



SP-1 — NOVAK Execution Integrity Standard (Full GitHub-Ready Document)

(Save as: */standards/SP-1_Execution_Integrity_Standard.md*)



NOVAK SP-1 — EXECUTION INTEGRITY STANDARD

NOVAK Protocol Standards Series — SP-1

Version 1.0 — January 2025

Status: Open Draft

Author: Matthew Novak

Category: PBAS-01 (Proof-Before-Action Systems)

Table of Contents

1. Introduction
2. Purpose & Scope
3. Terminology
4. Execution Integrity Model
5. Integrity Preconditions
6. Core Requirements
7. Correctness Conditions
8. Execution Integrity Receipt (EIR) Requirements

9. Recursive Global Audit Chain (RGAC) Binding Conditions
 10. Safety Preconditions & Gate Conditions
 11. Compliance Levels (CL-1 → CL-5)
 12. Security Properties
 13. Non-Goals
 14. Conformance Testing
 15. References
-

1. Introduction

NOVAK SP-1 defines the foundational **Execution Integrity Standard** for all Proof-Before-Action Systems (PBAS).

This standard establishes the requirement that **no automated system may execute an action unless mathematical proof of correctness is provided first.**

This principle is the opposite of the historical “execute-then-log,” “execute-then-audit,” and “execute-then-investigate” paradigms used in government, finance, robotics, medicine, and AI systems.

NOVAK defines a new execution model:

Action is permitted only if the system can produce a cryptographically verifiable proof that the inputs, rules, and outputs are correct and unmodified.

SP-1 is the root of all other NOVAK standards (SP-2, SP-3, IBF, PBAS category definition).

2. Purpose & Scope

SP-1 establishes:

- The formal definition of **Execution Integrity**
- The functional model for **Proof-Before-Action**
- Mandatory integrity conditions
- Required cryptographic structures
- Compliance requirements
- Conformance testing structure

SP-1 applies to:

- AI systems
- Robotic control systems
- Healthcare automation
- Government benefit determinations
- Military decision systems
- Financial transaction engines
- Any system where incorrect execution can cause harm

This standard is system-agnostic and does not prescribe specific technologies except where cryptographic binding is required.

3. Terminology

These terms are **normative** for SP-1.

Term	Definition
Execution Integrity	A property where an action can only occur if inputs, rules, and outputs are mathematically proven correct.

Proof-Before-Ac	The requirement that verification must occur <i>before</i> execution.
HVET	Hash-Verified Execution Trace (defined in SP-2).
EIR	Execution Identity Receipt (defined in SP-2).
RGAC	Recursive Global Audit Chain (defined in SP-2).
Safety Gate	The deterministic gate that permits or blocks execution (defined in SP-3).
PL-X	Physical-Layer Drift and Corruption model.
PS-X	Psycho-Social Intent Manipulation model.
PBAS	Proof-Before-Action System, NOVAK's category.

4. Execution Integrity Model

A system S has Execution Integrity (EI) if and only if **all five** of the following are true:

1. **Input Integrity** — all input data is known, attested, immutable, and bound to the execution.
2. **Rule Integrity** — the governing rules are fixed, versioned, cryptographically identified, and immutable during execution.
3. **Output Integrity** — the output is deterministically derived from the inputs + rules.
4. **Identity Integrity** — the execution is tied to an immutable identity (human or machine).
5. **Temporal Integrity** — the proof must be tied to an unforgeable timestamp.

These are bound together through the **Integrity Binding Function (IBF)** defined in the formal spec.

5. Integrity Preconditions

Before any execution occurs:

5.1 Condition P-1: Known Inputs

The system must be able to enumerate, serialize, and cryptographically commit to every input.

5.2 Condition P-2: Known Rules

The ruleset must be immutable for the duration of execution.

5.3 Condition P-3: Deterministic Execution

Given the same inputs and rules, the system must always produce the same output.

5.4 Condition P-4: No Hidden State

Execution must not depend on any invisible, mutable, or contextual state.

