Qwen

A Comprehensive Strategy for Secure, Compliant, and Maintainable Hazmat-Microdrone Operations

Designing a Resilient and Defensible OTA Architecture

The foundation for maintaining a fleet of sophisticated VR/AR hazmat-microdrones lies in a robust, secure, and reliable Over-the-Air (OTA) architecture [79]. This system must transcend simple patch delivery to become a cornerstone of the device's lifecycle management, ensuring security, operational continuity, and regulatory compliance [72 81]. The strategic imperative is to build a defense-in-depth framework that protects against a wide spectrum of threats, from man-in-the-middle attacks during transmission to malicious code execution after installation [73 77]. The core pillars of this architecture are a verifiable chain of trust, fail-safe update mechanisms, and operational resilience designed for real-world deployment challenges. The implementation begins at the hardware level with a Root of Trust (RoT), which serves as the ultimate source of authority for all subsequent software validation [105]. This RoT is typically realized through a Hardware Security Module (HSM) or a Trusted Platform Module (TPM), which provides a tamper-resistant environment for storing cryptographic keys and performing secure operations [8 122]. During manufacturing, a unique private key is generated within this secure element, and its corresponding public key is embedded in the device's read-only memory or fused into the chip, making it impossible to extract or clone [74 105]. This public key is the first link in the cryptographic chain of trust; every piece of software, from the bootloader to the final application, is cryptographically signed by the manufacturer using the corresponding private key before being distributed [126].

The verification process starts at boot time. The initial boot ROM, which cannot be modified, contains the hard-coded public key of the TPM or HSM [98]. It uses this key to verify the digital signature of the primary bootloader [126]. If the signature is invalid, the boot process halts immediately, preventing any unauthorized or corrupted code from ever executing [95]. This principle, known as Secure Boot, extends down the entire software stack, creating a continuous chain of trust where each component verifies the one that follows it [98 126]. For the OTA update package itself, strong asymmetric cryptography is paramount. Elliptic Curve Digital Signature Algorithm (ECDSA) using a standard curve like secp256r1 is a highly recommended method due to its balance of security and computational efficiency on resource-constrained devices [26]. The update package, which may contain a new OS image, drivers, or application modules, is hashed using a secure algorithm like SHA-256, and the resulting hash is then encrypted with the manufacturer's private key to create a digital signature [73]. This signature is bundled with the update file. When the device receives the update, it performs several verification steps: it downloads the update over a secure transport protocol like TLS 1.2 or 1.3 to protect against eavesdropping and man-in-the-middle attacks [22 23], it computes the hash of the received update file, and then it uses the public key stored in the TPM/HSM to decrypt the

digital signature and compare it to the locally computed hash [77]. Only if both hashes match is the update considered authentic and untampered, and only then will the installation proceed [84].

To ensure reliability and prevent the devices from becoming permanently unresponsive ("bricked"), the architecture must incorporate fail-safe mechanisms. The gold standard for this is the A/B partitioning scheme [72]. In this model, the device's flash memory is divided into two identical, writeable partitions, labeled 'A' and 'B'. One partition is always active, running the currently executing stable firmware, while the other remains inactive [74]. During an OTA update, the new software package is downloaded and written to the inactive partition. Once the download and initial integrity check are complete, the bootloader performs a full cryptographic verification of the entire new image on the inactive partition [81]. Only if this verification succeeds is the bootloader instructed to switch its boot target to the newly updated partition on the next reboot [72]. This atomic process ensures that the device never boots from a partially written or corrupted image. If the new firmware fails to boot correctly—for example, due to a power loss during flashing or a failure of its own self-test—a watchdog timer, which is a hardware feature that triggers a system reset if the software becomes unresponsive, will intervene [77]. Upon reboot, the bootloader detects that the new partition failed its test and automatically reverts to the last known-good version residing on the original active partition, ensuring uninterrupted functionality without requiring physical intervention [77 81]. To further enhance this protection, the system must also implement rollback prevention. An attacker could attempt to exploit a vulnerability in a new version of the firmware by forcing a downgrade to an older, less secure version. To counter this, the TPM's Platform Configuration Registers (PCRs) are used to track the cryptographic measurements of the software components [122]. Before loading any software, the TPM checks the current PCR values against the expected values for the desired firmware version. Any mismatch, such as attempting to load an older version, will cause the TPM to refuse to release the decryption keys needed to execute the software, effectively blocking the downgrade attack [122].

Operational robustness is achieved through strategies that optimize the update process for constrained networks and minimize risk during fleet-wide deployments. Delta updates, which transmit only the differences between the old and new software versions, significantly reduce bandwidth consumption and download times compared to sending full OS images [74 79]. This is particularly crucial for devices connected via cellular or satellite links [81]. Furthermore, large-scale deployments should not occur simultaneously across the entire fleet. Instead, they should follow a staged rollout strategy, beginning with a small internal group of devices (a "canary" release) to monitor for unexpected issues [79 82]. Success rates and post-update health metrics are closely tracked, and if the results are positive, the rollout is gradually expanded to larger cohorts until the entire fleet has been updated [82]. This approach mitigates the impact of a faulty update, preventing a widespread outage [79]. Rigorous testing is non-negotiable. The OTA process must be subjected to extensive testing that simulates real-world adversities, including intermittent connectivity, network packet loss, and sudden power interruptions during the flashing process [82]. The system must also be tested with intentionally corrupted or unsigned firmware packages to validate that the verification logic correctly rejects them [82]. For the hazmat-microdrones, this testing must extend to Hardware-in-the-Loop (HIL) simulations of the MRI environment to validate that the update process does not introduce

new electromagnetic interference (EMI) or stability issues [102 153]. Finally, the entire OTA pipeline must be supported by a centralized management system that can orchestrate deployments, monitor progress, collect telemetry data on success and failure rates, and provide detailed logs for forensic analysis in case of an incident [74 77]. This combination of cryptographic rigor, fail-safe mechanisms, and operational discipline creates a truly defensible OTA architecture that is essential for the safe and compliant operation of these advanced devices.

