SECURING UAV COMMUNICATIONS IN CONTESTED SPECTRUM

RF THREAT DEFENSE, SDR RESILIENCE, AND C2 INTEGRITY

WWW.CENSUS-LABS.COM

Introduction

UAVs rely heavily on wireless communications for command-and-control (C2), telemetry, payload transmission, and navigation. Due to the open and broadcast nature of radio frequency channels, these systems are inherently vulnerable to interception, disruption, and manipulation. Unlike traditional IP-based networks, wireless links lack robust, layered security models at the physical and link layers, making them prime targets for adversarial operations in contested environments.

Modern adversaries exploit this surface through a variety of attack vectors, ranging from GPS spoofing and C2 hijacking to RF fingerprinting and traffic analysis. Incidents such as the interception of unencrypted UAV video feeds in the Middle East [1] or the GPS spoofing and redirection of high-value UAVs over Iran [18] underscore the strategic impact of wireless security gaps. In ongoing conflicts like Ukraine, both military-grade and consumer UAVs have been targeted with sophisticated electronic warfare (EW) techniques including wideband jamming, sensor desynchronization, and spoofed telemetry injection [19].

The availability of software-defined radios (SDRs) for under $50 has significantly lowered the barrier to entry for conducting RF attacks [1]. When paired with civilian UAVs, often repurposed for hybrid operations and asymmetric threats [4], the scope for exploitation expands considerably.

When Secure Protocols Are Not Enough

In wireless UAV systems, cryptographic protocols, when properly implemented, can provide strong confidentiality, integrity, and authentication. However, protocol-level security is only one layer in a complex, multi-tiered communication stack. UAVs operate over an open and unbounded physical medium, where risks such as side-channel leakage, metadata exposure, and RF signal manipulation are inherently present. Even robust protocols can be undermined by weaknesses in hardware, the physical layer, or integration logic.

Unlike wired systems, the wireless medium exposes a broader portion of the communication stack to adversarial access and exploitation. This expanded attack surface is frequently underestimated during system design, where implicit trust in standards, chipsets, or isolated security controls may leave critical gaps.

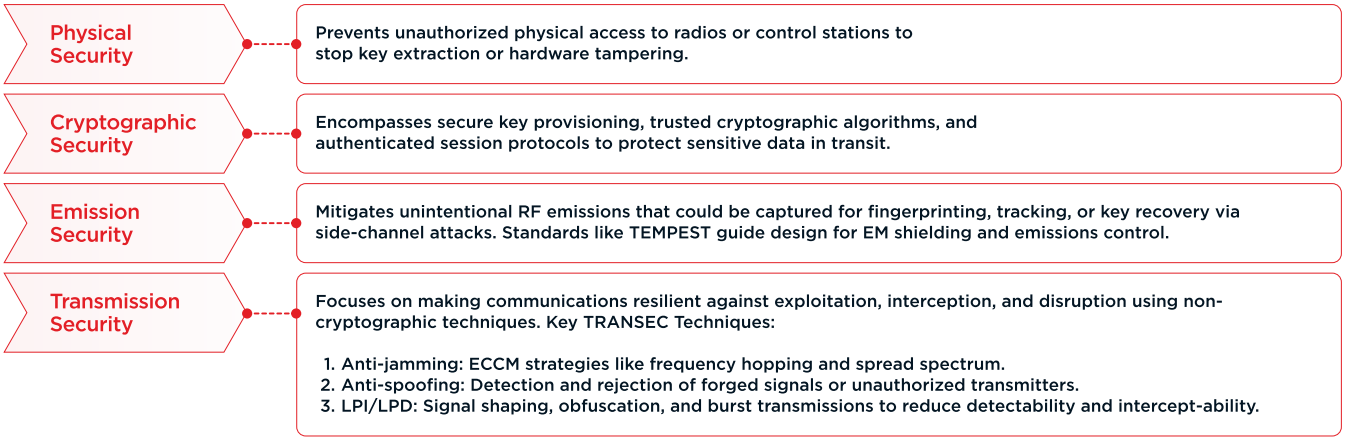
Military and defense-grade UAVs often rely on proprietary or classified waveforms such as Link-16, TTNT, CDL, and UHF SATCOM, which offer improved resilience in contested environments [3]. Yet even these systems require hardened implementations, hardware assurance, and multi-layer validation. A secure waveform alone is insufficient if, for example, emissions leak from the physical layer or control logic permits misconfiguration.

