PART 7 — SECURITY MODEL & THREAT SURFACES

NOVAK has a radically different security model from any existing system.
It is designed to withstand:

- insider threats
- criminal actors
- corrupted institutions
- malicious AI
- rogue robots
- regulatory bias
- cross-jurisdiction fraud
- nation-state attacks
- physical tampering
- timestamp forgery
- hardware compromise
- behavioral deception
- environmental manipulation
- full-stack cyber warfare

NOVAK's architecture is built under the principle:

> **"If a system can act without proving correctness, it can be compromised without detection."**

NOVAK eliminates this possibility through:

- deterministic execution (L1)
- non-malleable data and output (L2–L4)
- pre-execution hashing (L5)
- identity-bound execution (L6)
- recursive verifiability (L7)
- temporal ordering (L8)
- global consistency (L9)
- cross-domain interoperability (L10)
- public verifiability (L11)
- minimal trust (L12)
- regulatory determinism (L13)
- machine non-deviation (L14)
- universal auditability (L15)
- **physical (PL-X)** and **psycho-social (PS-X)** enforcement

NOVAK is the **closest possible model to an unbreakable execution system** under modern computing theory and adversarial models.

I. SECURITY PRINCIPLES THAT GOVERN NOVAK

NOVAK security is built on **seven foundational principles**:

1. Proof-before-action

No system, human, AI, robot, or government can act without providing cryptographic proof.

2. Identity-bound execution

All actions permanently bind the initiator.

3. Deterministic rule-of-law

No ambiguous, interpretive, or stochastic behaviors allowed.

4. Universal immutability

Tampering anywhere invalidates everything forward.

5. Layered physical-to-social defenses

PL-X + PS-X protect both electrons **and** human behavior.

6. Zero implicit trust

All decisions must be verifiable publicly.

7. Global recursive auditability

Every action becomes part of an infinite audit chain.

II. THREAT SURFACE ANALYSIS

NOVAK categorizes threats into nine major domains:

1. Hardware Threats
2. Firmware Threats
3. OS Kernel Threats
4. Network/Transport Threats
5. API/Application Threats
6. AI/Model Threats

7. Robotics/Physical Action Threats
8. Government/Regulatory Threats
9. Human/Psycho-Social Threats

Each is described below with how NOVAK defeats them.

---

1. HARDWARE THREAT DOMAIN

(PL-X Addendum — Physical Layer Enforcement)

Threats:

- Fault injection
- Clock skew attacks
- Timing-source manipulation
- Voltage glitching
- EM interference
- Hardware trojans
- PUF manipulation
- TPM spoofing
- Side-channel leakage
- Rowhammer and bit-flip injection

NOVAK Defenses:

- PL-X metastability detection

- device-hash binding in EIR
- drift-profile sealing
- propagation-delay fingerprints
- thermal/EM environmental hashing
- recursive hardware attestation in RGAC
- deterministic timing validation

If physical state deviates → Safety Gate blocks execution.

---

2. FIRMWARE THREAT DOMAIN

Threats:

- malicious firmware flashing
- persistent pre-boot malware
- DMA-based privilege escalation
- microcode manipulation
- hidden instruction injection

NOVAK Defenses:

- immutable firmware regions
- PUF-anchored boot lineage
- firmware-hash sealing in HVET
- pre-execution firmware proof (L1–L5)

- EIR checks jurisdiction/device coherence

Firmware not matching canonical hashes = absolute execution halt.

---

3. OPERATING SYSTEM THREAT DOMAIN

Threats:

- kernel rootkits
- syscall hooking
- nondeterministic scheduling
- kernel logging manipulation
- process impersonation

NOVAK Defenses:

- determinized kernel syscall graph
- identity-bound system processes
- memory state commitments
- monotonic scheduler enforcement
- immutable syscall lineage in RGAC

Any deviation → chain invalidation → execution impossible.

---

4. NETWORK THREAT DOMAIN

Threats:

- packet replay
- identity spoofing
- routing manipulation
- man-in-the-middle (MITM)
- timestamp forgery
- session hijacking

NOVAK Defenses:

- identity-bound packet envelopes
- monotonic timestamp lineage (T)
- non-replayable routing-chain signatures
- packet-hash insertion into EIR
- global consistency (L9)

If the network cannot prove integrity, NOVAK refuses the data.

