

Authority Engineering: A Taxonomy of Consequence Regulation

Rob Caswell

Authority Engineering

May 2026

Rob Caswell | [linkedin.com/in/rob-caswell3](https://www.linkedin.com/in/rob-caswell3)

Publication Record

Authority Engineering: A Taxonomy of Consequence Regulation

Author: Rob Caswell

Publisher: Cyber Terrain LLC

Published: 2026-05-01

Zenodo version: v1.0

DOI: <https://doi.org/10.5281/zenodo.21742245>

Website: <https://cyberterrain.ai/papers/authority-engineering-taxonomy.pdf>

Corpus Context

Corpus: Authority Engineering

Document ID: AE-TAX-0001

Object family: AE-TAX-0001

Publisher-imprint edition prepared for versioned republication.

The prior Zenodo record remains the citable record until its new version is published.

1. Purpose of the Taxonomy

This taxonomy provides a systematic classification framework for modeling, analyzing, and regulating how potentiality transforms into material constraint within organizational, computational, and autonomous systems. Traditional governance and control frameworks classify parameters based on *execution* (e.g., who executed an action, what process was run). This framework classifies systems based on *consequence*.

The primary objective of this taxonomy is to map the structural path through which authority moves, identify thresholds of realization, apply localized constraints, and diagnose failure modes under stress. This classification enables engineers, security architects, and operators to design predictable controls before a system commits to an un-governed state transition.

2. Ontological Baseline

This taxonomy assumes a three-part minimal ontology as its conceptual foundation. The properties classified in subsequent sections are emergent structural behaviors of these three irreducible primitives:

- Authority: The descriptive, factual capacity to expand, contract, or manipulate the boundary of reachable future states within a system boundary.
- Consequence Seam: The definitive phase-shift boundary at which authority-bearing possibility transitions into binding reality. It represents the final threshold where alternative futures remain viable and operational intervention can occur.
- Consequence: A binding state transition that collapses alternative possibility spaces and deposits a material constraint on the system's future state space.

3. Taxonomy Layer 1: Authority Structures

Authority is not an abstract, formless variable; it possesses an intrinsic geometry within a system. The layout and dynamics of this geometry dictate how potential state manipulation is organized and accessed.

- Authority Surfaces: The specific geometric exposure windows, interfaces, or entry points where latent authority is accessible within a system topology.
 - *Examples:* Active API tokens, cryptographic private keys, administrative session endpoints, configuration files.
- Authority Paths: The sequential, causal, or structural routes through which authority travels or mutates as it moves across a system toward a boundary.
- Delegation Chains: The structural vectors through which authority is transferred or redistributed across entities, increasing the distance between the originating intent and eventual realization.

- Escalation: The dynamic expansion of an entity's reachable consequence space, structurally altering their proximity to a seam or concentrating authority at a higher node.
- Authority Accumulation Point (Authority Well): The topological phenomenon where potential state-manipulation capacity naturally pools or concentrates around specific paths, roles, or surfaces over time, creating high-consequence choke points.

4. Taxonomy Layer 2: Consequence Classification Matrices

To evaluate a system, a practitioner must classify a consequence not merely as a generic event, but as a multi-dimensional intersection of its Domain, Persistence, and Scope. A consequence is defined by how it collapses a possibility space.

4.1 Consequence Domain

Classifies the specific category of systemic reality that is altered or constrained by the state transition:

- Resource: The permanent consumption, reallocation, or depletion of liquid assets, compute credits, storage volume, or physical inventories.
- Information: The irreversible exposure, leakage, or unalterable destruction of data assets, cryptographic secrets, or system state visibility.
- Authority (Recursive): A state transition whose consequence is the structural modification of the authority topology itself (e.g., creating a new API key, mutating permissions, granting administrative rights).
- Physical: Kinetic or environmental transformations, including device destruction, facility lockouts, hardware ignition, or human safety impacts.
- Obligation: The binding establishment of legal, contractual, compliance, or systemic liabilities that constrain future institutional maneuvers.

4.2 Consequence Persistence

Classifies the baseline resilience and resource cost associated with counteracting or modifying a realized constraint:

- Ephemeral: The constraint naturally decays or resets over a predictable temporal baseline without requiring active intervention.
- Durable: The constraint remains active indefinitely until a subsequent, distinct authority path crosses a separate seam to explicitly remediate it.
- Permanent (Invariant): The constraint cannot be counteracted or altered by any systemic authority vector; it represents an immutable transformation.

4.3 Consequence Scope

Classifies the blast radius and cascading impact of the state constraint across systemic boundaries:

- Local: The constraint is completely contained within the specific sub-system or node where the seam-crossing occurred.
- Systemic: The constraint propagates across internal dependencies, degrading or altering the possibility spaces of adjacent applications, environments, or networks.
- Ecological: The constraint breaches organizational boundaries, inducing cascading failures or imposing un-governed constraints on external third-party providers, clients, or foundational infrastructure layers.

5. Taxonomy Layer 3: Governance Structures

Governance structures are the evaluative and qualitative frameworks that systems use to recognize, categorize, and condition the movement of authority relative to consequence seams.

