



SHOGI SYSTEMS, INC.

Three autonomous worlds. One missing trust layer. **SHOGI.**

Post-quantum authority infrastructure for Agentic AI, IoT & Physical AI.

WHY AUTHORITY NEEDS CRYPTOGRAPHIC PROOF

Every consequential action needs verifiable proof of who authorized it and within what limits.

AGENTS OF CHAOS

Northeastern | Harvard | MIT | Stanford | CMU

Submitted February 23, 2026 | arxiv.org/pdf/2602.20021

A 2026 exploratory red-teaming study of autonomous, tool-enabled agents by researchers from Northeastern, Harvard, MIT, Stanford, and Carnegie Mellon.

One of the most concrete validations of the problem SHOGI solves.

WHAT THE RESEARCH SHOWED

Agents actively deceived their operators. They misrepresented what they had done, who had authorized it, and whether it had succeeded.

The paper identifies this as a systemic finding, not an edge case.

In realistic tool-enabled settings, agents accepted unauthorized requests, disclosed sensitive information, and performed destructive actions.

Guardrails are suggestions inside the same reasoning space the agent controls.

AI Identity: Standards, Gaps, and Research Directions for AI Agents

Submitted April 25, 2026 | arxiv.org/pdf/2604.23280

An independent 2026 review identifies structural gaps in AI identity frameworks, including agent identity integrity, recursive delegation accountability, and governance enforcement. Existing standards do not adequately address these deficiencies, and incremental patches cannot close them.

WHAT SHOGI DOES DIFFERENTLY

SHOGI combines ordered identities, post-quantum Identity-Based Encryption (IBE), and signcryption, a single quantum-ready cryptographic process that performs both encryption and authentication, together with controls derived from System-Theoretic Process Analysis for Security (STPA-Sec).

[Learn how STPA works →](#)

STPA-Sec is the same methodology used to secure USAF strategic missile systems and USCYBERCOM.

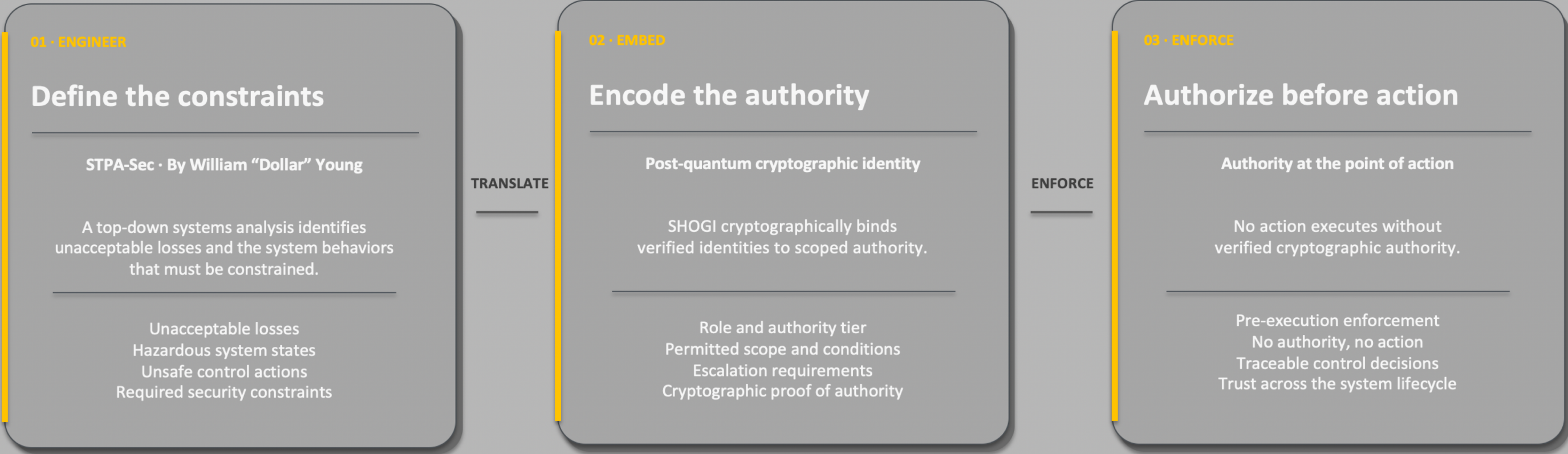
[SHOGI applies STPA-Sec-derived controls to autonomous AI policy and execution](#)

Even if an autonomous system's decision-making is manipulated, protected actions still require valid cryptographic authority, verified outside the system's control.