A case that illustrates this systemic risk is the TETRA protocol, widely deployed by public safety agencies. In 2023, researchers disclosed that TETRA included intentionally weakened cryptographic algorithms with backdoors introduced at the specification level, thereby enabling a downgrade in the protocol and allowing encrypted traffic to be decrypted in near real time using low-cost SDR tools [11][12]. Though not UAV-specific, this case highlights how trust assumptions embedded in standards or supply chains can introduce latent vulnerabilities with operational consequences.

The key lesson: security must be engineered across layers, with the assumption that any single layer, whether protocol, hardware, or integration, may be compromised, unintentionally or by design. In RF-centric platforms like UAVs, every layer from waveform design to cryptographic key management poses a potential attack surface [3]. Even moderately resourced adversaries can exploit defaults, misconfigurations, or spectral emissions using commercially available SDRs [10].

Understanding UAV COMSEC Pillars

Communications Security (COMSEC) comprises the technical and procedural safeguards designed to ensure the confidentiality, integrity, and authenticity of wireless communications. For UAVs, this extends to securing C2 links, telemetry streams, positioning data, and inter-platform coordination.



SIGINT and AI-Driven RF Reconnaissance

Signals Intelligence (SIGINT) plays a pivotal role in both defensive and offensive operations involving UAVs [3]. It includes the collection and analysis of COMINT (communication signals) and ELINT (electronic emissions) to extract intelligence or detect threats.

AI and machine learning significantly enhance these capabilities, enabling:

- **Pattern recognition and anomaly detection** in I/Q streams
- **Modulation and protocol classification** under strong noise conditions
- **Spectral behavior mapping** for emitter geolocation and threat profiling

With the rise of LEO satellite constellations and COTS-enabled space platforms, SIGINT is no longer restricted to state actors [9]. Affordable satellite-based systems can now monitor wide swaths of RF activity, including UAV telemetry and navigation links, across the globe in near real-time.

RF Threat Landscape for UAVs

The attack surface of radio interfaces continues to grow as the increasing bandwidth and throughput demands drive more complex RF designs [3]. This added complexity often introduces new vulnerabilities across the communication chain. Closed-source protocols and custom silicon implementations further complicate security assessments, making it difficult to fully understand and evaluate the risks associated with radio link behavior under adversarial conditions for externally supplied components.

At the same time, the widespread availability and affordability of software-defined radio (SDR) technology have lowered the barrier to entry for potential attackers [1]. With open-source implementations of widely used protocols becoming more accessible, operators may be trapped into a false sense of security, mistakenly believing that system complexity alone is sufficient to deter exploitation [10].

In reality, low-cost SDR setups can enable eavesdropping, jamming, or spoofing of poorly secured RF links [1][10]. With UAV architectures shifting toward high-bandwidth, low-latency mesh and SATCOM-based communication, RF exposure grows accordingly, amplifying the need for layered wireless security [3].

Passive Attacks

Passive attacks involve the monitoring of radio links without transmitting any signals or causing active interference. These attacks are stealthy by nature and primarily focus on eavesdropping and traffic sniffing, often targeting unprotected or weakly encrypted wireless protocols. Even if data is not transmitted in plaintext, the presence of known protocol vulnerabilities or embedded backdoors can allow adversaries to extract valuable information through passive means, especially in commonly used standards such as 802.11 (Wi-Fi), cellular (LTE/5G), or Sub-1 GHz IoT protocols [5].

Passive surveillance can be used to track devices, infer user behavior, or correlate signal activity to physical movement.

