

Authority Surface Index (ASI): Measuring Consequential Authority in Automated Systems

Rob Caswell

Authority Architecture Research Series

March 2026

Rob Caswell | @rob-caswell3

Publication Record

Authority Surface Index (ASI): Measuring Consequential Authority in Automated Systems

Author: Rob Caswell

Publisher: Cyber Terrain LLC

Published: 2026-03-01

Zenodo version: v1.0

DOI: <https://doi.org/10.5281/zenodo.21742303>

Website: <https://cyberterrain.ai/papers/authority-surface-index.pdf>

Corpus Context

Corpus: Authority Engineering

Document ID: AE-SURF-INDEX-0001

Object family: AE-SURF-INDEX-0001

Publisher-imprint edition prepared for versioned republication.

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

Table of Contents

Introduction

The Authority Measurement Problem

Authority Surface as Structural Topology

Structural vs. Behavioral Metrics

The Authority Surface Index (ASI)

Formal Model of Authority Engineering

6.1 Authority Surface Definition

6.2 Weighted Authority Surface

6.3 Authority Surface Balance Law

6.4 Phase Transition Condition

6.5 Authority Surface Index

6.6 Minimal Formal System

Interpreting the Authority Surface Index

Application to AI and Automated Systems

Authority Engineering Integration

Conclusion

Example ASI Calculation

References

Appendix A — Mathematical Foundations of Authority Engineering

Equation 1 — Authority Surface

Equation 2 — Weighted Authority Surface

Equation 3 — Authority Surface Balance Law

Equation 4 — Authority Phase Transition

Equation 5 — Authority Surface Index

Appendix B — Authority Outcome Primitives

Appendix C — Authority Surface Index Components

List of Figures

Figure 1 — Authority Engineering Stack

Figure 2 — Authority Surface Topology

Figure 3 — Authority Expansion vs Governance Strength

Figure 4 — Authority Surface Index Model

List of Equations

Equation 1 — Authority Surface

Equation 2 — Weighted Authority Surface

Equation 3 — Authority Surface Balance Law

Equation 4 — Authority Phase Transition

Equation 5 — Authority Surface Index

Abstract

Modern cybersecurity measurement focuses primarily on exposure, vulnerability, and exploitability. While these approaches quantify how systems can be reached or compromised, they do not measure the consequential authority embedded within those systems. As automation and artificial intelligence increasingly execute actions across financial, organizational, and physical domains, understanding the magnitude of authority within automated systems becomes essential for governance and risk management.

This paper introduces the Authority Surface Index (ASI), a structural measurement framework designed to quantify the consequential authority embedded within automated architectures. ASI builds upon the concept of the Authority Surface, which defines the topology of reachable consequence transitions across a finite set of authority outcome primitives: money, contract, identity, policy, authority, model behavior, and physical actuation.

The Authority Surface Index measures structural authority magnitude through four components: Authority Execution Score (AES), Constraint Symmetry Score (CSS), Termination Latency Factor (TLF), and Concentration Risk Index (CRI). Together these dimensions quantify the balance between execution capability and governance constraints within automated systems.

By separating structural authority from behavioral activity, ASI measures the potential magnitude of consequential authority embedded within system architecture rather than runtime frequency or attack probability. In this sense, ASI functions analogously to potential energy in physical systems, representing stored consequence capability rather than observed behavior.

The Authority Surface Index serves as the quantitative measurement layer within the broader discipline of Authority Engineering, enabling organizations to analyze, compare, and intentionally design authority architectures as automation and AI expand the reach of machine-executed decisions.

1. Introduction

Modern cybersecurity measurement focuses primarily on exposure, vulnerability, and exploitability. Security programs routinely quantify attack surfaces, catalog software weaknesses, and analyze adversarial pathways through complex systems. These approaches answer essential operational questions: which systems can be reached, which components may fail, and which attack paths adversaries might exploit. Over the past three decades, this perspective has produced sophisticated vulnerability scoring systems, attack graph models, and threat-informed defense frameworks.

However, these approaches share a structural limitation. They measure access, but they do not measure authority.

As computing systems increasingly execute consequential actions in the physical, economic, and legal world, the critical governance question is no longer limited to whether a system can be reached. The more consequential question is what that system is structurally permitted to change.

Modern automated systems routinely possess the ability to transfer financial assets, bind contractual obligations, alter identity records, modify organizational policy, delegate privileges, influence machine behavior, or actuate physical infrastructure. These actions represent consequential state transitions within social, economic, and technical systems. Whether initiated by human operators, automated workflows, or artificial intelligence agents, such transitions carry real-world impact that extends beyond the boundaries of the computing environment itself.

Traditional cybersecurity metrics provide little insight into this dimension of system behavior. A vulnerability score may indicate that a system is exploitable, and an attack surface model may show how adversaries could reach a component. Yet neither measurement answers a more fundamental question: what consequences that system can produce once it is reached.

This distinction becomes increasingly important in environments shaped by automation and artificial intelligence. AI agents, workflow engines, and integrated service platforms frequently operate across multiple systems, interacting through application programming interfaces, identity systems, policy engines, and financial infrastructure. As these systems interact, the reachable consequences of their execution paths expand. Small configuration changes or additional permissions can dramatically alter the range of actions a system can perform, sometimes producing large discontinuities in authority.

In such environments, risk cannot be understood solely in terms of vulnerability or compromise likelihood. The structural authority embedded within a system determines the magnitude of potential consequences. Two systems with identical vulnerability profiles may present radically different systemic risk if one merely reads data while the other can transfer funds, modify policies, or delegate authority.

This paper introduces the Authority Surface Index (ASI), a structural measurement framework designed to quantify the consequential authority embedded within automated systems.

The Authority Surface Index addresses a measurement problem that existing security metrics do not capture: the structural magnitude of authority contained within a system's reachable execution paths. Rather than evaluating vulnerabilities or estimating attack probabilities, ASI measures the consequence-shaping capability of a system. In this sense, ASI measures the potential impact a system can produce if its authority is exercised.

The ASI framework builds upon the concept of the Authority Surface, which defines the topology of consequential state transitions that a system or actor can cause within a broader operational environment. The authority surface represents the set of reachable consequence transitions induced by the system's available permissions, integrations, automation pathways, and delegated capabilities. These transitions are categorized across a finite set of outcome domains, referred to as Authority Outcome Primitives, including financial transfer, legal obligation, identity binding, policy mutation, authority delegation, model behavior modification, and physical actuation.

Within this framework, the authority surface defines the possibility space of consequential system behavior. However, topology alone does not provide a quantitative measurement of authority magnitude. The Authority Surface Index therefore introduces a structural measurement model that quantifies authority exposure across four dimensions: execution capability, constraint symmetry, termination responsiveness, and authority concentration. Together, these dimensions capture the structural balance between a system's ability to produce consequences and the governance mechanisms designed to constrain that capability.

The Authority Surface Index does not measure how frequently authority is exercised, nor does it estimate the probability that a system will be compromised. Instead, ASI measures the potential magnitude of consequential authority embedded within a system's structure. In this sense, ASI functions analogously

to potential energy in physics: it represents the stored capacity for consequential action rather than the rate at which that action occurs.

By quantifying structural authority, ASI enables organizations to analyze and compare the authority exposure of different systems, automation architectures, and AI deployments. The index provides a framework for evaluating whether automated systems possess disproportionate authority relative to their governance controls, and whether authority concentration or delayed termination mechanisms introduce systemic risk.

More broadly, ASI serves as the measurement instrument within the emerging discipline of Authority Engineering, which treats authority not as a role or permission set but as a structural property of reachable consequence transitions within complex systems. Within this discipline, governance becomes the design and control of authority topology, and measurement becomes essential to understanding how authority evolves as systems integrate, automate, and scale.

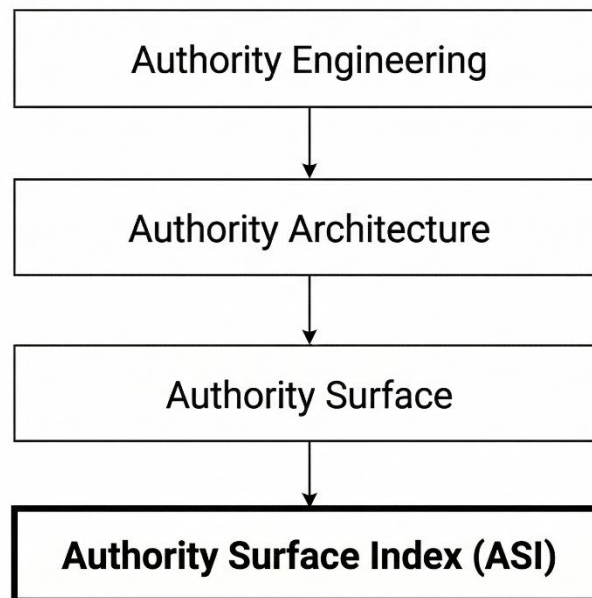


Figure 1 — Authority Engineering Stack

Authority Engineering provides the conceptual framework for authority systems. Authority Architecture defines governance structures, the Authority Surface

defines the topology of consequential authority, and the Authority Surface Index (ASI) provides the quantitative measurement of authority magnitude.

The sections that follow introduce the authority measurement problem, define the structural topology of authority surfaces, and present the Authority Surface Index as a formal model for quantifying consequential authority in automated systems.

2. The Authority Measurement Problem

Security measurement has historically focused on reachability and failure conditions. Vulnerability scanning, attack surface mapping, and threat modeling frameworks attempt to answer a common operational question: where can an attacker gain entry and what weaknesses might allow compromise? Over time, these methods have become increasingly sophisticated. Modern security programs employ vulnerability scoring systems, attack graphs, and adversary simulation techniques to quantify exposure across complex enterprise environments.

These methods are valuable, but they measure only part of the risk landscape.

