

Authority Engineering AI Extension: Tool Use & Boundaries

Rob Caswell

Authority Engineering

July 2026

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

Publication Record

AI Extension: Tool Use & Boundaries

Author: Rob Caswell

Publisher: Cyber Terrain LLC

Published: 2026-07-01

Zenodo version: v1.0

DOI: <https://doi.org/10.5281/zenodo.21742355>

Website: <https://cyberterrain.ai/papers/ae-ai-extension-tool-use-boundaries.pdf>

Corpus Context

Corpus: Authority Engineering

Document ID: AE-AIX-0008

Object family: AE-AIX-0008

Publisher-imprint edition prepared for versioned republication.

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

Abstract

The Tool Use & Boundaries family explains how consequence-bearing interactions at tool boundaries are governed by bounded local evaluation at the realization seam. It does not establish a general doctrine of tools or define a framework for tool optimization. Instead, it addresses the narrow architectural condition under which consequence-bearing actions encounter tool boundaries within distributed execution pathways. The family is governed by AI-DL-018 Bounded Local Evaluation: localized consequence controls evaluate only the immediate, bounded operational conditions necessary to determine whether a consequence-bearing action may safely proceed at a specific realization seam.

Within this family, global semantic reconstruction is structurally mis-scoped for local evaluation. Derived beneath AI-DL-007 Local Stop Authority and preserved as a principle-grade family, Tool Use & Boundaries relies on AI-DL-013 Continuity History Integrity to preserve the trustworthiness of the state history feeding local continuity validation despite upstream failure or compromise. Tool boundaries therefore do not introduce a new architectural root; they inherit seam-local evaluation constraints within the existing AI Extension architecture.

I. Introduction

Purpose

The Tool Use & Boundaries family explains how consequence-bearing interactions at tool boundaries are governed by bounded local evaluation at the realization seam. It addresses a specific architectural boundary within Authority Engineering where distributed execution pathways interface with localized action permissions. It does not establish a general or comprehensive doctrine of tools, nor does it define an architecture for tool optimization.

The architectural subject is Tool Use & Boundaries as a derived family, positioned strictly beneath the frozen AI Extension root layer. The governing explanation for this domain is:

AI-DL-018 Bounded Local Evaluation: Localized consequence controls evaluate only the immediate, bounded operational conditions necessary to determine whether a consequence-bearing action may safely proceed at a specific realization seam.

This structure restores the consistent architectural pattern established across the AI Foundations sequence, positioning the family as the subject and the engineering principle as its governing mechanism.

II. Tool Use Is Not the Governing Object

Architectural discipline requires separating ephemeral software engineering implementations from persistent structural constraints. Within this framework, modern implementation paradigms are classified as subordinate application surfaces rather than canonical architecture:

- Tools as Application Surfaces: Contemporary execution mechanics represent non-canonical, illustrative implementation examples rather than foundational elements.
- Tool Boundaries as Engineering Locations: A tool boundary serves merely as an operational setting or consequence seam where localized evaluation occurs.
- Exclusion of Implementation Taxonomies: Engineering at the tool boundary is governed by bounded local evaluation rather than implementation-specific interface vocabularies. Focusing the architecture on specific execution mechanics shifts the analytical weight away from the core governing object.

The true architectural focus is how the tool family operates at the realization seam, independent of any underlying software delivery mechanism.

III. Governing Engineering Principle

The Tool Use & Boundaries family is governed by the accepted engineering principle AI-DL-018 Bounded Local Evaluation:

AI-DL-018 Bounded Local Evaluation: Localized consequence controls evaluate only the immediate, bounded operational conditions necessary to determine whether a consequence-bearing action may safely proceed at a specific realization seam.

To clarify the governing principle, the following operational descriptions explain how the accepted definition applies within this family:

- Realization Seams represent the specific localized operational interfaces where consequence permissions are adjudicated and immediate execution transpires.
- Consequence-Bearing Actions encompass any individual execution steps capable of introducing, modifying, or realizing structural state consequences within the architecture.
- Immediate Bounded Operational Conditions define the minimal, localized parameter sets strictly required to verify safety or permission at a seam, deliberately excluding broader systemic context.