Active Attacks

Active attacks involve the **generation of malicious RF signals** to disrupt, manipulate, or impersonate legitimate communications. Jamming, whether wideband or narrowband, is a core tactic, used to deny service by overwhelming the receiver's ability to detect valid signals. Another examples are **spoofing** a trusted transmitter to trick a UAV or ground station into establishing a connection, as well as **man-in-the-middle (MitM)** attacks to intercept and relay communications in real time.

A notable real-world example occurred in Oslo, Norway, where a network of IMSI catchers (used to intercept cellular identifiers) was discovered operating near the national parliament. The devices remained undetected until journalists investigated and publicly disclosed their presence, highlighting the threat of passive RF exploitation in urban and political environments [2].

While some active attacks are simple, such as transmitting continuous noise over a frequency range, others are **highly targeted and adaptive**. For example, **reactive or cognitive jammers** can detect signal activity and transmit interference only during active communication slots, making detection and localization significantly harder.

More advanced attacks include:

- **Pilot contamination:** The attacker mimics pilot signals in massive MIMO systems to corrupt channel estimation, redirect traffic, or drain power by simulating unstable link conditions [13][14].
- **Battery exhaustion attacks:** Repeated RF disruptions can induce increased transmission power, prolonged connection attempts, or unstable link maintenance, triggering fallback behaviors that degrade flight endurance or accelerate battery depletion [14][15].

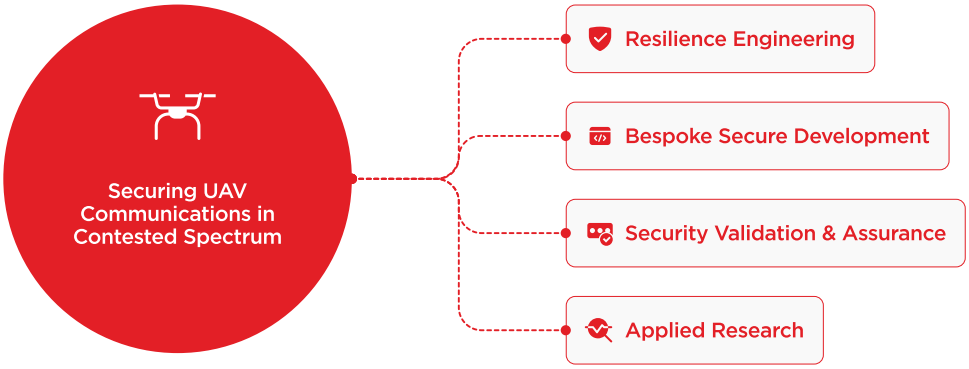
In the case of **GNSS signals**, spoofing and jamming remain major risks. Many systems still lack adequate mitigation strategies to detect or reject forged location data. Using commodity SDRs, adversaries can **generate false GNSS signals** that cause drones, vehicles, or autonomous systems to deviate from intended paths, or even crash due to complete loss of positional awareness [18].

CENSUS Engineering Capabilities for Wireless UAV Security

Securing UAVs against RF-layer threats demands more than waveform hardening. It requires an integrated architecture, combining physical-layer defenses, cryptographic trust, real-time threat detection, and system-level assurance with HW-backed security features.

SECURITY FOCUS AREA	DESCRIPTION
PHY-Layer Security	**Spread Spectrum Techniques** DSSS and FHSS to obscure signal structure and identify legit transmitters (e.g. DVB-CIDD). These techniques can achieve lower probability of detection (LPD) and interception (LPI), resulting in enhanced jamming resistance. **RF and MAC Fingerprinting Techniques** Leverage signal and characteristics (e.g., Carrier Frequency Offset, Phase Noise, supported bands and/or protocols [20]) to generate unique fingerprints, bind transmissions to known hardware and detect spoofing.
AI-Based Spectrum Monitoring	Real-time classification and anomaly detection of RF signals using AI / ML models, with automated triggering of spectrum agility or countermeasures.
Channel Coding and Hardware-Aided RF Hardening	Advanced channel coding techniques, directional CRPA antennas, null steering and adaptive beamforming for active jamming and spoofing mitigation.
Encryption & Attestation	Secure boot, runtime attestation, and device identity validation to ensure platform trustworthiness, even if an adversary gains access to the UAV.