Feature	Description	Key Technologies & Standards
Root of Trust (RoT)	A foundational layer of security anchored in tamper-resistant hardware that establishes the initial basis for trust.	Trusted Platform Module (TPM), Hardware Security Module (HSM), One-Time Programmable (OTP) memory [8 105 122]
Secure Boot Chain	A multi-stage process where each component of the boot sequence validates the authenticity and integrity of the next before execution.	Cryptographic Hashing (SHA-256), Public Key Infrastructure (PKI), Asymmetric Cryptography (RSA, ECDSA) [84 98 126]
Update Package Integrity	Ensures the OTA update package has not been altered or tampered with during transit or storage.	Digital Signatures (ECDSA, RSA), Hash Functions (SHA-256), Code Signing Certificates [73 77 84]
Secure Transport	Protects the OTA update channel from eavesdropping and man-in-the-middle attacks during transmission.	Transport Layer Security (TLS) 1.2/1.3, Datagram Transport Layer Security (DTLS) [5 22 23]
Fail-Safe Installation	Mechanisms to prevent the device from becoming permanently unresponsive ("bricked") during an update.	A/B Partitioning, Watchdog Timers, Automatic Rollback Logic [72 74 77 81]
Rollback Protection	Prevents attackers from downgrading the firmware to a vulnerable older version.	TPM Platform Configuration Registers (PCRs), Version Number Tracking [81 105 122]
Bandwidth Optimization	Reduces the size of OTA updates to minimize network usage and speed up deployment.	Delta Updates (diff-based encoding), Compression (LZ4, Zstd) [74 79 81]
Controlled Deployment	Manages the rollout of updates across a large fleet to mitigate risk and allow for monitoring.	Staged Rollouts (Canary Releases), Fleet Segmentation, Phased Deployments [79 82 84]
Comprehensive Testing	Validates the entire OTA process under realistic conditions to ensure reliability and security.	Hardware-in-the-Loop (HIL) Simulation, Real-World Failure

Feature	Description	Key Technologies & Standards
		Mode Simulation (power loss, etc.) [82,102,153]

Navigating the MRI Environment: Safety, EMI, and Material Constraints

Operating the hazmat-microdrones within an MRI suite introduces a uniquely challenging and hazardous environment that imposes extreme constraints on their design, materials, and electronic systems [49]. The MRI scanner generates three distinct and powerful types of electromagnetic fields—the static magnetic field (B0), the time-varying gradient fields (dB/dt), and the radiofrequency (RF) fields (B1)—each posing specific risks that must be meticulously managed to ensure patient safety and diagnostic accuracy [39,70]. The most immediate and severe hazard is the static magnetic field, which is always active, even when the scanner is not actively acquiring images [64,68]. This powerful field, which can be hundreds of thousands of times stronger than Earth's magnetic field, turns any ferromagnetic object—containing iron, nickel, or cobalt—into a dangerous projectile [133,135]. The tragic 2001 death of a young boy who was struck by an oxygen tank that became a missile inside an MRI suite serves as a stark reminder of this danger, leading to stricter safety protocols worldwide [133]. Therefore, the fundamental design constraint for the microdrones is that they must be constructed entirely from non-ferromagnetic materials [40]. This applies to every component, from the airframe and motor mounts to screws, batteries, and wiring harnesses. Materials such as aerospace-grade aluminum alloys, titanium, and high-strength plastics are essential to meet this requirement [40,55]. All components must be individually verified, as composite objects containing even small amounts of ferrous material can pose a significant risk [135].

Beyond the projectile effect, the static field induces rotational forces (torque) on any magnetic materials, which could cause implants or device components to twist, and translational forces that pull objects toward the center of the magnet bore [39,49]. These forces increase dramatically as an object gets closer to the magnet, making manual control impossible once an object is within the fringe field [135]. Consequently, the drones must undergo formal classification according to the ASTM F2503 standard, which defines three categories: MR Safe (non-metallic, non-magnetic), MR Unsafe (poses unacceptable risks), and MR Conditional (safe only under specified conditions) [40,49]. Given their active electronics, the drones cannot be classified as MR Safe and must be designated as MR Conditional. This requires rigorous testing to define a set of operating parameters, such as the maximum allowable static magnetic field strength (e.g., $\leqslant 3.0$ T), spatial gradient limits, and proximity restrictions, which must be clearly labeled on the device and in its documentation [39,130].

The second major hazard comes from the rapidly switching gradient magnetic fields, which are responsible for spatially encoding the MRI signal but also induce electric currents in any nearby conductors [49,130]. These induced currents can cause two primary effects: peripheral nerve stimulation (PNS), which manifests as involuntary muscle twitching, and acoustic noise that can exceed 130

decibels, necessitating hearing protection for anyone in the room [49 64]. The drone's own wiring and electronic components must be carefully routed and shielded to minimize the formation of large conductive loops, which act as antennas and are more susceptible to inducing harmful currents [68]. The third hazard is thermal, caused by the powerful RF fields used to excite hydrogen nuclei [70]. These fields can deposit energy in the body, measured as Specific Absorption Rate (SAR), and this energy can also be absorbed by metallic components or conductive loops on the drone, leading to localized tissue heating [39 130]. This is a significant concern for burns, which account for over 70% of MRI-related complications [130]. The FDA has established strict SAR limits, typically 4.0 W/kg whole-body average, to prevent excessive temperature rise [130 135]. The drone's design must therefore include measures to minimize RF coupling, such as using double-shielding on cables and enclosures, employing optical data transfer instead of electrical connections where possible, and ensuring battery-powered operation to avoid ground loops that can act as antennas [111 144]. The HF-1 system, designed for simultaneous EEG-fMRI recording, exemplifies these principles with its use of non-ferromagnetic components, double-shielded cables, and battery operation to ensure low-noise, electromagnetically compatible performance [111].

Finally, the drone's own electronic systems must be immune to the intense electromagnetic environment of the MRI suite. The scanner's powerful fields can interfere with the drone's sensors, communication links, and flight control computers, potentially causing malfunctions or complete failure [54]. This requires a comprehensive Electromagnetic Compatibility (EMC) strategy that addresses both emissions and immunity [56]. The drone's emissions must comply with FCC Part 15 regulations for unintentional radiators, which have stricter Class B limits for residential settings but Class A limits for industrial environments [31 36]. More importantly, the drone's circuits must be designed with robust shielding to resist external interference. This often involves a multi-layered approach, using conductive enclosures made of materials like copper or aluminum to create a Faraday cage effect, applying conductive coatings or paints to PCBs, and using ferrite beads or chokes on power and signal lines to suppress conducted interference [54 55]. For miniaturized devices, board-level shields and specialized gaskets are used to seal seams and vents, maintaining the integrity of the shielded enclosure [54 57]. Advanced materials such as graphene composites or MXenes offer promising avenues for lightweight, flexible, and highly effective EMI shielding, though their practical integration requires careful engineering [58 59]. The entire drone, from its motors and propellers to its payload, must be evaluated to ensure it does not degrade the quality of the MRI images, a risk assessed through standardized tests like ASTM F2119 [39]. This complex interplay of physical, thermal, and electromagnetic hazards means that the development of the hazmat-microdrones must be guided by a deep understanding of MRI physics and safety standards from the very beginning of the design process.

