PROVISIONAL PATENT APPLICATION HARDWARE SYSTEM

The Smart Post / OMNI-SHIELD Hardware

- **Invention Title:** VOICE-ACTIVATED BIOMETRICALLY SECURED INFRASTRUCTURE FOR INFINITELY ADJUSTABLE UTILITY SEAT POST ASSEMBLIES AND INTEGRATED VEHICLE FRAME FUSION MECHANISMS

- **First Named Inventor:** * Given Name(s): John Lawrence
    - Family Name: Coulson
    - City of Residence: Whistler
    - State/Province: British Columbia
    - Country: Canada

- **Correspondence Address:**
    - Name: John L. Coulson
    - Address: Suite 201 – 1330 Cloudburst Drive
    - City: Whistler
    - State/Province: BC
    - Country: Canada V8N 1E7
    - Email: jlc@sidogger.com

- **U.S. Government Agency Interest:** NO.
- **Entity Status:** "Micro Entity"

1. **INVENTOR & ASSIGNEE DATA**

- **Inventor:** John Lawrence Coulson
- **Assignee/Entity:**

Flowchart 1: The Biometric Actuation Loop

This chart maps how the voice command actually moves the hardware.

- **BOX 1: User inputs localized vocal command (e.g., "Drop 50mm") via paired smart device microphone or headset.**
- **BOX 2: Smart device application receives the acoustic signal and routes it to the localized neural net template.**
- **BOX 3: Application performs Biometric Cadence Matching, comparing the live audio against the stored authorized user profile.**
- **BOX 4 (Decision Node): Is the biometric match confirmed?**
- *If NO:* Reject command, log failed attempt, END.
- *If YES:* Proceed to BOX 5.
- **BOX 5: Application generates and transmits an encrypted actuation token via BLE/NFC to the Seat Post Micro-Controller Unit (MCU).**
- **BOX 6: Seat Post MCU decrypts the token and actuates the internal electro-hydrostatic servo valve to achieve the requested height or dampening profile.**

- BOX 7: Seat Post MCU transmits a "Successful Actuation" confirmation signal back to the user's smart device interface.

Flowchart 2: The Proximity Tether & Lock-Down Sequence

This chart maps the exact trigger for the anti-theft frame fusion.

- BOX 1: Seat Post MCU establishes a continuous, encrypted proximity handshake (BLE/NFC) with the authorized smart device.
- BOX 2: Seat Post MCU continuously monitors the Received Signal Strength Indicator (RSSI) of the handshake loop.
- BOX 3 (Decision Node): Has the RSSI dropped below the predetermined minimum safety threshold (indicating the user has walked away)?
- *If NO:* Maintain standard unlocked operation. Return to BOX 2.
- *If YES:* Proceed to BOX 4.
- BOX 4: Seat Post MCU initiates Anti-Theft Protocol and triggers the high-torque micro-linear solenoids.
- BOX 5: Hardened steel locking pins (or expansion collet) radially eject into the inner sidewalls of the vehicle frame tube, structurally fusing the post to the vehicle.
- BOX 6: Seat Post MCU activates the onboard multi-axis accelerometer to monitor for physical tampering.
- BOX 7: If tampering is detected, the backup cellular module transmits an emergency alert and live GPS tracking coordinates to the user's application.

Flowchart 3: Offline Emergency Failsafe Protocol *This chart proves the hardware cannot permanently trap the user if the external digital network fails.*

- **BOX 1:** Primary smart device proximity tether (BLE) is severed due to catastrophic device failure or battery depletion.
- **BOX 2:** Seat Post MCU defaults to high-security locked state (Radial expansion pins remain deployed).
- **BOX 3:** User initiates manual override by physically engaging the concealed secondary Failsafe Node (touching the capacitive fingerprint scanner or emergency NFC fob).
- **BOX 4:** Failsafe Node processes the localized biometric/NFC input against the onboard, encrypted offline memory core.
- **BOX 5 (Decision Node):** Is the localized physical authentication confirmed?
  - *If NO:* Reject input, maintain structural fusion (locked state).
  - *If YES:* Proceed to BOX 6.
- **BOX 6:** Seat Post MCU transmits localized command to micro-linear solenoids to instantly retract radial locking pins.
- **BOX 7:** Structural fusion is released; manual mechanical control is restored to the authorized user without requiring the mobile application.

