AZ MANDIBLE

Complete Design Specification

Field / OPSEC / Military-Tier Variants

Paintball-Framed Public Positioning · Buddy-System Distribution

Internal Design Document

July 2026

Version 1.0 — Full Consolidation

1. Purpose & Scope

This document consolidates the complete design of the AZ Mandible platform as developed through iterative specification. It covers the core silent intent and private voice system, the OPSEC/field variant, higher tactical tiers, mechanical construction, integrity architecture, power, authentication, distribution policy, and support model. Public positioning is recreational (elite paintball / advanced recreational tactical gear). Real capability travels through peer networks.

2. Product Ladder

Four tiers form the product family. Hardware architecture is shared; capability and consequence increase with tier. Tiers III and IV remain US-only.

Tier	Name	Core Focus	Distribution
I	Field / OPSEC	Private voice + silent tongue-click intent	US + International
II	Drone Control	Adds silent drone command layer	US + International
III	Sniper Team	Adjustable settings + kill switch	US-only
IV	Elite Operators	Full hardened stack + maximum integrity	US-only

Early direct pricing guidance: Tier I roughly $1,600–$2,200; Tier II $2,800–$4,500; Tier III $3,500–$5,500+; Tier IV $5,500–$8,000+. Hardware cost remains a minority of price; software and integrity behavior carry the value.

3. Core Capabilities

3.1 Private Voice Path

User speech is captured by microphone, processed, and re-emitted only through bone conduction into the jaw. Result: clear to the wearer, near-silent to the surrounding room. This is the central OPSEC claim of the voice system.

3.2 Silent Intent (Tongue-Click) Layer

A piezoelectric sensor on the mandible detects differentiated tongue clicks. Classification supports a small, expandable vocabulary (e.g. sharp single = select/yes, double = cancel/no, hard = confirm, soft = modifier, triple = special). Adaptive baseline and threshold tracking are used. This layer provides discrete, silent command capability and is the foundation for later speech-like expansion.

3.3 Radio Link

Encrypted radio link with rotating channel control. Target design goal includes multi-mile range under favorable conditions; real on-body performance must be measured. External antenna uses the same visual language as the casing. Titanium core is treated as compatible with reception rather than hostile to it.

3.4 Independent Encryption

Each unit carries its own encryption material. No central key authority. Encryption logic may differ by market/region. Philosophy: reconstruction of a clean, stable, fully compatible software image is deliberately costly (A.R.K.-style rotational integrity applied to the audio/firmware stack).

4. Mechanical Design

4.1 Overall Structure

- Outer shell: multi-layer plastic (cosmetic, sensor-bearing, and structural outer).
- Inner core: titanium — structural backbone and conductive reference electrode.
- Three-layer plastic inner core region; designated inner conductive/ADS layer is a hard integrity surface.

- Electronics submerged in non-conductive (dielectric) cooling-style fluid inside a sealed chamber.
- Mesh of material inside the cooling chamber participates in breach detection.
- Mineral electrode pouches in the shell structure; breach that reaches the critical layer creates a conductive path to the titanium core.
- Bottom-mount clip or hatch for external power, USB-C style connector.
- External antenna matched to casing style.

4.2 Sealed Nature

Once assembled, the unit is not intended to be opened. Opening or penetrating the protected chamber is an integrity event. All normal diagnostics are therefore software/read-only. Physical autopsy is a deliberate later decision, not a routine step.

4.3 Audio Coupling

Tongue-click and voice pickup are improved by design: mechanical rods or coupling from inner core to outer shell, and/or an inner-mouth microphone option. Treated as an engineering problem solvable by iteration, not a fixed physics ceiling.

5. Integrity Architecture

5.1 Philosophy

Prefer device loss over useful compromise. Apply A.R.K. rotational integrity and EmbryoLock-style destructive principles to the live firmware and audio stack. Hardware may be copied; clean, stable, non-degrading software behavior is the expensive part to reproduce.

5.2 Software Responses

On confirmed integrity event the system may:

- Wipe sensitive material
- Rotate internal coding and protective state
- Spoof behavior (appear alive while non-functional)
- Brick critical functions permanently
- Delete software payload (especially on battery-removal / power-loss paths)

5.3 Physical Detection

Breach detection uses continuity involving the cooling chamber mesh, electrode pouches, and titanium core. Normal state: fluid remains dielectric, no path to core. Critical-layer breach: conductive path forms → integrity logic fires. Different failure types can map to different lockdown methods (adaptive response, not a single static rule).

