

AZ Mandible

Military / Field Variant — Design Specification (Paintball Framing)

1. Market Positioning

Public face: advanced / elite paintball and recreational tactical gear. Marketing, imagery, and public documentation stay inside that lane. Real adoption occurs through peer networks once users observe actual field utility. The product is never publicly sold or advertised as military equipment.

2. Core Capability

- Private voice path: speech is captured, processed, and re-emitted only through bone conduction into the jaw — near-silent to the surrounding room.
- Silent intent layer: differentiated tongue clicks classified for discrete commands (select, cancel, confirm, modifier, etc.).
- Radio link with rotating channel control for short-to-medium range private coordination.
- Independent per-unit encryption; no central key authority.
- Integrity system: detect compromise or improper opening and respond with wipe / rotate / spoof / brick logic.

3. Mechanical Design

Structure

- Outer shell: multi-layer plastic (cosmetic + sensor-bearing).
- Inner core: titanium (structural + conductive reference).
- Three-layer plastic inner core region; break of the designated inner conductive/ADS layer is treated as a hard integrity event.
- Bottom-mount clip or hatch for external power, USB-C style connector.
- External antenna in the same visual language as the casing (no exotic appearance).

Audio Capture Path

Tongue-click and voice pickup improved by mechanical design (core-to-shell rods or equivalent coupling) and/or an inner-mouth mic option. Treated as a solvable design problem rather than a hard physics limit.

4. Integrity & Anti-Tamper System

Software (A.R.K.-style audio variant)

- Rotating protective state, epistemic denial, progressive degradation under probing.
- On confirmed compromise: wipe, rotate coding, spoof behavior, and/or permanent brick.
- Battery removal / power-loss path can trigger full software destruction (EmbryoLock philosophy).

Physical Detection

- Conductive detection (mesh, simple continuity path, or core-to-shell path) monitors opening or separation.
- Break of the designated inner plastic/conductive layer is a hard trigger.

Presence & Safety Interlocks

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

5. Authentication & Pairing

Buddy-system model. Pairing uses a spoken code (example form: “tango foxtrot”) or equivalent tongue-click sequence. No heavy central public-key infrastructure. Device authenticates the voice / click pattern locally. Open-air room recording does not capture the private bone-conduction channel.

6. Power

Primary operational mode supports external power via bottom USB-C style hatch/clip. This removes the most severe battery constraints for extended use. Internal cell remains for short untethered periods and for integrity monitoring.

7. Distribution & Support Policy

- Public sales channel presents the product as elite paintball / recreational gear.
- Real field adoption travels through peer / buddy networks.
- Higher-consequence configurations remain restricted (US-only for tiers above II).
- Field damage + valid written statement → possible 50–100% replacement discount.
- Integrity trigger outside policy or no valid statement → full-price replacement only; unit return may be required.
- Returned units feed design hardening.

8. Tier Context (Reference)

Tier	Focus	Notes
I – Field / OPSEC	Private voice + silent intent	Core unit, international OK under policy
II – Drone	Adds silent command layer	International OK under policy
III – Sniper Team	Adjustable + kill switch	US-only
IV – Elite	Full hardened stack	US-only

9. Standing Design Principles

- Hardware may be identified or copied; software maturity and integrity behavior stay ahead.
- Independent encryption per unit; reconstruction of clean, stable behavior is deliberately costly.
- Prefer device loss over useful compromise.
- Public story stays recreational; capability travels through trusted networks.
- Field users are protected from accidental total loss by presence and recent-use interlocks.