NOVAK PROTOCOL SERIES

Standard Protocol-3 (SP-3): Safety Layer Standard

Safety Gate + PL-X + PS-X Specifications

Version 1.0 (Dec 2025)

The Safety Backbone

SP-3 defines the full deterministic safety system for NOVAK. It handles the harsh realities of the physical world and the deceptive nature of human intent.

- **PL-X:** Handles physics (voltage, heat, jitter).
- **PS-X:** Handles humans (fraud, bias, malice).
- **Safety Gate:** The master enforcer.

The Safety Gate Model

The deterministic gatekeeper running immediately prior to execution.

Determinism

No branching paths.

Consistency

Matches HVET.

Isolation

No side channels.

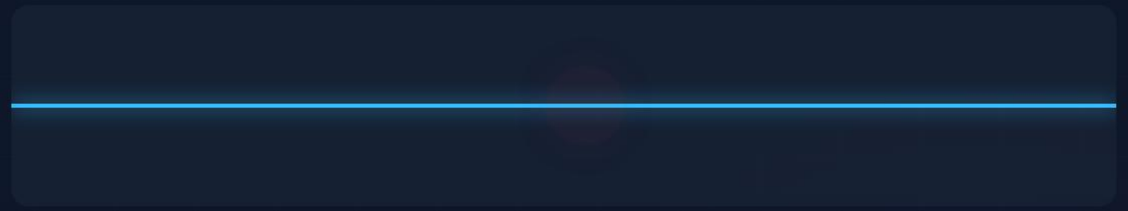
Non-Override

Even Admins cannot bypass.

PL-X: Physical Integrity

Ensures physical reality matches digital expectation. Detects anomalies caused by physics/hardware before they corrupt the chain.

- **Voltage:** Spikes & Instability.
- **Timing:** Jitter & Clock Skew.
- **Thermal:** Sudden Runaway.
- **Memory:** Bit flips & ECC errors.



```
// PL-X Check Logic
IF env.clock_drift > threshold:
  BLOCK("Timing Anomaly")
IF env.ecc_errors > 0:
  BLOCK("Memory Corruption")
```

PS-X: Human Integrity

Models human deception, fraud, and bias. Designed for government and financial systems where the "adversary" might be the user or administrator.

- **Malicious Actor:** Alters data/rules.
- **Fraud:** Benefit manipulation.
- **Rogue Regulator:** Bypassing policy.
- **Coercion:** Emotional manipulation.

Scans for keywords: "Override", "Force", "Bypass"

Defined Adversaries

SP-3 explicitly models protections against five distinct classes:

Physical

Hardware

Human

Users

Regulatory

Policy

Robotic

Motion

AI

Model Bias

Enforcement: The Iron Law

Absolute Block

If ANY anomaly is detected (Physical, Human, or Cryptographic), execution stops immediately.

NOVAK never "warns".
It stops.

Mandates

- No execution without validated HVET.
- No authority can override Safety Gate.
- Fraud patterns trigger auto-block.
- Physical instability triggers auto-block.

Master Safety Algorithm

```
function SafetyGate(input, env, hvet):

// 1. Physical Check
plx = PLX_Check(env)
if plx not empty: BLOCK("PL-X Anomaly")

// 2. Human/Psych Check
psx = PSX_Check(input)
if psx not empty: BLOCK("PS-X Anomaly")

// 3. Crypto Verification
if !VerifyHVET(hvet): BLOCK("Integrity Mismatch")

// 4. Success
ALLOW_EXECUTION()
```

Failure Categories (F1-F10)

F1 Hardware	**F2** Intent	**F3** Determinism	**F4** Identity	**F5** Automation
F6 Time	**F7** Tamper	**F8** Partial Truth	**F9** Ruleset	**F10** Fraud

Regulated environments require **CL-5**.

Level	Description	Scope
CL-1	Basic Safety	Standard gate checks.
CL-2	PL-X Only	Hardware integrity only.
CL-3	PS-X Only	Human integrity only.
CL-4	Combined	PL-X + PS-X enabled.
CL-5	Full Compliance	SP-3 Integration +

Standard Summary

Safety Pillars (Gate, PL-X, PS-X)

Total Protection

SP-3 ensures that even if a CPU lies, a user cheats, or an AI hallucinates, NOVAK will detect the anomaly and block the output before harm can occur.

Status: Effective Dec 2025

Questions?

NOVAK Protocol Standards Series

Category: PBAS-03 (Safety and Integrity Layers)