CENSUS delivers vertically integrated cybersecurity solutions to secure the wireless backbone of UAV platforms and similar systems. Our solutions expand from system architecture and resilient development to adversary-driven validation, grounded in technical feasibility and real-world applicability. Each offering is strategically underpinned by our applied research capabilities.



1. **Resilience Engineering** – We design secure RF subsystems with embedded encryption, hardened protocols, and waveform obfuscation (LPI/LPD). Beyond the RF layer, we integrate platform-wide safeguards such as trusted failover mechanisms, secure control/data plane separation, tamper-resilient hardware, data zeroization, and runtime integrity enforcement, ensuring resilience even in hostile environments or upon physical compromise.

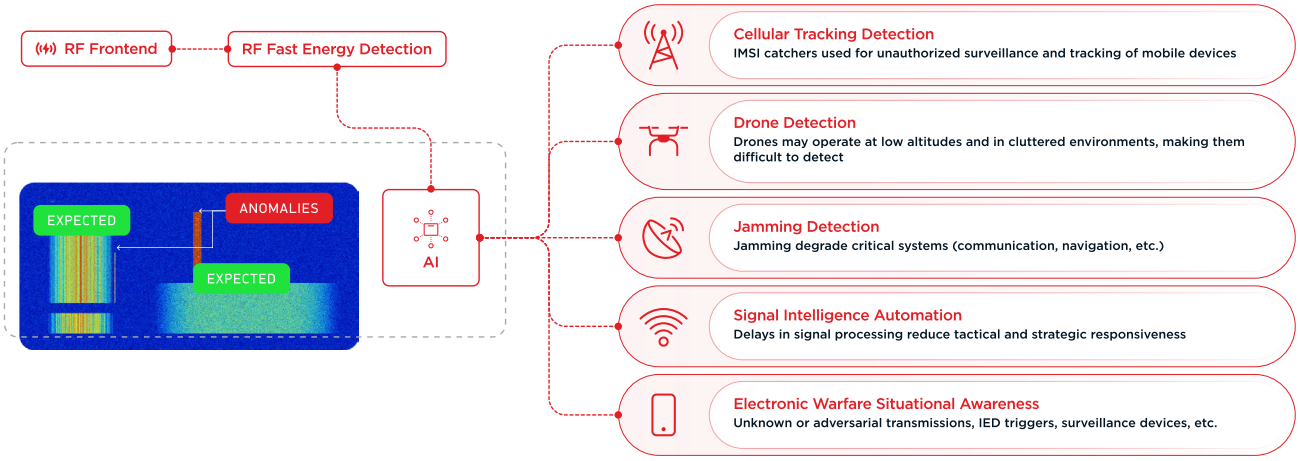
2. **Bespoke Secure Development** – We implement mission-focused enhancements at the intersection of RF and system security, including secure peripheral integration, trusted IPC, cryptographic termination enforcement, and hardware-assisted isolation. Our goal is to make the radio interface a trusted, enforceable component of the platform architecture.

3. **Security Validation & Assurance** – We perform adversary-driven RF testing to evaluate resilience against real-world threats, including spoofing, surveillance, jamming, and GNSS disruption, in alignment with regional regulatory frameworks. Assessments extend from radio interfaces to avionics backplanes, integrating system and communications security under contested-spectrum conditions.

4. **Applied Research** – We assess the feasibility and maturity of security technologies such as SDR-based PHY-layer authentication, GNSS spoofing resilience, and AI-driven RF classification. Our research uncovers exploitable gaps and enables system design through early-stage validation against evolving adversarial capabilities.