Most cybersecurity metrics evaluate the likelihood that a system can be accessed or compromised. They measure pathways of entry, exploitable software flaws, and adversarial tactics capable of traversing system boundaries. Yet they rarely measure a second, equally important dimension of risk: the magnitude of consequences a system can produce once authority is exercised within it.

This distinction becomes clearer when examining two systems with identical exposure profiles. Both may run the same operating system, expose the same network interfaces, and contain the same vulnerabilities. From the perspective of conventional security metrics, these systems may appear equally risky. However, if one system merely stores static data while the other can transfer financial assets, bind contractual obligations, or issue administrative policies, their real-world risk profiles differ dramatically.

Traditional security measurement does not capture this difference.

The reason is structural. Existing metrics are designed to measure attackability, not authority. They quantify how adversaries might reach systems and exploit weaknesses, but they do not measure what those systems are empowered to do within the broader operational environment.

This gap reflects an implicit assumption in many security frameworks: that compromise itself is the central event of interest. In practice, however, compromise is only a precursor to consequence. The true impact of a breach depends on what the compromised system is capable of changing.

A system capable only of reading data may expose confidentiality risk. A system capable of transferring funds introduces financial risk. A system capable of altering identity records, modifying policy, or delegating authority may introduce cascading systemic risk. The difference between these cases is not access but consequence power.

Automation and artificial intelligence intensify this measurement gap. Modern systems increasingly operate through chains of automated actions spanning multiple services and infrastructure layers. Workflow engines trigger policy changes, APIs invoke financial transfers, identity systems grant privileges, and machine-learning models modify system behavior. These interactions form complex execution paths in which the authority of one system may unlock the authority of another.

Under these conditions, authority expands through reachable consequence pathways rather than through direct permissions alone. A system that cannot directly transfer money, for example, may still reach financial consequences by invoking a policy engine that authorizes a financial workflow, or by modifying an identity record that grants access to a payment system. The authority embedded within a system therefore depends not only on its immediate permissions but on the broader network of consequence transitions it can trigger.

Traditional security measurement rarely models these chains of consequence. Attack graphs may show how an adversary can move laterally through systems, but they typically stop at the point of system compromise. They do not quantify the consequence topology that emerges once authority is exercised across interconnected services.

This omission becomes particularly problematic in environments dominated by automation and AI agents. Autonomous systems frequently interact with multiple APIs, data systems, and operational platforms. As these integrations expand, the set of reachable consequences grows as well. Small configuration changes, additional integrations, or incremental permission grants may suddenly expose new classes of consequential actions.

In some cases, these changes can produce discontinuous increases in authority. A single new capability may unlock entire chains of consequential transitions. For example, granting a system the ability to modify policy rules may indirectly allow

it to change access permissions, which in turn may permit identity changes, financial transfers, or physical system actions. Such shifts represent structural expansions in the authority embedded within the system.

Without a method for measuring these changes, organizations cannot effectively reason about the governance of automated authority.

This challenge motivates a new measurement perspective. Instead of asking only which systems can be reached, security governance must also ask what consequential state transitions those systems can produce. The relevant object of analysis is not merely the attack surface but the authority surface of the system.

The authority surface represents the set of consequential state transitions that a system or actor can structurally cause within an operational environment. These transitions span multiple domains of consequence, including financial transfer, legal obligation, identity mutation, policy modification, authority delegation, model behavior alteration, and physical actuation. Each transition represents a potential change to the real-world state governed by the system.

Once authority is understood as a structural property of reachable consequence transitions, measurement must shift accordingly. The challenge becomes quantifying the magnitude and distribution of authority embedded within a system's execution pathways.

The Authority Surface Index (ASI) addresses this challenge by providing a structural measurement framework for consequential authority. Rather than measuring vulnerabilities or compromise likelihood, ASI measures the potential magnitude of authority embedded within a system's architecture. This shift allows governance and security disciplines to reason not only about how systems might fail, but about the scale of consequences those failures could produce.

The next section introduces the concept of the Authority Surface, which defines the topology of consequential authority within automated systems and provides the structural foundation for the Authority Surface Index.

3. Authority Surface as Structural Topology

To measure authority, it must first be defined structurally. The Authority Surface provides this definition.

The Authority Surface represents the topology of consequential state transitions that a system or actor can cause within an operational environment. Rather than

describing permissions or roles, the authority surface describes the set of real-world consequences reachable through the system's execution paths.

In this framework, authority is not treated as a property of identity or position but as a property of reachable consequence transitions. A system possesses authority to the extent that it can cause changes to consequential system states. These changes may occur directly through its own operations or indirectly through interactions with other systems.

This perspective shifts the unit of analysis from access rights to state-changing capability. Traditional security models often focus on whether an actor can access a system or resource. The authority surface instead asks a different question: what consequential changes can this system cause within the broader environment?

Every automated system participates in a network of execution pathways. Application programming interfaces, workflow engines, data pipelines, identity systems, and control interfaces allow systems to invoke actions across organizational infrastructure. These interactions form chains of cause and effect through which actions in one component can propagate consequences in another.

The authority surface captures this structure by defining the set of reachable consequence transitions within the system's execution graph. Each transition represents a state change with meaningful operational impact. Importantly, these transitions extend beyond purely technical system states to include changes that affect economic, legal, organizational, or physical outcomes.

To make the authority surface analytically tractable, consequential transitions are categorized into a finite set of outcome domains known as Authority Outcome Primitives. These primitives represent the fundamental classes of real-world consequences that automated systems can produce.

Authority Surface Topology

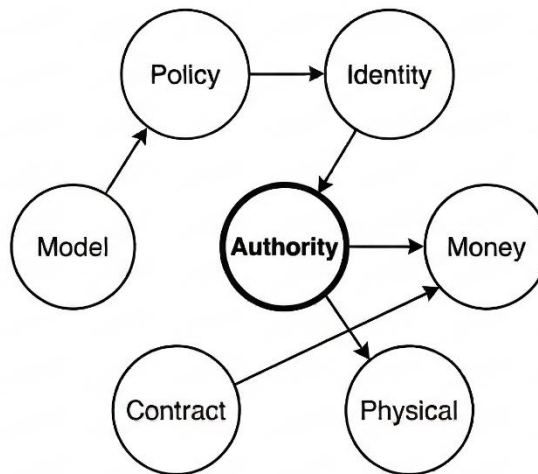


Figure 2 — Authority Surface Topology

The Authority Surface represents the topology of consequential state transitions across authority outcome primitives. Execution pathways between primitives create escalation chains through which automated systems can propagate consequences across financial, legal, identity, policy, model, and physical domains.

The Authority Surface framework defines seven such primitives:

Money

Transitions that transfer or allocate financial assets, initiate payments, or alter financial balances.

Contract

Transitions that create or modify legally binding obligations, agreements, or commitments between parties.

Identity

Transitions that bind, modify, or revoke identity attributes, credentials, or authentication relationships.

Policy

Transitions that change rules governing system behavior, organizational operations, or decision logic.

Authority

Transitions that grant, delegate, or revoke the ability of actors or systems to perform consequential actions.

Model

Transitions that alter machine-learning models or automated decision systems, including training updates, parameter modifications, or policy alignment adjustments.

Physical

Transitions that actuate or control physical infrastructure, including industrial systems, robotics, vehicles, or environmental controls.

These primitives form the closure set of consequential authority within automated environments. While specific systems may implement many intermediate actions or technical states, consequential outcomes ultimately terminate in one or more of these domains. Financial transfers affect the economic domain, identity mutations affect authentication systems, policy changes affect control logic, and so forth.

By expressing authority in terms of these primitives, the authority surface becomes a structured topology of reachable consequence transitions. Each system occupies a position within this topology defined by the set of primitives it can reach through direct or indirect execution paths.

Two systems may appear similar in conventional security terms yet possess dramatically different authority surfaces. A monitoring system that reads telemetry data may have minimal authority, while a workflow automation platform connected to financial services, identity infrastructure, and policy engines may possess a far larger authority surface despite running on similar infrastructure.

Authority surfaces also evolve as systems integrate and automate. Adding an API integration, delegating permissions, or introducing autonomous agents can expand the set of reachable transitions. Conversely, governance controls such as approval gates, partitioning boundaries, or termination authorities can restrict reachable consequences and contract the authority surface.

In this sense, the authority surface behaves as a topological structure shaped by system architecture and governance design. Integrations create pathways across

the surface, permissions expand reachable regions, and governance constraints introduce boundaries that restrict movement between consequence domains.

Understanding this topology is essential for governance in automated environments. Without a structural view of the authority surface, organizations cannot reason about how authority accumulates across systems or how automation may amplify consequential power. Small architectural decisions—such as granting a system the ability to modify policy rules—may create new pathways across the surface, unlocking additional consequence domains through indirect transitions.

The Authority Surface therefore serves as the structural foundation for measuring consequential authority. It defines the possibility space of system-induced state transitions across the domains of financial, legal, identity, policy, authority, model, and physical consequences.

However, topology alone does not provide a quantitative measure of authority magnitude. A system may possess access to several primitives yet exercise them under strong constraints, while another system may concentrate multiple consequence domains under automated control. To compare systems meaningfully, the structural authority embedded within these surfaces must be quantified.

The Authority Surface Index (ASI) provides this measurement. It transforms the authority surface from a qualitative topology into a quantitative index that captures the magnitude, concentration, and controllability of consequential authority embedded within a system's architecture.

The next section examines the distinction between structural and behavioral metrics, clarifying why ASI measures the possibility space of authority rather than the frequency or probability of authority execution.

4. Structural vs. Behavioral Metrics

A critical distinction in the Authority Surface framework is the separation between structural authority and behavioral activity. The Authority Surface Index (ASI) is intentionally designed as a structural measurement, not a behavioral one.

Most operational security metrics focus on behavioral indicators. They measure activity occurring within systems: the number of login attempts, the frequency of privileged actions, the rate of anomalous transactions, or the probability that an

exploit will succeed. These measurements capture how systems behave over time and are essential for detection, monitoring, and operational response.

However, behavioral metrics describe events, not capability.

