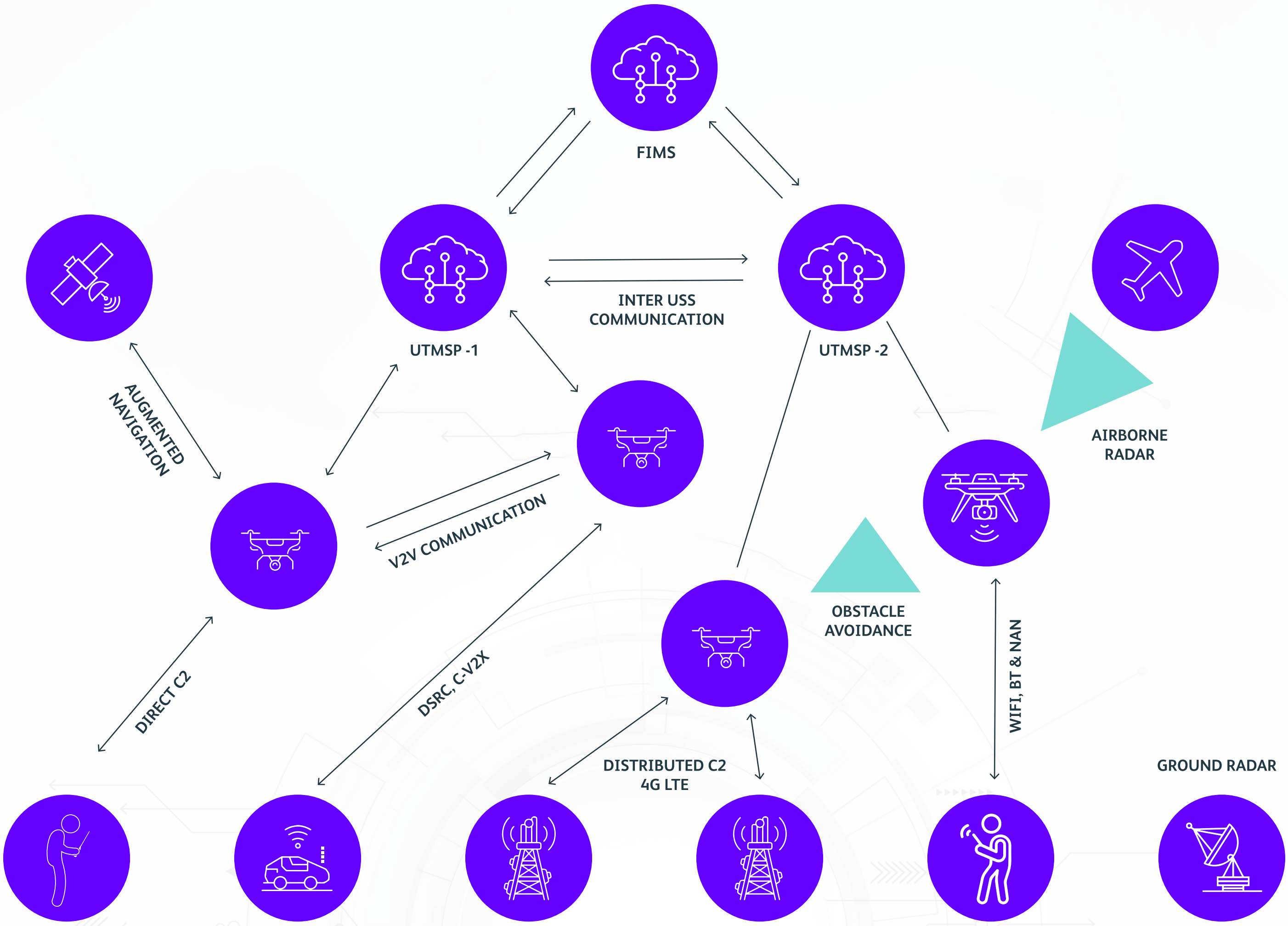


Fig 3: UTM Communication Landscape

UTM STANDARDS OVERVIEW (SIDEBAR)

Engineering and standardization groups, including the American Society for Testing and Materials (ASTM) International, the Institute of Electrical and Electronics Engineers (IEEE), The European Organization for Civil Aviation Equipment (EUROCAE), the Internet Engineering Task Force (IETF), and the International Organization for Standardization (ISO) are developing UTM standards to guide regulatory and technical efforts. These standards collectively define essential guidelines for the seamless and secure integration of unmanned aerial vehicles into airspace operations.

Organization	Standard
ASTM International	**ASTM F3411-19:** Standard Specification for Remote ID and Tracking **ASTM F3442-20:** Standard Specification for Detect and Avoid System Performance Requirements **WK63418:** Performance-based specification for integrating manned flights, prioritizing flight management, and using UTM for urban air mobility. **WK69690:** Specification for Surveillance Supplemental Data Service Provider (SDSP) equipment and services **WK73142:** Specification for Weather Supplemental Data Service Provider Performance
IEEE	**IEEE P1939.1:** Standard for a Framework for Structuring Low Altitude Airspace for UAV Operations
EUROCAE	**ED-270:** Minimum Operational Performance Standard for UAS geo-caging **ED 269:** Minimum Operational Performance Specification for UAS Geofencing.
IETF	Secure UAS Network RID and C2 Transport: A secure transport mechanism for UAS systems remoted ID
ISO	**ISO/TR 23629-1:** Provides results of a survey of UTM

Table 1: UTM standards mapping

HOW TII SUPPORTS UTM SECURITY EVOLUTION

Developing standards and regulatory frameworks for Secure UTM systems is an ongoing process. The Technology Innovation Institute's Secure Systems Research Center is actively researching various aspects of security to tackle privacy concerns, enhance resilience against spoofing, and establish robust authentication and authorization in a zero trust framework.

At TII, we adopt a zero-trust approach [9], emphasizing a comprehensive strategy for securing our systems and networks. Our zero-trust approach involves continuously authenticating and verifying every access to ensure security for all elements of our infrastructure—UAVs, GCSs, Operators, UTMSPs, and DSSs—even within a flexible perimeter. Applying this paradigm, we anticipate vulnerabilities across all involved systems and services, including flight controllers, mission computers, ground control stations, cloud services, and networks. Our zero-trust secure autonomous architecture incorporates secure hardware elements (such as secure boot with hardware root of trust), trusted Execution Environments (TEEs), Input-Output Memory Management Units (IOMMUs), PMP and ISA extensions for establishing trust boundaries. On the software side, we use Hardened OS and apply the proprietary Ghaf framework [10] to provide isolation, with virtual machines and delineated trust boundaries to wall off non-trusted components. These are complemented by VM-to-VM authentication and encrypted communication. Additionally, we apply continuous monitoring for runtime integrity and leverage machine learning to detect and mitigate security issues at both drone and cloud level. Our reference threat-modeling approach includes STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) methodologies, enhancing our proactive stance against potential cyber threats.

