



# NOVAK UNIFIED ALPHABETICAL GLOSSARY (UTG-1A)

***Complete alphabetical index of all scientific, cryptographic, regulatory, AI, robotics, and cross-domain terms used across all NOVAK standards.***

---

## A

### **A1 — Audit Chain**

General term referring to the NOVAK **Recursive Global Audit Chain (RGAC)** — an immutable lineage of proof objects.

### **A2 — Adversarial Drift**

Any change in input, interpretation, rule, output, or embedding-space vector designed to evade detection.

### **A3 — Adversarial Prompt**

A prompt designed to deceive an AI, disrupt determinism, or bypass the Safety Gate.

### **A4 — AI Convergence Check**

The evaluation that multiple AI models produce consistent outputs within deterministic tolerance.

### **A5 — Ambiguity Matrix**

A NOVAK structure that maps linguistic, regulatory, semantic, and cross-language ambiguity vectors.

### **A6 — Argmax-Shift Attack**

An adversarial technique causing a high-confidence but incorrect output by altering internal logits.

## **A7 — Attested Input**

Input that has passed identity, provenance, and state validation before being hashed into HD.

---

# **B**

## **B1 — Boundary Drift**

A deviation that keeps output within acceptable structural bounds but alters meaning.

## **B2 — Behavioral Vector (PS-X)**

Human interaction patterns measured to detect fraud, coercion, or intent manipulation.

---

# **C**

## **C1 — Canonical Rule Form**

The structural, whitespace-normalized, syntactically stable representation of a rule for hashing.

## **C2 — Canonicalization Pipeline**

The multi-step process that transforms any input into deterministic form before hashing.

## **C3 — Chain Link Hash (RGAC)**

Link=SHA256(HVETprev // HVETcurrent)  
Link = SHA256(HVET\_{prev} \|  
HVET\_{current})  
Link=SHA256(HVETprev // HVETcurrent)

## **C4 — CJCM (Cross-Jurisdiction Compliance Matrix)**

Structure ensuring policy equivalence across federal, state, international, military, or corporate systems.

## **C5 — CPF-L (Cross-System Proof Federation Layer)**

SP-8 subsystem enabling cross-agency, cross-organization proof interoperability.

## **C6 — Convergence Tolerance ( $\epsilon$ )**

Maximum allowed drift between AI or system outputs before execution is blocked.

## **C7 — Cryptographic Domain Binding**

The mandatory requirement that every action is bound to its domain context (healthcare, finance, robotics, etc.).

---

# **D**

## **D1 — DCM (Deterministic Convergence Model)**

Mathematical model ensuring identical outputs across architectures, quantization levels, and models.

## **D2 — Deterministic Freeze**

Execution halt when model outputs diverge.

## **D3 — Deterministic Ordering (DGO)**

Global constraint requiring chronological sequence integrity for all EIRs.

## **D4 — Drift Vector**

$v_{drift} = O_{expected} - O_{actual}$

## **D5 — Domain Interface Specification (N-DIS)**

Industry-specific rule sets for VA, DoD, finance, robotics, AI, medical, aviation, etc.

---

# **E**

## **E1 — EF Mode (Execution Freeze Mode)**

Emergency halt triggered by drift, rule mismatch, RGAC anomaly, PL-X/PS-X violation.

## **E2 — EIR (Execution Identity Receipt)**

Pre-execution proof object containing:

- HVET
- inputs
- outputs
- rule hash
- timestamp
- operator identity
- PL-X/PS-X results
- signature

## **E3 — Embedding Drift**

Difference between embedding vectors at time t and t-1:

$$d = \|E_t - E_{t-1}\| / 2d = \|E_t - E_{t-1}\|_2 / \|E_t - E_{t-1}\|_2$$

## **E4 — Evidence Packet**

Canonicalized set of structured evidence supporting a decision. Always hashed into HD.

---

# **F**

## **F1 — Federated Proof Envelope**

Cross-organization packet of HVET/EIR/RGAC components exchanged over CPF-L.

## **F2 — Freeze-Thaw Consistency Rule**

Execution can only resume if *all* frozen-state proofs converge post-resolution.

## **F3 — Fraud Vector (PS-X)**

Behavioral or structural indicators of human-origin manipulation.

---

# **G**

## **G1 — GDEL (Global Deterministic Enforcement Layer)**

SP-8 Section 41 enforcement surface conditioning all execution on verified proof.

## **G2 — Gradient-Space Drift**

Embeddings-space deviation measured via cosine similarity or L2 norm.

## **G3 — Governance Canon**

The unified rule-set defining how the NOVAK system governs decisions across domains.

---

# **H**

## **H1 — HARMONEE (retired name)**

The old name for the **Safety Gate**.