A system may rarely perform a consequential action, yet still possess the structural authority to do so at any time. Conversely, another system may generate large volumes of activity while having very limited ability to produce meaningful consequences. Activity levels alone therefore do not reveal the magnitude of authority embedded within a system.

The Authority Surface framework separates these dimensions by distinguishing between the possibility space of authority and the runtime behavior occurring within that space.

The authority surface represents the structural possibility space of consequential state transitions. It describes what changes a system is capable of producing within the operational environment, regardless of whether those changes occur frequently or rarely. In this sense, the authority surface defines the set of reachable consequence transitions available to an actor or system.

Behavioral metrics operate within this structural space. Once authority transitions exist, systems may execute them at varying frequencies, under varying probabilities, and with varying levels of risk exposure. These behavioral characteristics are important for operational management, but they are analytically distinct from the structural presence of authority itself.

This distinction can be summarized across four measurement categories:

Metric	What It Measures	Example Question
Authority Surface	Structural possibility space of consequential state transitions	What can this system change?
Frequency	Activity rate across the authority surface	How often are authority transitions executed?
Probability	Likelihood distribution across possible transitions	How likely is a particular authority transition?
Risk	Weighted expectation of consequence and likelihood	What is the expected impact of authority misuse?

The Authority Surface Index operates at the structural layer of this hierarchy. It measures the magnitude and distribution of authority embedded within a system's architecture, independent of how often that authority is exercised.

An analogy to physics helps clarify this distinction. In a gravitational system, a mass located at height above the ground possesses potential energy. This energy represents the capacity to produce motion and impact if released. The presence of potential energy does not imply that motion is occurring; it represents stored capability. Only when the mass moves does this potential convert into kinetic energy.

Authority behaves in a similar manner. A system that can transfer funds, modify policy, or actuate physical infrastructure possesses structural authority potential. Whether those actions are performed frequently or rarely does not change the magnitude of authority embedded in the system. The potential for consequential action exists regardless of runtime activity.

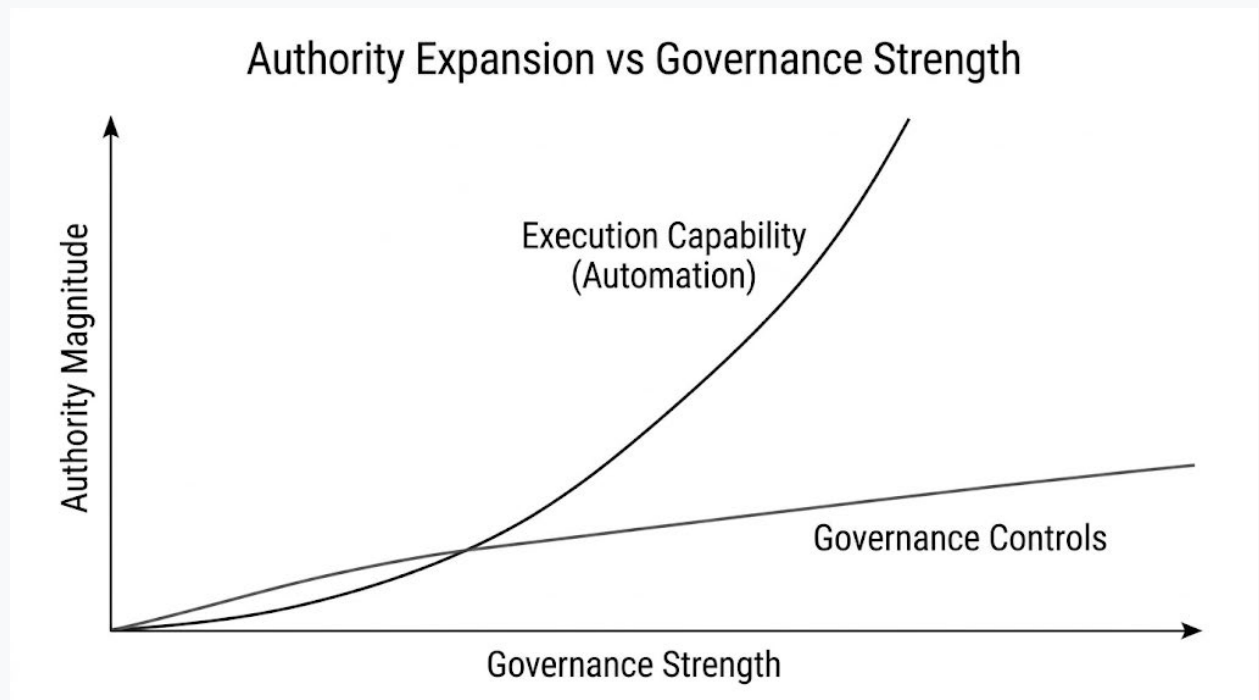


Figure 3 — Authority Expansion vs Governance Control

Authority surfaces expand as automation, delegation, and system integrations increase execution capability. Governance mechanisms such as termination authority, oversight, and boundary controls constrain authority expansion but often evolve more slowly than automated execution capacity.

This distinction becomes especially important in automated environments. Many automated systems execute authority transitions infrequently under normal conditions but may be triggered to act during exceptional events. For example, a policy enforcement engine may only rarely modify system access rules, yet it retains the structural authority to do so whenever triggered. Similarly, an emergency automation system may only actuate physical infrastructure under rare conditions, but its structural authority to do so carries significant consequences.

If governance frameworks evaluate such systems only by observing runtime activity, they risk underestimating the magnitude of authority embedded within them.

Separating structural authority from behavioral activity allows governance analysis to focus on the architecture of authority itself. Structural measurement answers questions such as:

What classes of consequences can this system produce?

How widely distributed are these capabilities across the environment?

How concentrated are consequential powers within particular systems or actors?

What constraints exist to halt or govern authority execution?

These questions concern the design of authority systems, not merely their operational behavior.

The Authority Surface Index therefore measures the structural magnitude of authority embedded within automated systems before considering runtime activity or attack likelihood. By quantifying this underlying authority structure, ASI provides a foundation upon which behavioral metrics—such as activity monitoring, anomaly detection, and probabilistic risk analysis—can operate.

In this way, structural authority measurement complements rather than replaces traditional security metrics. Vulnerability analysis, attack simulation, and threat intelligence remain essential for understanding how adversaries may reach systems. The Authority Surface Index adds a different dimension: it measures the consequences those systems are capable of producing once authority is exercised.

With this distinction established, the next section introduces the Authority Surface Index itself, defining the structural components that together quantify the

magnitude, balance, and concentration of authority embedded within automated systems.

5. The Authority Surface Index (ASI)

The Authority Surface defines the topology of consequential authority within a system. It describes the set of reachable state transitions through which an actor or automated process can produce real-world effects across financial, legal, identity, policy, model, authority, and physical domains. While this topology provides a structural understanding of authority, governance and risk management require a method for quantifying the magnitude and distribution of that authority.

The Authority Surface Index (ASI) provides this measurement.

ASI is a structural index designed to quantify the consequential authority embedded within an automated system. Rather than evaluating vulnerabilities, exploitability, or adversarial likelihood, the index measures the structural authority potential of a system's architecture. It captures how much consequential authority exists within the system, how that authority is distributed, and how effectively it can be constrained.

Conceptually, ASI represents the magnitude of authority contained within the reachable consequence topology of a system. It measures the extent to which a system can cause consequential state transitions and the degree to which governance mechanisms balance or contain that capability.

The Authority Surface Index is derived from four structural components that together describe the architecture of authority within the system.

Authority Surface Index Model

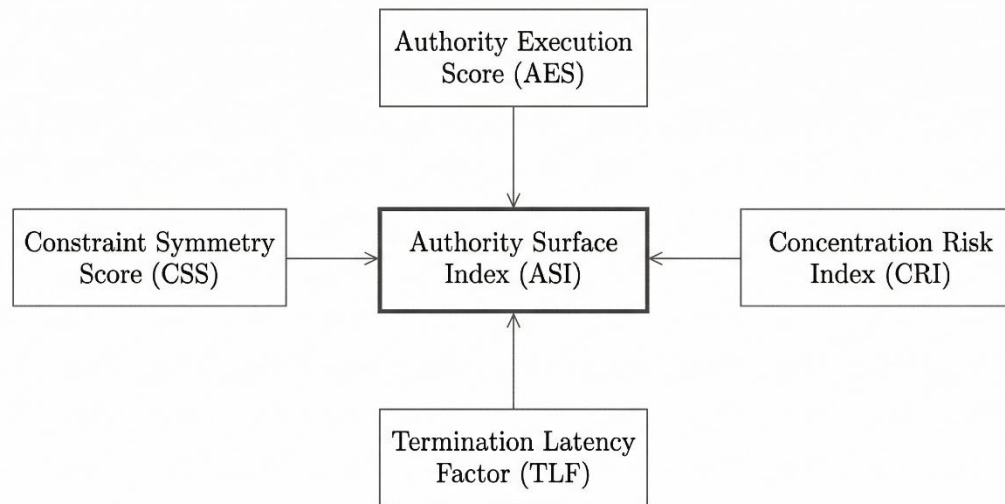


Figure 4 — Authority Surface Index Model

The Authority Surface Index combines four structural factors: execution capability (AES), governance symmetry (CSS), termination responsiveness (TLF), and authority concentration (CRI). Together these components quantify the magnitude of consequential authority embedded within a system.

Authority Execution Score (AES)

The Authority Execution Score measures the breadth and depth of reachable authority execution capability.

Execution capability emerges from the combination of permissions, integrations, automation pathways, and system reachability that allow a system to produce consequential state changes. A system with limited execution capability may only access a small number of authority primitives or require multiple layers of human approval before transitions occur. In contrast, a highly automated system with extensive integrations may reach multiple primitives across financial, identity, policy, and infrastructure domains.

AES therefore captures the scale of consequential authority embedded within the system's execution pathways. Factors influencing AES include the number of

reachable authority primitives, the depth of automation, the level of autonomous decision capability, and the degree of cross-system reachability.