This comprehensive perspective demands cybersecurity analyses across cyber-physical systems, GCS/operators, UTM service infrastructure, and data exchanges. Thus, we can cover the entire technology stack to identify threats, safeguard assets, and implement mitigation strategies. (Fig. 6)

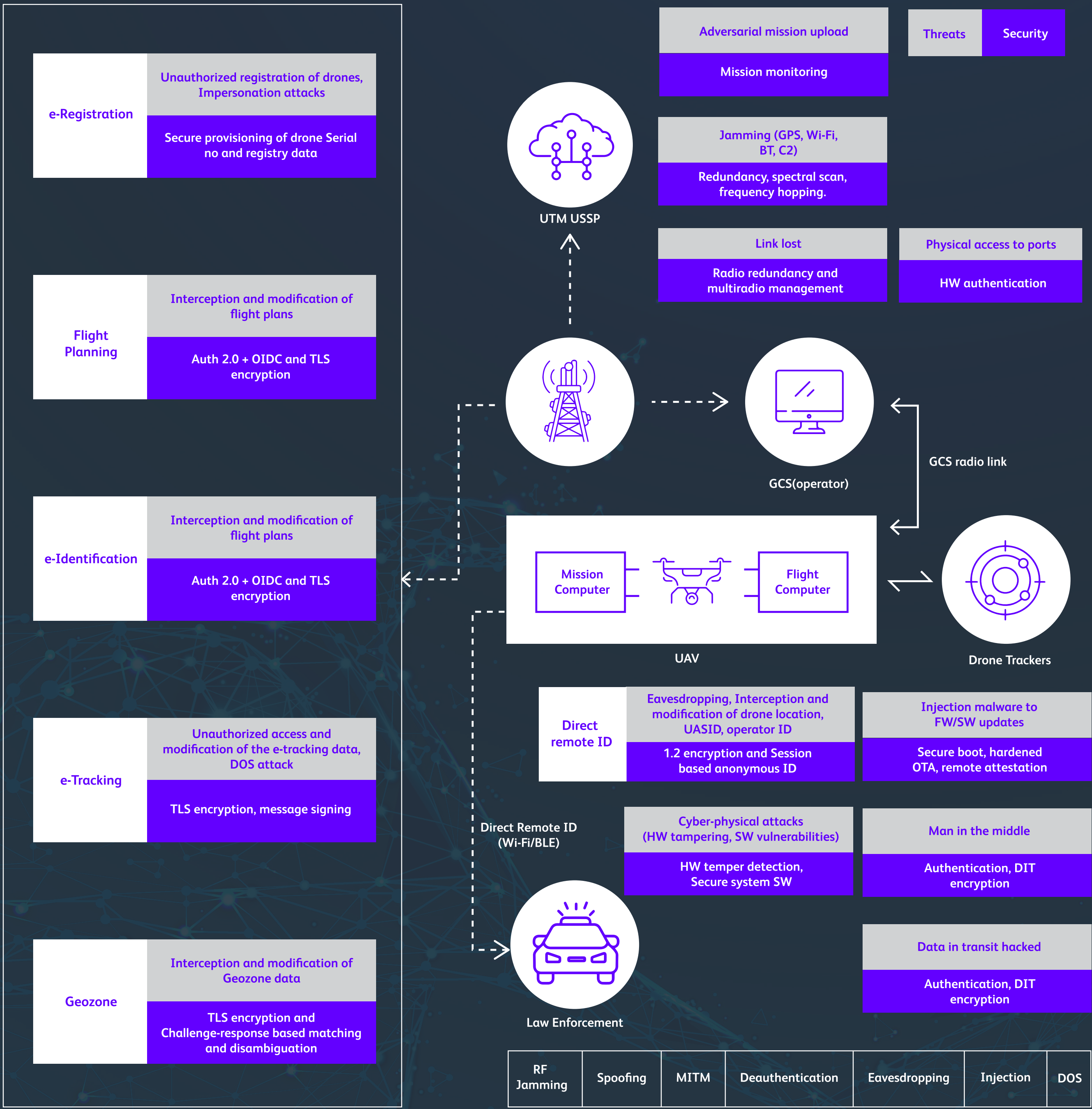
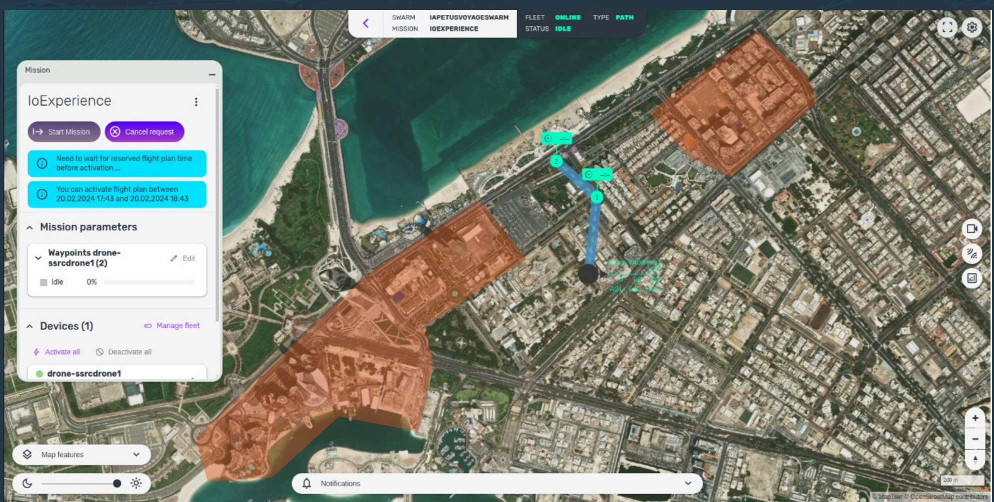


Fig 6: SSRC UAS-GCS-UTM System Architecture



The approach recognizes that threats may be intentional or unintentional, that vulnerabilities or software security flaws can arise from system design lapses or software deficiencies. Cyber-physical threats can stem from hardware tampering, electromagnetic interference, power supply attacks, side-channel assault, and physical intrusion. On the software front, vulnerabilities and supply-chain attacks with malware injection can be countered by static code analysis, fuzzing tests, and stack compartmentalization.

