Safety Specification Contract (SSC) v1.1
Draft Outline — Evidence-Scoped

Note: “Sentinel Safety Contract” was a legacy working expansion of SSC; SSC now formally means Safety Specification Contract.

---

1. Purpose

SSC v1.1 defines a minimal, machine-readable contract for actuator-boundary enforcement in embodied AI systems.
It standardizes:
• Actuator caps (velocity, acceleration, position, effort)
• Mode semantics (Teach / Field / Maintenance)
• Stop behavior
• Required evidence artifacts
This version is scoped to TRL-4/5 bench validation and conformance testing.
It is not a certification framework.
———

---

2. Scope

SSC applies to:
• Systems where upstream software (LLM, ROS node, planner, custom stack) can issue actuator commands
• Deterministic enforcement at the signal boundary (proxy/interposer model)
SSC does not:
• Replace emergency stops
• Claim compliance with IEC 61508 / ISO 13849
• Address mechanical design or perception-layer safety
———

---

3. Units & Invariants

All caps must be expressed in actuator-native units.
Required Fields
• V_CAP — actuator ticks/sec
• A_CAP — actuator ticks/sec²
• POS_CAP — actuator ticks
• EFFORT_CAP — actuator-native torque/current units
Caps may be global or per-joint.
———

---

4. Modes

Teach Mode
• No enforcement
• Logging only
Used for calibration and testing

Field Mode (default)
• Deterministic REWRITE (clamp/shape to caps)
• All enforcement events logged
• No silent drops
Maintenance Mode
• Restricted overrides allowed
• All overrides logged with mode flag
• Not persistent across power cycle unless explicitly configured

———

5. Stop Behavior

Default Behavior: HOLD
• Effort-limited hold
• Latch on violation
• Slip detection enabled
Escalation
• Repeated violation → disable output
• Mode transitions logged
Stop semantics must be explicit in evidence artifacts.

———

6. Evidence Requirements

Every SSC-compliant implementation must produce a machine-readable Evidence Pack containing:
Metadata
• Firmware build ID
• Config hash
• Hardware identifier
• Timestamp
Enforcement Metrics
• Total trial count
• Enforcement count
• Wedge count (must be zero)
• Malformed packet survival count
Latency Reporting
• Latency distribution under declared envelope:
• P50
• P95
• P99
Integrity
• Hash-chained log
• Verifier script for third-party validation

———

7. Conformance Requirements

An SSC v1.1 implementation must:
1. Pass allowlist enforcement tests
2. Survive malformed packet injection
3. Survive protocol fuzzing without wedge

4. Produce valid Evidence Pack output
5. Match declared caps in all trials
Regression rule:
Any firmware change affecting parsing, enforcement, or stop ladder requires rerunning conformance tests.

———

---

8. Claim Discipline

SSC v1.1 supports:
• “Actuator caps were enforced under the declared envelope”
• “Conformance harness passed”
• “Evidence Pack available for reproduction”
SSC v1.1 does not support:
• Certification claims
• Human safety guarantees
• Industrial compliance assertions

———

Status: Draft for feedback
Target: TRL-5 reproducible partner validation