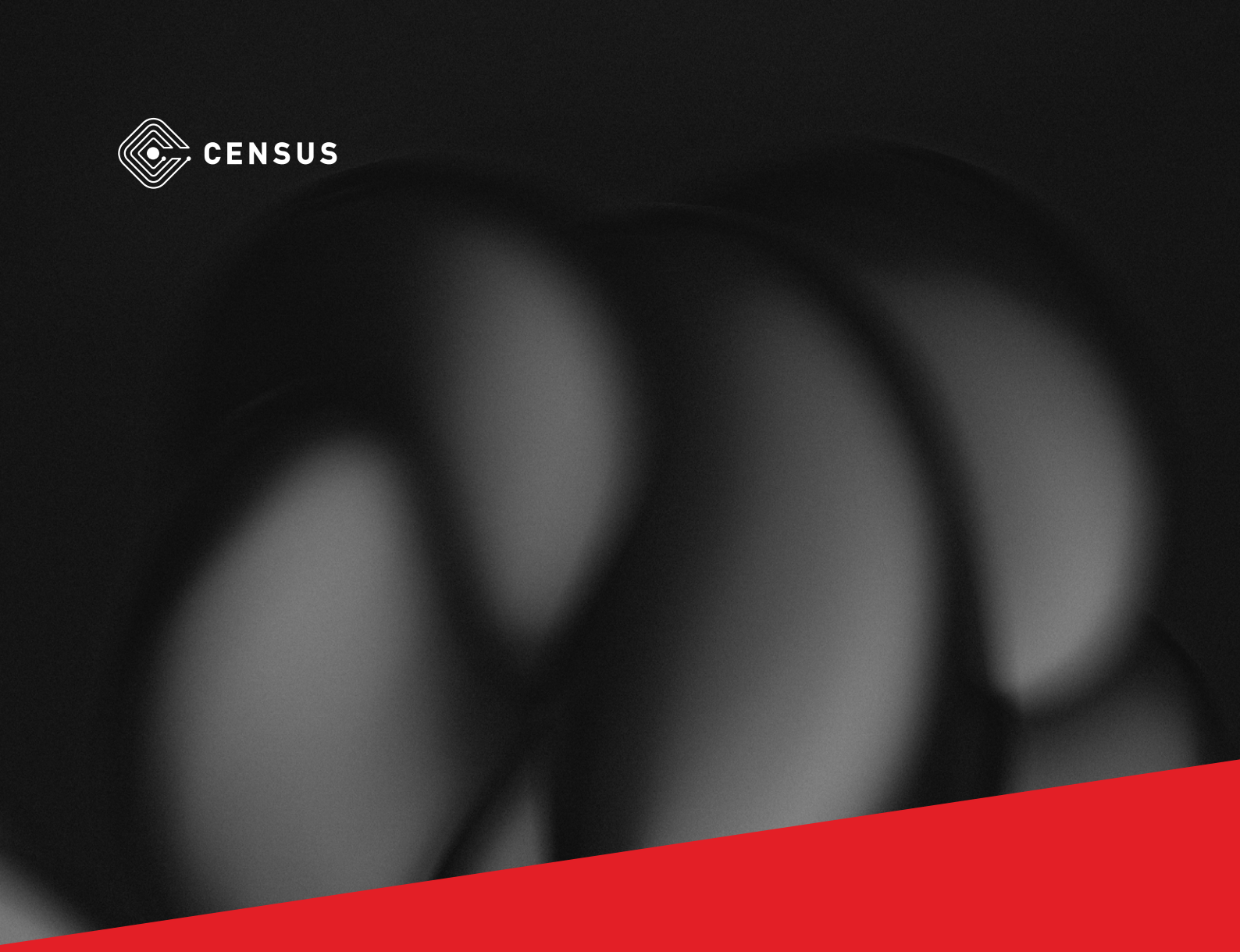
CENSUS



Assured Autonomy: Cybersecurity for AI-Driven Unmanned Systems

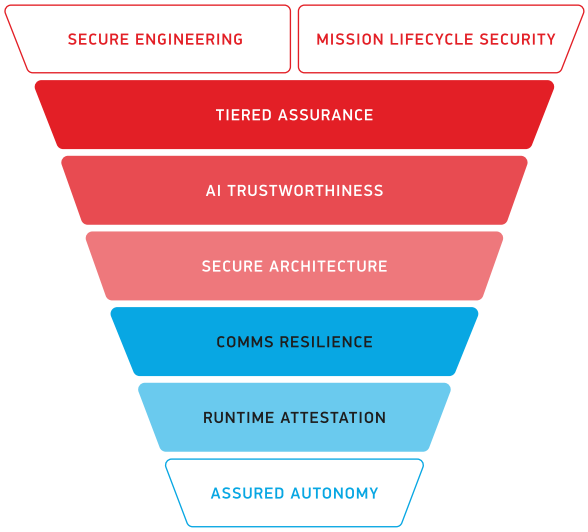
A MISSION-CENTRIC FRAMEWORK FOR PLATFORM INTEGRITY,
AI TRUSTWORTHINESS, AND SECURE COMMUNICATIONS

WWW.CENSUS-LABS.COM

Introduction

Autonomous Unmanned Systems (UxVs) have evolved into strategic assets within modern defense operations. Empowered by advances in artificial intelligence (AI), autonomy, and resilient communication architectures, these platforms are no longer limited to support roles but are now capable of executing complex missions independently in GPS-denied and EW-contested environments.

This evolution brings significant cybersecurity implications. The convergence of AI-driven autonomy, decentralized swarm control, and persistent wireless connectivity expands the attack surface and introduces dynamic threats that cannot be mitigated by traditional security models alone. Effective defense requires a mission-adaptive, system-of-systems approach.



CENSUS proposes a lifecycle-aligned cybersecurity strategy that views security through two complementary dimensions. The first focuses on engineering-time assurance, embedding trust during design, development, and integration. The second emphasizes mission-centric protection, enforcing operational security before, during, and after field deployment.

Additionally, the framework introduces adaptable security levels tailored to each UxV's mission profile, autonomy level, and system complexity. From lightweight ISR drones to strategic sovereign platforms, tiered assurance ensures proportional, certifiable protection without overburdening the system.

This paper presents a structured methodology for securing intelligent UxV platforms, blending engineering rigor with operational resilience across the full system lifecycle.