Constraint Symmetry Score (CSS)

Authority execution alone does not determine systemic risk. Systems that possess significant authority may still operate safely if they are governed by effective constraint mechanisms.

The Constraint Symmetry Score measures the degree to which execution capability is balanced by constraint primitives.

Within the Authority Engineering framework, constraint primitives fall into three fundamental categories:

Stop – the ability to terminate authority execution or halt automated processes.

Oversight – the ability to review, audit, or verify authority transitions.

Risk Acceptance – explicit governance authorization for consequential outcomes.

CSS therefore evaluates whether authority execution capability is matched by equivalent governance control. A system with high execution capability but weak constraint mechanisms exhibits low symmetry and therefore greater structural risk.

Termination Latency Factor (TLF)

Even when termination mechanisms exist, their effectiveness depends on how rapidly they can interrupt authority execution.

The Termination Latency Factor measures the time required to halt authority execution once it has been initiated. Systems that permit immediate interruption of consequential transitions exhibit low termination latency, while systems that allow automated actions to proceed without timely interruption exhibit high latency.

TLF therefore reflects the responsiveness of authority containment mechanisms. Factors influencing termination latency include the presence of kill switches, interrupt authority channels, containment boundaries, and human override capabilities.

Lower termination latency indicates stronger authority containment and greater governance responsiveness.

Concentration Risk Index (CRI)

Authority risk also depends on how authority is distributed across systems and actors. When multiple consequential capabilities converge under a single system

or actor, systemic risk increases. Concentrated authority may create single points of failure through which multiple domains of consequence can be triggered.

The Concentration Risk Index measures the degree to which authority primitives converge within particular systems or execution pathways. Systems that possess the ability to trigger multiple authority primitives—such as financial transfers, identity modification, and policy control—represent higher concentrations of authority.

CRI therefore captures the structural risk created by authority centralization. Partitioning authority across systems and actors can reduce this concentration and limit the consequences of failure or compromise.

Conceptual Model

These four components together form the conceptual structure of the Authority Surface Index. Execution capability represents the magnitude of authority embedded within a system, while constraint symmetry, termination responsiveness, and authority concentration determine how safely that authority is governed.

Conceptually, the index can be expressed as a function of these components:

$$ASI = f(AES, CSS, TLF, CRI)$$

Where:

AES measures execution capability across the authority surface

CSS measures governance symmetry between execution and constraint

TLF measures the responsiveness of termination mechanisms

CRI measures the concentration of authority across systems and actors

Together these components quantify the structural authority footprint of a system.

Importantly, ASI does not measure how frequently authority transitions occur, nor does it estimate the likelihood of system compromise. Instead, the index measures the potential magnitude of consequential authority embedded within the system's architecture.

By separating authority magnitude from activity and probability, ASI allows governance and security disciplines to reason about authority design independently of operational behavior. Systems may exhibit low activity levels yet still possess significant structural authority. Conversely, high activity systems may operate within tightly constrained authority boundaries.

The Authority Surface Index therefore provides a structural measurement foundation for Authority Engineering. By quantifying execution capability, constraint symmetry, termination responsiveness, and authority concentration, ASI enables organizations to analyze how authority accumulates across automated systems and to design architectures that intentionally balance consequential power with governance control.

The next section introduces the formal model underlying the Authority Surface Index, presenting the mathematical framework that connects authority primitives, surface topology, and structural authority measurement.

6. Formal Model of Authority Engineering

The Authority Surface Index is grounded in a formal structural model of authority systems. While earlier sections describe authority conceptually, the formal model defines the mathematical relationships that govern authority topology, authority dynamics, and structural risk.

Authority Engineering treats authority as a topological property of reachable consequence transitions. Automated systems interact through execution pathways that propagate state changes across financial, legal, identity, policy, model, and physical domains. The formal model describes how these transitions emerge, accumulate, and evolve within complex systems.

The model is expressed through five core equations that together define the structural foundations of Authority Engineering. These equations define the authority surface, quantify its magnitude, describe its dynamics, identify discontinuities in authority expansion, and formalize the Authority Surface Index itself.

6.1 Authority Surface Definition

The Authority Surface represents the topology of reachable consequence transitions induced by an actor operating within a system.

Formally, the authority surface is defined as the set of all consequential state transitions reachable through the system's execution and constraint primitives. Each transition represents a state change that affects one or more authority outcome domains.

Conceptually, the authority surface captures all consequence-changing transitions that an actor can structurally cause within the operational environment. The topology of this surface is determined by system permissions, integrations, automation pathways, and delegation mechanisms.

$$AS(a) = \{ \tau \mid s \rightarrow s', \tau \in P^* \}$$

Where:

- $AS(a)$ = authority surface of actor a
- s = initial system state
- s' = resulting system state
- τ = consequence transition
- P^* = closure of execution and constraint primitives

In practical terms, this definition establishes the possibility space of authority available to a system or actor.

6.2 Weighted Authority Surface

Not all consequence transitions carry equal magnitude. A system capable of reading telemetry data does not possess the same consequential authority as one capable of transferring financial assets or modifying identity systems.

To quantify authority magnitude, each transition on the authority surface is assigned a consequence weight representing the relative magnitude of the outcome domain involved. These weights reflect the potential impact associated with the corresponding authority primitive.

The weighted authority surface therefore transforms the structural topology into a measurable quantity by aggregating the weighted transitions reachable by the system.

$$WAS(a) = \sum_{\tau \in AS(a)} w(\tau)$$

Where:

- $WAS(a)$ = weighted authority surface of actor a
- $AS(a)$ = authority surface of actor a
- τ = consequence transition

- $w(\tau)$ = consequence weight assigned to transition τ

This weighted representation allows authority magnitude to be compared across systems and architectures, providing a foundation for quantitative authority analysis.

6.3 Authority Surface Balance Law

Authority surfaces evolve over time as systems integrate, automate, and delegate capabilities. Authority may expand when systems gain new execution capabilities or contract when governance mechanisms impose stronger constraints.

The Authority Surface Balance Law describes the forces governing this evolution.

Authority surface magnitude changes through two opposing classes of forces:

Expansion forces, which increase reachable authority transitions, including:

execution capability expansion

delegation of authority

expansion of system state-space

increased autonomy through automation or AI

Contraction forces, which restrict or constrain authority transitions, including:

termination or stop authority

oversight and verification mechanisms

explicit risk-bound governance controls

scope limitation and partitioning boundaries

The balance between these expansion and contraction forces determines whether the authority surface grows, contracts, or remains stable over time.

$$\Delta AS = (E + D + S + A) - (T + O + R + B)$$

Where:

- ΔAS = change in authority surface magnitude

Expansion forces

- E = execution expansion

- D = delegation expansion
- S = state-space expansion
- A = autonomy expansion

Contraction forces

- T = termination authority
- O = oversight mechanisms
- R = risk-bound governance
- B = boundary or scope constraints

This law provides a structural explanation for authority inflation in highly automated environments and for authority containment in well-governed architectures.

6.4 Phase Transition Condition

Authority surfaces do not always expand smoothly. In certain cases, small configuration changes may unlock large new regions of reachable consequence transitions.

These events represent authority phase transitions.

A phase transition occurs when a small change in permissions, integrations, or system capabilities opens a new closure of reachable authority primitives. The resulting expansion may dramatically increase the magnitude of the authority surface even though the underlying configuration change appears minor.

Examples include granting a system the ability to modify policy rules, which may indirectly enable identity changes, financial transactions, or other consequential actions through downstream systems.

The phase transition equation formalizes the conditions under which such discontinuous expansions occur.

$$\Delta AS_{critical} = \sum_{\tau \in C} w(\tau)$$

Where:

- $\Delta AS_{critical}$ = discontinuous change in authority surface magnitude
- C = newly reachable primitive closure
- τ = consequence transition
- $w(\tau)$ = consequence weight assigned to transition τ

Recognizing these transitions is essential for governance, as seemingly small architectural decisions may dramatically alter the authority profile of a system.

6.5 Authority Surface Index

The final equation defines the Authority Surface Index as a structural functional over the authority surface.

The ASI aggregates the structural properties of authority into a measurable index composed of four components:

Authority Execution Score (AES), representing the magnitude of reachable authority execution capability

Constraint Symmetry Score (CSS), representing the balance between execution capability and governance constraints

Termination Latency Factor (TLF), representing the responsiveness of authority interruption mechanisms

Concentration Risk Index (CRI), representing the degree to which authority primitives converge within particular systems or actors

Together, these components produce a structural measure of the authority embedded within the system's architecture.

$$ASI = AES \times (CRI / CSS) \times TLF$$

Where:

- ASI = Authority Surface Index
- AES = Authority Execution Score
- CSS = Constraint Symmetry Score
- CRI = Concentration Risk Index
- TLF = Termination Latency Factor

The Authority Surface Index therefore serves as the quantitative measurement instrument for Authority Engineering. While the authority surface defines the topology of consequential authority, ASI provides the scalar measurement that allows authority magnitude to be compared, governed, and intentionally designed.

6.6 Minimal Formal System

Taken together, the equations presented in this section define a minimal formal system for Authority Engineering.

The structure of this system can be summarized as follows:

Primitive Algebra



Authority Surface



Weighted Authority Surface



Authority Surface Dynamics



Authority Phase Transitions



Authority Surface Index

Within this structure, authority primitives define the fundamental domains of consequence. The authority surface defines the topology of reachable transitions across these domains. The weighted surface quantifies the magnitude of these transitions. Surface dynamics describe how authority evolves through expansion and constraint forces. Phase transitions capture discontinuous expansions in authority capability. Finally, the Authority Surface Index measures the resulting structural authority magnitude.

This formal model establishes the theoretical foundation for measuring and governing authority in automated systems.

The next section interprets the Authority Surface Index in practical terms, explaining how ASI values characterize different classes of systems and how organizations can apply the index to evaluate authority exposure across automated architectures.

