SUPPLYSHIELD AI

San Marcos, Texas | CAGE: [PENDING] | NAICS: 334413 (Semiconductor)

PRODUCT: IM-1 SOVEREIGN NODE

Hardware-Layer Interdiction Governor for Agentic Systems

Status: PRELIMINARY DESIGN

Rev: 2.4

Date: FEB 2026

---

1. GENERAL DESCRIPTION

The **IM-1 "Sovereign Node"** is a discrete hardware interposer designed to secure Cyber-Physical Systems (CPS) against "Agentic Sabotage" and "Hallucination-Induced Kinetic Failure."

Unlike software firewalls, the IM-1 operates on a **Non-Von Neumann Spintronic Architecture**, physically isolating the actuator (motor, solenoid, or pump) from the Host NPU. It utilizes **Impedance Spectroscopy (EIS)** to verify sensor integrity and enforces a deterministic "Physics Envelope" that cannot be overridden by software logic, Prompt Injection, or Model Context Protocol (MCP) exploits.

2. KEY CAPABILITIES

- **Zero-Trust Physics:** Operates independently of the Host OS/Kernel. If the AI "crashes," the Governor defaults to a Safe State (Open Circuit).
- **Spintronic Interdiction:** Utilizes Magnetic Tunnel Junction (MTJ) logic for radiation-hardened, non-volatile state enforcement.
- **Anti-Hallucination (EIS):** Injects 1kHz–100kHz tones to verify sensor impedance, detecting spoofing or degradation before digitization.
- **Windowed Watchdog (WWDT):** Enforces a cryptographic 850ms "Goldilocks" timing window to prevent Replay Attacks and Agentic Lag.

3. APPLICATIONS

- **Defense & UAS:** Group 1-3 Interceptors (Anti-Kamikaze Logic).
- **Critical Infrastructure: Project Vault** / Strategic Resilience Reserves (Class 5 Vault Door Interdiction).

- **MedTech:** Class III Infusion Pumps (Compliance with FDA Sec 524B & "Hardware Warning" Standards).
- **Space Systems: Starshield** / Orbital Edge (Galvanic Isolation for Third-Party Hosted Payloads).

---

4. TECHNICAL SPECIFICATIONS (Target)

PARAMETER	SPECIFICATION	UNIT
Input Voltage	3.3 to 5.5 (Direct LiPo Compatible)	VDC
Power Consumption	12 (Passive Monitoring)	mW
Interdiction Latency	< 10 (Hardware Cutoff)	ms
Watchdog Window	15 (Min) – 850 (Max)	ms
Logic Architecture	Spintronic MTJ (Non-Volatile)	--
Operating Temp	-40 to +125 (Mil-Spec)	°C
Radiation Hardness	> 100 (Starshield Compatible)	krad
Interface	I2C, SPI, Analog Sense (0-5V)	--

---

5. INTELLECTUAL PROPERTY & COMPLIANCE

Protected by United States Patent Law:

- **US Patent App. 63/975,274:** *System and Method for Deterministic Hardware Governance & Spintronic Interdiction.*

- **US Patent App. 63/967,221:** *Autonomous Interdiction & Hybrid Compliance Verification in Disconnected Environments.*
- **US Patent App. 63/957,597:** *Autonomous Real-Time Regulatory Synchronization.*

Regulatory Alignment:

- **EU AI Act (Art. 14):** Provides the mandatory "Human Oversight" physical interface.
- **FDA Sec 524B:** Satisfies "Post-Market Cybersecurity" physical fail-safes.
- **NDAA FY2026:** Compliant with Sec 889 "Covered Telecommunications" exclusion (Domestic Fabrication).

---

6. FUNCTIONAL BLOCK DIAGRAM

1. **Input Stage:** Signal received from Host NPU (PWM/UART).
2. **Verification Stage:**
    - **Path A:** Impedance Check (Sensor Reality).
    - **Path B:** Logic Check (Safety Envelope / 850ms Timer).
3. **Decision Stage:** Spintronic Logic Gate (AND Operation).
4. **Output Stage:** MOSFET Gate Driver.
    - If **PASS**: Signal flows to Actuator.
    - If **FAIL**: Physical Open Circuit (Ground).

---

7. CONTACT & ORDERING

SupplyShield AI

Sovereign Hardware for the Agentic Era

- **HQ:** San Marcos, Texas, USA
- **Web:** www.supplyshieldai.com
- **Email:** aadarsh@supplyshieldai.com
- **Cage Code:** [Pending Registration]

CONFIDENTIAL // PROPRIETARY INFORMATION OF SUPPLYSHIELD AI