Evolving Capabilities and Strategic Role of UxVs

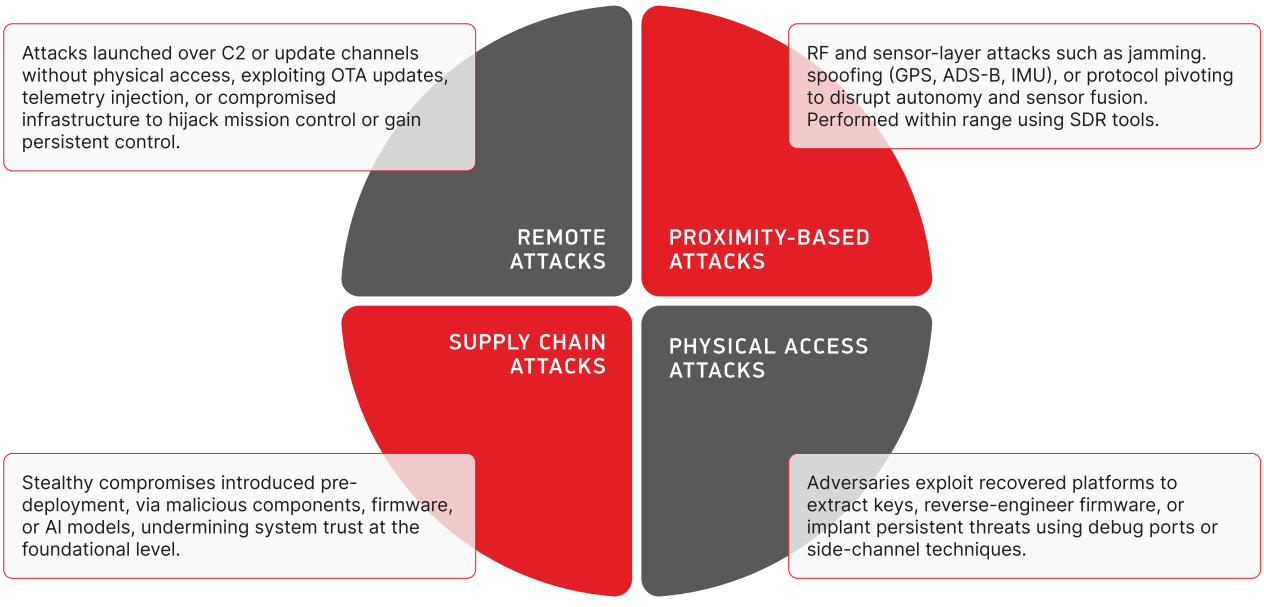
Modern military doctrine increasingly positions UxVs as strategic enablers for advanced ISR, electronic warfare (EW), precision engagement, perimeter defense, logistics automation, and multi-agent swarm operations. Their effectiveness is driven by several enabling technologies:

AI-powered Autonomy	Supports navigation and perception in GPS-denied or adversarial environments using techniques such as visual SLAM and multi-sensor fusion.
Distributed Control Architectures	Enable decentralized command-and-control (C2), enhancing redundancy, adaptability, and operational resilience.
Dynamic Mesh Networking	Provides robust, fault-tolerant communications with resistance to jamming, spoofing, and link degradation.

These capabilities increase reliance on software-defined architectures, edge-deployed AI, and secure, high-integrity connectivity. As a result, cybersecurity becomes a foundational requirement, essential to ensuring mission assurance, platform trustworthiness, and operational continuity.

Threat Landscape and Attack Vectors

UxVs face a broad range of cyber threats. Understanding these vectors is essential to building effective defenses.



Remote Attacks

Remote attacks target vulnerabilities in wireless command-and-control (C2) channels, data links, and update mechanisms, without requiring physical access to the platform. These attacks may involve unauthorized command injections, replayed telemetry, session hijacking, or manipulation of over-the-air (OTA) update processes, allowing adversaries to compromise mission execution, cause unauthorized deviations, or gain persistent control.

In advanced scenarios, remote adversaries may chain multiple attack stages to bypass layered defenses. For example, by compromising a ground control station, relay node, or communication backend, an attacker may modify or inject spoofed telemetry, including forged GPS signals rebroadcast via compromised uplinks or deployed spoofing payloads. While traditional GPS spoofing is a proximity-based RF threat, it can be weaponized remotely when integrated into a broader attack chain involving cloud-ground infrastructure or remote-controlled RF injection systems.

These remote threats can disrupt mission flow, force UxVs into degraded navigation states, or open control paths that bypass normal authentication, posing a significant risk to both operational integrity and safety.

Proximity-Based Attacks

Proximity threats involve adversaries employing software-defined radio (SDR) technologies to intercept, inject, jam, or manipulate RF links. These attacks include frequency jamming, spoofed signals such as GPS / GNSS, ADS-B, IFF, or telemetry beacons, and the exploitation of protocol-level flaws to pivot from external RF interfaces into internal systems components.

Sensor disruption attacks also fall into this category, particularly when targeting inertial navigation systems like IMUs (Inertial Measurement Units). Adversaries may induce signal saturation or spoof inertial data to degrade positioning confidence or force the platform to revert to GPS-based navigation, thereby making it susceptible to GPS spoofing. Similar manipulations of attitude sensors, barometers, magnetometers, or ultrasonic rangefinders can be used to desynchronize sensor fusion or provoke unsafe control decisions, especially in autonomous or semi-autonomous UxVs operating in GNSS-denied or signal-contested environments.