Flowchart 4: Kinematic Energy Harvesting & Bi-Directional Power Routing *This chart maps the logic of how the post generates power and decides where to distribute it.*

- **BOX 1:** Kinetic physical motion during transit drives the internal piston through the magnetic stator coil, actively generating electrical current.
- **BOX 2:** Onboard rectifier conditions the current and routes it to the Power Management MCU.
- **BOX 3 (Decision Node):** Is the primary internal lithium-capacitor matrix below the required operational threshold (e.g., less than 95% charged)?
  - *If YES:* MCU routes harvested energy directly to the internal battery matrix to ensure safety systems (solenoids/biometrics) remain powered. Return to BOX 1.
  - *If NO (Internal matrix is fully saturated):* Proceed to BOX 4.
- **BOX 4 (Decision Node):** Is an external peripheral device (e.g., smartphone, GPS unit) tethered to the active auxiliary external charging port?
  - *If NO:* MCU shunts/dissipates excess energy or disengages magnetic induction resistance (freewheel mode). Return to BOX 1.
  - *If YES:* Proceed to BOX 5.
- **BOX 5:** Power Management MCU dynamically diverts the excess continuous harvested energy to the external charging port.
- **BOX 6:** Tethered peripheral device receives active, continuous charging from the seat post infrastructure while the vehicle is in motion.

2. SPECIFICATION: ARCHITECTURAL OVERVIEW & ENABLEMENT

The present invention relates to an electromechanically controlled, biometrically tethered, infinitely adjustable seat post assembly configured for integration with vehicles (e.g., bicycles, electric velocipedes, mobility scooters) and dynamic structural seating. Unlike conventional mechanical or basic wireless electronic dropper posts that rely entirely on localized manual actuation buttons, the present architecture utilizes a contactless, voice-activated biometric and or security code input and control mesh tethered to an external localized computing platform or smartphone mobile application.

Subsystem A: The Biometric Voice-Actuation & Dynamic Dampening Node

The assembly comprises an inner telescoping shaft and an outer structural sleeve configured to fit within a vehicle frame tube or seating receiver. The core fluid/mechanical actuation chamber within the inner shaft contains an electro-hydrostatic or electronic linear servo valve assembly linked to a specialized embedded micro-controller unit (MCU) outfitted with a low-power Bluetooth Low Energy (BLE), Near-Field Communication (NFC), or soft-SIM cellular module.

- **Vocal Cadence Profiling:** Actuation commands (e.g., "Saddle Drop 50mm," "Maximum Rise") are received via a localized microphone matrix on a paired smart device or handlebar headset. The pairing app processes the acoustic signal using a localized neural net template to confirm both string command matching and owner voice biometric validation before transmitting an encrypted command token to the post MCU.
- **On-the-Fly User Adjustable Dampening System:** The inner hydrostatic or pneumatic column features a user-adjustable electronic dampening valve assembly (such as a magnetorheological fluid bypass or adjustable electronic orifice servo). Managed via the user smart application interface, the user can command the internal fluid dynamics to instantly shift profiles:

1. *Soft Dampening:* Lowers the orifice fluid restriction to provide active bump and micro-vibration shock absorption during casual, bumpy, or endurance riding.

2. *High-Stiffness Lock:* Maximizes fluid bypass restriction to form a high-stiffness structural support profile optimized for aggressive climbs or high-efficiency competitive power transfer.

Subsystem A.1: Kinematic Energy Harvesting, Power Management, & Bi-Directional Auxiliary Output
To ensure continuous operation of the MCU, biometric sensors, and solenoid actuators, the inner telescoping shaft integrates a linear electromagnetic induction generator (or piezoelectric harvesting array) surrounding the hydrostatic dampening chamber. As the seat post absorbs micro-vibrations and structural impacts during transit, the kinetic oscillation of the internal piston passes through a magnetic stator coil, actively generating electrical current. This scavenged kinematic energy is routed through an onboard rectifier to continuously trickle-charge the primary internal lithium-capacitor matrix, rendering the seat post largely self-sustaining under standard transit conditions.