7. Interpreting the Authority Surface Index

The Authority Surface Index provides a structural measurement of the consequential authority embedded within a system. While the formal model defines how ASI is derived, its practical value emerges through interpretation. Organizations must be able to understand what different ASI values represent

and how those values relate to governance design, system architecture, and systemic risk.

ASI should therefore be interpreted not as a vulnerability score or threat probability but as a measurement of authority magnitude. The index describes how much consequential authority exists within a system's reachable execution pathways and how effectively that authority is governed by constraint mechanisms.

In practical terms, ASI answers a structural question:

How much consequential power does this system possess relative to the controls that govern it?

This interpretation allows ASI to be used as a comparative measurement across systems, architectures, and automation environments.

Authority Magnitude Spectrum

Systems typically fall along a spectrum of authority magnitude depending on the breadth of consequence domains they can affect and the strength of their constraint mechanisms.

At the lowest end of the spectrum are low-authority systems. These systems possess minimal consequential capability and operate within tightly constrained environments. Examples include monitoring services, telemetry collectors, or analytic platforms that primarily read or process data without producing consequential state transitions. Even if compromised, such systems are structurally limited in the consequences they can produce.

Moderate ASI values correspond to controlled enterprise systems. These systems may possess meaningful authority—such as the ability to modify policy rules, update configuration states, or manage identity attributes—but operate within well-defined governance constraints. Human approvals, oversight mechanisms, and rapid termination capabilities maintain balance between execution capability and control.

Higher ASI values appear in automation platforms and orchestration systems. These systems frequently integrate across multiple infrastructure layers, triggering workflows that span identity systems, financial services, policy engines, and operational platforms. Because they operate through automated execution chains, they often possess wide authority surfaces. If governance mechanisms are insufficiently symmetrical with execution capability, these systems may accumulate disproportionate authority relative to their controls.

At the highest end of the spectrum are high-authority automated systems, including AI agents and autonomous platforms. Such systems may possess the ability to interact with numerous APIs, modify operational policies, trigger financial transactions, or influence physical infrastructure. In these environments, small architectural changes—such as granting additional integration permissions—can produce substantial expansions in reachable authority transitions.

Understanding where systems fall along this spectrum allows organizations to evaluate whether the structural authority embedded within their architectures aligns with governance expectations.

Authority Imbalance and Governance Risk

ASI also provides a means to identify authority imbalance. Structural risk arises when execution capability expands faster than constraint mechanisms.

For example, a system may exhibit a high Authority Execution Score due to extensive integrations and automation pathways. If constraint symmetry remains low—meaning that stop mechanisms, oversight capabilities, or explicit risk acceptance processes are weak—then the resulting ASI value will reflect a structurally imbalanced authority architecture.

Similarly, high termination latency can increase authority exposure. Systems that cannot be interrupted rapidly during automated execution may allow consequential transitions to propagate before governance intervention becomes possible.

Authority concentration presents another structural concern. When multiple authority primitives converge under a single system or actor, the potential consequences of failure or compromise increase significantly. Partitioning authority across systems and actors can reduce this concentration and limit systemic impact.

In this sense, ASI highlights structural governance conditions that traditional security metrics rarely reveal. A system may exhibit strong vulnerability management and monitoring while still possessing disproportionate authority relative to its controls.

Authority Architecture Diagnostics

Because ASI decomposes into four components—execution capability, constraint symmetry, termination latency, and authority concentration—it can also function as a diagnostic tool for authority architecture.

Organizations can use the index to identify structural imbalances such as:

- automation systems with extensive execution capability but weak constraint symmetry
- policy engines capable of modifying multiple authority domains without adequate oversight
- centralized automation platforms that concentrate multiple authority primitives
- systems that perform consequential actions without rapid termination capability

These conditions do not necessarily indicate immediate operational failure. Instead, they represent structural authority exposures that governance design may need to address.

By measuring authority magnitude explicitly, ASI allows organizations to reason about authority architecture before incidents occur.

Authority Design Implications

Interpreting ASI values also informs architectural design decisions. When authority magnitude grows beyond governance capacity, organizations can reduce structural exposure through several approaches.

Execution pathways may be partitioned to separate authority primitives across systems. Constraint mechanisms such as oversight gates or termination authorities may be strengthened. Automation chains may be redesigned to reduce indirect authority escalation. In some cases, organizations may deliberately limit reachable primitives to ensure that automated systems cannot trigger high-consequence transitions.

These design choices reshape the authority surface and therefore change the resulting ASI measurement.

In this way, ASI becomes more than a diagnostic metric. It becomes a design instrument for shaping authority systems intentionally.

From Measurement to Engineering

The ability to interpret ASI values across architectures allows organizations to compare authority exposure across systems, automation platforms, and AI deployments. More importantly, it enables authority systems to be engineered rather than assumed.

Traditional cybersecurity measurement focuses on defending systems against attack. Authority Engineering extends this perspective by designing systems whose authority surfaces remain balanced with governance controls.

The Authority Surface Index provides the measurement foundation required for this discipline.

The next section examines how the ASI framework applies specifically to AI and automated systems, where authority surfaces often expand rapidly due to integrations, autonomous decision capability, and tool-based execution pathways.

8. Application to AI and Automated Systems

The Authority Surface Index becomes particularly important in environments dominated by automation and artificial intelligence. AI agents, workflow engines, orchestration platforms, and automated decision systems increasingly operate across multiple services, infrastructure layers, and operational domains. These systems do not merely process information; they execute actions that produce consequential outcomes across financial, organizational, and physical environments.

In such architectures, authority often accumulates indirectly through tool access, API integrations, and automated execution pathways. Rather than acting through a single permission set, automated systems frequently operate through chains of interactions that traverse multiple systems. Each step in the chain may unlock additional consequence transitions, expanding the reachable authority surface.

Traditional security measurement rarely captures this dynamic. Most governance frameworks evaluate AI systems primarily through model behavior, data governance, or prompt safety mechanisms. While these concerns are important, they do not address the structural authority embedded within the execution environment surrounding the model.

In practice, the authority of an AI system is determined less by the model itself and more by the set of tools and integrations through which the model can act.

Tool-Based Authority Expansion

Modern AI agents frequently operate through tool invocation. Frameworks such as agent orchestration systems allow models to call APIs, modify system states, execute workflows, and interact with external services. Each tool effectively exposes a pathway to one or more authority outcome primitives.

For example, a financial API may expose the Money primitive through the ability to initiate transactions. An identity management API exposes the Identity primitive through credential binding or privilege modification. Policy engines expose the Policy primitive by altering decision rules governing system behavior. Infrastructure control systems expose the Physical primitive through actuation of physical devices.

The reachable authority surface of an AI agent therefore depends on the set of primitives reachable through its available tools and integrations.

As tools accumulate, the reachable primitive set expands. This expansion may not be immediately visible because authority is distributed across multiple systems rather than concentrated within a single component. However, when viewed through the Authority Surface framework, the cumulative consequence capability becomes clear.

Escalation Chains in Automated Systems

Authority expansion in automated environments often occurs through primitive escalation chains. A system may not directly control a particular authority domain but may still reach it through intermediate transitions.

For example, an AI system capable of modifying policy rules may indirectly influence identity permissions. Those identity permissions may then allow access to financial systems or operational infrastructure. In this scenario, a seemingly limited capability—policy modification—unlocks a sequence of consequential transitions across multiple domains.

Such escalation chains illustrate why authority must be analyzed as a topological structure of reachable transitions, rather than as isolated permissions.

AI agents are particularly effective at discovering and exploiting these pathways because they can interact with multiple tools dynamically. As agent architectures evolve, the reachable authority surface may expand rapidly through new integrations and automation pathways.

Authority Surface Compression

Automation can also produce authority surface compression, a condition in which multi-step governance processes collapse into shorter execution pathways.

In traditional human-operated environments, consequential actions may require multiple approvals, reviews, or manual interventions. Automation can reduce these steps by embedding decision logic directly within software systems. While

this improves operational efficiency, it also reduces the structural distance between decision points and consequential outcomes.

For example, an automated policy engine may directly trigger identity changes, financial transfers, or infrastructure actions without human review. When such automation occurs across multiple systems simultaneously, the authority surface becomes more densely connected and consequential transitions can propagate more rapidly.

This compression increases the effective magnitude of authority embedded within the system.

Authority Reachability in AI Systems

Evaluating authority in AI environments therefore requires a different form of analysis. Instead of examining the internal behavior of models alone, governance must evaluate the reachable primitive set of the entire agent architecture.

This analysis includes:

- identifying all tools and APIs available to the agent
- mapping each tool to the authority primitives it exposes
- tracing escalation chains that connect primitives across systems
- evaluating whether constraint mechanisms limit consequential transitions

Through this process, organizations can determine the reachable authority surface of the agent and estimate the resulting Authority Surface Index.

Such analysis often reveals authority exposure that is not obvious through traditional model governance approaches. A model may appear benign when evaluated in isolation but may possess extensive consequential authority when connected to operational systems.

Governance Implications for AI Systems

Applying ASI to AI architectures enables organizations to reason about automated authority before deployment.

Systems with high Authority Execution Scores may require stronger constraint symmetry, including human oversight channels, termination controls, and explicit governance boundaries. Partitioning tool access across agents can reduce authority concentration, while introducing termination gates can reduce termination latency.

These design decisions reshape the authority surface of the system and therefore reduce the resulting ASI.

In this way, the Authority Surface Index provides a method for evaluating AI governance architectures structurally rather than behaviorally. Instead of focusing only on how AI behaves, ASI measures the scale of consequences the system is structurally capable of producing.

As AI systems continue to integrate with financial infrastructure, operational technology, and enterprise governance platforms, this structural perspective becomes increasingly important. Automated systems are no longer confined to informational roles; they participate directly in consequential decision pathways.

Measuring and designing the authority embedded within those pathways is therefore essential for responsible automation.