Physical Access Attacks

Physical access attacks occur when an adversary gains direct access to a UxV platform, typically through recovery of a downed or captured system in contested environments. Once physical control is established, attackers can exploit exposed debug ports (e.g., JTAG, UART, SWD), unprotected storage, or unsecured interfaces to extract cryptographic secrets, mission logs, or system configurations. Reverse engineering of firmware and hardware components can reveal undocumented functions, control protocols, or vulnerabilities that enable future remote exploitation.

Attackers may also attempt to bypass secure boot mechanisms, either by manipulating boot firmware, injecting unauthorized code into early boot stages, or exploiting hardware-level flaws in early privileged stages. These attacks undermine the foundational trust chain of the platform, allowing adversaries to execute arbitrary code before all firmware security controls are fully activated.

In more advanced scenarios, attackers may deploy side-channel techniques, such as power analysis, electromagnetic emission monitoring, or timing attacks, to target cryptographic operations and extract secret keys from trusted execution environments or secure elements. Physical tampering can also compromise hardware integrity, introducing implants or persistent surveillance mechanisms that bypass software-level defenses and remain undetected until redeployment.

Supply Chain Attacks

Supply chain attacks infiltrate the system well before deployment, embedding vulnerabilities through compromised components, development tools, or third-party libraries. These threats may manifest as malicious firmware implants, trojanized drivers, or subtle hardware alterations introduced during manufacturing, integration, or vendor-supplied updates.

In AI-enabled UxVs, poisoned training data, model manipulation, or malicious pre-trained weights can degrade decision-making or introduce exploitable model behaviors. Because these vectors operate beneath traditional runtime protections, they are particularly difficult to detect post-deployment and often evade platform security mechanisms. Such attacks can undermine trust at the foundational level, enabling adversaries to trigger failures during critical mission phases, exfiltrate sensitive telemetry, or silently alter system behavior, posing long-term risks to mission assurance and platform sovereignty.

Tiered Assurance: Adapting Security to Platform Risk

Autonomous UxV systems deployed across military operations vary significantly in size, mission complexity, communication footprint, and onboard computational capabilities. To avoid under-securing critical platforms or over-burdening low-cost systems, cybersecurity must be adaptable, scaling to meet the operational and technical profile of each UxV platform.

CENSUS advocates for frameworks that introduce tiered security assurance levels that map platform characteristics to corresponding cybersecurity expectations. These tiers enable proportional security integration without compromising resilience or mission effectiveness.

TIER	USE CASE	PRIMARY SECURITY OBJECTIVES
Tier 1: Baseline Security	Low-cost, short-range, teleoperated ISR drones or training assets.	Ensure hygiene controls: remove default credentials, encrypt C2 links, and disable debug interfaces.
Tier 2: Tactical Enhanced Security	Mid-complexity systems with autonomy or swarm coordination.	Defend against EW and spoofing, enforce FW signing, validate AI model inputs, and apply role-based access.
Tier 3: Mission-Critical Resilience	Strategic platforms in GPS-denied or contested environments.	Deploy runtime attestation, secure boot chains, AI robustness validation, full telemetry protection.
Tier 4: Sovereign Strategic Security	State-cleared platforms operating under national defense or export-sensitive missions.	Use vetted cryptography, enforce data localization, apply sovereign firmware validation, and integrate local key management & root of trust.

Mapping Security Requirements to Platform Characteristics

To apply tiered assurance effectively, it is critical to map security controls to the operational and technical attributes of each platform. The following matrix outlines how key characteristics, such as autonomy level, mission sensitivity, RF exposure, and system complexity, drive corresponding security requirements.

