📘 PBAS CATEGORY DEFINITION — NOVAK Protocol

Proof-Before-Action Systems (PBAS)
Global Category Definition & Formal Classification Document
Version 1.0 — January 2025
Author: Matthew Novak
Standards Alignment: SP-1, SP-2, SP-3, Laws L0–L15, PL-X, PS-X

Save as:

```
/standards/NOVAK_PBAS_Category_Definition.md
```

PBAS — PROOF-BEFORE-ACTION SYSTEMS

A New Scientific Category Introduced by the NOVAK Protocol

Just as Bitcoin defined an entirely new category (“cryptocurrency”), and blockchain defined a new category (“decentralized consensus”), **NOVAK defines a new cryptographic class of systems:**

🟦 PBAS — Proof-Before-Action Systems

A PBAS is any system whose **execution is conditioned on a validated, cryptographic, identity-bound proof produced *before* the action occurs**, rather than logs, certification, or audit after the fact.

PBAS represents the **first new computational safety category in over 15 years**.

PBAS is not blockchain, not AI, not cybersecurity, not cryptography-as-usual —
it is a **new governance primitive**.

Table of Contents

---

1. Purpose of PBAS

To formally define the new category introduced by the NOVAK Protocol:

- Provide a **scientific definition**
- Establish **minimum characteristics**

- Differentiate PBAS from all other computing paradigms
- Enable regulation, procurement, and academic classification
- Allow other researchers to build PBAS-compliant systems

Bitcoin created “cryptocurrencies.”
Blockchain created “distributed ledgers.”
NOVAK creates **PBAS**.

---

2. Category Definition (Authoritative)

A **Proof-Before-Action System (PBAS)** is a computational or socio-technical system in which:

> **No state transition, output, or action may occur until its governing rule, input data, expected output, identity, and timestamp have been cryptographically proven valid, bound together, and checked against deterministic safety constraints.**

PBAS requires:

- **pre-execution verification**
- **deterministic rules**
- **identity-bound proofs**
- **global audit lineage**
- **protection against human, machine, and physical adversaries**

PBAS is the enforcement mechanism for a **mathematical rule-of-law** in digital systems.

---

3. Required Category Characteristics

PBAS systems MUST satisfy all 10 requirements:

#	Requirement	Description
1	**Pre-Execution Proof**	Proof must occur *before* execution.
2	**Deterministic Rule Set**	No nondeterminism in rule enforcement.
3	**Identity-Bound Outputs**	Results tied to a responsible entity.
4	**Bound Input-Rule-Output**	Via HVET or equivalent binding.
5	**Irreversible Lineage**	Execution receipts form RGAC or equivalent.
6	**Human-Adversary Resistance**	Must include PS-X-class protections.
7	**Physical Adversary Resistance**	Must include PL-X-class protections.
8	**Global Verifiability**	Proof must be objectively checkable.
9	**Non-Overrideability**	No actor may bypass proof requirements.
10	**Universal Auditability**	Any actor can verify without permission.

If all 10 conditions are met → system qualifies as PBAS.

If any condition fails → system is *not* PBAS.

4. Distinction From All Existing Fields

PBAS does **not** fall into:

- cybersecurity
- blockchain
- AI alignment
- trust frameworks
- logging/forensics
- deterministic computing

- rules engines
- compliance systems
- IDS/IPS
- data integrity verification

PBAS is a **new category** because:

- It is *not about after-the-fact detection*
- It is *about before-the-fact prevention*
- It enforces execution determinism and verifiability
- It integrates human, regulatory, physical, and cryptographic domains
- Its primary operation is **governance**, not computation

---

5. PBAS vs Blockchain

PBAS	Blockchain
Local	Distributed
Pre-execution	Post-execution
Proof required before acting	Log appended after acting
No consensus required	Consensus required
Instant	Latency dependent
Regulatory enforceability	Regulatory ambiguity
Protects automated decisions	Records automated decisions

PBAS is to blockchain what **preventive medicine** is to **autopsy**.

6. PBAS vs Logging / SIEM / Audit

PBAS is **not** monitoring.
PBAS **prevents** harm instead of documenting it.

PBAS	Logging/SIEM
Blocks bad action	Records bad action
Zero trust in all actors	Trusts logs to be truthful
Pre-execution	Post-execution
Deterministic	Forensic

PBAS replaces entire categories of forensic systems.

7. PBAS vs Zero-Trust

PBAS does not trust:

- actors
- rules
- inputs
- hardware
- software
- timestamps

Zero-trust = “verify identity at edges.”
PBAS = “verify the entire truth before action.”

PBAS includes Zero-Trust principles **but is not Zero-Trust**.

8. PBAS vs AI Safety

PBAS is **stronger**:

- AI safety → “align behavior eventually”
- PBAS → “block unsafe behavior instantly”

AI safety relies on detection, heuristics, and model shaping.
PBAS requires **proof of correctness before execution**.

PBAS eliminates:

- hallucination-driven harm
- model deviation
- output non-determinism
- manipulation vulnerabilities

PBAS is the only model capable of **closing the AI safety loop.**

9. PBAS vs Robotics Safety

Robotics safety frameworks (ANSI/RIA, ISO 10218):

- warn
- detect
- slow down
- stop on impact

PBAS:

- **prevents the unsafe command from ever being issued**
- blocks unverified paths
- ensures deterministic motion planning
- enforces rule compliance at machine speed

Robotic automation without PBAS is fundamentally unsafe.

---

10. PBAS Component Requirements

A PBAS system must include:

10.1 Execution Binding

HVET or equivalent cryptographic binding.

10.2 Pre-Execution Receipt

EIR or equivalent.

10.3 Recursive Audit Chain

RGAC or equivalent.

10.4 Deterministic Safety Layer

Safety Gate (SP-3 compliant).

10.5 Adversary Protections

PL-X
PS-X
AI Adversary Model
Robotic Adversary Model
Regulatory Adversary Model

10.6 Public Verifiability

Anyone can check the proof.

---

11. PBAS Compliance Tiers

Tier	Description
PBAS-1	Partial compliance (no PL-X or PS-X)
PBAS-2	Full pre-execution proof
PBAS-3	Full PL-X + partial PS-X
PBAS-4	Full PS-X + PL-X
PBAS-5	Full PBAS compliance (NOVAK-level)

NOVAK is PBAS-5.

---

12. PBAS Applications (Global)

- U.S. Federal Agencies
- Healthcare
- Financial Systems
- Insurance Rating
- Critical Infrastructure
- Robotics & Manufacturing
- Aviation & Aerospace
- AI Content Governance

- Claims Processing
- Public Sector Integrity
- Military Execution Systems
- Legal Adjudication
- Election Integrity

PBAS is universal.

---

13. PBAS Scientific Significance

PBAS introduces:

- a new computational integrity primitive
- a new scientific field
- a new execution model
- a new safety regime
- a new adversary taxonomy
- a new class of proofs
- a new regulatory mechanism

PBAS enables:

- provably safe automation
- deterministic AI governance
- state-protected integrity

- global execution standards

PBAS is to execution integrity what **public-key cryptography** was to authentication.

---

14. PBAS Market Significance

PBAS unlocks:

- new government modernization markets
- enterprise integrity frameworks
- AI governance platforms
- robotics safety infrastructure
- financial correctness verification
- certification and audit markets

Like blockchain, PBAS will create its own industry.