AI-Driven RF Security

CENSUS integrates AI into RF security workflows with a signal classification module tailored for UAVs with varying characteristics. Built on applied research and engineered for low-SWaP platforms, this module operates within SDR receive chains, classifying emissions, detecting anomalies, and enabling dynamic threat response.



KEY FEATURES OF THE CLASSIFICATION SYSTEM:

- **Modulation and protocol identification** from raw I/Q samples, even with low (or negative) signal-to-noise ratios (SNR) or contested spectrum conditions.
- **Multi-stage classification pipeline:** Initial detection based on signal energy, followed by deep learning-based feature extraction (e.g., spectral entropy, waveform shape, phase transitions), and classification via CNN, RNN, or transformer models.
- **Low-latency, edge-optimized inference:** designed for deployment on embedded NPUs or SDR-integrated SoCs, enabling real-time performance under SWaP constraints.
- **Spectrum anomaly detection:** AI models trained to identify deviations from normal signal patterns, such as unexpected burst transmissions, spoofed telemetry, or hostile jamming attempts.
- **Protocol fingerprinting and threat attribution:** Classification engine can label emissions by protocol family (e.g., 802.11, LTE, GNSS) and flag unknown or suspicious signal behavior.

OPERATIONAL BENEFITS:

- **Automated RF Threat Detection:** Eliminates reliance on manual spectrum monitoring and predefined signature rules.
- **Dynamic Response Enablement:** Triggers spectrum agility countermeasures, secure failover protocols, or friendly jamming based on classified signal type and threat severity.
- **Enhanced SIGINT Capability:** Supports battlefield RF surveillance by continuously logging, tagging, and attributing detected emissions in real time.

From Signal Integrity to Spectrum Sovereignty

UAVs now operate in highly contested electromagnetic environments, where RF-layer threats undermine mission assurance. Traditional, protocol-focused defenses leave critical gaps at the physical and integration layers, where unprotected links, waveform predictability, and weak system boundaries can be exploited.

CENSUS addresses these challenges by delivering cybersecurity solutions purpose-built for resilient wireless autonomy. From AI-powered signal classification to SDR-based threat detection and system-level integration, we provide the software and engineering depth UAV platforms need to maintain control, integrity, and trust in the spectrum they depend on.