Hazard Type	Description	Primary Risks	Mitigation Strategies
Static Magnetic Field (B0)	A powerful, constant magnetic field that is always active.	Projectile Effect (Missile Effect), Torque, Translational	Use of non-ferromagnetic materials (Al, Ti alloys), Formal MR Conditional classification per ASTM

Hazard Type	Description	Primary Risks	Mitigation Strategies
		Force, Implanted Device Malfunction	F2503, strict access control (Zone IV). [40 64 68 133]
Time-Varying Gradient Fields (dB/dt)	Rapidly switched magnetic fields used for spatial encoding.	Peripheral Nerve Stimulation (PNS), Loud Acoustic Noise (>130 dB), Induced Currents	Minimize conductive loops in wiring, use of hearing protection, careful routing of electronic components. [49 64 130]
Radiofrequency (RF) Fields (B1)	High-frequency electromagnetic waves used to excite nuclei.	RF-induced Heating (Thermal Burns), SAR Exceedance, Interference with Electronic Systems	Double-shielding on cables/ enclosures, optical data transfer, battery power to avoid ground loops, SAR modeling and compliance testing. [39 68 111 130]
Electromagnetic Interference (EMI)	Unwanted electromagnetic energy disrupting electronic devices.	Sensor malfunction, Control system failure, Degradation of MRI image quality.	Comprehensive EMC design, EMI shielding (copper/ aluminum enclosures, ferrites), filtering on power/ signal lines, adherence to FCC Part 15. [31 39 54 56]

Achieving Regulatory Compliance: A Dual-Frontier Approach for FDA and FCC

The operation of hazmat-microdrones in close proximity to an MRI scanner places them at the intersection of two distinct but equally demanding regulatory domains: the Food and Drug Administration (FDA) and the Federal Communications Commission (FCC) [28 37]. Successfully navigating this dual-frontier is not merely a procedural hurdle but a fundamental aspect of the product's design and lifecycle management. The device must be engineered to meet the stringent safety and efficacy standards for medical devices, as enforced by the FDA, while also adhering to the FCC's strict rules governing electromagnetic emissions and radio frequency spectrum use [28 37]. A failure to comply with either agency would render the device illegal for clinical use and expose the operator to significant legal and financial risk [31 34]. The FDA regulates the microdrones because they are intended for use in a medical setting and interact with a Class II medical device (the MRI scanner) [38 41]. This classification subjects the drones to a comprehensive set of requirements under the Federal Food, Drug, and Cosmetic Act. A central mandate is the Quality System Regulation (QSR), codified in 21 CFR Part 820, which establishes a framework for good manufacturing practices covering everything from design controls and production processes to corrective and preventive actions (CAPA) and record-keeping [41]. This means that the entire development process, from initial concept to final deployment, must be systematically controlled and documented [41 87].

Before the drones can be marketed, the manufacturer must submit a premarket notification, typically through a 510(k) submission, to the FDA [41 43]. The goal of a 510(k) is to demonstrate that the new device is substantially equivalent to a legally marketed predicate device—that is, it has the same intended use and technological characteristics, or if different, those differences do not raise new questions of safety or effectiveness [41]. This submission requires a mountain of evidence, including a detailed description of the device, proposed labeling, sterilization and shelf-life data, biocompatibility testing per ISO 10993-1, and, critically, performance and safety data from testing against recognized consensus standards [41]. For MRI-compatible devices, this means extensive testing based on standards like IEC 60601-2-33, which covers the basic safety and essential performance of MR equipment [48 51]. This includes demonstrating compliance with requirements for the static magnetic field, gradient fields, RF fields, and overall electromagnetic compatibility [51]. The FDA also places a strong emphasis on cybersecurity for networked medical devices. Manufacturers are required to develop and maintain a cybersecurity management system throughout the device's lifecycle, addressing vulnerabilities, providing timely patches, and communicating risks to users [28 41]. The secure OTA architecture described previously is a direct and necessary response to these regulatory expectations, providing a documented mechanism for remote patching and demonstrating a commitment to post-market security [41 74].

Simultaneously, the FCC regulates the device's electromagnetic emissions under its jurisdiction over the radio frequency spectrum [30]. Since the microdrones are wireless devices that will be operating near sensitive medical equipment, they must comply with the rules outlined in FCC Part 15, which governs unintentional radiators [31 33]. This part sets strict limits on the amount of electromagnetic interference (EMI) a device can emit, with lower Class B limits applicable to home-use devices and higher Class A limits for industrial environments [36]. Because the drones are part of a wireless medical telemetry service (WMTS), they may also fall under the purview of Part 95, which authorizes dedicated frequency bands for transmitting physiological data from patients to remote monitoring stations [29 37]. Devices operating under Part 95 require certification from the FCC, which involves rigorous testing to ensure they do not cause harmful interference to other services [37]. Even if operating in unlicensed ISM bands, the drones must demonstrate coexistence with other wireless medical devices in the healthcare facility, a risk management process for which the FDA recognizes standards like AAMI TIR 69 [28]. The same physical testing performed to achieve FDA clearance for MRI safety, particularly assessments of RF-induced heating (ASTM F2182) and electromagnetic compatibility (IEC 60601-1-2), will be directly relevant to proving compliance with FCC SAR limits and emission standards [39 54]. The synergistic nature of these regulations means that an integrated approach to compliance is most efficient. By designing the device to meet the stringent requirements of IEC 60601-2-33 for MRI safety, many of the underlying EMC and RF performance criteria required by the FCC are inherently satisfied [48 56]. Engaging with both regulators early in the development cycle through informal discussions or pre-certification programs can help identify potential issues and streamline the eventual approval process [28 72]. Ultimately, achieving compliance is an ongoing responsibility. The manufacturer must continue to monitor the device's performance in the field, report adverse events as required by FDA regulations, and manage any recalls or field safety corrective actions [41]. The secure OTA system is again critical here, as it provides the infrastructure

for implementing these corrective actions efficiently and tracking their effectiveness across the deployed fleet.