Furthermore, the onboard power management system is configured with bi-directional power routing logic. The externally exposed, weather-sealed static charging port (which may utilize a magnetic induction pad, USB-C, or proprietary tether) also functions as an active auxiliary power output hub. As continuous kinetic motion generates electrical current that saturates the internal battery matrix, the MCU dynamically diverts excess harvested energy to this external port. This allows the user to tether and actively charge peripheral electronic devices (e.g., smartphones, GPS head units, portable illumination systems, or wearable biometric sensors) directly from the seat post while in transit, effectively transforming the structural seating infrastructure into an active, self-generating mobile power bank.

Subsystem B: The Proximity-Triggered Frame-Fusion Anti-Theft Lockout

To permanently neutralize component and systemic vehicle theft, the seat post introduces an automated mechanical lockout mechanism that structurally unifies the internal hardware component directly with the hollow inner walls of the surrounding vehicle frame.

```
[Vehicle Frame Inner Sidewall]
      ▲
      │  (Radial Force Ejection)
┌─────┴───────────────────────────────────┐
│ [Hardened Steel Locking Pin / Toothed Collet]│
├─────────────────────────────────────────┤
│      [High-Torque Micro-Linear Solenoid]      │
├─────────────────────────────────────────┤
│         [Embedded Security MCU Node]         │
└─────────────────────────────────────────┘
```

- **Tether Disconnect Logic:** The embedded security MCU continuously pings the user's authenticated device via a secure proximity handshake loop. The moment this RSSI signal drops below a designated threshold (indicating the verified user has walked out of immediate proximity), the MCU activates the anti-theft protocol.

- **Active Ejection Mechanics:** Upon loss of user proximity, an internal high-torque micro-linear solenoid or stepper-driven mechanical cam fires radially outward from the internal base of the seat post housing. Hardened steel locking pins, micro-spikes, or a segmented toothed expansion collet forcibly eject through specific apertures in the lower post wall, making aggressive mechanical contact with the inner structural sidewalls of the vehicle frame's hollow seat tube channel, which also renders the seat post in-effective while locked down. Aka - ZERO adjustability features.

- **Impenetrable Structural Fusion:** This radial force firmly locks the post into the frame tube via a high-friction, teeth-biting interface. Any attempt to forcibly slide, rotate, twist, or extract the post without a valid proximity handshake causes the components to wedge tighter, structurally welding the seating infrastructure to the frame channel. This rendering the seat post immovably permanent and forces a complete mechanical immobilization of the drivetrain loop.

Subsystem B.1: The "Zero-Power" Offline Failsafe & Emergency Authentication:

In the event of catastrophic primary device failure (e.g., the user's paired smart device loses power), the post architecture features a concealed, localized failsafe authentication node located beneath the saddle mounting bracket. This node comprises an ultra-low-power capacitive fingerprint biometric scanner and an emergency near-field NFC physical contact pad. The authorized user can physically touch the concealed sensor or tap an authorized physical NFC fob (such as an emergency keycard or wearable ring) to manually decrypt the local MCU, instantly retracting the radial locking pins and restoring standard mechanical operation without relying on the external smart device tether.

Subsystem C: Integrated Telematics, Tamper Detection & FanAdClic Gateway

- **Tamper-Activated GPS Tracking:** The housing features an integrated multi-axis accelerometer and gyro sensor array linked directly to a fallback GPS chip and dedicated capacitor battery storage. If localized motion, vibration, or impact is detected while the proximity lock is active, a loud audible onboard acoustic alarm is triggered, an automated emergency alert is sent instantly to the registered user's phone, and the system initiates live real-time GPS tracking to locate the compromised vehicle.

- **The APE-X (APE-X.ai) Data Opt-In Bridge:** The accompanying mobile app embeds a specialized commercial tokenization gateway linked to the APE-X digital ecosystem, structurally utilizing the biometric and behavioral verification frameworks detailed in USPTO Patent #12,333,564 (Issued June 17, 2025.) Users who voluntarily opt-in to share telemetry profiles authorize the automated, secure routing of operational data (e.g., travel length, location tracking vectors, usage density metrics) directly to verified manufacturing networks and regional outdoor cycling advertisers. In exchange for verified human data profiles, the APE-X.ai node pushes hyper-localized promotional credits, interactive consumer coupons, secure digital tokens, and navigation direction links natively synced with maps directly to the user interface during transit sessions.