6. Core Requirements (R-Series)

SP-1 defines 14 mandatory requirements:

R-1 — Proof-Before-Action

No action may occur until a valid EIR exists.

R-2 — Cryptographic Binding

Inputs, rules, and outputs must be bound together using the function IBF().

R-3 — Immutability During Execution

No component may change during evaluation.

R-4 — Deterministic Output

Execution must be pure.

R-5 — Canonical Serialization

All components must be serialized using a canonical representation.

R-6 — Universal Verifiability

Any third party must be able to mathematically verify the execution.

R-7 — Zero Consensus Requirement

Execution integrity must not depend on network consensus.

R-8 — No Blockchains Required

SP-1 forbids reliance on blockchain consensus to enforce correctness.

R-9 — Human & Machine Symmetry

The standard applies equally to human-triggered and machine-triggered actions.

R-10 — Identity Binding

Each execution must bind a unique identity.

R-11 — Temporal Binding

Each execution must include a verifiable timestamp.

R-12 — Rejection on Failure

If integrity cannot be proven, execution **must be blocked**.

R-13 — Safety Gate Enforcement

SP-3's Safety Gate must approve or deny the action.

R-14 — Auditability

The system must record a verifiable, tamper-proof audit record.

7. Correctness Conditions

A system S is considered correct under SP-1 if:

1. **All required components are present**

2. No component has been modified after attestation
 3. The IBF hash matches the EIR
 4. RGAC extension is valid
 5. No PL-X or PS-X anomaly was detected
 6. Safety Gate approved execution
-

8. Execution Integrity Receipt (EIR) Requirements

Each EIR must contain:

- EIR ID
- HVET structure (HR, HD, HO, timestamp, HVET)
- Identity of executor
- Version of ruleset
- Full IBF hash
- Signature (optional but recommended)

EIR must be:

- Immutable
 - Human-readable
 - Machine-verifiable
-

9. Recursive Global Audit Chain (RGAC) Binding Conditions

The RGAC must satisfy:

- 1. Append-only structure**
- 2. Each entry references the previous HVET**
- 3. Tampering breaks the chain**
- 4. Verification must be $O(n)$**
- 5. Chain must not require consensus**

RGAC is not a blockchain — it is a **local, cryptographically secure audit chain**.

10. Safety Preconditions & Gate Conditions

The Safety Gate (SP-3):

- Blocks execution if integrity cannot be proven
 - Blocks execution if PL-X anomalies exist
 - Blocks execution if PS-X manipulation is detected
 - Allows execution only after EIR validation
-

11. Compliance Levels

NOVAK SP-1 defines 5 compliance levels:

Level	Definition
CL-1	Basic input/output binding
CL-2	Full HVET + deterministic execution
CL-3	Full EIR compliance
CL-4	Full RGAC compliance
CL-5	Full NOVAK compliance (SP-1 + SP-2 + SP-3)

NOVAK-compliant systems must meet **CL-5**.

12. Security Properties

SP-1 guarantees:

- **Pre-execution tamper detection**
 - **Prevention of silent corruption**
 - **Prevention of benefit fraud**
 - **Defense against malicious automation**
 - **Defense against rule manipulation**
 - **Universal verification without blockchain or consensus**
-

13. Non-Goals

SP-1 does *not* provide:

- Encryption
- Authentication

- Network security
 - Privacy guarantees
 - Blockchain anchoring (optional but out of scope)
-

14. Conformance Testing

Compliance tests include:

- Deterministic execution tests
 - IBF hash verification
 - EIR integrity tests
 - Safety Gate rejection tests
 - RGAC tampering tests
 - Regression tests
-

15. References

- NOVAK SP-2 Cryptographic Standard
- NOVAK SP-3 Safety Standard
- IBF Formal Specification
- PBAS Category Definition
- Dolev–Yao Model
- NIST SP-800-160

- Bitcoin Whitepaper (as historical precedent)