---

5. API / APPLICATION THREAT DOMAIN

Threats:

- data injection
- schema violation
- API impersonation

- hidden-state logic
- fuzzy or probabilistic logic
- mutating decision paths

NOVAK Defenses:

- schema-lock via HD hashing
- pure functions only (L1)
- deterministic outputs only (L4)
- API-call hashing in HVET
- identity requirement for every call (L6)
- PS-X intent-modeling against fraud

Applications must become **deterministic rule engines**, not flexible logic trees.

---

6. AI / MACHINE LEARNING THREAT DOMAIN

Threats:

- hallucinations
- stochastic outputs
- model drift
- weight manipulation
- prompt exploitation

- adversarial perturbations
- AI impersonation
- self-modifying AI

NOVAK Defenses:

- determinized inference graphs
- model-weight hashing
- output pre-computation
- Safety Gate rule purity checks
- inference intent alignment (PS-X)
- RL/LLM/robotics bound to EIR identity
- chain-of-thought non-malleability enforcement

NOVAK is the **antidote** to undeterministic AI behavior.

---

7. ROBOTIC & AUTONOMOUS SYSTEMS THREAT DOMAIN

Threats:

- sensor spoofing
- motion drift
- unverified autonomous action
- unbounded state transitions

- adversarial environment manipulation
- malfunctioning control loops

NOVAK Defenses:

- deterministic motion graph hashing
- sensor attestation
- identity-bound physical movements
- Safety Gate trajectory prediction
- PL-X environment signatures
- unbreakable RGAC audit lineage

A robot cannot move unless the movement is proven safe, deterministic, and identity-bound.

---

8. REGULATORY / GOVERNMENT THREAT DOMAIN

This section is *critical* because NOVAK is built as a **regulatory execution engine**.

Threats:

- inconsistent decisions
- malicious or biased reviews
- corrupted officials
- hidden data
- altered case files

- invalid timestamps
- forged signatures
- falsified VA/IRS/DoD determinations
- silent modifications to public records

NOVAK Defenses:

- rule determinism (L13)
- public verifiability (L11)
- identity-bound rulings (L6)
- immutable audit lineage (RGAC)
- evidence attestation (HD)
- pre-execution determinism (SG)
- fraud vector detection (PS-X)

NOVAK prevents “bad government days.”
The rules, evidence, and outcomes must always match.

---

9. HUMAN & PSYCHO-SOCIAL THREAT DOMAIN

(PS-X Addendum — Psycho-Social Integrity Enforcement)

Threats:

- lying
- fraud

- social engineering
- malicious user intent
- emotional manipulation
- cognitive bias
- insider threats
- collusion
- duress actions
- impersonation

NOVAK Defenses:

- intent-profile hashing
- behavioral signature tracking
- fraud-pattern detection
- deception-surface bounding
- identity+device+jurisdiction triplet binding
- irreversible EIR identity sealing
- PS-X anomalies recorded permanently in RGAC

Humans cannot fake an action, motive, or identity.
NOVAK cryptographically binds behavior to identity.

III. NATION-STATE THREAT MODEL

NOVAK is designed to survive:

- APTs
- SCADA attacks
- supply chain compromise
- cross-border packet injection
- quantum adversaries (post-quantum upgrade-ready)
- deepfake identity attacks
- timestamp forgery at scale
- cross-jurisdiction evidence manipulation

NOVAK survives nation-state assaults because:

- no action can occur without proof
- identity cannot be swapped
- hardware roots are cryptographically sealed
- the audit chain is globally recursive
- correctness is enforced before the system does *anything*

This is something **no existing system** does.

IV. INSIDER THREAT MODEL

Insiders typically cause the worst breaches.

NOVAK prevents:

- silent log modifications
- unauthorized data changes

- identity spoofing
- tampering with case files
- deleting or altering records
- bypassing the chain of authority
- modifying outputs
- using privileged accounts to commit fraud

Why?
Because every insider action is:

- identity-bound (EIR)
- pre-hashed (HVET)
- globally audited (RGAC)
- physically anchored (PL-X)
- intent-profiled (PS-X)

Insiders cannot act without leaving a perfect, immutable, public forensic trail.

V. ATTACK SUMMARY TABLE

Threat Type	NOVAK Layer	Prevented By
Hardware tampering	PL-X + SG	L0, L6, L8, L14
Firmware compromise	SG + RGAC	L1, L4, L7
Kernel tampering	OS + RGAC	L2–L4, L11, L14
Network spoofing	Network Layer	L6, L8, L9
API injection	API Layer	L2–L4, L6

AI hallucination	AI Layer	L1, L4, L14
Robot deviation	Robotics Layer	L6, L14
Regulatory corruption	Gov Layer	L11, L13, L15
Human deception	PS-X	L6, L11, L12