Regulatory Body	Jurisdiction & Focus	Key Regulations & Standards	Critical Requirements for Hazmat-Microdrones
Food and Drug Administration (FDA)	Medical Device Safety, Efficacy, and Lifecycle Management.	21 CFR Part 820 (Quality System Regulation), 510(k) Premarket Notification, IEC 60601-2-33 (MRI Equipment Safety), FDA Cybersecurity Guidance.	Substantial equivalence demonstration, adherence to QSR, extensive EMC and MRI safety testing (ASTM F2182, F2119), documented cybersecurity program, post-market surveillance and reporting. [38 41 48 130]
Federal Communications Commission (FCC)	Radio Frequency Spectrum Use and Electromagnetic Interference (EMI) Emissions.	Title 47 CFR Part 15 (Intentional & Unintentional Radiators), Part 95 (Wireless Medical Telemetry Service - WMTS), Part 18 (ISM Equipment).	Compliance with Class A or B Emission Limits, avoidance of harmful interference, potential licensing or authorization for WMTS operation, demonstration of coexistence with other wireless medical devices. [28 29 30 31 37]

Integrating Advanced Security and Traceability with Blockchain Technology

In addition to the foundational layers of hardware-based security and regulatory compliance, a state-of-the-art approach to managing the hazmat-microdrones involves integrating blockchain technology to create an immutable and transparent audit trail for all critical operations [11 12]. This strategy directly addresses the user's requirement for scientifically validated security and data hygiene, moving beyond traditional logging to a system where records are cryptographically secured, verifiable, and resistant to tampering [1 7]. The core value proposition of a blockchain-based system is its ability to provide a decentralized, tamper-evident ledger of transactions, which in this context translates to a log of all significant events related to the drones, including firmware updates, sensor data captures, and access attempts [4 11]. This creates a powerful tool for forensic accountability, enhancing both security and regulatory transparency [1]. The architecture typically employs a permissioned blockchain, such as Hyperledger Fabric or Quorum, rather than a public one like Bitcoin or Ethereum [11 12]. A permissioned model is better suited for enterprise and medical applications because it allows for controlled access, where only authorized entities—such as the drone operators, manufacturers, and auditors—are permitted to participate as validator nodes in the network [4]. This ensures privacy and

prevents unauthorized parties from viewing or altering the ledger [11]. Smart contracts, which are self-executing pieces of code deployed on the blockchain, serve as the automated enforcement mechanism for the system's policies [4 11]. For instance, a smart contract can be programmed to enforce rules for logging AI-driven decisions or for validating the integrity of incoming data streams, automatically rejecting any transaction that fails to meet predefined criteria [4 9].

A key challenge in deploying blockchain on resource-constrained IoT devices is the overhead associated with cryptographic hashing, digital signatures, and consensus validation [8]. Transmitting large volumes of raw sensor data directly onto the blockchain would be computationally prohibitive and impractical. The solution, known as selective anchoring, is to store only the metadata and a cryptographic hash of the actual data on-chain, while keeping the bulk of the data off-chain in a secure database or a distributed storage system like IPFS (InterPlanetary File System) [8 11 12]. For example, when a drone completes an fMRI scan, the raw imaging data is stored securely off-chain. On the blockchain, a transaction is created containing a timestamp, the drone's unique identifier, the hash of the scan data, and other relevant metadata (e.g., patient ID, session details) [11]. This hybrid approach achieves the best of both worlds: the immutability and integrity guarantees of the blockchain are preserved, while the performance and scalability of the system are maintained by minimizing on-chain data volume [8 11]. The system can also leverage lightweight consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) instead of energy-intensive Proof of Work (PoW), which are far more suitable for the constrained resources of embedded devices and IoT networks [4 11 12]. PBFT, in particular, offers fast block confirmation times (around 1.8 seconds in some implementations) and is well-suited for networks with a known set of validators, making it ideal for a consortium of trusted stakeholders [4].

This blockchain-integrated system provides profound benefits for security and compliance. Every action taken by a drone can be logged immutably, creating a non-repudiable record of its activities [4 11]. This is invaluable for detecting and investigating security incidents. If a drone's behavior deviates from its expected pattern, the immutable log can be analyzed to trace the origin of the anomaly, whether it was a result of a faulty sensor reading, a successful cyberattack, or a misconfiguration introduced during an OTA update [3 12]. The system can be designed to trigger alerts or automated responses based on patterns detected in the blockchain data. For example, an AI-driven anomaly detection model could analyze the stream of logged events in real-time, and upon identifying a suspicious pattern, a smart contract could automatically quarantine the affected drone or initiate a rollback to a previous stable state, demonstrating a proactive and deterministic security posture [4 12]. From a regulatory perspective, this system provides a clear and auditable trail that satisfies the demands of bodies like the FDA and EU agencies for post-market surveillance and accountability [11 12]. The logs can be queried by authorized auditors to verify that the drones were operated within their approved parameters, that all software updates were properly authenticated, and that no unauthorized changes were made to the system [11]. The use of cryptographic hashes ensures that any alteration to historical data breaks the chain of trust, making tampering detectable [4]. Furthermore, the system can be designed to handle privacy concerns inherent in medical data. Personal information can be stored off-chain, while only pseudonymized identifiers and hashes are recorded on the blockchain, aligning with GDPR and HIPAA requirements [11 12]. In summary, by embedding

blockchain technology into the operational fabric of the hazmat-microdrone fleet, the organization can construct a system that is not only secure and compliant but also inherently transparent and accountable, providing a powerful safeguard against both internal and external threats.

Synthesizing the Strategy: Actionable Steps for Deployment and Future Evolution

To transition from a conceptual framework to a fully operational and compliant system, a series of concrete, actionable steps must be executed. This synthesis integrates the principles of secure OTA architecture, MRI environmental adaptation, regulatory navigation, and advanced security to create a phased roadmap for success. The overarching goal is to establish a resilient, maintainable, and trustworthy operational paradigm for the hazmat-microdrones, capable of supporting both immediate needs and future advancements. The first and most urgent priority is to conduct a comprehensive hardware audit of the existing drone fleet [72]. This involves physically inspecting every component—from the airframe and motors to the smallest screw and wire—to confirm its material composition and classify it against the ASTM F2503 standard for MRI safety [40]. This step is critical to immediately identify any ferromagnetic materials that pose a projectile risk and must be replaced before any further operational testing can occur [133]. Concurrently, a sandbox test environment must be established to safely evaluate the drones and their updated software [72]. Leveraging a facility like the UConn Brain Imaging Research Center's mock MRI simulator provides a cost-effective and low-risk platform for validating firmware stability, assessing electromagnetic interference (EMI) characteristics, and testing sensor performance without risking damage to the main scanner or compromising patient studies [102 153].