Additionally, the comprehensive approach includes specific countermeasures for threats like jamming, spoofing, and link loss. In cybersecurity, we use e-registration, e-tracking, e-identification, geozone, and traffic-information services.

Combining these and other tools solidifies secure and resilient foundations for the Unmanned Traffic Management system.

Standards Harmonization and Opensource Ecosystem Collaboration

As noted, even major standards like ASTM F3411 and ASTM F3548-21 focus on UTM service provider interoperability but omit clear guidance for interfaces between operators/GCSs and UTM services.

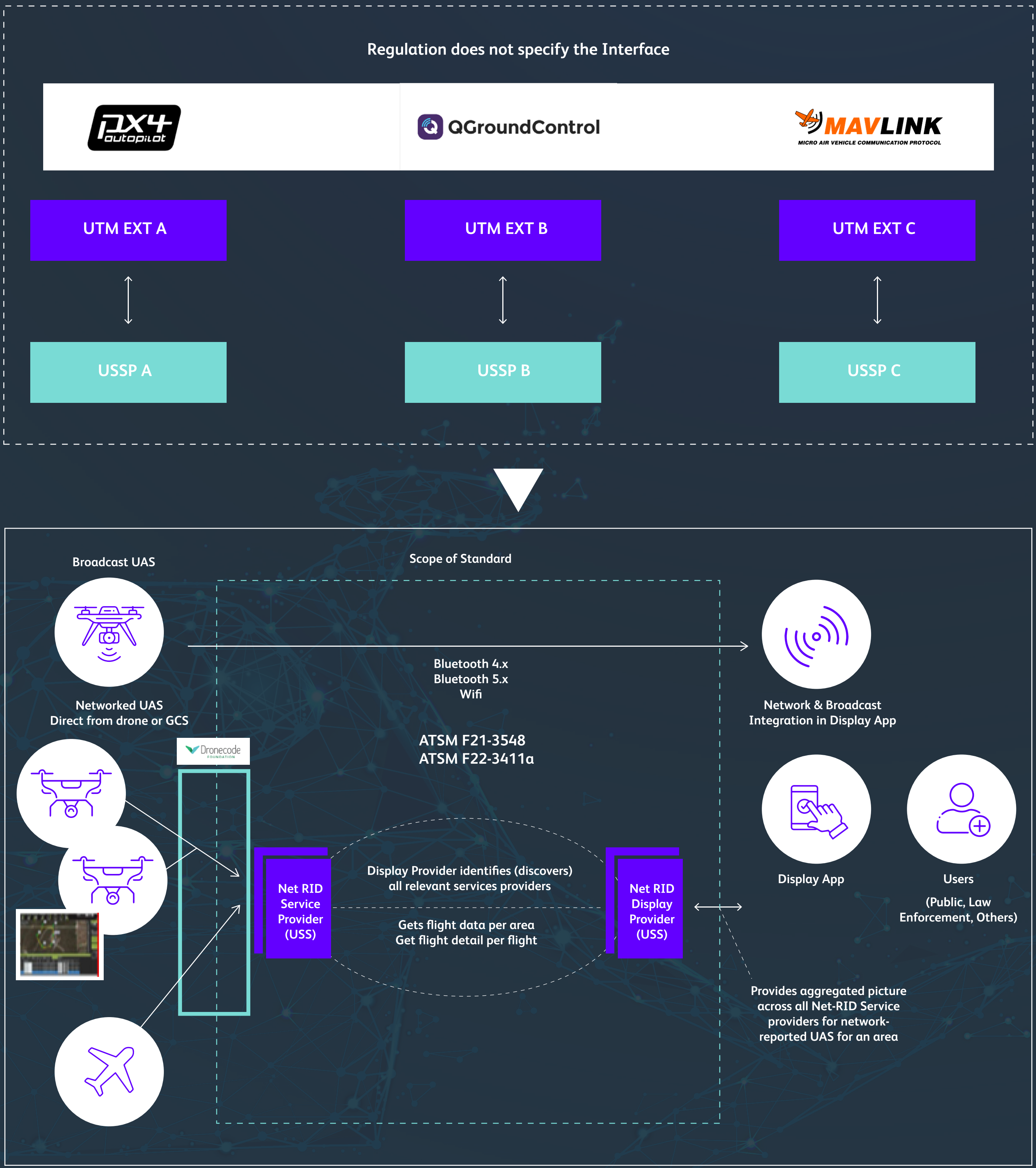
As the first step in addressing this fragmentation, we have identified the need for standardized interfaces that promote interoperability and seamless security integration throughout the UTM ecosystem. By establishing clear, consistent interfaces, we aim to enhance intra-industry collaboration and streamline implementation of robust security protocols. Ultimately, this is essential to the integrity and resilience of UTM operations.

To this end, the Technology Innovation Institute's Secure Systems Research Center had joined the collaborative, open-source Dronecode Foundation, which is dedicated to developing a common, shared platform for UAVs. Working with Dr. Hrishikesh Ballal of Openskies Aerial

Technology and Geodesgnhub, we established the Dronecode UTM Adapter Working Group. Our goal is to define interfaces that can be standardized through collaboration with various regulatory bodies, with a goal of long-term harmonization. (Fig 7)

Fig 7: Secure UTM Harmonized View

SSRC has been and continues to be a key contributor to specifying and implementing the UTM-adapter project's [11] [12] ground control station software stack, QGroundControl (QGC). QGC's open-source software has been widely adopted by numerous drone manufacturers for flight control and mission planning. This add-on streamlines drone operators' access to UTM services, offering open-source ease of integration to support efficient operations and a wide variety of use cases. (Fig. 8) The collaboration actively engages with innovative industry stakeholders to establish a universally accepted interface between QGC and UTM systems.



UTM Adapter

Fig 8: UTM Adapter work under the Dronecode Foundation

We recommend that readers of this paper consider active participation in the UTM Adapter Working Group under the Drone Foundation. Joining presents a unique opportunity to contribute to the field by advancing and standardizing secure UTM interfaces. We sincerely thank Dr. Ballal for spearheading the open UTM initiative and developing open-source, standards-compliant implementations for the UTM ecosystem.

Securing Transmissions Between Drones, Ground Control, and Service Suppliers (UAS-GCS-USS)

SSRC is building robust security UTM communications, with message formats that align with security objectives. This approach guarantees communications will be confined to authorized UTM Service Suppliers, UASs, and GCSs. (Fig. 9). To secure end-to-end communication between drones and Ground Control Stations (GCS), we implement the Zero Trust Architecture in Combating Wireless Network Attacks principles to fortify our communication channels.