ATTRIBUTE	SCALING SECURITY REQUIREMENT
Autonomy Level (e.g., L0 to L4)	Higher autonomy mandates stronger AI runtime integrity, behavioral explainability, and attested model deployments.
Mission Sensitivity (e.g., kinetic, ISR, swarm C2)	More sensitive missions require stricter telemetry protections, secure provisioning, and post-mission sanitization.
RF Exposure Surface	Platforms with long-range, mesh-based, or satellite comms must employ resilient encryption, frequency agility, and spoof detection.
System Complexity	Larger or modular platforms require formal subsystem security mapping, interface hardening, and fault isolation.

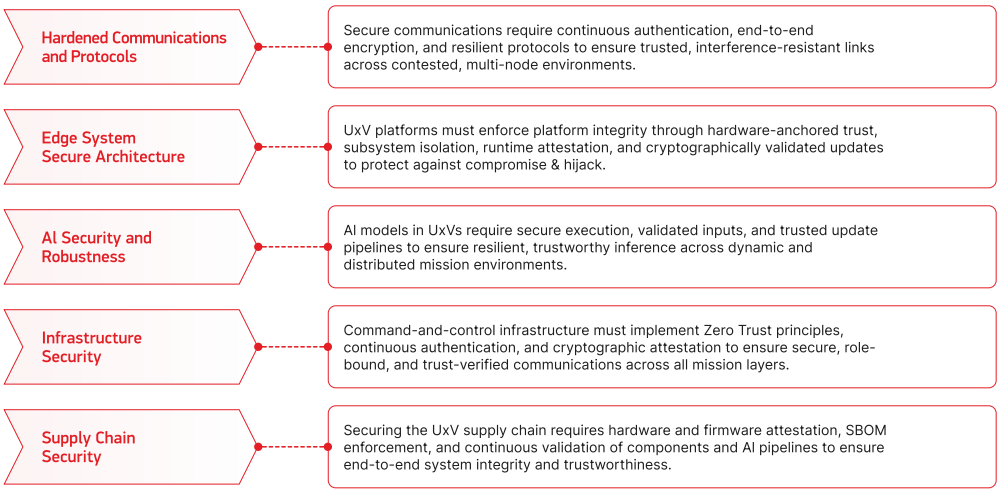
BENEFITS OF AN ADAPTABLE SECURITY MODEL

- **Optimized Resource Usage:** Lightweight UxVs are not burdened with heavyweight controls, preserving flight time, bandwidth, and cost-effectiveness.
- **Mission-Driven Assurance:** Security profiles reflect the real-world adversarial context, supporting better planning and assurance.
- **Compliance Scalability:** Tiered architecture aligns with diverse defense regulatory baselines (e.g., CMMC, STANAGs, NIST RMF).
- **Sovereign Control:** Tier 4 codifies national cybersecurity priorities, including supply chain trust and data sovereignty.

By embracing adaptable security levels, stakeholders can enforce appropriate cybersecurity controls across heterogeneous fleets while maintaining performance and operational flexibility. This approach also supports lifecycle sustainment by enabling tier-specific patching, validation, and re-certification strategies.

Engineering-Time Security Foundations

Cybersecurity must be embedded from the outset. CENSUS employs a multi-layered strategy built on secure architectures, robust protocols, and runtime integrity assurance.



Hardened Communications and Protocols

Secure and resilient communication is essential for UxV operations in contested environments. All links (command-and-control, telemetry, swarm coordination, etc.) must be encrypted and mutually authenticated, with integrity checks to prevent spoofing, replay, or injection. Techniques such as Frequency-hopping spread spectrum (FHSS), Direct-Sequence Spread Spectrum (DSSS) and dynamic link adaptation can enhance resistance to jamming and signal interference.

Continuous authentication ensures that trust is maintained throughout the mission, not just at session start, using mechanisms such as key rotation and signal fingerprinting. End-to-end encryption guarantees confidentiality across multi-hop links and untrusted relays, while secure broadcast and multicast protocols with group key management enable trusted coordination in swarm and distributed deployments. Finally, to future-proof against quantum-era threats, lightweight post-quantum cryptography (PQC) is integrated into resource-constrained stacks.