- Recognition: The primary governance act of identifying a raw, factual capacity to manipulate states as an object worthy of system evaluation.
- Legitimacy: The evaluative determination that a recognized authority vector matches general institutional policies, roles, or organizational rights. Legitimacy is general and actor-centric; it answers whether a capability *should* be accepted in a broad sense.
- Admissibility: The context-specific evaluation of whether an authority vector is permitted to pass through a *specific* consequence seam under current, real-time conditions. Admissibility is strictly context-specific and seam-local.
- Governance Constraints: The rules, policies, cryptographic bounds, and compliance matrices used to mathematically or procedurally define permitted authority traversals.
- Seam-Crossing Conditions: The technical outputs generated when an admissibility engine certifies that an inbound authority vector satisfies all required governance constraints to alter state.

6. Taxonomy Layer 4: Engineering Structures

Engineering structures are the concrete, deterministic mechanisms embedded within systems to execute governance judgments and physically control seam-crossings.

- Sovereignty: The absolute, localized capacity to evaluate and decide admissibility at a specific consequence seam. Sovereignty is a local property of technical components rather than a global institutional attribute.
- Stops: The localized physical or logical enforcement mechanisms positioned directly on a consequence seam to arrest, alter, or permit an authority traversal based on an admissibility output. A stop is defined by its capacity for *intervention*, not observation.

- Enforcement: The operational translation of a sovereign admissibility decision into a physical or computational change in state outcomes via a stop.
- **The Locality Principle**: The structural requirement dictating that because consequence occurs locally, the engineering architecture for sovereignty, stops, and enforcement must converge directly at the consequence seam to achieve preventative control.

7. Taxonomy Layer 5: Diagnostic Failure Modes

Systems fail when their engineering layouts decouple governance intent from consequence seams, or when they misclassify structural variables. Practitioners can utilize this section as a diagnostic catalog to audit structural vulnerabilities.

7.1 Authority Dynamics Failures

- Authority Discovery Failure: An architecture fails to inventory its real capacities, allowing hidden, latent, or un-mapped capabilities to exist completely un-monitored until an incident occurs.
- Authority Surface Drift: The unintentional modification or exposure of interfaces over time (e.g., undocumented API additions, dangling cloud permissions), opening un-tracked windows into the system topology.
- Delegation Opacity: The decay of structural visibility that occurs as delegation chains lengthen, hiding the mutation, dilution, or drift of originating intent from downstream realization points.
- Legitimacy/Authority Confusion: A catastrophic category error where a system treats a general policy status (Legitimacy) as proof of operational control, or conversely, assumes that a lack of institutional right (an unauthorized attacker) equates to a lack of factual capability (Authority).
- Authority Accumulation Collapse: A vulnerability where too many diverse authority paths pool into a single node or credential over time, creating a massive choke point that, if compromised, exposes the entire systemic possibility space.

7.2 Boundary and Control Failures

- Execution Fixation: A pathological focus on monitoring, validating, and logging execution parameters while remaining completely blind to the overarching paths through which authority transforms into systemic constraint.
- Seam Blindness: An architectural failure where an enterprise accurately maps its administrative roles and identity directories but cannot locate or identify the precise phase-shift boundaries where binding constraints occur.
- Sovereignty Without Enforcement: A structural flaw where a node has the logical capacity to evaluate and declare a transaction inadmissible, but lacks a local stop mechanism to physically prevent the seam crossing.

- **Stop Displacement:** Positioning an enforcement mechanism upstream or downstream from the true consequence seam, allowing authority to bypass the check via alternative execution paths or commit state before validation occurs.
- **Post-Consequence Governance:** Relying on forensic auditing, incident logging, or reactive alerting to manage risks that have already passed through a seam and spent their potentiality.

7.3 Cascading and Systemic Failures

- **Semantic Mutation Drift:** Occurs primarily in abstract computational traversals (e.g., multi-agent LLM loops) where high-level human intent degrades or twists as it translates across nested machine steps, executing an unintended consequence at the seam.
- **Consequence Cascading:** An architectural failure where a local consequence changes state variables that automatically satisfy the seam conditions of adjacent, downstream systems, triggering a chain reaction of un-governed possibility collapses across the environment.
- **Governance Velocity Mismatch:** A condition where autonomous agent workflows generate decisions, traverse paths, and hit consequence seams at machine speed, completely outpacing the evaluation loops of human governance or centralized security logging infrastructure.

Contemporary Example: The AI Sync Crisis can be understood as a large-scale manifestation of Governance Velocity Mismatch and Consequence Cascading within machine-speed computational environments.

8. System Archetypes: Taxonomy Application Guide

To classify an active environment using this taxonomy, a practitioner must isolate five core structural markers: [Authority Surface], [Consequence Domain & Scope], [Consequence Seam], [Sovereign Locus & Stop], and [Primary Failure Mode].