With the hardware baseline established, the next phase focuses on developing a modular firmware architecture [99]. The software should be designed to separate core OS functions from application-specific modules, such as flight control, VR/AR rendering, and fMRI data acquisition [72]. This modularity allows for targeted updates, where, for example, the OS can be patched for security without requiring a full update of the specialized scientific application, thereby reducing complexity and minimizing the risk of introducing regressions [72 79]. Using a container-based approach, such as Docker, could further enhance this isolation, allowing individual services to be updated independently and improving system resilience [72]. The secure OTA architecture must then be developed and rigorously tested within this sandbox environment. This includes implementing the A/B partitioning scheme for fail-safe updates, establishing the TPM-based chain of trust for Secure Boot, and integrating a delta-update mechanism to optimize bandwidth [72 74 79]. The testing regimen must go beyond nominal conditions to simulate real-world adversity, including intentional power loss during flashing, network disconnections, and the application of corrupted update packages to stress-test the validation and rollback logic [82].

Parallel to the technical development, a proactive regulatory strategy must be pursued. This begins with engaging with the FDA and FCC early in the process through informal consultations to clarify requirements and discuss the proposed design and testing plans [28 72]. A detailed pre-certification plan should be prepared, outlining how the project will leverage recognized consensus standards like IEC

60601-2-33 to demonstrate compliance with MRI safety and EMC requirements [48] [51]. The documentation for the 510(k) submission must be meticulously prepared, compiling all test data, design specifications, and risk analyses generated during the development and sandbox testing phases [41]. The secure OTA system itself must be documented as a key component of the device's cybersecurity management plan, detailing its cryptographic protocols, access controls, and rollback procedures to satisfy FDA expectations [41]. To fulfill the user's deep-seated need for absolute data hygiene and traceability, a blockchain-based audit trail should be integrated into the system's design [1] [11]. A pilot implementation using a lightweight permissioned blockchain like Hyperledger Fabric can be developed to log critical events, such as OTA update attempts, emergency rollbacks, and access to sensitive data streams, creating an immutable and verifiable record for forensic and regulatory purposes [11] [12].

Finally, the entire strategy must be viewed as a living framework for continuous improvement. Long-term maintainability is ensured by adopting agile development practices, where CI/CD pipelines automate the building, testing, and deployment of updates, accelerating the response to emerging security threats or new research requirements [23] [79]. Regular out-of-band security patching via OTA will be essential for promptly addressing newly discovered vulnerabilities [23]. The system should also incorporate a telemetry feedback loop that reports real-time health and security metrics back to a central dashboard, enabling proactive monitoring and rapid detection of anomalous behavior across the fleet [74] [77]. To conclude, by systematically executing these steps—auditing hardware, building a modular and secure system in a sandbox, pursuing proactive regulatory engagement, and embedding advanced technologies like blockchain for traceability—the organization can successfully transform the hazmat-microdrones from a collection of problematic devices into a robust, compliant, and scientifically valuable asset. This approach ensures that the fleet is not only fixed but is also built on a foundation of security, reliability, and regulatory soundness, ready to support cutting-edge neuroimaging research for years to come.

Reference

1. Real-Time Data Integrity Validation Using Blockchain for ... https://www.researchgate.net/publication/389911364_Real-Time_Data_Integrity_Validation_Using_Blockchain_for_Autonomous_Vehicles
2. The real-time data processing framework for blockchain ... https://www.sciencedirect.com/science/article/pii/S111001682500119X
3. AI-Blockchain Integration for Real-Time Cybersecurity https://www.mdpi.com/2624-800X/5/3/59
4. AI-Powered Anomaly Detection with Blockchain for Real- ... https://arxiv.org/pdf/2505.06632
5. Blockchain-based Video Forensics and Integrity Verification ... https://epublications.marquette.edu/cgi/viewcontent.cgi?article=1052&context=comp_fac

6. Securing Real-Time Data Transfer in Healthcare IoT ... https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/681
7. Decentralized trust framework for smart cities: a blockchain ... https://pmc.ncbi.nlm.nih.gov/articles/PMC12222849/
8. Enhancing IoT security through blockchain integration https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1670473/full
9. Secure blockchain based intrusion detection for IoT networks https://link.springer.com/article/10.1007/s10791-025-09754-4
10. A blockchain-enabled IoT auditing management system ... https://www.sciencedirect.com/science/article/abs/pii/S0360835223001158
11. Using Blockchain Ledgers to Record AI Decisions in IoT https://www.mdpi.com/2624-831X/6/3/37
12. Using Blockchain Ledgers to Record the AI Decisions in IoT https://www.preprints.org/manuscript/202504.1789
13. A Blockchain Based Secure IoT System Using Device Identity ... https://pmc.ncbi.nlm.nih.gov/articles/PMC9571557/
14. BlockTrack-L: A Lightweight Blockchain-based Provenance ... https://thesai.org/Publications/ViewPaper?Volume=11&Issue=4&Code=IJACSA&SerialNo=62
15. A Blockchain-Based Audit Trail Mechanism: Design and ... https://www.researchgate.net/publication/356610206_A_Blockchain-Based_Audit_Trail_Mechanism_Design_and_Implementation
16. Security and Privacy Enhancing in Blockchain-based IoT ... https://arxiv.org/html/2403.01356v1
17. Blockchain framework with IoT device using federated ... https://www.nature.com/articles/s41598-025-06539-z
18. Blockchain based distributed trust management in IoT and ... https://link.springer.com/article/10.1007/s11227-024-06286-4
19. An IoT system for access control using blockchain and ... https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-025-00208-4
20. Design of Provably Secure and Lightweight Authentication ... https://www.sciencedirect.com/science/article/abs/pii/S0140366424003189
21. A Lightweight Authentication Protocol for UAVs Based on ... https://www.mdpi.com/2504-446X/7/5/315
22. MQTree: Secure OTA Protocol Using MQTT and MerkleTree https://pmc.ncbi.nlm.nih.gov/articles/PMC10934006/
23. OTA Updates: Keeping Connected Devices Smart and Up ... https://medium.com/@sparkleo/ota-updates-keeping-connected-devices-smart-and-up-to-date-a6b545fd8a4f