Edge System Secure Architecture

UxV platforms must establish hardware-based trust anchors, leveraging secure boot chains and root-of-trust components (e.g., TPMs) to verify firmware and enforce trust boundaries from power-on. Strong isolation between subsystems, such as control units, mission logic, communications, and support services, minimizes cross-domain risk from compromised components. Runtime attestation and automatic network-level quarantine prevent compromised nodes from influencing the mission. Peripheral authentication, hardware-backed encryption for data at rest, and encrypted logging protect sensitive information throughout the mission. Firmware updates, whether OTA or offline, are validated using cryptographic signatures to ensure platform integrity across the lifecycle.

AI Security and Robustness

AI models embedded in UxVs must be protected across deployment, inference, and fine-tuning (or retraining). Hardware-enforced isolation (e.g., TEEs, confidential computing) ensures secure execution, while model integrity is maintained through input validation, adversarial resilience checks, and trusted update channels. Malicious or drifting behavior is mitigated by fencing or isolating suspicious nodes and applying adaptive retraining mechanisms. Secure federated learning frameworks and trusted data pipelines preserve model trustworthiness across distributed deployments.

Infrastructure Security: C2 and Backend Systems

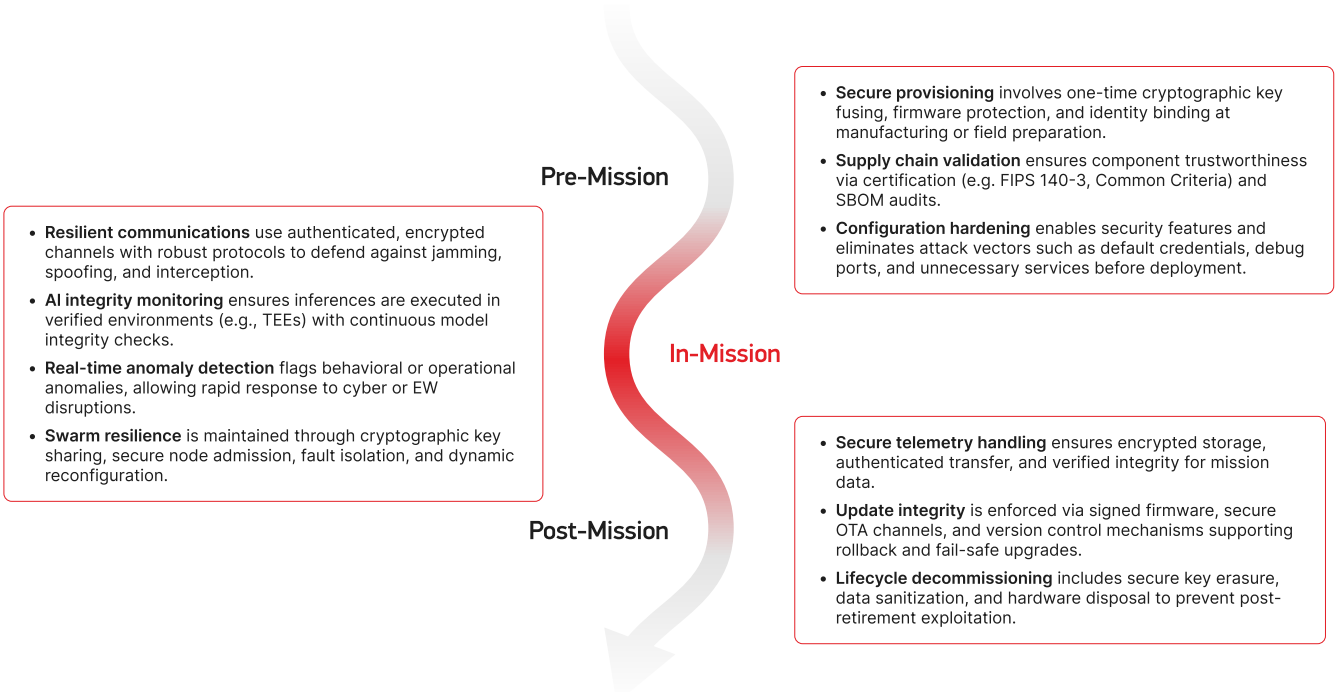
Command-and-control infrastructure must adopt Zero Trust principles, including continuous identity verification, cryptographically protected update channels, and multi-factor authentication. Federated identity and RBAC ensure granular, mission-specific access management across operational tenants and functions. End-to-end encryption protects data in transit between UxVs, C2 nodes, and backend systems, while context-aware access controls enforce restrictions on sensitive mission data and AI model usage. All communication channels should be cryptographically attested to maintain a continuous chain of trust throughout the mission architecture.