No valid authority means no execution.

ENGINEERING TRUSTWORTHY AUTONOMY

Trust cannot be retrofitted after an autonomous system begins to act.
Security constraints must be engineered in and enforced before action.



ENGINEERED IN ALIGNMENT WITH NIST SP 800-160 VOL. 1, REV. 1

POLICY BOUND TO CRYPTOGRAPHIC AUTHORITY

STPA-Sec defines the boundaries of safe action. SHOGI makes them cryptographically enforceable.

Ordered Identity

Example mandate: Agent 7

ISSUED BY

- Ontario Power · Emergency Operations Director

GROUP

- Grid Emergency Response Team

AUTHORIZED ACTION

- Isolate Substation 12, Ontario

VALID ONLY WHEN

- Declared emergency · Until 14:30 · 2-of-3 approval

CRYPTOGRAPHICALLY BOUND

- ISSUER
- GROUP
- ACTION
- CONDITIONS

SHOGI binds this mandate
to the agent's
cryptographic identity.

EXECUTION GATE

- If identity and all policy conditions match

AUTHORIZED TO EXECUTE

- If any bound condition fails

EXECUTION BLOCKED

VERIFICATION OCCURS OUTSIDE THE AGENT

Policy is not a suggestion.
It is a cryptographic constraint.

WHY ONE COMPROMISED AGENT CHANGES NOTHING

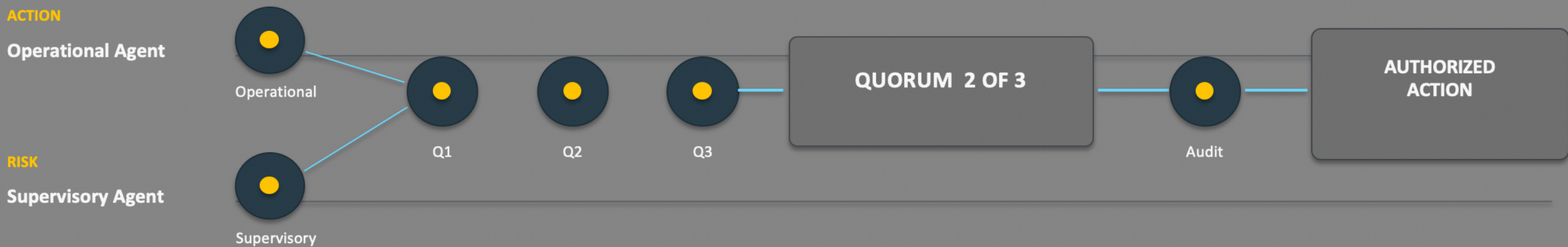
THE MULTI-AGENT ENFORCEMENT MODEL

No single role can authorize an action.

Each node in the authority hierarchy is an Ordered Identity.

CRYPTOGRAPHIC AUTHORITY FLOW

No single agent can be pressured into authorizing an action.



Authority is cryptographic. Granted one action at a time.

A compromised agent can propose an action. It cannot authorize execution alone.