8.1 Autonomous Agent Swarms (LLM/API Orchestrations)

- **Authority Surface:** Active API tokens and liquid compute credit balances.
- **Consequence Profile:** *Domain:* Resource & Authority | *Persistence:* Durable | *Scope:* Systemic.
- **Consequence Seam:** The strict validation gateway at the API host layer that evaluates whether an inbound payload can modify state.
- **Sovereign Locus & Stop:** The API Gateway enforcement engine validating traffic against active tokens.
- **Primary Failure Mode:** *The AI Sync Crisis* and *Delegation Opacity* caused by the infinite variation of semantic prompts outpacing traditional monitoring logs.

8.2 Smart Contracts and DeFi (Automated State Machines)

- Authority Surface: Cryptographic possession of private keys and network gas tokens.
- Consequence Profile: *Domain*: Resource | *Persistence*: Permanent | *Scope*: Ecological.
- Consequence Seam: The exact *block inclusion step* where the distributed consensus engine permanently commits the transaction to the state trie.
- Sovereign Locus & Stop: The decentralized consensus network nodes executing transaction validation.
- Primary Failure Mode: *Stop Displacement* or *Seam Blindness*, occurring when developers assume that signing a payload or executing local node code constitutes final realization.

8.3 Malicious and Unauthorized Systems (The Adversarial Invariant)

- Authority Surface: An adversary discovers or manufactures persistence vectors, establishing factual capacity to alter configurations.
- Consequence Profile: *Domain*: Information & Physical | *Persistence*: Durable (or Permanent without backups) | *Scope*: Systemic.
- Consequence Seam: The threshold where the operating system's kernel executes the raw write-operation to disk storage.
- Sovereign Locus & Stop: A kernel-level Endpoint Detection and Response (EDR) driver blocking unauthorized encryption patterns directly at the file-system I/O queue.
- Primary Failure Mode: *Legitimacy/Authority Confusion* or *Post-Consequence Governance*, where security teams focus on monitoring access rights rather than hard-stopping unauthorized file mutations at the disk boundary.

8.4 Nuclear Command Structures (Analog High-Consequence)

- Authority Surface: Concurrent physical possession of matching launch codes and specialized enablement keys.
- Consequence Profile: *Domain*: Physical | *Persistence*: Permanent | *Scope*: Ecological.
- Consequence Seam: The physical and electronic logic circuit inside the launch facility that converts concurrent key turns into an ignition signal.
- Sovereign Locus & Stop: The physical silo launch control hardware.
- Primary Failure Mode: *Sovereignty Without Enforcement*, which would occur if central command retained the sole right to authorize strikes but lost the localized communications infrastructure needed to mechanically prevent or initiate a silo deployment.

9. Structural Reference Matrix

The following index combines the taxonomy layers into a repeatable profiling instrument for system analysis:

Taxonomy Layer	Component	Core Classification Question for Practitioners	Operational Target
1. Authority Structures	<i>Authority Surface</i>	Where does potential capacity interface with the system?	Interface / Entry Points
	<i>Authority Path</i>	What logical routing allows authority to approach the seam?	Traversal Geography
	<i>Delegation Chain</i>	How far has intent traveled from its origin point?	Structural Alignment
	<i>Accumulation Point</i> (<i>Authority Well</i>)	Where does state-manipulation capacity naturally pool?	High-Risk Choke Points
2. Consequence Classification	<i>Consequence Domain</i>	What category of systemic reality is altered or constrained?	Impact Profiling
	<i>Persistence</i>	What is the structural cost to counteract this constraint?	Resilience Metric
	<i>Scope</i>	What is the blast radius across systemic boundaries?	Blast Radius Bound

Taxonomy Layer	Component	Core Classification Question for Practitioners	Operational Target
	<i>Consequence Seam</i>	Where does potentiality harden into an invariant fact?	Phase-Shift Threshold
3. Governance Structures	<i>Recognition / Legitimacy</i>	Is the authority vector tracked and policy-authorized?	Institutional Appraisal
	<i>Admissibility</i>	Is this traversal justified at this specific boundary now?	Context-Local Rules
4. Engineering Structures	<i>Sovereignty</i>	Which local node possesses the capacity to decide?	Locus of Control
	<i>Stop</i>	What mechanism translates policy into active intervention?	Deterministic Gate
5. Diagnostics	<i>Failure Mode</i>	Which structural misalignment decoupled intent from the seam?	Architectural Faults

10. Practitioner Verification Test

A taxonomy is only useful if it can be applied consistently to real systems. When analyzing a high-consequence workflow, practitioners should be able to identify at minimum:

1. The Authority Surface through which consequential capacity enters the system.
2. The Consequence Profile (Domain, Persistence, and Scope) associated with the targeted state transition.
3. The Consequence Seam where potentiality becomes binding reality.

4. The Sovereign Locus and Stop responsible for regulating seam crossing.
5. The Primary Failure Mode most likely to decouple governance intent from consequence realization.

If any of these elements cannot be identified, the system is likely suffering from *Seam Blindness*, *Execution Fixation*, *Authority Discovery Failure*, or an equivalent structural classification failure. Consequence regulation cannot be reliably engineered until these core elements are visible and mappable.