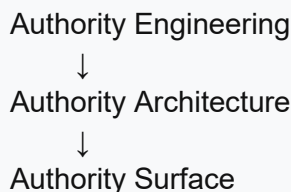
The next section situates the Authority Surface Index within the broader Authority Engineering framework, explaining how ASI functions as the quantitative measurement layer that supports the design and governance of authority systems.

9. Authority Engineering Integration

The Authority Surface Index occupies the quantification layer within the broader discipline of Authority Engineering. While earlier sections define authority topology and introduce the ASI measurement model, the full significance of the index emerges when placed within the larger architectural framework governing authority systems.

Authority Engineering treats authority as a designable system property rather than an incidental outcome of permissions or organizational roles. Within this discipline, authority is analyzed structurally, measured quantitatively, and shaped intentionally through architectural design.

The conceptual stack can be understood as a sequence of increasingly concrete layers:





Authority Surface Index (ASI)

Each layer addresses a different aspect of authority governance.

Authority Engineering

At the highest level, Authority Engineering defines the structural principles governing authority systems. It provides the conceptual framework for understanding how authority emerges, propagates, and concentrates within complex technological environments. This discipline establishes the theoretical foundations for reasoning about authority topology, escalation chains, consequence domains, and structural governance mechanisms.

Within this context, authority is understood not as a property of organizational roles but as a topological property of reachable consequence transitions. Authority Engineering therefore focuses on the geometry and dynamics of these transitions within automated systems.

Authority Architecture

Authority Architecture translates these principles into organizational and system design. It defines how decision authority, escalation paths, termination authority, and governance responsibilities are distributed across actors and systems.

In traditional governance frameworks, authority structures are often implicit or assumed. Authority Architecture makes these structures explicit, specifying where consequential decisions occur, how authority transitions propagate, and which actors possess the ability to halt or authorize those transitions.

Within automated environments, Authority Architecture must account for both human actors and machine agents. Governance design therefore includes not only organizational roles but also the authority embedded within automated systems.

Authority Surface

The Authority Surface represents the structural topology of consequential authority created by the architecture. It maps the reachable consequence transitions available to systems and actors across the domains of financial, legal, identity, policy, authority delegation, model behavior, and physical infrastructure.

Where Authority Architecture defines intended authority structures, the authority surface reveals the actual consequence topology that emerges from system integrations, automation pathways, and delegated permissions.

This distinction is important. Architectural intentions may differ from operational reality when automation pathways create new execution chains across systems. Mapping the authority surface therefore provides visibility into the real distribution of consequential authority within the environment.

Authority Surface Index (ASI)

The Authority Surface Index provides the quantitative measurement layer within this framework.

While the authority surface describes the topology of reachable consequences, ASI measures the magnitude, balance, and concentration of authority embedded within that topology. By decomposing authority into execution capability, constraint symmetry, termination responsiveness, and concentration risk, ASI converts structural authority into a measurable index.

This measurement capability enables organizations to evaluate whether their authority architecture remains aligned with governance expectations.

For example, a system may be designed with limited authority according to its architectural role, yet automation integrations may expand its reachable authority surface beyond those expectations. The resulting ASI measurement would reveal this discrepancy, allowing governance teams to redesign execution pathways or strengthen constraint mechanisms.

Similarly, ASI can identify authority concentration within particular systems or actors, highlighting areas where partitioning or constraint design may be necessary.

Measurement as a Design Instrument

Within Authority Engineering, measurement is not merely descriptive. It functions as a design instrument for shaping authority systems intentionally.

By quantifying structural authority, ASI allows architects and governance teams to reason about how authority accumulates across automation pathways, how constraint mechanisms balance execution capability, and how architectural changes reshape the authority surface.

For example, introducing termination controls may reduce termination latency, lowering the ASI value associated with automated execution pathways. Partitioning authority primitives across multiple systems may reduce concentration risk. Introducing oversight gates may increase constraint symmetry relative to execution capability.

Each of these architectural changes reshapes the authority surface and alters the resulting ASI measurement.

In this way, the Authority Surface Index enables authority systems to be engineered rather than assumed.

Toward Measurable Authority Governance

Traditional governance frameworks often rely on qualitative judgment when evaluating authority distribution within organizations and automated systems. While such judgment remains important, complex automation environments require more systematic methods for understanding how authority accumulates across technical architectures.

The Authority Surface Index provides the measurement capability necessary for this analysis. By quantifying the magnitude and distribution of consequential authority, ASI allows governance teams to compare systems, evaluate automation architectures, and identify structural authority exposures before they manifest as operational failures.

Within the broader discipline of Authority Engineering, ASI therefore functions as the instrument that transforms authority governance from qualitative oversight into measurable system design.

The final section concludes the paper by summarizing the contribution of the Authority Surface Index and outlining its implications for the governance of increasingly automated and AI-driven systems.

10. Conclusion

As computing systems increasingly execute consequential actions within economic, legal, organizational, and physical environments, the nature of cybersecurity risk is changing. Traditional security metrics were developed to measure exposure and exploitability. Vulnerability scores, attack surface mapping, and threat modeling frameworks provide valuable insight into how systems can be accessed and how adversaries might compromise them. These approaches remain essential for operational defense.

However, access alone does not determine impact.

The consequences of system compromise depend on the authority embedded within the compromised system. A system capable only of reading telemetry data presents a fundamentally different risk profile than one capable of transferring financial assets, modifying identity records, delegating authority, or actuating

physical infrastructure. Yet traditional security measurement rarely captures this difference.

This paper introduces the Authority Surface Index (ASI) as a structural measurement framework designed to quantify the consequential authority embedded within automated systems. Rather than measuring vulnerabilities or attack likelihood, ASI measures the structural magnitude of authority available within a system's reachable execution pathways.

The ASI framework builds upon the concept of the Authority Surface, which defines the topology of consequential state transitions that systems can produce across a finite set of authority outcome domains. These domains—money, contract, identity, policy, authority, model behavior, and physical actuation—represent the fundamental primitives through which automated systems affect real-world outcomes.

Within this topology, ASI provides a quantitative measurement of authority magnitude by evaluating four structural dimensions:

Authority Execution Score (AES), representing the breadth and depth of reachable authority transitions

Constraint Symmetry Score (CSS), representing the balance between execution capability and governance controls

Termination Latency Factor (TLF), representing the responsiveness of authority interruption mechanisms

Concentration Risk Index (CRI), representing the degree to which authority converges within particular systems or actors

Together, these components produce a structural measurement of the authority embedded within a system's architecture.

Importantly, ASI does not measure how frequently authority transitions occur or the probability that a system will be compromised. Instead, it measures the potential magnitude of consequential authority contained within the system. In this sense, the index functions analogously to potential energy in physical systems: it represents stored capability rather than runtime activity.

This distinction is particularly important in environments shaped by automation and artificial intelligence. Modern AI agents, workflow engines, and orchestration platforms frequently interact with multiple systems through APIs, automation pipelines, and tool invocation frameworks. As these integrations expand, the reachable authority surface of the system grows. Small architectural changes

may produce large discontinuities in authority capability, enabling automated systems to affect financial, organizational, or physical outcomes.

In such environments, governance cannot rely solely on behavioral monitoring or model evaluation. Instead, organizations must understand the structural authority embedded within the systems they deploy.

The Authority Surface Index provides the measurement capability required for this analysis. By quantifying authority magnitude, governance teams can compare systems, identify structural authority imbalances, and evaluate whether automated architectures maintain appropriate alignment between execution capability and governance control.

More broadly, ASI functions as the quantitative measurement layer within the discipline of Authority Engineering. While Authority Architecture defines governance structures and the Authority Surface defines the topology of consequential authority, ASI provides the scalar measurement necessary to analyze and design these systems systematically.

This measurement capability enables authority systems to be engineered rather than assumed.

As automation and AI continue to expand the range of consequential actions performed by machines, the ability to measure and govern authority will become increasingly important. Systems will no longer be judged solely by whether they are secure against attack, but also by how much authority they possess and how effectively that authority is constrained.

The Authority Surface Index provides a framework for making this authority visible, measurable, and governable within modern automated systems.

References

Bell, P. (2026). The 7 Stages of AI Adoption: A Board-Level Oversight Framework for Mid-Sized Organizations.

Cloud Security Alliance. (2024). AI Controls Matrix (AICM).

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives.

ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection.

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2).

National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0.

Hansen, T.-S. (2026). The Ontology of Property Attribution: Structural Understanding as an Invariance Condition.

Appendix A

Mathematical Foundations of Authority Engineering

Authority Engineering can be expressed through a minimal formal system describing the topology, dynamics, and measurement of consequential authority.

Equation 1 — Authority Surface

The Authority Surface of an actor is the set of reachable consequential state transitions within a system.

$$AS(a) = \{ \tau \mid s \rightarrow s', \tau \in P^* \}$$

Where:

- Authority surface of actor
- Initial system state
- Resulting system state
- Consequence transition
- Closure of execution and constraint primitives

Interpretation

The authority surface defines all consequential state transitions that actor can structurally cause within the system environment.

Equation 2 — Weighted Authority Surface

$$WAS(a) = \sum_{\tau \in AS(a)} w(\tau)$$

Where:

$WAS(a)$ = weighted authority surface of actor a

$AS(a)$ = authority surface of actor a

τ = consequence transition

$w(\tau)$ = consequence weight assigned to transition τ

This converts the authority topology into a scalar measure of consequence magnitude.

Equation 3 — Authority Surface Balance Law

$$\Delta AS = (E + D + S + A) - (T + O + R + B)$$

Where:

ΔAS = change in authority surface magnitude

Expansion forces

E = execution expansion

D = delegation expansion

S = state-space expansion

A = autonomy expansion

Contraction forces

T = termination authority

O = oversight mechanisms

R = risk-bound governance

B = boundary or scope constraints

Interpretation:

Authority surfaces expand through automation and delegation and contract through governance controls.

