PART 6 — IMPLEMENTATION LAYERS

NOVAK is a **vertically integrated deterministic integrity architecture**.
Every layer of the stack must obey the NOVAK Laws (L0–L15) and Addenda (PL-X, PS-X).
There is no "light" integration or partial compliance.

If a layer cannot satisfy NOVAK, it cannot participate in execution.

NOVAK spans:

1. Hardware Layer

2. Firmware Layer

3. OS Layer

4. Network Layer

5. API Layer

6. Application Layer

7. AI/ML Layer

8. Robotics & Autonomous Systems Layer

9. Regulatory & Government Execution Layer

Each layer has mandatory obligations.

I. HARDWARE LAYER (PL-X CORE)

NOVAK Laws Enforced:

- **L0 — Irreversibility**

- **L6 — Identity**

- **L8 — Temporal Order**

- **L14 — Machine Non-Deviation**

PL-X Addendum Applied:

Physical Layer Addendum PL-X is mandatory.
 It captures:

- metastability detection

- clock-skew analysis

- propagation-delay fingerprinting

- TPM/PUF identity sealing

- hardware-root-of-trust anchoring

- voltage drift and jitter measurements

- physical environment signatures (thermal, EM, vibration)

Hardware Requirements:

- deterministic clock source

- hardware monotonic counters

- secure PUF or TPM 2.0

- write-once firmware regions

- non-bypassable secure enclave

Hardware Outputs to NOVAK:

- **device-hash**

- **timing-state**

- **environment-hash**

- **drift-profile**

- **PUF signature**

These are included in EIR and HVET.

II. FIRMWARE LAYER

NOVAK Laws Enforced:

- **L1 — Deterministic Purity**

- **L4 — Output Non-Malleability**

- **L12 — Minimal Trust Surface**

Firmware Constraints:

All firmware routines must be:

- immutable

- deterministic

- cryptographically sealed

- validated by Safety Gate before use

- reproducible in execution

Firmware cannot:

- generate nondeterministic entropy

- bypass identity requirements

- alter hardware timing sources

- execute unverified routines

Firmware → NOVAK Outputs:

- **firmware-integrity-hash**

- **boot lineage proofs**

- **secure enclave attestations**

III. OPERATING SYSTEM (OS) LAYER

NOVAK Laws Enforced:

- **L2–L4 (Data & Output Non-Malleability)**

- **L11 (Public Verifiability)**

- **L14 (Machine Non-Deviation)**

Requirements:

OS kernels must:

- enforce deterministic system calls

- prohibit nondeterministic scheduling

- prohibit mutable kernel logging

- run all processes under identity-bound envelopes

- produce canonical syscall traces for HVET

OS → NOVAK Outputs:

- **syscall lineage**

- **memory state commitments**

- **process identity graphs**

All processes must run under EIR-bound identity contexts.

IV. NETWORK LAYER

NOVAK Laws Enforced:

- **L6 — Identity Binding**

- **L8 — Temporal Order**

- **L9 — Global Consistency**

Network Obligations:

- packets must be identity-bound

- packet replay forbidden

- timestamps must be monotonic

- routing metadata must be sealed

- session keys must be deterministic

- network malleability is disallowed

NOVAK-compatible network layers operate like **deterministic communication channels**, not probabilistic packet streams.

Network → NOVAK Outputs:

- **connection identity hashes**

- **packet lineage proofs**

- **routing-chain signatures**

V. API LAYER

NOVAK Laws Enforced:

- **L2–L4 — Purity & Non-Malleability**

- **L6 — Identity**

- **L12 — Minimal Trust Surface**

API Requirements:

- all API calls must be pure functions

- no hidden state

- response must be pre-determinable

- inputs must match canonical schemas

- identity is required for every call

API → NOVAK Outputs:

- **call-hash**

- **schema-lock proof**

- **request-intent profile (PS-X)**

If the API endpoint is nondeterministic → **blocked by Safety Gate**.