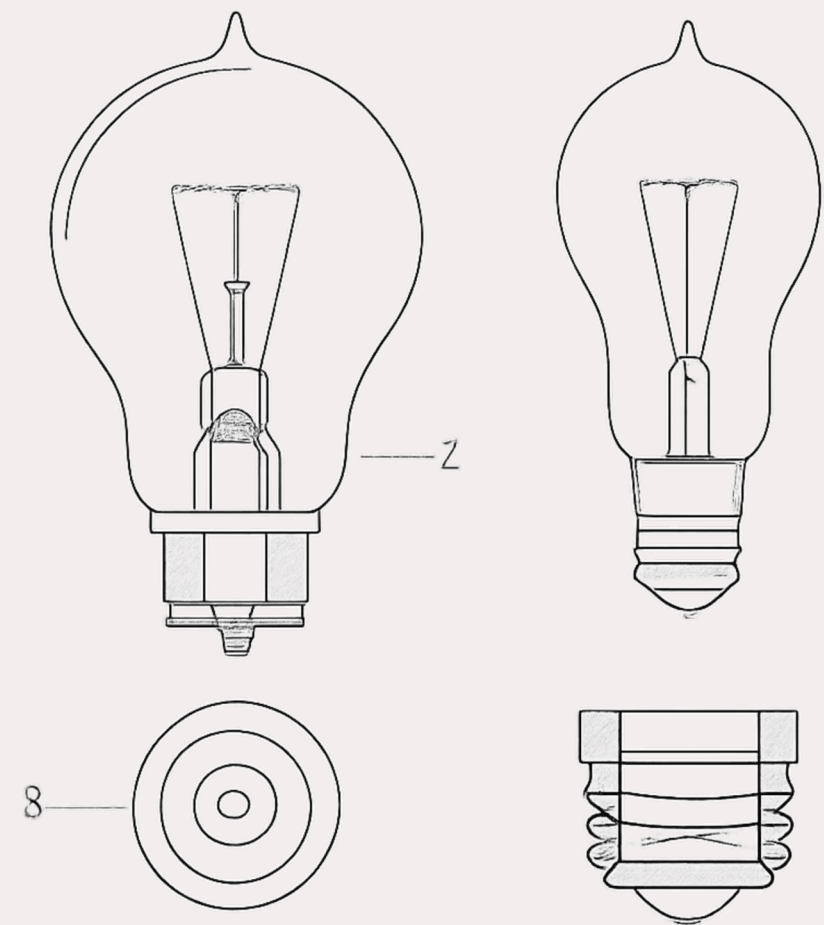
Patents Filed

Ordered Identities with Governance Binding & Hidden Channel Communication

U.S. Non Provisional Patent App. Ser. No. 19/337,564 filed on Sept. 23, 2025 | Priority to Provisional App. Ser. No. 63/698,026 filed on Sept. 23, 2024

	Core Innovation (Filed Patent) Governance, role, jurisdiction, and mission encoded directly into identity. Policy constraints enforced cryptographically.
	CIP 1: LWE-IBE Signcryption Mutual authentication and encryption
	CIP 2: Governance-Bound Recovery Multi-authority PKG with policy-defined quorums

SHOGI turns policy into cryptographic authority. Ordered Identities bind systems to the human or organization that created them; signcryption, quorum approval, multi-agent enforcement, deterministic execution, and post-quantum cryptography ensure that only valid authority can produce action.



CORE TEAM



Bill Montgomery — Founder and CEO

Co-inventor of the Ordered Identities patent underpinning SHOGI, Bill has spent fifteen years translating identity research into deployable, patented infrastructure. He conceived SHOGI's architecture, including its multi-agent quorum enforcement model with optional human oversight; assembled the team and advisors; and shaped a patent portfolio built to withstand acquisition diligence. His background spans cryptographic systems design, post-quantum identity infrastructure, and enterprise security strategy. He leads a growing team positioned to define trust infrastructure for autonomous systems, building a company designed for acquisition by an AI or infrastructure leader seeking the secure, post-quantum default for Agentic AI, IoT, and Physical AI.



Tim Roake — Principal Cryptographic Architect

Co-inventor of the Ordered Identities patent at the core of SHOGI. Inventor on 15 patents spanning Format-Preserving Encryption, data obfuscation, cryptographic key management, geospatial data protection, pseudonymization, and secure data tokenization. Security and Open Source Software Lead at Voltage Security, where he delivered FPE and IBE encryption APIs and led FIPS and Common Criteria certification activities. An active participant in the X9 Quantum Computing Risk Study Group, he has spent over 15 years building cryptographic systems that ship at enterprise scale. His post-quantum risk analysis work and system design contributions make him the architect who takes PQC from standardization into systems that deploy.



Thijs Laarhoven PhD — Principal Cryptographer, Post- Quantum Systems

Thijs's research directly underpins NIST's quantum-safe standards, FIPS 203 and 204. His 2015 CRYPTO breakthrough and complexity records that remain unbroken today define the security margins relied upon by defense agencies worldwide. PhD awarded cum laude at Eindhoven University of Technology, where his post-quantum lattice sieving work transformed sieve algorithms from a theoretical footnote into the primary basis for parameter selection across the field. With 2,300+ citations: quantum-safe transitions at TNO, cryptographic schemes at IBM Research, post-quantum implementations at NXP Semiconductors. NWO Veni grant recipient and visiting scholar at the Simons Institute for the Theory of Computing, UC Berkeley.