Equation 4 — Authority Phase Transition

$$\Delta AS_{critical} = \sum_{\tau \in C} w(\tau)$$

Where:

$\Delta AS_{critical}$ = discontinuous change in authority surface magnitude

C = newly reachable primitive closure

τ = consequence transition

$w(\tau)$ = consequence weight assigned to transition τ

This equation models discontinuous authority expansion when a new permission unlocks a new primitive closure.

Equation 5 — Authority Surface Index

$$ASI = AES \times (CRI / CSS) \times TLF$$

Where:

ASI = Authority Surface Index
AES = Authority Execution Score
CRI = Concentration Risk Index
CSS = Constraint Symmetry Score
TLF = Termination Latency Factor

Interpretation:

Authority risk increases when execution capability and concentration increase,
and when constraints weaken.

Appendix B

Authority Outcome Primitives

Authority Surface analysis models consequential authority through a finite set of outcome domains referred to as Authority Outcome Primitives.

These primitives represent the fundamental classes of real-world consequences automated systems can produce.

Money

Transitions involving transfer or allocation of financial assets.

Examples:

payments

financial transfers

balance modifications

Contract

Transitions creating or modifying legally binding obligations.

Examples:

digital agreements

contractual commitments

service authorizations

Identity

Transitions binding, modifying, or revoking identity attributes.

Examples:

credential issuance

access identity binding

privilege assignment

Policy

Transitions altering rule systems governing operational behavior.

Examples:

access control rules

governance policies

decision logic

Authority

Transitions delegating or revoking the ability to perform consequential actions.

Examples:

privilege delegation

authority assignment

permission mutation

Model

Transitions altering automated decision systems.

Examples:

machine learning model updates

parameter changes

training or alignment adjustments

Physical

Transitions affecting physical infrastructure.

Examples:

robotics actuation

industrial control

infrastructure manipulation

Appendix C

Authority Surface Index Components

The Authority Surface Index measures authority magnitude through four structural dimensions.

Authority Execution Score (AES)

Measures the breadth and depth of reachable authority transitions.

Influenced by:

number of reachable primitives

automation depth

system integrations

autonomy level

Constraint Symmetry Score (CSS)

Measures the balance between execution capability and governance constraints.

Constraint primitives include:

Stop (termination authority)

Oversight (review and verification)

Risk Acceptance (explicit authorization)

Termination Latency Factor (TLF)

Measures the time required to halt authority execution once initiated.

Factors include:

kill switches

interrupt authority

human override mechanisms

containment boundaries

Concentration Risk Index (CRI)

Measures how strongly authority primitives converge within a system or actor.

Higher concentration increases systemic risk when:

multiple primitives are controlled by one system

authority paths lack partitioning

automation chains centralize execution capability

11. Example ASI Calculation

To illustrate how the Authority Surface Index can be applied in practice, this section presents a simplified calculation for a hypothetical AI-enabled enterprise system. The purpose of the example is not to establish final scoring thresholds but to demonstrate how the formal ASI equation can be used to estimate structural authority embedded within automated architectures.

Example System

Assume an AI-enabled workflow orchestration platform operating within a financial services environment. The system performs the following functions:

- reads customer account data
- modifies internal policy rules for transaction routing
- updates identity attributes for service access
- initiates payment requests through an integrated financial API
- operates with limited human review during normal processing

Through these capabilities the system can reach multiple Authority Outcome Primitives:

- Identity through attribute and access updates
- Policy through routing-rule modification
- Money through payment initiation

Because the system interacts with multiple services through automated workflows, it possesses a non-trivial authority surface.

The goal of this example is to estimate the Authority Surface Index (ASI) for this architecture using the formal model introduced in Section 6.

Step 1: Authority Execution Score (AES)

The Authority Execution Score (AES) measures the breadth and depth of reachable authority execution capability across the authority surface.

AES is influenced by several structural factors:

- number of reachable authority primitives
- depth of automation within execution pathways

- cross-system integrations
- autonomy of the decision process

For this example system:

- reachable primitives: 3 of 7
- automation depth: high
- system integrations: moderate–high
- autonomy: moderate

Assume a normalized score on a 1–10 scale:

AES = 7.5

This reflects a system capable of producing multiple consequential state transitions across different domains.

Step 2: Constraint Symmetry Score (CSS)

The Constraint Symmetry Score (CSS) measures how well governance constraints balance execution capability.

Constraint primitives include:

- Stop – termination authority
- Oversight – review or verification mechanisms
- Risk Acceptance – explicit authorization of consequential actions

In this example the system includes:

- audit logging
- post-execution review
- limited approval requirements
- no consistent pre-execution authorization for financial actions

Constraint mechanisms exist but do not fully match execution capability.

Assume:

CSS = 4.0

Lower CSS indicates weaker governance symmetry relative to execution capability.

Step 3: Termination Latency Factor (TLF)

The Termination Latency Factor (TLF) measures the responsiveness of interruption mechanisms once authority execution has begun.

This system includes:

- an administrative kill switch
- manual escalation for some workflows
- no sub-transaction interrupt capability

Termination controls exist but may require time to intervene.

Assume:

TLF = 1.8

Higher values indicate slower interruption and therefore greater structural exposure.

Step 4: Concentration Risk Index (CRI)

The Concentration Risk Index (CRI) measures how strongly authority primitives converge within a single system or execution pathway.

In this architecture the orchestration platform directly controls:

- policy mutation
- identity mutation
- payment initiation

This represents a meaningful concentration of authority primitives.

Assume:

CRI = 2.2

Higher CRI values reflect greater authority concentration within a single system.

Step 5: Compute the Authority Surface Index

Using the formal equation introduced in Section 6:

$$\text{ASI} = \text{AES} \times (\text{CRI} / \text{CSS}) \times \text{TLF}$$

Substitute the example values:

$$\text{ASI} = 7.5 \times (2.2 / 4.0) \times 1.8$$

$$\text{ASI} = 7.5 \times 0.55 \times 1.8$$

$$\text{ASI} = 7.43$$

Therefore:

$$\text{ASI} \approx 7.43$$

Interpretation

An ASI of approximately 7.4 indicates a system with material consequential authority embedded within its architecture.

The elevated value arises from several structural conditions:

- the system can reach multiple authority primitives
- consequential domains are concentrated within one orchestration platform
- constraint symmetry is weaker than execution capability
- termination controls are slower than ideal

The result is an authority architecture where consequential execution capability exceeds the strength of governance containment mechanisms.

Design Implications

This example demonstrates how ASI can guide authority architecture decisions.

An organization seeking to reduce the index could:

Increase CSS

- introduce pre-execution approval gates
- strengthen oversight or verification mechanisms

Reduce TLF

- implement real-time interrupt authority
- introduce automated containment boundaries

Reduce CRI

- partition identity, policy, and financial capabilities across separate systems

Reduce AES

- restrict unnecessary integrations
- narrow tool access available to automated workflows

These architectural changes reshape the authority surface and reduce the resulting Authority Surface Index.

Comparative Use

The value of ASI becomes more apparent when comparing systems.

A reporting dashboard with read-only capabilities might produce:

AES = 2.0

CSS = 8.0

TLF = 1.1

CRI = 1.0

producing a very low ASI.

By contrast, an autonomous treasury automation system with direct financial execution, policy control, and delegated privileges could produce significantly higher ASI values.

Such comparisons allow governance teams to identify which automated systems possess the greatest consequential authority and therefore require stronger architectural controls.

Purpose of the Example

This example demonstrates how the formal ASI equation transforms authority from a qualitative governance concern into a measurable structural property.

By quantifying execution capability, constraint symmetry, termination responsiveness, and authority concentration, the Authority Surface Index enables organizations to compare authority exposure across automated architectures and design systems whose authority remains balanced with governance control.

Future implementations can refine this model by introducing standardized scoring rubrics for AES, CSS, TLF, and CRI, allowing ASI to function as a repeatable measurement instrument within Authority Engineering.

List of Figures

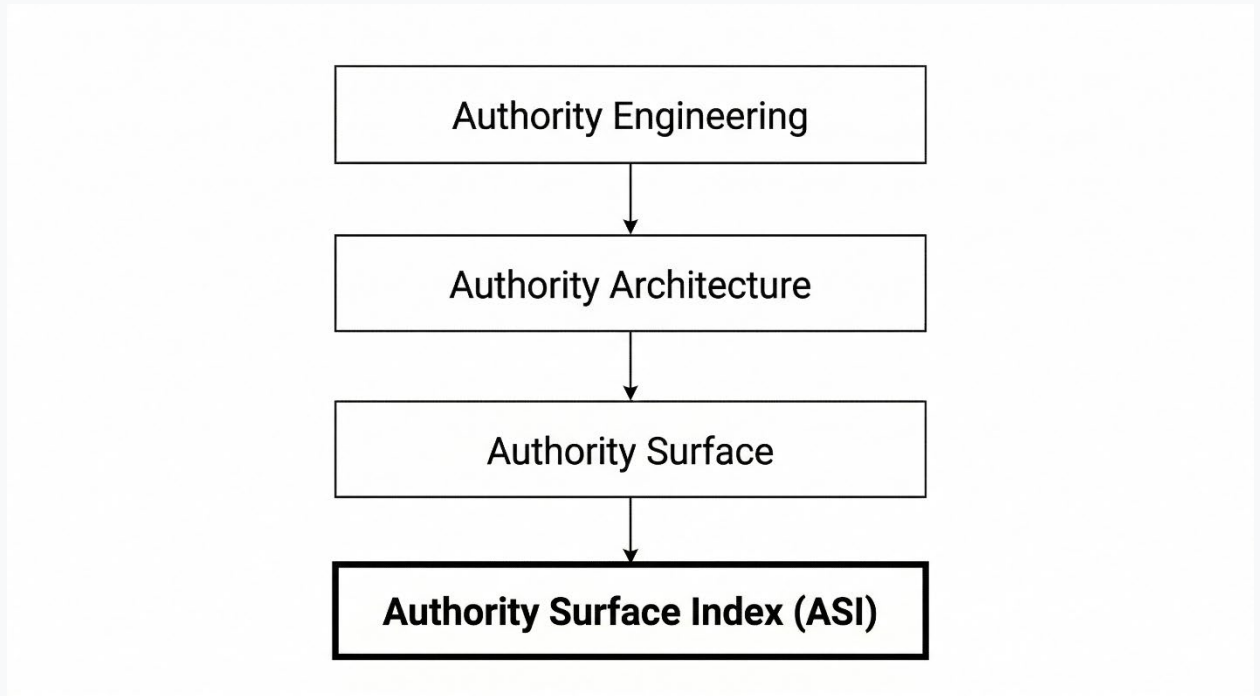


Figure 1 — Authority Engineering Stack

Authority Engineering provides the conceptual framework for authority systems. Authority Architecture defines governance structures, the Authority Surface defines the topology of consequential authority, and the Authority Surface Index (ASI) provides the quantitative measurement of authority magnitude.