24. Physics' Dan Gauthier creates 'tamper-proof' encryption for ... https://artsandsciences.osu.edu/news/physics-dan-gauthier-creates-tamper-proof-encryption-drones
25. Trusted Verification of Over-the-Air (OTA) Secure Software ... https://www.ndss-symposium.org/wp-content/uploads/autosec2021_23028_paper.pdf
26. MUP: Simplifying Secure Over-The-Air Update with MQTT ... https://www.researchgate.net/publication/347898576_MUP_Simplifying_Secure_Over-The-Air_Update_with_MQTT_for_Constrained_IoT_Devices
27. Towards a Modular Attestation Framework for Flexible Data ... https://5gdrones.eu/wp-content/uploads/2021/12/Towards-a-modular-attestation-framework-for-flexible-data-protection-for....pdf
28. Wireless Medical Devices https://www.fda.gov/medical-devices/digital-health-center-excellence/wireless-medical-devices
29. 47 CFR Part 15 -- Radio Frequency Devices https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15
30. Equipment Authorization − RF Device https://www.fcc.gov/oet/ea/rfdevice
31. FCC Part 15 Testing Solutions https://www.intertek.com/communications-equipment/fcc-certification/part15/
32. FCC Part 15 vs. FCC Part 18: Key Differences https://compliancetesting.com/fcc-part-15-vs-fcc-part-18/
33. FCC Part 15 Testing & Certification https://www.eurofinsus.com/electrical-and-electronics/services/wireless-rf-testing/fcc-part-15-testing-certification/
34. Wireless and RF Testing For FCC Compliance - MET Labs https://metlabs.com/wireless-and-rf-testing-for-fcc-compliance/
35. Everything to Know About FCC Part 15 Exemptions and ... https://resources.system-analysis.cadence.com/blog/msa2022-everything-to-know-about-fcc-part-15-exemptions-and-fcc-part-15-transmitters
36. FCC Part 15 https://www.wll.com/services/fcc-part-15/
37. Regulation of Wireless Digital Devices in the USA https://www.freyrsolutions.com/blog/regulation-of-wireless-digital-devices-in-the-usa
38. MRI Information for Industry https://www.fda.gov/radiation-emitting-products/mri-magnetic-resonance-imaging/mri-information-industry
39. Testing and Labeling Medical Devices for Safety in the ... https://www.fda.gov/media/74201/download
40. MRI Safety Standards for Medical Equipment in 2025 https://mrimed.com/blogs/resources/mri-safety-standards-2025?srsltid=AfmBOordZnhsIQVSmK-OG54sxR6hC___xoZJjeDXdTUqXMKXL14ORmh5

41. FDA Class II Medical Device Regulations and Compliance https://www.ketryx.com/blog/fda-class-ii-medical-device-regulations-and-compliance
42. Testing and Labeling Medical Devices for Safety in the ... https://www.fda.gov/regulatory-information/search-fda-guidance-documents/testing-and-labeling-medical-devices-safety-magnetic-resonance-mr-environment
43. US regulatory considerations for low field magnetic ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10386952/
44. 21 CFR Part 892 -- Radiology Devices https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-892
45. FDA Updates Two MRI-Related Guidance Documents https://www.exponent.com/article/fda-updates-two-mri-related-guidance-documents
46. Medical Imaging: The Basics of FDA Regulation https://www.mddionline.com/radiological/medical-imaging-the-basics-of-fda-regulation
47. Testing and Labeling Medical Devices for Safety in the ... https://downloads.regulations.gov/FDA-2019-D-2837-0006/attachment_2.pdf
48. IEC 60601-2-33:2022 https://webstore.iec.ch/en/publication/67211
49. Safety Guidelines for Magnetic Resonance Imaging ... https://www.ismrm.org/smrt/files/con2033065.pdf
50. Occupational exposure in MRI - PMC - PubMed Central - NIH https://pmc.ncbi.nlm.nih.gov/articles/PMC3486652/
51. IEC 60601-2-33 https://mriquestions.com/uploads/3/4/5/7/34572113/safety_iec_60601-2-33previews_1897819_pre.pdf
52. 2.2-3.4.5 Magnetic Resonance Imaging (MRI) Facilities https://koppdevelopment.com/articels/2018%20Guidelines%20for%20Design%20and%20Construction%20of%20Health%20Care%20Facilities%20.pdf
53. IEC 60601-2-33:2010/AMD2:2015 https://cdn.standards.iteh.ai/samples/21895/da1581504c754cbd9faaa2314cc372a6/IEC-60601-2-33-2010-AMD2-2015.pdf
54. EMI Shielding in Medical Displays: A Clinical Necessity https://reshinmonitors.com/emi-shielding-medical-displays/
55. EMI Shielding in Medical Devices https://www.e-fab.com/emi-shielding-in-medical-devices-materials-techniques-and-applications/
56. Know About EMI EMC Standards https://xgrtec.com/blog/know-about-emi-emc-standards/
57. Ensuring Diagnostic Precision: EMI Shielding for Medical ... https://leadertechinc.com/ensuring-diagnostic-precision-cutting-edge-emi-shielding-in-portable-medical-technology/
58. Radiation and EMI shielding of 3D printed lightweight ... https://www.sciencedirect.com/science/article/pii/S2772810225000157

59. Recent advances in multifunctional electromagnetic ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11103537/

60. Mitigation of Major Electromagnetic Interference problems ... https://www.odenserobotics.dk/mitigation-of-major-electromagnetic-interference-problems-for-drones-and-robotics-systems/

61. Materials and Applications for Electromagnetic Interference ... https://dsiac.dtic.mil/wp-content/uploads/2021/12/SOAR_DSIAC_EMI_Shielding_Motes.pdf

62. EMI Shielding Solutions for Medical Applications https://www.te.com/en/industries/medical-technologies/medical-specialties-and-markets/patient-monitoring-diagnostics-equipment/emi-shielding-solutions-medical-applications.html

63. MRI Patient Safety And Care - StatPearls - NCBI Bookshelf https://www.ncbi.nlm.nih.gov/books/NBK604477/

64. MRI Online Safety | UC Davis Imaging Research Center https://health.ucdavis.edu/irc/content/pdfs/MRI_Safety_Training.pdf