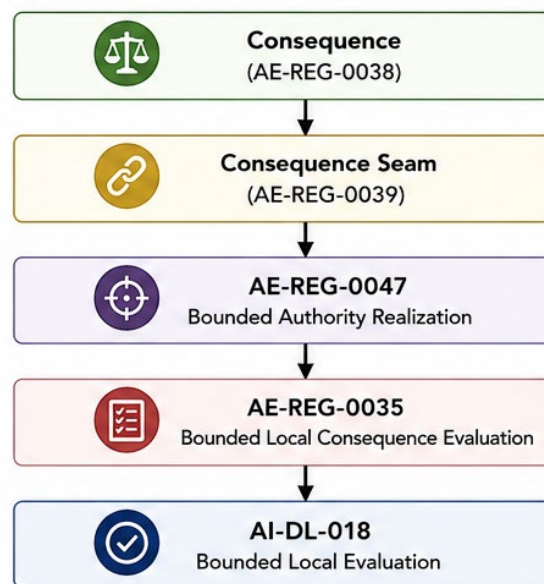
Once decision-making authority is localized to a seam via parent architectural layers, the valid decision scope for actions correspondingly contracts. A localized control point cannot mandate or wait for global systems synthesis; it must evaluate only what local realization strictly requires.

IV. Derivation

The legitimacy of this family depends entirely on its structural derivation from foundational primitives and preceding registry rules.

4.1 The Governing AE Spine Diagram

Figure 4.1: Governing Authority Engineering Spine



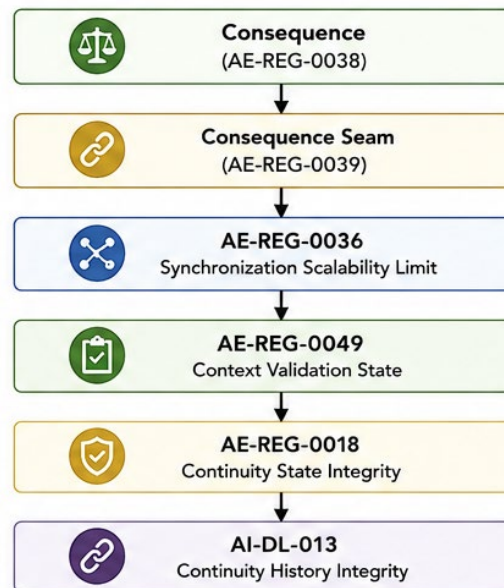
The direct AE dependency chain traces how primitive authority constraints narrow down sequentially to local evaluation scope.

4.2 The Parent AI Root Relationship

Separately, at the Level 2 inter-family review layer, AI-DL-018 establishes its contextual inheritance beneath the parent AI architecture. The principle derives from AI-DL-007 Local Stop Authority: once local seam authority establishes that the local realization boundary decides whether a consequence may proceed, the valid decision scope contracts to the bounded local conditions of that seam. This contraction of valid evaluation scope forms the architectural basis for AI-DL-018.

4.3 The Supporting Path Diagram

Figure 4.3: Supporting State History Integrity Path



The supporting path establishes the necessary state-trustworthiness conditions under distributed execution pressure.

V. Bounded Local Evaluation

This section explains how the governing engineering principle operates within the Tool Use & Boundaries family.

5.1 Scope of Local Evaluation

The boundary of valid local evaluation is determined entirely by what local realization strictly requires to execute safely. A localized control point evaluates the operational state presented directly at the seam interface, verifying that immediate parameters comply with local realization constraints. It is authorized to permit or halt realization based only on those immediate local conditions.

5.2 Bounded Operational Conditions

Bounded conditions define the limits of the information available to local evaluation. The evaluation is restricted to the immediate operational conditions necessary to determine whether a consequence-bearing action may safely proceed at the realization seam. Information beyond those local conditions falls outside the valid scope of the evaluation and therefore cannot become part of the local realization decision.