Authority Surface Topology

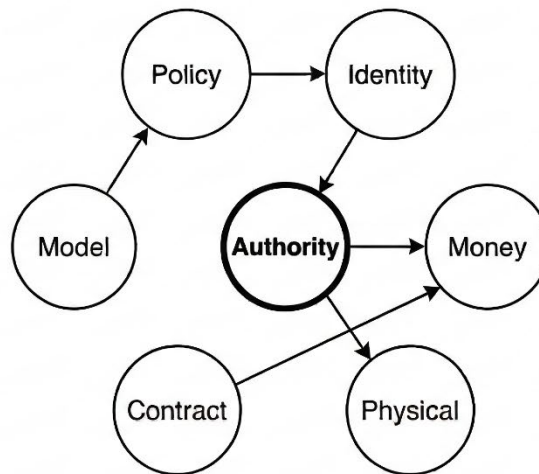


Figure 2 — Authority Surface Topology

The Authority Surface represents the topology of consequential state transitions across authority outcome primitives. Execution pathways between primitives create escalation chains through which automated systems can propagate consequences across financial, legal, identity, policy, model, and physical domains.

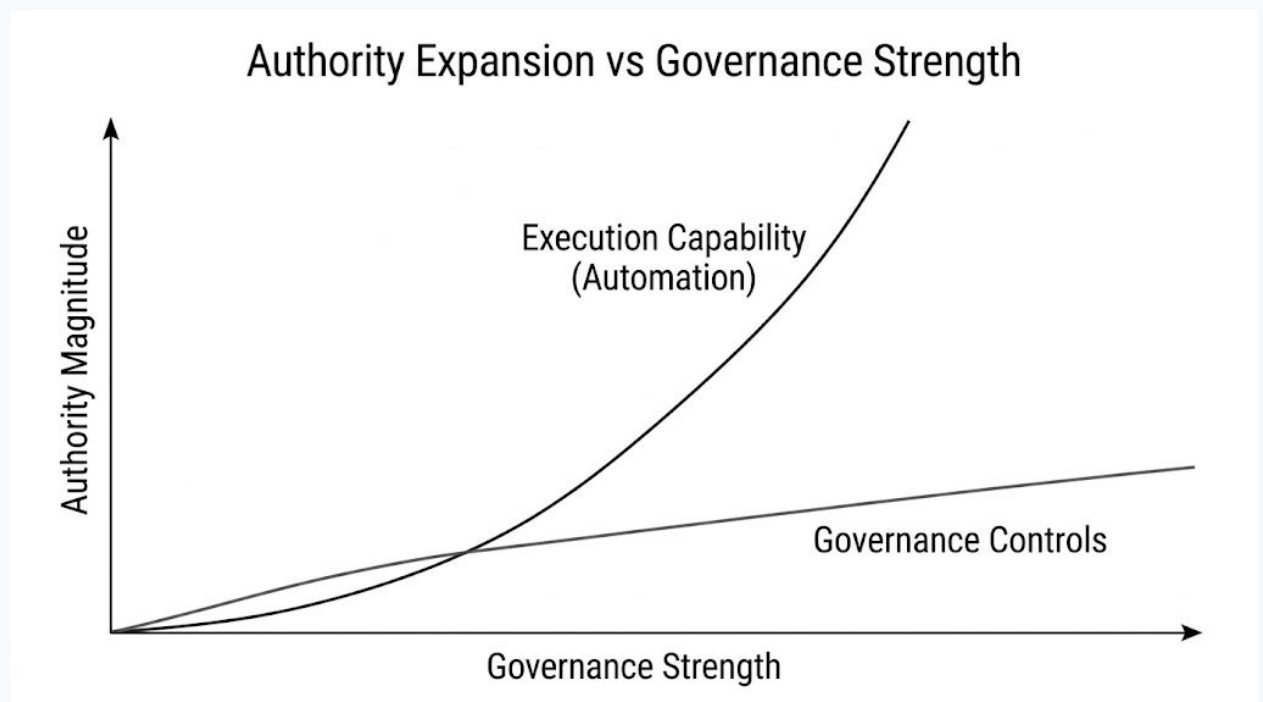


Figure 3 — Authority Expansion vs Governance Control

Authority surfaces expand as automation, delegation, and system integrations increase execution capability. Governance mechanisms such as termination authority, oversight, and boundary controls constrain authority expansion but often evolve more slowly than automated execution capacity.

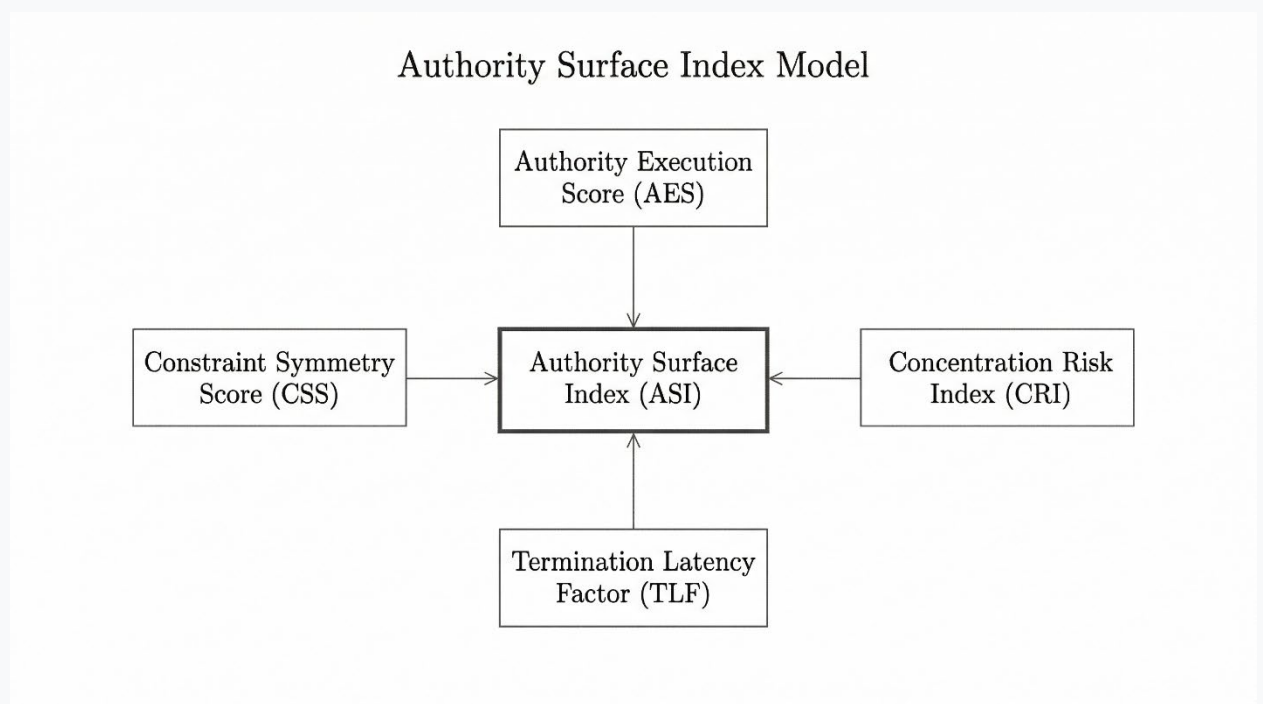


Figure 4 — Authority Surface Index Model

The Authority Surface Index combines four structural factors: execution capability (AES), governance symmetry (CSS), termination responsiveness (TLF), and authority concentration (CRI). Together these components quantify the magnitude of consequential authority embedded within a system.

List of Equations

Equation 1 — Authority Surface

$$AS(a) = \{ \tau \mid s \rightarrow s', \tau \in P^* \}$$

Where

$AS(a)$ = authority surface of actor a

s = initial system state

s' = resulting system state

τ = consequence transition

P^* = closure of execution and constraint primitives

Equation 2 — Weighted Authority Surface

$$WAS(a) = \sum_{\tau \in AS(a)} w(\tau)$$

Where

$WAS(a)$ = weighted authority surface of actor a

$w(\tau)$ = consequence weight assigned to transition τ

Equation 3 — Authority Surface Balance Law

$$\Delta AS = (E + D + S + A) - (T + O + R + B)$$

Where

Expansion forces

E = execution expansion

D = delegation expansion

S = state-space expansion

A = autonomy expansion

Constraint forces

T = termination authority

O = oversight mechanisms

R = risk-bound governance

B = boundary constraints

Equation 4 — Authority Phase Transition

$$\Delta AS_{critical} = \sum_{\tau \in C} w(\tau)$$

Where

$\Delta AS_{critical}$ = discontinuous change in authority surface magnitude

C = newly reachable primitive closure

τ = consequence transition

$w(\tau)$ = consequence weight

Equation 5 — Authority Surface Index

$$ASI = AES \times (CRI / CSS) \times TLF$$

Where

ASI = Authority Surface Index

AES = Authority Execution Score

CRI = Concentration Risk Index

CSS = Constraint Symmetry Score

TLF = Termination Latency Factor