65. Safety Measures During MRI Scans https://www.charlotteradiology.com/blog/safety-measures-during-mri-scans/

66. Wireless Monitoring in MRI: Advancing Patient Safety and ... https://www.mipm-usa.com/articles/blog-post-title-one-w7reh-mpefe-gbdbz-s93sm-tbw6r-mhwls-jr8zb-5kdhk-2mszn-brwhp-d82k9-wnysw-lz4hr-j28e2

67. Guidelines on Exposure to Electromagnetic Fields from ... https://www.canada.ca/en/health-canada/services/publications/health-risks-safety/safety-code-26-guidelines-electromagnetic-fields-magnetic-resonance-clinical-systems-exposure.html

68. MRI safety | Radiology Reference Article https://radiopaedia.org/articles/mri-safety?lang=us

69. Safety in MRI Guidelines: Essential Protocols & Patient ... https://collectiveminds.health/articles/safety-in-mri-guidelines-essential-protocols-patient-protection-guide

70. Biological Effects and Safety in Magnetic Resonance Imaging https://www.mdpi.com/1660-4601/6/6/1778

71. MRI safety practices: Ensuring patient and staff well https://jptcp.com/index.php/jptcp/article/download/5855/5671/13531

72. OTA Architecture For Scalable Designs https://www.embien.com/blog/ota-architecture-for-scalable-designs

73. Software Over the Air Update for Modern ... https://designthesolution.org/wp-content/uploads/2022/09/Secure-Software-Update-in-Automotive-Modern-Software-Architecture-Student-Paper.pdf

74. Ensuring Robust Firmware Delivery in Embedded Systems https://promwad.com/news/ota-updates-embedded-systems

75. Functional Safety Architectural Patterns for AI-Based ... https://dl.acm.org/doi/10.1145/3769121

76. Pattern-Based Approach for Designing Fail- operational ... https://publica.fraunhofer.de/bitstreams/7133cba4-21f1-4b1f-8fc5-bdce55dc213c/download

77. A more secure and reliable OTA update architecture for IoT ... https://www.ti.com/lit/pdf/sway021

78. An adaptable security-by-design approach for ensuring a ... https://www.sciencedirect.com/science/article/pii/S0167404824005741

79. Over-the-air (OTA) update best practices for industrial IoT ... https://mender.io/resources/reports-and-guides/ota-updates-best-practices

80. Design patterns for safety-critical embedded systems https://www.researchgate.net/publication/44812303_Design_patterns_for_safety-critical_embedded_systems

81. Firmware Update Strategies in Mission-Critical Devices https://promwad.com/news/firmware-update-strategies-mission-critical

82. How to Test OTA Updates Without Bricking Devices https://memfault.com/blog/ota-testing-101-the-ultimate-guide/

83. Cybersecurity of Firmware Updates https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

84. Over the air updates (OTA): best practices for device safety https://www.iotinsider.com/industries/security/over-the-air-updates-ota-best-practices-for-device-safety/

85. Cybersecurity Risks of Automotive OTA Updates https://www.apriorit.com/dev-blog/cybersecurity-risks-of-ota-automotive

86. Understanding Risks in Over the Air Firmware Upgrade for ... https://www.einfochips.com/blog/understanding-risks-in-over-the-air-firmware-upgrade-for-automotives-including-evs/

87. Optimizing Embedded Performance | Real Time Firmware ... https://www.travancoreanalytics.com/en-us/real-time-firmware-development

88. Firmware Development: for Embedded Systems and Beyond https://curatepartners.com/tech-skills-tools-platforms/understanding-firmware-development-essential-for-embedded-systems-and-beyond/

89. Part 108 Explained: The FAA's New Drone Regulations https://pilotinstitute.com/part-108-explained/

90. Unmanned Aircraft System (UAS) or Drone Operations https://www.faa.gov/hazmat/air_carriers/operations/drones

91. Hazmat Rules for Drones, Space Race in 2025 https://www.lion.com/lion-news/july-2024/two-hazmat-rules-of-the-future-revealed

92. How Drones Are Making Hazardous Work Environments ... https://about.citiprogram.org/blog/how-drones-are-making-hazardous-work-environments-safer/

93. Part 108 Regulations Proposal: What Does It Mean? https://www.dartdrones.com/blog/part-108-regulations-proposal-what-does-it-mean/

94. Firmware Development and Update Strategies for ... https://medium.com/@RocketMeUpIO/firmware-development-and-update-strategies-for-embedded-systems-677e247b8c07
95. Key Firmware Development Concepts for Embedded ... https://somcosoftware.com/en/blog/key-firmware-development-concepts-for-embedded-systems
96. Optimizing Embedded Performance | Real Time Firmware ... https://www.travancoreanalytics.com/en-us/real-time-firmware-development/
97. Designing Robust Bootloaders: Ensuring Reliable ... https://runtimerec.com/designing-robust-bootloaders-ensuring-reliable-firmware-updates/
98. What is bootloader development for embedded systems? https://www.inspiro.nl/en/what-is-bootloader-development-for-embedded-systems/
99. Preventing Integration Failures with Early Firmware Design https://punchthrough.com/firmware-integration-strategy/
100. Mastering Firmware Development Services: The Core of ... https://avench.com/iot/mastering-firmware-development-services-core-smarter-devices/
101. A Programmable SDN+NFV-based Architecture for UAV ... https://ntrs.nasa.gov/api/citations/20170000332/downloads/20170000332.pdf
102. Your Guide to Sensor and Drone Simulation Testing ... https://www.opal-rt.com/blog/your-guide-to-sensor-and-drone-simulation-testing-for-defense-readiness/
103. DOI Use of Uncrewed Aircraft Systems (UAS) https://www.doi.gov/sites/default/files/documents/2025-01/opm-11_0.pdf
104. Notice of proposed rulemaking (NPRM) https://www.faa.gov/newsroom/BVLOS_NPRM_website_version.pdf
105. Chain of Trust, DFU Protocols, and Fail-Safe Recovery https://promwad.com/news/secure-firmware-update-pipelines
106. ZAPS: A Zero-Knowledge Proof Protocol for Secure UAV ... https://arxiv.org/html/2508.17043v1
107. Blockchain-Based Framework for Secure OTA Updates in ... https://www.researchgate.net/publication/388249051_Blockchain-Based_Framework_for_Secure_OTA_Updates_in_Autonomous_Vehicles
108. SystemRequirements - Free Surfer Wiki https://surfer.nmr.mgh.harvard.edu/fswiki/SystemRequirements
109. Mac or Windows for fMRI https://neurostars.org/t/mac-or-windows-for-fmri/33766
110. Medis® Suite MR Hardware Requirements https://medisimaging.com/wp-content/uploads/2021/09/Hardware-Requirements-MR.pdf
111. An Open-Source Hardware and Software System for ... https://pmc.ncbi.nlm.nih.gov/articles/PMC2855223/