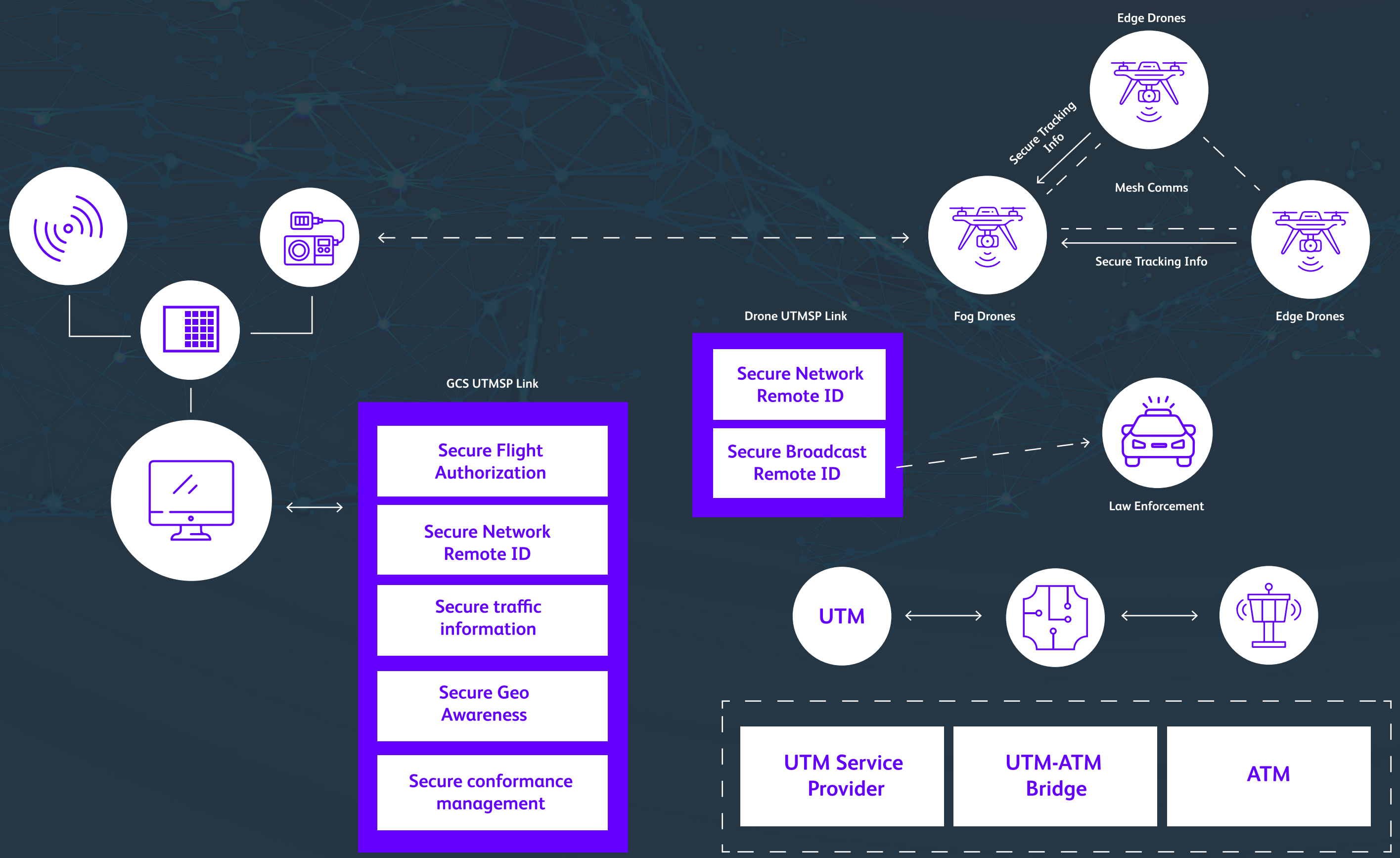


Fig 9: SSRC UAS-GCS-UTM service communication Architecture

TII SSRC's six-component approach ensures the security and integrity of UTM communications. (Fig. 10) Each UTMSP session implements in-transit encryption using TLS/SSL certificates. Authorization is managed through OAuth 2.0, facilitated by our secure Flight and Mission Operation (FMO) GCS client. Messages incorporate digital signatures attesting to the authenticity of sender and recipient, verifying the sender's identity, and preventing any tampering with message content. We use individual UTM certificates with a hierarchical chain of trust for data integrity and authentication. Non-repudiation audit logs also use UTM certificates with a hierarchical chain of trust. Additionally, data at rest is encrypted using a trusted platform module embedded in the SOC platform.