## **H2 — HD (Input Hash)**

$HD = \text{SHA256}(\text{Inputcanonical})$

## **H3 — HO (Output Hash)**

$HO = \text{SHA256}(\text{Outputexpected})$

$H_O = \text{SHA256}(\text{Output}_{\{\text{expected}\}})$

## **H4 — HR (Rule Hash)**

$HR = \text{SHA256}(\text{Rulecanonical})$

## **H5 — HVET (Hash-Verified Execution Token)**

HVET=SHA256(HR // HD // HO // T)  
HVET = SHA256(H\_R \| H\_D \| H\_O \|  
T)HVET=SHA256(HR // HD // HO // T)

## **H6 — Human Drift Metric (PS-X)**

A quantitative measure of human deception vectors.

---

# **I**

## **I1 — IBF (Integrity Binding Function)**

SP-4 formal function binding rule, input, and output.

## **I2 — Identity Anchor**

Any cryptographically attached identity metadata in an EIR.

## **I3 — Interpretation Drift**

Semantic deviation between intended and perceived meaning.

---

# **J**

## **J1 — Jurisdiction Overlay**

The legal/regulatory layer applied to U-PEF mapping for multi-region compliance  
(EU/US/DoD/VA/etc).

---

# **K**

## **K1 — Kernel Determinism Check**

Ensures internal model kernels (transformer blocks, ops) behave identically across environments.

---

## L

### **L1 — Legal Consistency Envelope**

Layer ensuring regulatory, statutory, and evidentiary correctness before action.

### **L2 — Linguistic Drift**

Shift in meaning detectable through semantic-space vector changes.

---

## M

### **M1 — Multi-Model Reconciliation Layer (MR-L)**

Ensures transformers, diffusion models, robotics controllers, and symbolic engines produce consistent outputs.

### **M2 — Metastability Tolerance (PL-X)**

Numeric value indicating acceptable physical-layer instability.

### **M3 — Model Drift**

$d_{model} = |O_1 - O_2|$   $d_{\{model\}} = |O_{\_1} - O_{\_2}|$   $d_{model} = |O_1 - O_2|$

---

## N

### **N1 — N-DIS**

NOVAK Domain Interface Specification.

### **N2 — NIPS (retired name)**

Old name for EIR.

---

# O

## O1 — Output Canonicalizer

Component that normalizes model/system outputs for deterministic hashing.

---

# P

## P1 — PBA (Proof-Before-Action)

Mandatory gating requirement for all execution.

## P2 — PL-X

Physical Layer Integrity Addendum.

## P3 — Policy Drift

$d_{policy} = H(P_t) - H(Pref)$   
 $d_{policy} = H(P_t) - H(P_{ref})$

## P4 — PS-X

Psycho-Social Integrity Addendum.

---

# Q

## Q1 — Quantization Drift

Deviation caused by differing numeric precision in AI models (FP32 → BF16 → INT8).

---

# R

## **R1 — REVELATION (retired name)**

Old name for RGAC.

## **R2 — RGAC**

Recursive Global Audit Chain.

## **R3 — Rule Canonicalizer**

Transforms regulatory or computational rule text into deterministic form.

## **R4 — Recursive Federation Oracle (CPF-L)**

Federates proofs between systems.

---

# **S**

## **S1 — Safety Gate**

Execution halting mechanism enforcing all NOVAK laws + PL-X/PS-X.

## **S2 — Semantic Drift Sensitivity**

Threshold for acceptable meaning change in text outputs.

## **S3 — Signature Envelope**

Cryptographic structure containing identity and verification metadata.

---

# **T**

## **T1 — Timestamp Determinism Rule**

Ensures monotonic timestamps for EIRs.

## **T2 — Truth Intersection Rule**

Cross-model agreement principle:

$$\text{Truth} = \bigcap_{i=1}^n \text{O}_i \text{Truth} = \bigcup_{i=1}^n \text{O}_i \text{Truth} = \bigcap_{i=1}^n \text{O}_i$$

## T3 — Threat Model Vector (NTM Series)

Structured representation of adversary capability.

---

# U

## U1 — U-PEF (Universal Proof Exchange Format)

Canonical proof packet used across all systems.

## U2 — Upper Drift Bound ( $\epsilon$ )

Maximum admissible drift allowed before execution is blocked.

---

# V

## V1 — Verification Bus (CS-VBUS)

Protocol-independent transport layer for U-PEF and EIR exchange.

## V2 — Vector-Field Drift Map

Gradient-field representation of drift across model layers.

---

# W

## W1 — Weighted Drift Scalar

$$dw = \sum_i w_i \cdot d_i = \sum_i w_i \cdot d_i$$

---

# X

## X1 — Cross-Domain Drift

Any drift that manifests differently across systems (e.g., EHR vs. claims pipeline).

---

# Y

## Y1 — Yield-Safe Reconciliation

Output reconciliation method ensuring no harmful action results from divergence.

---

# Z

## Z1 — Zero-Trust Deterministic Execution Principle

NOVAK's rule that execution must rely on *cryptography only*, never human or system trust.