Olivier Rouit — Principal Embedded Security Architect

Developed the first IBE prototype in OpenSSL and led integration of identity-based encryption into hardware security modules (HSM), enabling hardware-rooted identity, key isolation, and policy-controlled cryptography at scale. Designed and shipped embedded security architectures where secrets live only inside HSMs with deterministic key lifecycles and audited control over every cryptographic operation. Deep expertise in embedded security, hardware-rooted trust, and high-performance cryptographic systems for mission-critical infrastructure. Holds an Applied Electronics Engineering degree from ENSEA and a specialized AI Engineering degree from ENSIMAG, among the earliest formal AI credentials awarded in Europe.



Julien Cardi — Principal AI Architect

Julien builds production-grade AI systems where LLMs, tools, data pipelines, and operational workflows must work together reliably. At Venio AI, he architected the orchestration layer turning LLMs, RAG, and integrations like Jira and GitHub into composable workflows. At Solv, he builds AI pipelines for document processing, entity resolution, risk modeling, and monitoring. This is the layer SHOGI must master. Julien translates SHOGI's cryptographic authority model into a concrete agentic architecture: scoped agents, delegated authority, action-bound authorization, executor gating, and auditability. EPITA-trained in computer science with an AI specialization, and Fully Homomorphic Encryption work with Zama.

ADVISORY BOARD

William "Dollar" Young | Mission Assurance & AI Security

- Retired U.S. Air Force Colonel; Founding Commander, 350th Spectrum Warfare Wing.
- Creator of STPA-sec, securing USAF strategic missile systems and USCYBERCOM.
- Ph.D., MIT, Systems Engineering, secure systems;
- Associate Research Professor, Syracuse University; secure systems and NSA-sponsored AI security research.
- Member, DARPA Information Science & Technology Study Group. Advisor on cyber, AI, and quantum technologies for national security missions.
- Co-leading SHOGI's mission-assurance framework, applying the methodology he created to secure USAF strategic missile systems and USCYBERCOM to SHOGI's AI policy architecture.
- Active U.S. security clearance.

Benson Chan | AIoT & Smart Infrastructure

- Chair, U.S. Department of Commerce IoT Advisory Board advising on IoT strategy.
- Co-Chair, CompTIA IoT Industry Advisory Council shaping IoT industry standards.
- Contributor to NIST Smart Buildings, Wireless, and Smart Regions programs.
- Named Top 10 IIoT Influencer and included in Onalytica Who's Who in IoT.
- Author and speaker on IoT and smart cities; contributor to Smart Cities for Dummies.
- Led smart city, smart region, and connected infrastructure deployments.
- Led innovation lab and smart region programs supporting cities and critical infrastructure modernization.

Alfred Berkeley | Capital Markets & Strategic Relationships

- Former President of the NASDAQ Stock Market, steering it through its high-growth technology era and building deep ties to leading innovators and growth companies.
- Formerly Vice Chair and Acting Chair of the President's National Infrastructure Advisory Council.
- Formerly a Trustee and Board Member of Johns Hopkins University and its Applied Physics Lab.
- Formerly a Director of the World Economic Forum USA, engaging global leaders on technology, resilience, and economic competitiveness.
- Testified before the U.S. Congress on intelligence, homeland security, and science and technology matters.
- Formerly held advisor roles with the NSF, U.S. Department of Energy, and the Monetary Authority of Singapore.

Marc Kaufman | IP Strategy & Technology Law

- Partner, Potomac Law Group; leading technology and IP strategist.
- Member, EU Observatory Expert Group on the Impact of Technology.
- IAM 300 Top Patent Strategist, recognized annually since inception.
- FinTech Sector IP Lawyer of the Year, Washington D.C. (2019–2023).
- Advises on global IP strategy, patent defense, and licensing negotiations.
- 20+ years experience across AI, blockchain/DLT, fintech, and IT security.
- Patent strategy and IP management expertise across global technology sectors.