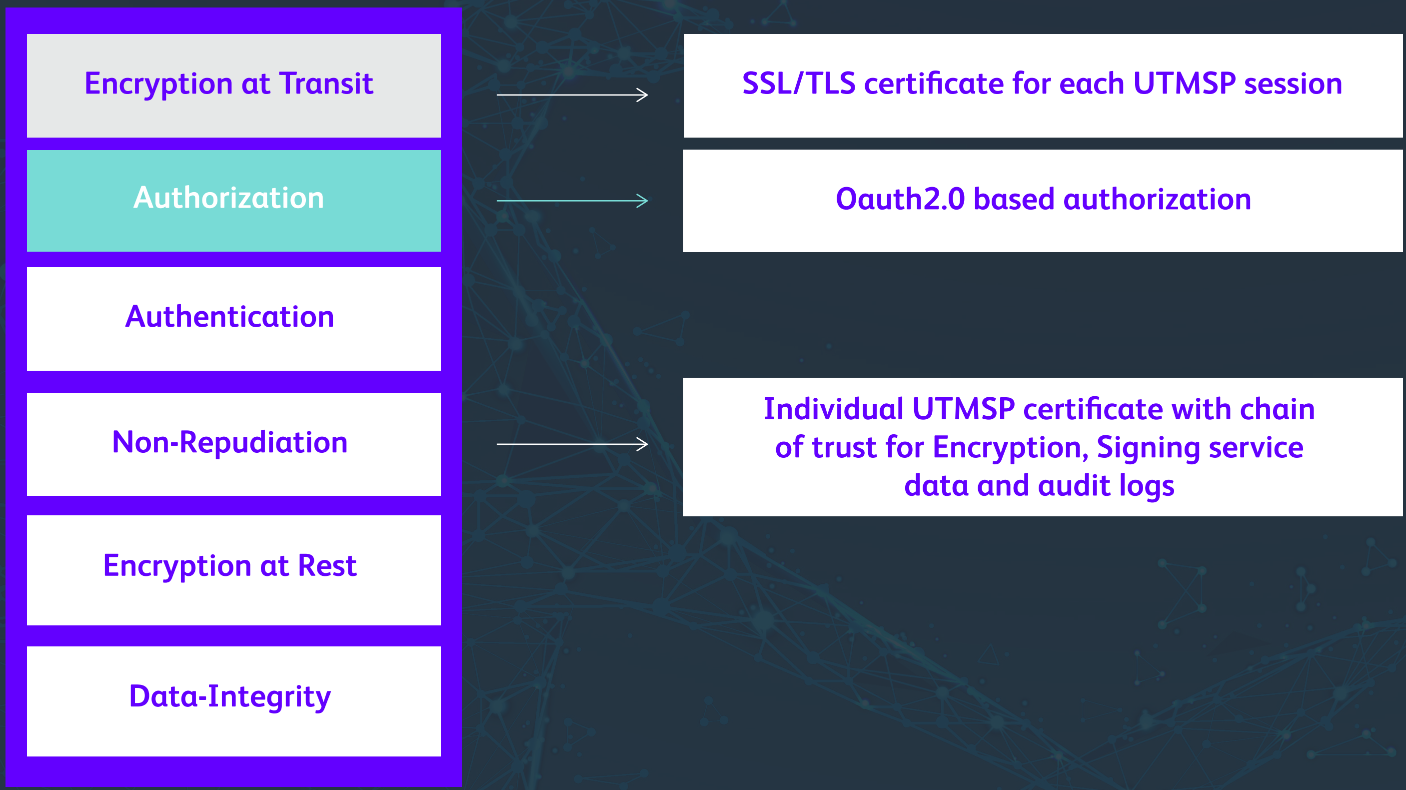


Fig 10: SSRC UAS-GCS-UTM secure communication attributes

Secure Remote ID

SSRC has made significant strides in security with conceptual prototype modules of a Secure Remote ID for broadcast and network applications [13] . These modules establish a foundational root of trust with the UTM Certificate Authority (CA). They provide secure authentication for protecting the flight controller, signed telemetry, and data at rest protection. These innovative conceptual prototypes exemplify SSRC's dedication to advancing authentication and secure communication within the UTM framework.

Potential privacy issues arise with broadcast and network remote ID, which could unveil sensitive details about drone operators. Risks encompass spoofing, tampering, tracking, interference, and data integrity threats. Our secure remote ID mitigation approach includes mutual and continuous authentication based on certificates. (Table 2) Operator privacy is preserved using de-anonymization with session-based anonymous IDs. Communication resilience is achieved through multiband, multi-radio attributes for seamless handover in higher interference environments.

Threat	Mitigation Approach
Remote Identification Authenticity and Integrity	Mutual & Continuous Authentication
Operator Privacy	De-anonymization-Session based anonymous identity
Remote identification Ambiguity	Challenge-response based matching and disambiguation
Communication Resilience	Multiband multi-radio system

Table 2: SSRC remote ID threat mitigation approach

Secure Runtime Assurance

The SSRC is developing a Secure Runtime Assurance (SRTA) framework that adds a security layer to existing RTA frameworks, reinforced by AI and machine learning [14] . SRTA augments UTM, adding real time conformance monitoring, weather data, and traffic information, with adaptive responses to emerging situations. (Fig 11) SRTA's hierarchical decision-making aligns UTM systems to coordinate responses from individual drones to the UTM control center. Safety Integrity Level (SIL) prioritization and multiple redundancy mechanisms from the SRTA framework bolster resilience of drone, swarm, and command systems. And, once again, this comprehensive approach prioritizes safety and security throughout the UTM ecosystem, addressing the unique challenges posed by dynamic interactions in autonomous systems of systems.