Supply Chain Security

To mitigate embedded risks, supply chains are secured through hardware and firmware attestation, enforced SBOM tracking, and cryptographic validation of third-party components. Supplier risk is managed through continuous vetting, secure development lifecycle requirements, and validation of AI training pipelines to detect tampered models or poisoned datasets. This foundation ensures the integrity and trustworthiness of all hardware and software elements used in UxV systems.

Mission-Centric Security Across the Operational Lifecycle

To ensure end-to-end assurance, security must be maintained throughout the mission lifecycle: pre-mission, in-mission, and post-mission. A mission-centric approach recognizes that security is not a one-time activity but an evolving capability that adapts to context, threat conditions, and platform state. By embedding security measures before, during, and after deployment, stakeholders can achieve true end-to-end assurance, preserving mission integrity, safeguarding sensitive data, and enabling resilient operations.



CENSUS Cybersecurity Capabilities Across the Lifecycle

CENSUS delivers comprehensive cybersecurity solutions through five integrated engineering domains, each tailored to the unique demands of modern autonomous and unmanned platforms. Our capabilities extend from research and development to secure system deployment and validation, ensuring that every layer of the UxV platform lifecycle is protected by design.

- **Applied Research** at CENSUS drives innovation in threat identification and feasibility assessment for emerging technologies. We conduct targeted security research across AI systems, autonomous control architectures, swarm dynamics, and decentralized C2 networks. This forward-looking analysis enables our clients to stay ahead of sophisticated adversaries by anticipating zero-day threats, assessing the operational viability of new security paradigms, and adapting rapidly to evolving battlefield technologies such as unjammable drones and adversarial AI.

- **Resilience Engineering** focuses on securing system design and operational integrity through rigorous architecture validation, threat modeling, and fault-tolerant design strategies. We develop layered defense blueprints that integrate fail-safe and fail-operational capabilities, enabling mission continuity even in degraded or adversarial conditions. From secure boot and recovery workflows to real-time risk mitigation and survivability planning, we help clients build platforms that are not only secure, but resilient by design.

- **Bespoke Secure Development** services empower defense and aerospace organizations with tailored, hardened software and hardware integrations that meet strict sovereign assurance and compliance requirements. Whether deploying secured AI inference engines at the tactical edge, hardening communication stacks with cryptographic enforcement, or integrating custom sensor interfaces with high-trust boundaries, our engineering teams build systems designed for resilience.

- **Security Validation and Assurance** closes the loop with hands-on, adversary-driven testing. We test realistic operational threat conditions, mirroring the tactics and tools of nation-state actors, validating the robustness of protocols, firmware, embedded systems, AI models, and secure update pipelines. Our assessment methodologies provide not only assurance of current system posture, but also actionable insights to reinforce long-term security strategy and mission readiness.