5.4 Presence & Environmental Interlocks

- Heat / presence sensor: live user detected → destructive path blocked or limited.
- Recent-use time window: distinguishes active field use from cold or seized device.
- Low-temperature threshold (design example: below –12 °C): treated as non-living or laboratory context; integrity response permitted.

These interlocks exist so that accidental field damage does not automatically equal total loss, while still allowing strong response when the device is cold, unused, or under examination.

5.5 Cause-of-Failure Record

A single protected save file records the cause of failure. This record is written when a critical event occurs and is intended to survive long enough for later inspection. Inspection reads the cause first; only then is a decision made whether opening the sealed unit is justified. Lithium cells are electrically isolated from the rest of the system to prevent backfeed that could corrupt monitoring or the save path.

5.6 Battery Isolation

Lithium batteries are isolated to prevent backfeed into monitoring and integrity circuits. Power-loss / battery-removal can still serve as a trigger for software destruction under the EmbryoLock-style rule set.

6. Power

Primary extended-use mode: external power via bottom USB-C style hatch or clip. This removes the most severe wearable battery constraint. Internal cell supports short untethered operation and integrity monitoring. Connector design must include strain relief and basic electrical protection; the hatch is a new mechanical and potential attack surface that must be engineered carefully.

7. Authentication & Pairing

Buddy-system model. Pairing uses a spoken code (example form: “tango foxtrot”) or an equivalent tongue-click sequence. What is audible in the open air is not necessarily what the device authenticates; the device works from the private channel / translated click or voice material. No heavy central public-key infrastructure. Simple, human-scale, network-local.

8. Distribution & Public Positioning

Public marketing and documentation present the product as elite paintball / advanced recreational tactical gear. Ads stay in that lane. Real adoption and field use travel through peer (buddy) networks once capability is observed. Higher-consequence tiers (III and IV) are not sold outside the US. International movement, if any, is limited to Tier I and II under the stated policy.

Strategic note: the design accepts that capable actors may eventually reverse hardware. The counter is software maturity, rotational integrity, and the cost of producing a clean, reliable clone that still behaves correctly under the integrity model.

9. Support & Replacement Policy

- Legitimate field damage accompanied by a valid written statement → possible 50–100% discount on replacement.
- Integrity trigger outside policy, or no valid statement → full price only.
- Qualified users may still access military-discount path when policy is followed.
- Return of the failed unit may be required; returned units feed design hardening.
- Non-compliant users simply pay full price or leave the ecosystem.

10. Software Direction

Base firmware began as simple peak detection (YES/NO), moved to adaptive thresholding, then to tongue-click classification with CSV export for data collection. Higher variants add private voice path, radio, encryption, and the full integrity state machine. A.R.K. principles (rotating protective state, epistemic denial, no recovery material, high reconstruction cost) are applied to the audio/firmware layer. All diagnostics after sealing are software-only; the cause-of-failure save file is the primary forensic output.

11. Recommended Development Order

1. Finish and validate the basic tongue-click + bone-conduction prototype (current hardware path).
2. Measure private audio leakage and on-body radio behavior.
3. Implement and test the exact presence / temperature / recent-use interlock decision tree.
4. Build the sealed chamber + dielectric fluid + mesh + electrode continuity path on a higher-tier prototype.
5. Add external power hatch and confirm mechanical/electrical robustness.
6. Field early Tier I units through buddy networks under the paintball-framed public story.
7. Iterate software lead (A.R.K.-style behavior) so clones remain behind in reliability and integrity behavior.
8. Only then expand Tier II (drone) and, later, US-only Tier III/IV.

12. Open Items (Still Required)

- Measured on-body radio range with the chosen external antenna.
- Measured acoustic leakage of the bone-conduction private voice path.
- Exact numeric thresholds and logic for presence, recent-use window, and low-temperature interlock.
- Final mechanical design of the USB-C hatch (strain relief, sealing, electrical protection).
- Production approach for the sealed fluid chamber and continuity mesh that keeps false triggers acceptable.
- Long-term software maturity plan that actually creates years of lead over clean clones.

13. Standing Design Principles

1. Hardware may be identified or copied; software integrity behavior stays ahead.
2. Prefer loss of the device over useful compromise.
3. Independent encryption per unit; no central recovery authority.
4. Public story remains recreational; capability moves through trusted networks.
5. Field users are protected from accidental total loss by presence and recent-use interlocks.
6. Once sealed, the unit is not opened for routine diagnosis; software reports cause first.
7. Different failure types may produce different lockdown responses (adaptive, not monolithic).
8. Support policy is simple: play by the rules and receive consideration, or pay full price.