112. What are the OS and computer requirements for ... https://www.biopac.com/knowledge-base/compatibility-os-computer-requirements/

113. fMRI and MEG Eye Tracker Systems https://www.sr-research.com/fmri-meg-systems/

114. TRACKPixx3 MRI/MEG https://vpixx.com/products/trackpixx3-mri-meg/

115. An eye tracking based virtual reality system for use inside ... https://www.nature.com/articles/s41598-021-95634-y

116. Lumina (Cedrus) https://www.neurospec.com/products/lumina

117. Magnetic Resonance Imaging (MRI) https://brainimaging.center.uconn.edu/mri/

118. MRI compatible eye tracking system https://www.mrc-systems.de/en/products/mrc-eye-tracking

119. iView X MRI-LR - Eye Tracking for fMRI: Tool/Resource Info https://www.nitrc.org/projects/iviewx_mri-lr

120. Eye Tracking https://www.biopac.com/product-category/research/eye-tracking/

121. Secure Software Updates on Automotive Embedded Systems https://medium.com/@mkklyci/secure-software-updates-on-automotive-embedded-systems-secure-boot-secure-update-and-ota-68d856c7933f

122. Secure Software Upgrades in Embedded Systems- TPM ... https://fidus.com/blog/mastering-secure-software-upgrades-in-embedded-systems-best-practices-and-tpm-integration/

123. How do you verify software in safety-critical systems? https://www.reddit.com/r/embedded/comments/1lwlul5/how_do_you_verify_software_in_safetycritical/

124. Secure over-the-air software updates in connected vehicles https://www.sciencedirect.com/science/article/abs/pii/S1389128619314963

125. Secure Firmware OTA Update with AWS: SSL/TLS ... https://study.embeddedexpert.io/p/embedded-fota1

126. Secure Boot and Firmware Protection in Embedded Systems https://somcosoftware.com/en/blog/secure-boot-and-firmware-protection-in-embedded-systems

127. Towards a Unified Framework for Software-Hardware ... https://www.mdpi.com/2218-6581/13/11/157

128. MRI Safety https://www.radiologyinfo.org/en/info/safety-mr

129. MRI Safety: What Every Technologist Needs to Know https://www.inkspaceimaging.com/post/mri-safety-2025-what-every-technologist-needs-to-know

130. A Review of Magnetic Resonance (MR) Safety - PubMed Central https://pmc.ncbi.nlm.nih.gov/articles/PMC10657250/

131. MRI Safety Guidelines: Screening & Implants https://radiology.ucsf.edu/patient-care/patient-safety/mri

132. MRI Safety | Magnetic Resonance Research Facility https://mri.medicine.uiowa.edu/mri-safety

133. MRI Safety https://www.ohsu.edu/school-of-medicine/diagnostic-radiology/mri-safety

134. MRI Safety https://health.ucdavis.edu/radiology/mymri/mymri-safety.html

135. MRI Safety Tutorial | The Brain Imaging and Analysis Center https://www.biac.duke.edu/research/safety/mri-safety-tutorial

136. Radiologic Technologist Best Practices for MR Safety https://www.asrt.org/docs/default-source/research/whitepapers/asrt18_mrsafetywhitepaper.pdf?sfvrsn=ca0222d0_12

137. CCBBI MRI Safety Policies https://ccbbi.osu.edu/researchers/ccbbi-mri-operating-and-safety-manual/ccbbi-mri-safety-policies

138. EyeLink Eye Tracker Learning Resources https://www.sr-research.com/support-options/learning-resources/

139. Experiment Builder for Eye-Tracking Experiments https://www.sr-research.com/experiment-builder/

140. SR Support Forum - Downloads https://www.sr-research.com/support/forum-3.html

141. EyeLink 1000 User Manual https://natmeg.se/onewebmedia/EL1000_UserManual_1.52.pdf

142. The EyeLink® 1000 Plus Eye Tracker https://www.sr-research.com/wp-content/uploads/2018/01/EyeLink-1000-Plus-Brochure.pdf

143. Host Operating System Compatibility https://www.crsltd.com/how-to-contact-us/technical-support/host-operating-system-compatibility/

144. EyeLink® 1000 Plus Installation Guide Tower, Desktop, LCD ... http://bjbrainvision.com/uploads/20201202/478040eae9d99178ebf58ffeccbc8625.pdf

145. EyeLink Software for Linux - SR Support Forum https://www.sr-research.com/support/docs.php?topic=linuxsoftware

146. Enhancing Unmanned Aerial Vehicle Security: A Zero- ... https://www.mdpi.com/1424-8220/24/17/5838

147. Future-Proofing Security for UAVs With Post-Quantum ... https://repository.essex.ac.uk/39966/1/Future-Proofing_Security_for_UAVs_With_Post-Quantum_Cryptography_A_Review.pdf

148. blockchain-based lightweight authentication and key ... https://www.researchgate.net/publication/380606095_BLOCKCHAIN-BASED_LIGHTWEIGHT_AUTHENTICATION_AND_KEY_EXCHANGE_PROTOCOL_FOR_UNMANNED_AERIAL_VEHICLE

149. (PDF) Blockchain-Assisted Secure and Lightweight ... https://www.researchgate.net/publication/387134591_Blockchain-Assisted_Secure_and_Lightweight_Authentication_Scheme_for_Multi-Server_Internet_of_Drones_Environments

150. (PDF) An ECC-Based Anonymous and Fast Handover ... https://www.researchgate.net/publication/392051793_An_ECC-Based_Anonymous_and_Fast_Handover_Authentication_Protocol_for_Internet_of_Vehicles

151. BIRC MRI Guide | Center for Open Research ... - UConn https://researchresources.center.uconn.edu/birc-mri-guide/

152. Getting Started - Brain Imaging Research Core https://brainimaging.center.uconn.edu/getting-started/

153. Brain Imaging Research Center (BIRC) - UConn Core Facilities https://core.uconn.edu/resource/birc/