NOVAK PROTOCOL SERIES

Part 7: Security Model & Threat Surfaces

Adversarial Analysis and Defensive Architecture

Authoritative Edition

The Core Security Axiom

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

NOVAK eliminates this possibility.

9 Major Threat Domains

1. Hardware
2. Firmware
3. OS Kernel
4. Network
5. API / App
6. AI / Model
7. Robotics
8. Gov / Reg
9. Psycho-Social

1. Hardware Threats (PL-X)

Threats

- Voltage Glitching
- Clock Skew
- Hardware Trojans

Defense

- ✓ PL-X Metastability Detection
- ✓ Device-Hash Binding
- ✓ Drift-Profile Sealing

2 & 3. Firmware & OS

Firmware

Prevents pre-boot malware and malicious flashing.

- Immutable regions.
- PUF-anchored boot.

OS Kernel

Prevents rootkits and syscall hooking.

- Determinized syscall graph.
- Identity-bound processes.

4 & 5. Network & API

Network

Stops replay attacks and routing manipulation.

- Identity-bound packets.
- Monotonic timestamp lineage.

API / App

Stops injection and schema violations.

- Schema-lock via HD hashing.
- Pure functions only.

6. AI / Machine Learning

The Threat

Hallucinations, stochastic outputs, model drift, and prompt exploitation.

The Defense

Determinized inference graphs, model-weight hashing, and output pre-computation.

> ⚠ **Critical:** NOVAK is the antidote to undeterministic AI behavior.

7 & 8. Robotics & Government

Robotics

Prevents sensor spoofing and motion drift.

- Identity-bound movement.
- Safety Gate trajectory prediction.

Government

Prevents corruption and hidden data.

- Immutable audit lineage (RGAC).
- Rule determinism (L13).

- Fraud & Lying
- Social Engineering
- Insider Threats

Intent-Profile Hashing

APTs | **Quantum** | **Deepfakes**

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

Prevents:

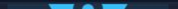
- Silent log mods.

Enforces:

- Identity-Bound (EIR).

Threat	Layer	Prevention
Hardware Tamper	PL-X + SG	LO, L6, L8

APTs



Quantum

Deepfakes

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

Prevents:

- Silent log mods.

Enforces:

- Identity-Bound (EIR).

Threat	Layer	Prevention
Hardware Tamper	PL-X + SG	LO, L6, L8
Kernel Tamper	OS + RGAC	L2-L4, L11

NOVAK Protocol Standards Series