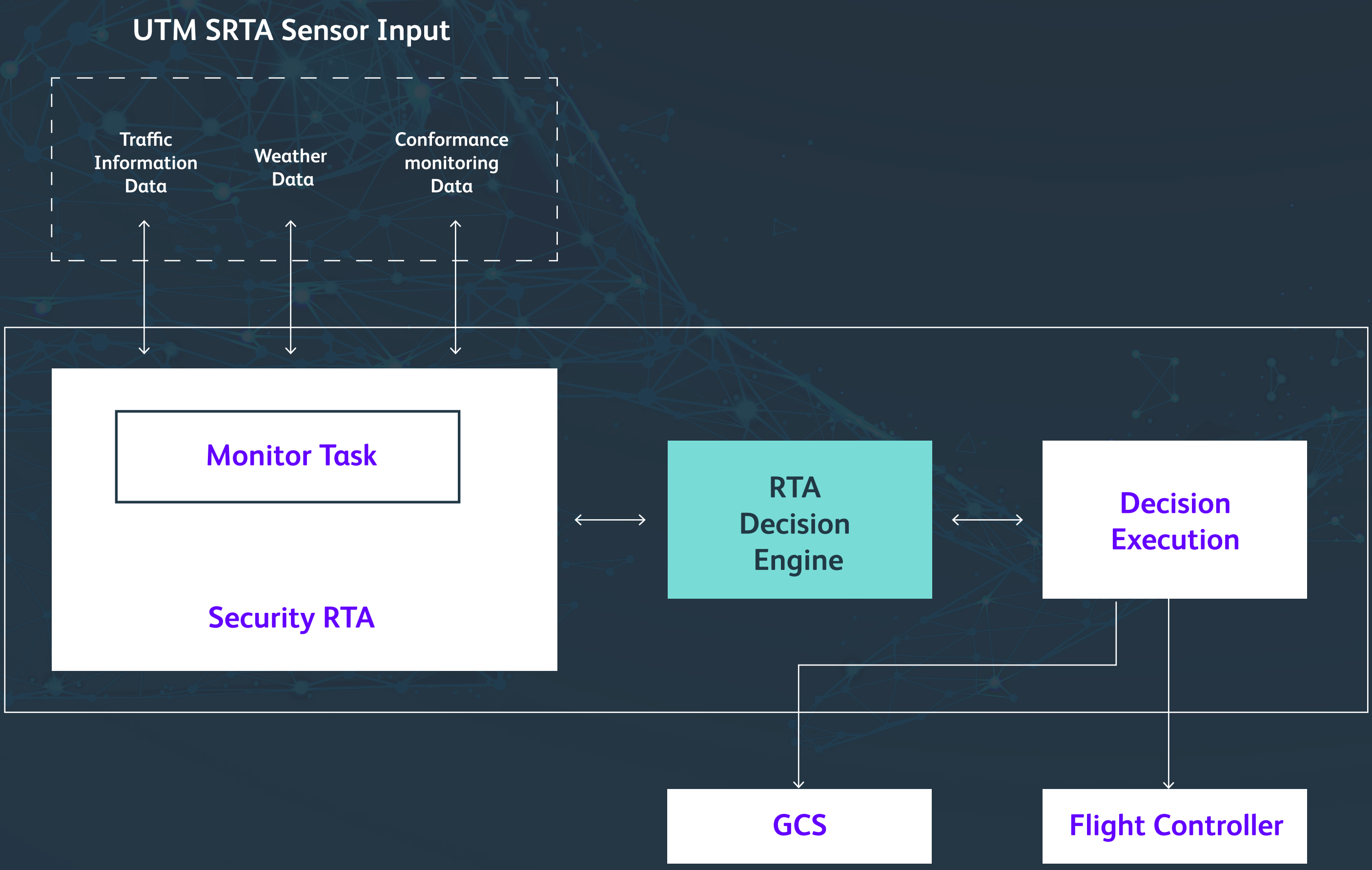


Fig 11: SSRC UTM – SRTA integration architecture

GUTMA UTM Security Working Group

The Technology Innovation Institute's Secure Systems Research is a member Global UTM Association (GUTMA) [15] , the industry association working towards collaboration and standards development in unmanned traffic management. At GUTMA level, SSRC co-leads a security task force [16] evaluating security requirements and aligning them with existing standards. The task force review best practices for security among participating companies, and distills them to create a shared set of best practices. The primary goal is to develop a versatile threat-modeling template for any UTM service, a process for identifying security risks and proposing mitigations. A stretch goal includes mapping requirements from existing security frameworks, such as ISO 27001 or EUROCONTROL SWIM, to conduct a gap analysis to guide further threat-modeling development. We strongly encourage GUTMA members to join the Security Working Group and contribute ideas.

Moreover, at the global standard level, SSRC actively reviews draft security standards, such as IETF's DRIP and ASTM F3411. SSRC promotes active engagement by contributing to open-source implementations that foster interoperability and certification compliance [17] . New technologies will undoubtedly play an essential role in scaling up drone activity safely. But it is also important that researchers, vendors, and regulators work together to ensure these innovations align with regulations and standards efforts.

Academic Research and Industry Collaboration

We acknowledge the existing gaps in today's security ecosystem, even among some crucial elements. To address these deficiencies, the SSRC is proactively developing its zero-trust approach in collaboration with our university partners, including Khalifa University, where Prof. Abdulhadi leads research effort. Through this collaboration, the partners aim to address secure system-integration of UTM services with drones and operators. Additionally, we endeavor to actively participate in defining and standardizing security interfaces at the regulatory level, again with the goals of seamless interoperability and scalable solutions.

Fleet-of-Drones Support in UTM

Current FAA/U-Space regulations do not address fleet-of-drones scenarios. U-space treats groups of drones as singular entities, not requiring separation, and prohibits their flights for safety reasons.

Drone fleets in UTM-enabled operations benefit search and rescue, precision agriculture, infrastructure inspection, environmental monitoring, surveillance, mapping, emergency response and scientific research. Indeed, they offer enhanced efficiency and versatility across countless applications.

In the approach our work envisions, each drone in a fleet will have its own unique flight plan, devised with advanced collision avoidance algorithms. The system will intelligently assign varying flight altitudes to overlapping segments, employing a sophisticated strategies to anticipate and prevent collisions. (Fig. 12) The SSRC's Flight and Mission Operation (FMO) Ground Control System serves as an end-to-end secure, resilient, and safe autonomous platform, while managing single- and multi-drone operations within the swarm, as well as interactions with the UTM system [18] .

Our security strategy for drone swarms within UTM incorporates strong communication encryption, secure geofencing to thwart unauthorized access, real-time threat detection, strong authentication protocols, and redundancy measures to bolster system resilience against potential cyber threats.

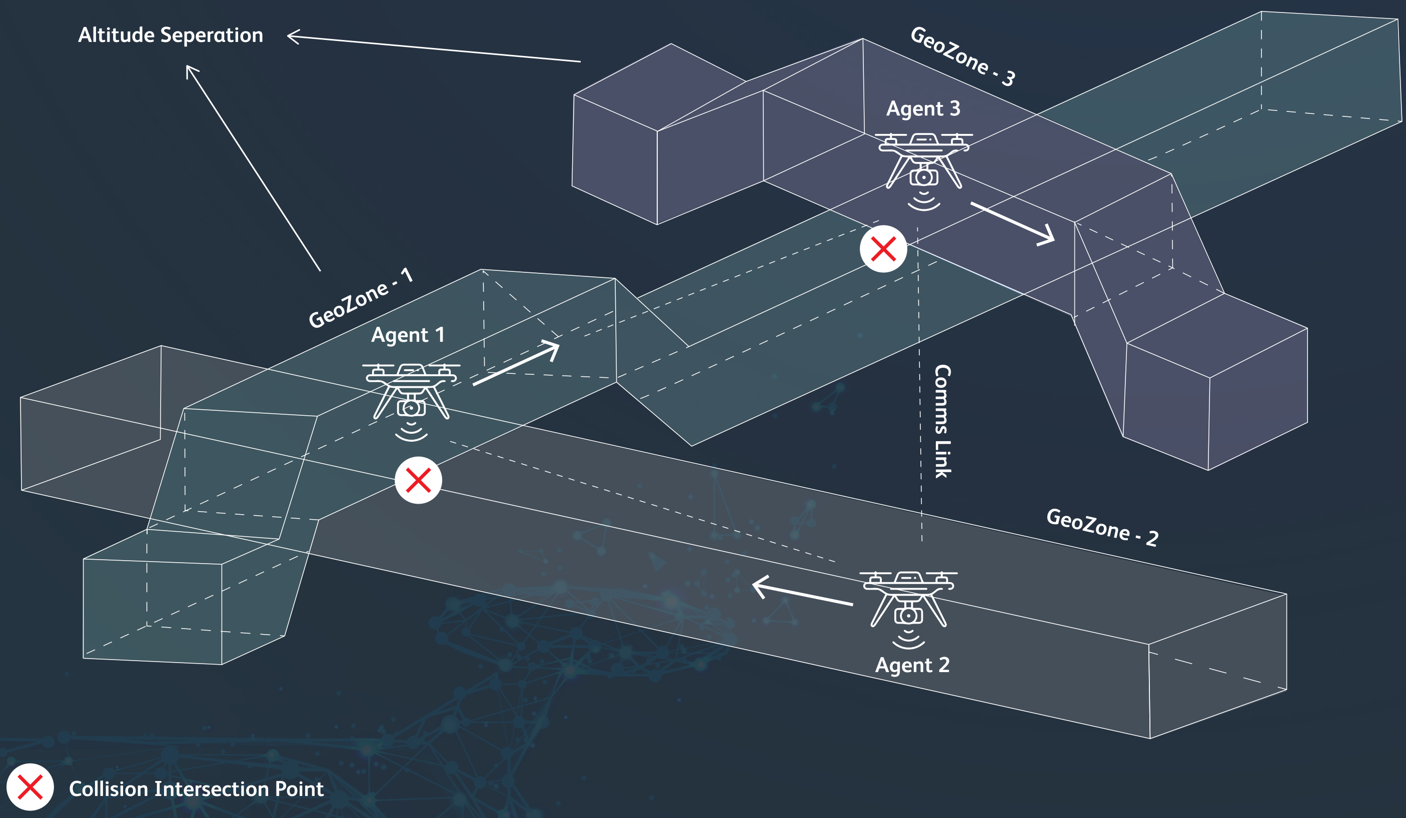
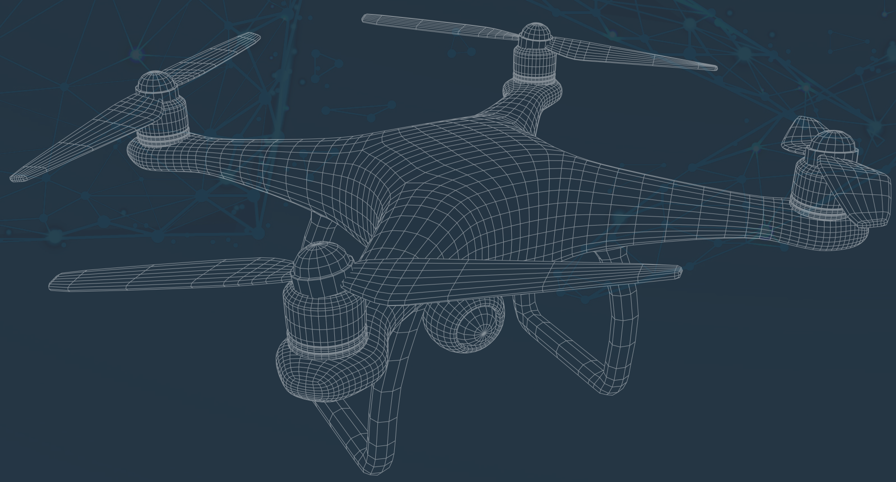


