PART 2 — WHAT NOVAK IS

This section establishes **the formal structure**, **cryptographic definitions**, and **plain-language explanations** of the NOVAK Protocol. No concepts are omitted, simplified, or reinterpreted. This version incorporates **all fifteen NOVAK Laws**, **both Industry Addenda**, and **all mandatory subsystem terminology mappings**.

I. FORMAL DEFINITIONS

1. NOVAK Protocol — Formal Definition

NOVAK is an **authoritative proof-before-action execution-integrity system** governing how any rule, computation, regulatory decision, AI output, robotic motion, or human-entered action must execute.

Formally:

> **NOVAK = (R, D, I, O, HVET, EIR, RGAC, SG, T)**
>
> where:
>
> - **R** = deterministic regulatory or computational rules
> - **D** = attested, non-malleable input domain
> - **I** = identity-bound actor (human, machine, or institution)
> - **O** = deterministic, non-malleable output domain
> - **HVET** = Hash-Verified Execution Trace
> - **EIR** = Execution Identity Receipt *(formerly "NIPS")*
> - **RGAC** = Recursive Global Audit Chain *(formerly "REVELATION")*
> - **SG** = Safety Gate — Deterministic Safety Layer *(formerly "HARMONEE")*

- **T** = globally ordered timestamp lineage

NOVAK enforces that:

∀ action A, A may not execute unless:

1. **R is deterministic (L1).**
2. **D is non-malleable and attested (L2–L3).**
3. **O is predetermined and deterministic (L1, L4).**
4. **All commitments (R, D, I, O, T) are hashed into an HVET (L5–L6).**
5. **An EIR is generated binding the actor identity to the full execution (L6).**
6. **The Safety Gate validates all proofs before execution (L7–L8).**
7. **The RGAC records the action into an irreversible global audit chain (L7–L15).**
8. **All physical-layer and psycho-social constraints are validated (PL-X, PS-X).**

This framework makes **undetected tampering logically impossible**.

---

2. Mandatory Terminology Lineage

NOVAK requires explicit historical mappings:

Old Term	Updated NOVAK Term	Reason
NIPS	**EIR — Execution Identity Receipt**	NIPS lacked identity-binding and proof finality. EIR enforces cryptographic actor lineage.
REVELATION	**RGAC — Recursive Global Audit Chain**	Expands from simple logging to infinite-depth audit recursion.
HARMONEE	**Safety Gate — Deterministic Safety Layer**	HARMONEE enforced purity; SG enforces *pre-execution determinism*.

Every Part, including future Parts 3–10, will reference these mappings where relevant.

---

3. HVET — Formal Definition

Hash-Verified Execution Trace (HVET) is:

> A deterministic cryptographic hash commitment formed from:
> **HVET = H(HR ∥ HD ∥ HI ∥ HO ∥ T)**

Where:

- **HR** = hash of deterministic rule
- **HD** = hash of attested input data
- **HI** = hash of identity commitment
- **HO** = hash of deterministic output
- **T** = globally ordered timestamp

Properties enforced by Laws L0–L15:

- irreversible (L0)
- input-bound and output-bound (L2–L4)
- identity-anchored (L6)
- temporally ordered (L8)
- globally consistent (L9)
- publicly verifiable (L11)
- minimal trust dependency (L12)
- universally auditable (L15)

---

4. EIR — Execution Identity Receipt (formerly NIPS)

EIR is the cryptographic receipt that binds the actor identity to the entire execution event.

EIR ensures:

- identity cannot be swapped
- fraud cannot mask origin
- no computation proceeds without full cryptographic self-identification
- every actor becomes permanently accountable to every action they initiate

This satisfies:

- **L6 — Execution Identity Law**
- **PS-X — Psycho-Social Fraud Surface Mitigation**
- **PL-X — Hardware-backed identity seals (TPM, PUF, secure enclave)**

---

5. RGAC — Recursive Global Audit Chain (formerly REVELATION)

The **RGAC** is a **forever-growing**, **globally consistent**, **cryptographically chained** record of every HVET and EIR ever produced under NOVAK.

RGAC ensures:

- infinite audit recursion (L7)
- global ordering (L8)
- jurisdictional interoperability (L10)
- public verifiability (L11)
- minimal trust footprint (L12)

- regulatory determinism (L13)
- no machine deviation (L14)
- universal auditability (L15)

Unlike blockchain:

- no miners
- no probabilistic finality
- no consensus forks
- no economic incentives
- no ledger duplication overhead
- no hash-power dependency

RGAC is **authoritative**, not competitive.

---

6. Safety Gate — Deterministic Safety Layer (formerly HARMONEE)

Safety Gate (SG) enforces the rule:

> **No action is permitted until the system proves that:**
> **R is deterministic, D is attested, I is bound, O is precomputed,**
> **and all integrity proofs are satisfied.**

SG applies:

- L0–L8 at computation time
- L9–L15 at audit time
- PL-X constraints (physical layer verification)

- PS-X constraints (socio-cognitive fraud prevention)

SG is the mechanism that elevates NOVAK from *checksum* to *governance engine*.

II. SIMPLE DEFINITIONS (FOR NON-TECHNICAL READERS)

Because NOVAK will be read by Congress, industry, agencies, businesses, courts, and citizens, the simple definitions are required.

What NOVAK Is (Simple)

- **NOVAK is a system that forces computers, AI, robots, agencies, and people to prove correctness before they act.**
- **NOVAK guarantees actions cannot be changed, faked, or tampered with without detection.**
- **NOVAK makes every action traceable back to the exact identity that performed it.**
- **NOVAK creates a global audit trail that never breaks and never loses order.**
- **NOVAK stops errors, fraud, manipulation, and accidental decisions before they occur.**

What HVET Is (Simple)

- HVET is the **digital fingerprint** of an action.
- It proves what rule was used, what data was used, who did it, and what the result was.
- It cannot be faked or altered.

What EIR Is (Simple)

(formerly NIPS)

- EIR is the **receipt proving who did something**.
- Every action has a person, machine, agency, or system tied to it forever.

What RGAC Is (Simple)

(formerly REVELATION)

- RGAC is a **never-ending audit trail** connecting every action ever taken.
- It is impossible to rewrite or delete an entry.

What Safety Gate Is (Simple)

(formerly HARMONEE)

- Safety Gate is the mechanism that **stops bad decisions before they happen**.
- If anything is wrong—data, rule, person, identity, hardware—NOVAK refuses to act.

III. WHY THIS MATTERS

NOVAK solves systemic problems that governments, corporations, AI systems, and regulatory bodies have struggled with for decades:

- inconsistent decisions

- altered records
- identity spoofing
- timestamp fraud
- silent tampering
- non-deterministic software
- regulatory ambiguity
- undetectable machine deviation

NOVAK creates the first **mathematically enforced rule-of-law engine**.

This is why NOVAK is essential.