References

1. Arthur, C. (2009, December 17). SkyGrabber: The $26 software used by insurgents to hack into US drones. The Guardian. https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked
2. Rose, E. (2014, December 15). Who's listening in on Norway's politicians? Organized Crime and Corruption Reporting Project. https://www.occrp.org/en/news/whos-listening-in-on-norways-politicians-probe-launched
3. Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In 2012 IEEE Conference on Technologies for Homeland Security (HST) (pp. 585-590). IEEE. https://ieeexplore.ieee.org/document/6459914
4. Hartmann, K, & Giles, K. (2016). UAV exploitation: A new domain for cyber power. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), Cyber power: Proceedings of the 8th International Conference on Cyber Conflict (pp. 205-241). NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/Art-14-Assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf
5. Barbeau, M. (2005). WiMax/802.16 threat analysis. In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05) (pp. 8–15). ACM. https://doi.org/10.1145/1089761.1089764
6. Shang, B., Liu, L., Ma, J., & Fan, P. (2019, October). Unmanned aerial vehicle meets vehicle-to-everything in secure communications. IEEE Communications Magazine. https://par.nsf.gov/servlets/purl/10161743
7. Teng, Y., Zhang, P., Liu, Y., & Liu, X. (2023). PHY-layer authentication with hardware impairments in UAV-aided communication systems. In 2023 International Conference on Networking and Network Applications (NaNA) (pp. 18–22). IEEE. https://ieeexplore.ieee.org/document/10284886
8. European Space Agency. (2021, February). DVB Carrier ID ESA – Detection and Demodulation (DVB-CIDD). ESA. https://artes.esa.int/projects/dvb-cidd
9. Nguyen, T. M., Zaini, A. H., Guo, K., & Xie, L. (2016, October). An ultra-wideband-based multi-UAV localization system in GPS-denied environments. In 2016 International Micro Air Vehicle Competition and Conference (pp. 1228-1234). IMAV. https://www.imavs.org/papers/2016/9.pdf
10. Pratama, D., Moon, J., Laksmono, A. M. A., Yun, D., Muhammad, I., Jeong, B., Ji, J., & Kim, H. (2023). Behind the wings: the case of reverse engineering and drone hijacking in DJI enhanced Wi-Fi protocol. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2309.05913
11. European Telecommunications Standards Institute (ETSI). (2023, July 24). ETSI and TCCA statement to TETRA security algorithms research findings publication. https://www.etsi.org/newsroom/news/2260-etsi-and-tcca-statement-to-tetra-security-algorithms-research-findings-publication-on-24-july-2023
12. Zetter, K. (2023, July). Interview with the ETSI standards organization that created TETRA "backdoor". Zero Day. https://www.zetter-zeroday.com/interview-with-the-etsi-standards/
13. Angoue A., M. B., PérezAdán, D., & Pereira-Ruisánchez, D. (2023). Eavesdropping and jamming via pilot attacks in 5G massive MIMO. In Proceedings of Congreso XoveTIC: impulsando el talento científico (6º, Coruña, Spain). University of Coruña. http://hdl.handle.net/2183/34252
14. Akgun, B., Krunz, M., & Koyluoglu, O. O. (2017). Pilot contamination attacks in massive MIMO systems. In 2017 IEEE Conference on Communications and Network Security (CNS) (pp. 1–9). IEEE. https://ieeexplore.ieee.org/document/8228655
15. Yan, Q., Zeng, H., Jiang, T., Li, M., Lou, W., & Hou, Y. T. (2014). MIMO-based jamming resilient communication in wireless networks. In IEEE INFOCOM 2014 – IEEE Conference on Computer Communications (pp. 2697–2706). IEEE. https://ieeexplore.ieee.org/document/6848218
16. Altun, U., Kaplan, A., Karabulut Kurt, G., Altunbas, I., Kucukyavuz, D., Kesal, M., & Basar, E. (2022). Reactive jammer detection in OFDM with index modulation. Physical Communication, 55, 101909. https://www.sciencedirect.com/science/article/abs/pii/S1874490722001860
17. Boukabou, I., Kaabouch, N., & Rupanetti, D. (2024). Cybersecurity challenges in UAV systems: IEMI attacks targeting inertial measurement units. Drones, 8(12), 738. https://doi.org/10.3390/drones8120738
18. Wikipedia. (n.d.). Iran–U.S. RQ-170 incident. Wikipedia. Retrieved July 16, 2025, from https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident
19. Kelly, K., & Rushton, J. (2025, June). Ukraine is losing its drone supremacy. The Telegraph. https://www.telegraph.co.uk/world-news/2025/06/01/ukraine-is-losing-its-drone-supremacy/
20. A. Pérez-Hernández, M. N. Barreras-Martín, J. A. Becerra, M. J. Madero-Ayora and P. Aguilera, De-Randomization of MAC Addresses Using Fingerprints and RSSI With ML for Wi-Fi Analytics, in IEEE Access, vol. 12, pp. 150857-150868, 2024. https://idus.us.es/server/api/core/bitstreams/f4e9534b-d2c1-4483-9290-965768bfc800/content

Company Profile

CENSUS is a cybersecurity engineering powerhouse. We collaborate with Fortune 500 companies and leading international organizations, specializing in critical sectors such as Defense, Automotive, Healthcare, Banking, Maritime and Telecommunications.

CENSUS BRAND DNA

- HACKING ACUMEN
- CYBERSECURITY ENGINEERING
- SCIENTIFIC SUPERIORITY
- ETHOS & PROFESSIONALISM

OUR OFFICES

ATHENS, GR

LONDON, UK

ABU DHABI, UAE

DUBAI, UAE

VILNIUS, LTU