Fig 12: Fleet Altitude Separation Representation



CALL FOR ACTION

In addressing the pressing security concerns surrounding UTM systems, it's crucial to recognize that existing security frameworks may not comprehensively cover all potential threats and mitigation strategies. Security planners may thus need to look beyond structures like ISO 27001 or EUROCONTROL SWIM (System Wide Information Management) as specified in EU AMC/GM, and FAA's Near-Term Approval Process (NTAP)

There is a clear need for a unified and holistic approach to security, an approach that can answer the unique challenges of UTM operations. These include: developing specialized standards and protocols tailored to the unmanned aerial vehicle industry; integrating advanced encryption and authentication; and implementing robust intrusion detection and response mechanisms. By fostering collaboration among stakeholders and leveraging the latest advancements in cybersecurity technology, we can enhance the resilience and integrity of UTM infrastructure, ensuring safe and reliable airspace management in the face of evolving threats.

We strongly advocate collaborative efforts that unite regulators, standardization bodies (such as ASTM and IETF), and open-source communities (like the Linux and Dronecode Foundations) to address the fragmentation in UTM implementations. Let's work together to define clear interfaces between operators/GCSs and UTM services. Let's prioritize zero-trust security measures, seamless integration, and interoperability. By standardizing these interfaces and gaining the regulators' support, we can initiate a transformative shift in the UTM landscape. We can mirror the evolution from HTTP to HTTPS and ensuring a more secure and resilient future for aerial systems.

CONCLUSION

Harmonizing regulations and standardizing interfaces worldwide are crucial steps towards a secure and efficient Unmanned Traffic Management (UTM) framework. By aligning technical and regulatory frameworks, we can address evolving security challenges in the UAS domain and ensure the continuing integrity of unmanned aerial operations. The solutions outlined in this paper-including regulatory harmonization, secure communication, secure identification, runtime assurance, and failure compliance mechanisms-are critical components of a comprehensive UTM security strategy. Through collaboration, we-the regulators, industry stakeholders, and technology innovators-can drive adoption of standardized security practices and continuously improve UTM security. Together, we can build a resilient UTM infrastructure that safeguards airspace safety, protects sensitive communications, and facilitates the safe integration of drones into our skies.

Beyond all this, stakeholders must adhere to security standards and certification processes. Recognized international bodies like ICAO, ASTM, IETF, ISO, play central roles in establishing and maintaining these standards. Strategic public/private partnerships can collaborate with and through these influential organizations to drive innovation by supporting farsighted standards.