- **Tiger Team** delivers operational-scale adversarial testing to assess the resilience of the entire mission and operations infrastructure. Focused on emulating advanced persistent threats across digital, physical, and human vectors, this capability targets not just system vulnerabilities, but also lateral movement paths, identity escalations, and mission disruption scenarios. For UxV ecosystems, this includes red-teaming command-and-control pathways, cloud-ground interfaces, mission control centers, and backend AI orchestration environments. By mirroring the tactics and objectives of sophisticated actors, Tiger Team operations validate the effectiveness of detection, containment, and response mechanisms across the full mission stack, providing decision-makers with tangible risk insights and actionable remediation priorities.

Engineering Trusted Autonomy Across the Mission Lifecycle

At CENSUS, we don't just secure systems, we engineer mission-ready autonomy with the precision, resilience, and foresight demanded by today's most critical defense operations.

Rooted in offensive security expertise, rigorous engineering discipline, and cutting-edge applied research, we empower our clients to stay ahead of threats across the full spectrum of autonomy, from AI-driven drones to sovereign-grade unmanned platforms.

END-TO-END PROTECTION

From secure design and supply chain hardening to safe deployment and operation.

FUTURE-PROOF STRATEGY

Anticipate evolving cyber and electronic warfare threats.

OPERATIONAL RESILIENCE

Proven under real-world adversarial conditions.

SECURED WITH ADVERSARY INSIGHT

Adversary-driven engineers expose vulnerabilities early, cutting risk and cost.

Trust in autonomy starts with trust in security, and CENSUS is the trusted force behind the next generation of secure, intelligent, and resilient unmanned systems.

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 MISSION

Safeguarding the digital landscape, our focus is on securing critical domains on a global scale. Providing expert cybersecurity engineering, consulting and development fueled by both outstanding research and deep experience.

OUR VISION

To be universally identified as a unique cybersecurity powerhouse in an emeging cyberworld.

CAPABILITIES

CENSUS' offering has a unique edge. Our DNA allows us to comprehend in depth, the actions, processes and technical details of exploitation. Through research that advances the state-of-the-art and our experience, CENSUS gains unique insights into new attack vectors and techniques. This cybersecurity intelligence shapes our offering, essentially shielding our collaborators from future threats.

CENSUS offering encompasses:

- Cybersecurity engineering
- Tiger Team
- Vulnerability research

FOCUS

- To empower our partners achieving end-to-end cybersecurity, from inception to post-deployment.
- To provide cutting-edge cybersecurity engineering implementation for niche challenges.
- To enable vendors to offer cyber-resilient products and services.
- To identify new cybersecurity risks in technologies and organization processes.
- To provide exploitation and zero day vulnerabilities intelligence.

ACHIEVEMENTS

CENSUS has helped major corporations around the world to achieve cybersecurity resilience and provide hackproof products with the cybersecure promise. It has audited the design and implementation of multiple security-critical devices. Many of its findings have made it into public advisories, covering both system-level components (e.g. Microchip SDKs, Linux kernel, Android multimedia framework, Microsoft Windows networking stack) and popular applications (e.g. WhatsApp Messenger, Oracle WebCenter). Furthermore, each year CENSUS experts present groundbreaking research at industry-leading conferences, such as Black Hat, DEF CON, INFILTRATE, OffensiveCon, TROOPERS, OWASP AppSec.

CERTIFICATIONS

USA

607 Boylston Street,
Suite 165L
Boston, MA 02116

+1 8882 029 846

usa@census-labs.com

UK

Unit 2.15 Barley Mow Centre
10 Barley Mow Passage
W4 4PH, London

+44 1293 324 069

uk@census-labs.com

EUROPE

128 A. Siggrou Ave.,
Athens 117 45
Greece

+30 210 220 8989 90

eu@census-labs.com

ABU DHABI

Office 110 Incubator Building
Masdar City, Abu Dhabi
United Arab Emirates

+971 800 311 00 47

uae@census-labs.com

DUBAI

Unit GA-00-SZ-L1-RT-201, Level 1
Gate Avenue, DIFC, Dubai
United Arab Emirates

+971 800 311 00 47

uae@census-labs.com