VI. APPLICATION LAYER

NOVAK Laws Enforced:

- **L1–L6 (Determinism & Non-Malleability)**

- **L11 — Public Verifiability**

- **L14 — Machine Non-Deviation**

Requirements:

Applications must:

- run deterministic logic

- expose rule-pure functions

- separate UI from computation deterministically

- enforce attestation boundaries

Decision-making applications (e.g., medical, VA, IRS, DoD, banking) must:

- encode rules as pure functions

- allow no ambiguous interpretation

- produce HO (output hash) before execution

Application → NOVAK Outputs:

- **rule-purity proofs**

- **schema-sealed input domains**

- **intent-pattern metadata (PS-X)**

VII. AI / MACHINE LEARNING LAYER

This is one of the most important sections.

NOVAK Laws Enforced:

- **L1 — Deterministic Purity**

- **L14 — Machine Non-Deviation**

- **L3–L4 — Non-Malleability**

- **L6 — Identity Binding**

- **L5 & L7 — Pre-Execution Proof & Recursion**

AI Hard Requirements:

AI models **must not**:

- produce nondeterministic outputs

- hallucinate

- drift

- deviate

- alter internal weights without attestation

- fail to pre-compute output hashes

AI systems under NOVAK must provide:

1. **Deterministic inference**

2. **Model-weight lineage hashing**

3. **Pre-execution output prediction**

4. **Identity-bound inference context**

5. **Safety Gate pre-check of model purity**

AI models must operate like **deterministic computational graphs**, not stochastic black boxes.

AI → NOVAK Outputs:

● **model-weight hash**

● **inference-graph hash**

● **prediction hash**

● **intent alignment score (PS-X)**

This prevents AI from:

● drifting

● hallucinating

● self-modifying

● deviating from the rule-of-law

AI becomes **bounded, predictable, auditable, identity-linked, and deterministic**.

VIII. ROBOTICS & AUTONOMOUS SYSTEMS LAYER

NOVAK Laws Enforced:

● **L1 — Determinism**

- **L6 — Identity Binding**

- **L8 — Temporal Order**

- **L14 — Machine Non-Deviation**

- **PL-X — Physical-Layer Integrity**

- **PS-X — Intent Behavior Integrity**

Requirements:

Robots must:

- bind physical motion to identity

- pre-compute allowed motion trajectories

- make no unverified movements

- reject ambiguous sensor data

- generate motion-output hashes (HO)

- store all actions in RGAC

Every robotic movement is:

- identity bound

- deterministic

- safety-checked

- pre-hashed

- globally auditable

A robot cannot "slip", "drift", or "wander" without detection.
 NOVAK enforces **absolute execution determinism**.

IX. REGULATORY & GOVERNMENT SYSTEM LAYER

NOVAK is fundamentally a **regulatory execution engine**.
 This layer is where the Laws L13–L15 become dominant.

NOVAK Laws Enforced:

- **L13 — Regulatory Determinism**

- **L14 — Machine Non-Deviation**

- **L15 — Universal Auditability**

Requirements for Government Systems:

Regulatory systems must:

1. encode laws as deterministic rule sets

2. enforce identity-binding for every adjudication

3. ensure every decision is pre-auditable

4. attach EIR to every regulatory action

5. publish RGAC entries for public verification

6. prevent agency-level deviations

7. prove every decision is rule-pure and deterministic

Government → NOVAK Outputs:

- **regulatory rule hashes**

- **case-data attestation hashes**

- **jurisdictional identity binding**

- **public audit chain entries**

This makes government:

- fraud-resistant

- tamper-resistant

- consistent

- fair

- deterministic

- non-discriminatory

- mathematically accountable

NOVAK becomes the world's first **cryptographic rule-of-law engine**.

X. INTEGRATION SUMMARY TABLE

Layer	Obligations	Laws	Addenda	Outputs
Hardware	PUF, TPM, timing, drift	L0, L6, L8, L14	PL-X	device-hash, timing-state
Firmware	Deterministic syscall context	L1, L4, L12	PL-X	firmware-integrity-hash
OS	Deterministic kernel	L2–L4, L11	PL-X	syscall lineage
Network	Identity-bound packets	L6, L8, L9	—	routing lineage
API	Pure function endpoints	L2–L4, L6	PS-X	schema-lock proofs
App	Rule-pure logic	L1–L6	PS-X	HO, rule-purity proofs
AI/ML	Deterministic inference	L1, L14	PS-X	inference-graph hash

| Robotics | Identity-bound motion | L6, L14 | PL-X | motion lineage |
| Gov/Reg | Deterministic rule-of-law | L13–L15 | both | public RGAC entries |