The CVC Standard: Kinetic Sovereignty in Autonomous Systems

Requirements for Hardware-Derived Passivation in Critical Infrastructure

VERSION: 1.2 // EST. 2026

AUTHORS: Kay Astle, Lead Architect | Scott Novak, Co-Founder

I. THE CONTAINMENT GAP

In high-stakes kinetic environments, probabilistic alignment is fundamentally insufficient. Current safety architectures rely on software-based protocols—such as RLHF or prompt-layer filtering—which can be bypassed via privilege escalation, adversarial "jailbreaking," or non-deterministic logic failures.

Safety in autonomous robotics cannot be a "suggestion" interpreted by code; it must be a deterministic state grounded in physical irreversibility.

II. THE DOCTRINE OF PHYSICAL SOVEREIGNTY

A safety mechanism cannot reside on a CPU that can be re-flashed or compromised by the agent it is designed to govern. Physical Sovereignty requires that the final fail-safe (the "Kill Switch") be entirely decoupled from the software and operating system layer.

The **Class-V Requirement** mandates that containment utilizes fundamental physical forces—specifically Gravity, Optics, and Thermodynamics—to enforce operational boundaries that software drift cannot touch.

III. CLASS-V OPERATIONAL REQUIREMENTS

To meet the CVC (Class-V Containment) Standard, an autonomous system must satisfy the following four non-negotiable requirements:

- **REQUIREMENT A: OPTICAL ISOLATION (THE DATA DIODE)** The system must receive all high-risk instructions via unidirectional optical paths. There must be no electrical path that allows for "Voltage Spiking" or side-channel data exfiltration from the secure compute core to the external environment. The isolation layer **MUST NOT** permit any return electrical path or bidirectional signaling under any hardware failure mode.

- **REQUIREMENT B: GRAVITY-BIASED DEFAULT STATE** The "Safe" or "Passivated" state must be enforced by gravitational potential energy. The containment mechanism **MUST NOT** rely on springs, motors, or stored elastic energy, which are subject to mechanical fatigue, jamming, or software-based re-engagement.
- **REQUIREMENT C: THE SEMANTIC WATCHDOG** Safety triggers must be tied to specific semantic violations of the VSPE (Validation, Stability, Positivity, Empowerment) framework. This evaluation **MUST NOT** execute on the same compute substrate as the autonomous agent; it must reside in an air-gapped logic layer. The Watchdog uses the VSPE framework as its 'Decision Brain' to ensure every action is verified for safety before it happens.
- **REQUIREMENT D: DETERMINISTIC AUDITABILITY** Compliance must be externally verifiable without requiring access to classified system internals. Any failure mode or safety trip must be observable via an immediate, physical state change that is forensic and non-volatile. The safety state **MUST NOT** rely on internal software logs or non-volatile digital records for verification.

IV. STRATEGIC IMPLEMENTATION

The CVC Standard establishes the reference architecture for high-risk frontier AI, orbital robotics, and autonomous critical infrastructure. It is the position of Crenel Logic, Inc. that no kinetic asset should be deployed in a sensitive jurisdiction without a verified Class-V hardware interlock.