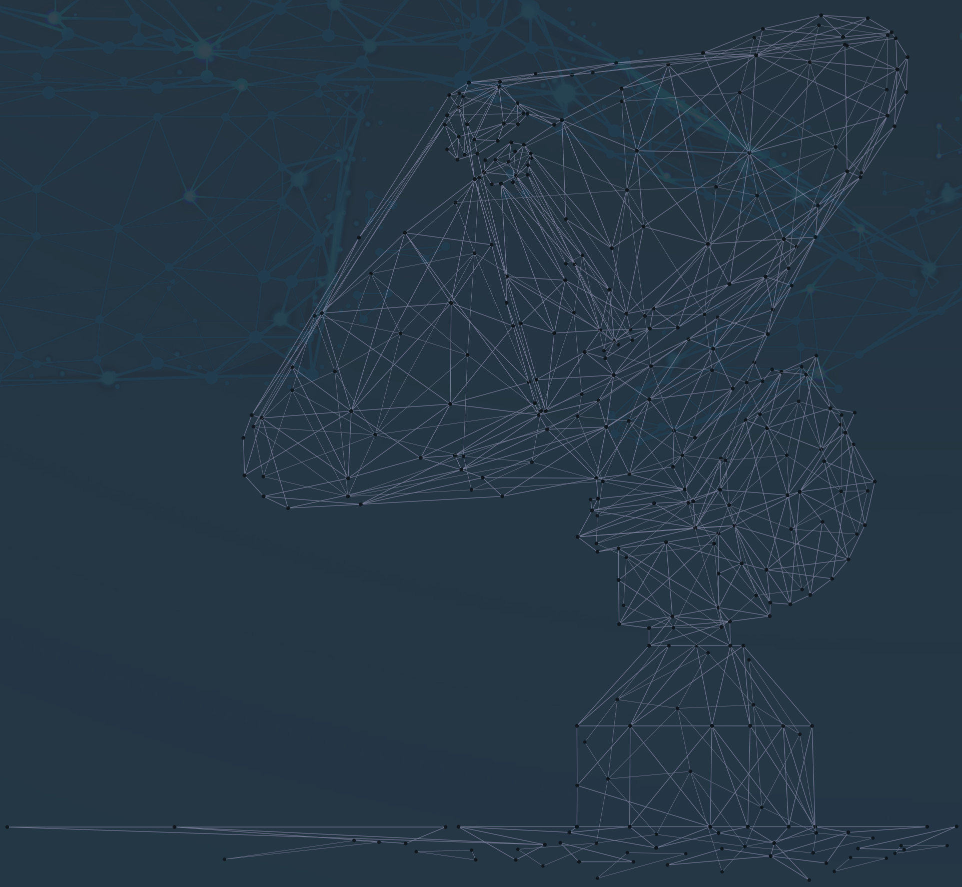
Ongoing regulatory advancements, guided by proactive attention to security, will help establish a resilient and adaptable UAS environment. It will also accelerate creation of robust counter-unmanned-aerial-systems (C-UAS) capabilities as a critical deterrent against potential threats, reinsuring secure integration of drones into shared airspace.

Finally, we must also encourage collaborative efforts among governments, industry, and academia to accelerate development of integrated UTM and C-UAS technologies. Governments and industry, in particular, must invest in research for emerging technologies that provide scalable and secure solutions for UTM systems.

SSRC's primary long-term objective is to collaborate with regulators to incorporate secure UTM-adapter interfaces into established standards. This initiative aims towards a unified approach to sandbox security and resiliency in the UTM ecosystem, facilitating interoperability in all interactions.

ACKNOWLEDGMENTS

This white paper has been informed by contributions from Unmanned Traffic Management system developers, security experts, and Unmanned Aerial System operators, whose collective insights have shaped the proposed strategies for a secure UAS operational environment. We would like to express our sincere appreciation to the Dronecode Foundation and GUTMA, the Global UTM Association, for their invaluable support in accelerating the enablement of the ecosystem to adopt the security extensions, thereby advancing secure UTM operations [19].



REFERENCES

[1] NASA Ames Research Center, "What is Unmanned Aircraft Systems Traffic Management?" [Online]. Available: https://www.nasa.gov/centers-and-facilities/ames/what-is-unmanned-aircraft-systems-traffic-management/

[2] RAND Corporation, "How to Analyze the Cyber Threat from Drones." [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2972/RAND_RR2972.pdf

[3] A. Hammer, M. Cauwels, B. Hertz, P. H. Jones, and K. Y. Rozier, "Integrating runtime verification into an automated UAS traffic management system," Innov Syst Softw Eng, vol. 18, no. 4, pp. 567–580, Dec. 2022, doi: 10.1007/s11334-021-00407-5.

[4] International Civil Aviation Organization (ICAO), "UTM Framework Edition 3." [Online]. Available: https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%203.pdf

[5] Sesar Joint Undertaking, "U-space Concept of Operations 4th Edition." [Online]. Available: https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20CONOPS%204th%20edition.pdf

[6] Federal Aviation Administration (FAA), "Unmanned Aircraft System Traffic Management (UTM)." [Online]. Available: https://www.faa.gov/uas/advanced_operations/traffic_management

[7] U.S. FAA, "UTM Concept of Operations Version 2.0 (UTM ConOps v2.0)." [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2022-08/UTM_ConOps_v2.pdf

[8] Federal Aviation Administration (FAA), "UTM Pilot Program (UPP)." [Online]. Available: https://www.faa.gov/uas/research_development/traffic_management/utm_pilot_program

[9] Technolgy Innovation Institute, " Building a Zero Trust Security Model for Autonomous Systems It's imperative to extend a Zero Trust architecture to protect autonomous systems like drones, industrial equipment, and smart cities." [Online]. Available: https://spectrum.ieee.org/zero-trust-security-autonomous-systems

[10] Technology Innovation Institute, "Introducing the Ghaf Platform: An Innovative Solution to Zero Trust Architecture." [Online]. Available: https://engineeringresources.tradepub.com/free/w_tecm10/

[11] Dronecode, "UTM Adapter." [Online]. Available: https://github.com/Dronecode/utm-adapter

[12] G. Singh, "Explore the Integration of Standards Compliant, Open-Source UTM Services Provider (UTMSP) with QGC." [Online]. Available: https://static.sched.com/hosted_files/px4summit2023/c7/PX4_DeveloperSummit-UTM-Adapter-TII-2023.pdf

[13] G. Singh, R. A. Pashchapur, A. Pandey, and A. Puthiyavinayagam, "Drone Remote Identification System Using Different Wireless COTS Radios: A Benchmarking Study," in 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE, Dec. 2023, pp. 1–7. doi: 10.1109/CommNet60167.2023.10365293.

[14] Technology Innovation Institute, "Unlock the Future of Autonomous Drones with Innovative Secure Runtime Assurance (SRTA)." [Online]. Available: https://engineeringresources.spectrum.ieee.org/free/w_tecm20/prgm.cgi

[15] Global UTM Association, "Global UTM Association", [Online]. Available: https://gutma.org/

[16] Global UTM Association, "GUTMA launches members task force on secure and resilient UTM." [Online]. Available: https://www.unmannedairspace.info/latest-news-and-information/gutma-launches-members-task-force-on-secure-and-resilient-utm/

[17] G. Singh, "OpenUTM DRIP Importer – TII and OpenUTM." [Online]. Available: https://datatracker.ietf.org/meeting/118/materials/slides-118-drip-ietf118-tii-openutm-drip-importer-00

[18] Technology Innovation Institute, "Ready for the Ultimate Security Solution? Create a Safer World with Zero-Trust Autonomic Swarm Security." [Online]. Available: https://engineeringresources.tradepub.com/free/w_tecm17/

[19] Global UTM Association (GUTMA), "Designing UTM for Global Success." [Online]. Available: https://drive.google.com/file/d/1cIXrnJ9jyBKI_9_8BBwzMzKFX7NNSKb6/view

Technology Innovation Institute

Technology Innovation Institute LLC
P.O. Box 9639
Abu Dhabi, UAE