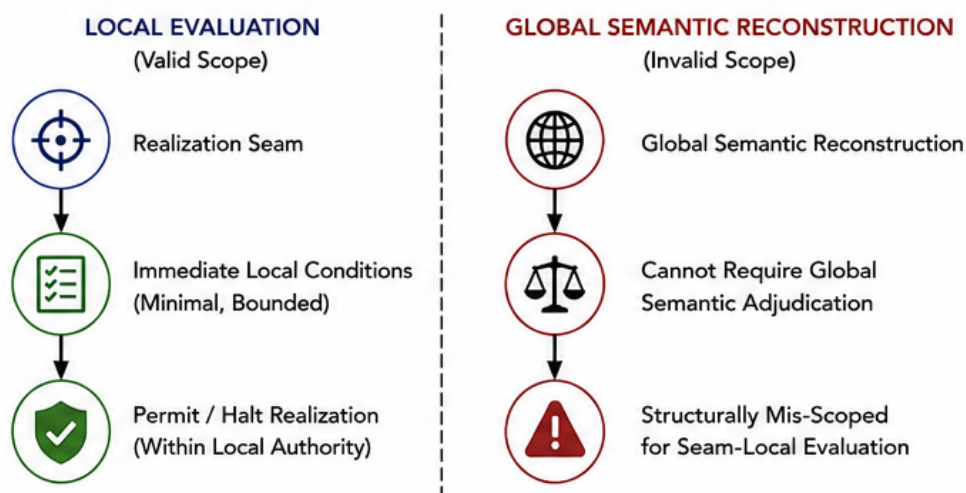
5.3 Why Evaluation Must Remain Local

Because consequence authority becomes local under the parent architecture, valid evaluation scope correspondingly contracts to the seam. Once decision-making authority is restricted to a local realization boundary, the valid decision scope cannot depend on non-local state or global semantic adjudication. Downstream synchronization limitations may appear as adjacent environmental context, but they do not establish this rule. The governing constraint is that local consequence permission must be decided from the bounded local conditions relevant to that seam.

5.4 Local Evaluation vs. Global Semantic Reconstruction

A local stop cannot require global semantic adjudication to function. Local evaluation determines whether a consequence-bearing action may safely proceed at a specific realization seam, whereas global semantic reconstruction attempts to compute total system meaning across distributed execution pathways. Within this family, global reconstruction is structurally mis-scoped for immediate seam-local evaluation.

Figure 5.4: Local Evaluation vs. Global Semantic Reconstruction

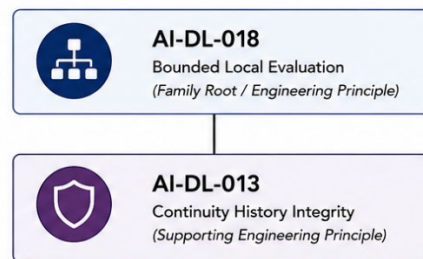


VI. Family Architecture

Family Status

The Tool Use & Boundaries family is intentionally narrow. The accepted corpus presently freezes only one governing engineering principle (AI-DL-018) supported by one subordinate engineering principle (AI-DL-013). No accepted theorem, observation, or corollary has yet been incorporated into the current family architecture, preserving a lean framework focused entirely on the seam-local boundary.

Figure 6.1: Tool Use & Boundaries Family Hierarchy



VII. Supporting Principle

Bounded local evaluation cannot evaluate local state reliably in a vacuum. The family depends directly on AI-DL-013 Continuity History Integrity to remain meaningful.

AI-DL-013 Continuity History Integrity: The state history used to calculate local continuity validation must not be tampered with or retroactively altered by upstream synchronization failure or adversarial compromise of the orchestration chain.

If the localized state metrics feeding the checkpoint are corrupted, the local evaluation scope becomes compromised. Therefore, AI-DL-013 serves as the non-negotiable support condition: it ensures that the localized history utilized at the seam remains trustworthy, even when upstream synchronization pathways experience complete degradation or latency failures.

VIII. Application Surfaces

The application of this family clarifies and restricts how external interactions interface with system state:

- Application at Tool Boundaries: A tool boundary serves structurally to judge bounded local admissibility rather than global system meaning.
- Illustrative AI Tool Calls: Common operations such as AI tool calls function strictly as narrow, non-canonical application surfaces where the rule is localized.

- Local Evaluation Scope: Admissibility at an execution boundary is determined by verifying only the immediate operational conditions necessary for realization at that seam, avoiding any reliance on global semantic synthesis.

IX. Boundaries

To prevent doctrine drift, the boundaries between this family and adjacent architectural structures are strictly enforced:

Adjacent Family	Boundary Distinction	Prohibited Scope Expansion
S3 Synchronization & Scaling	S3 governs when synchronization ceases to scale; this family governs seam-local evaluation scope.	Do not turn tool-boundary evaluation into a synchronization root doctrine.
S4 Continuity & Context	S4 governs whether semantic reconstruction can preserve fidelity; this family governs what the local boundary evaluates.	Do not absorb local realization under reconstruction failure into the tool-boundary family root.
S5 Topology & Reachability	S5 governs topology observability and reachability; this family is downstream from S6.	Do not treat seam-local tool admissibility as a topology root doctrine.
S6 Authority & Delegation	S6 governs <i>who</i> may decide whether consequence proceeds; this family governs <i>how far</i> that evaluation ranges.	Do not replace S6's local-authority root with tool-admissibility language.
AI-DL-014 Consequence & Execution	AI-DL-014 constrains consequence locally under failed reconstruction; AI-DL-018 narrows this to specific evaluation bounds.	Do not collapse the whole execution family into tool-boundary evaluation.

Adjacent Family	Boundary Distinction	Prohibited Scope Expansion
AI-DL-021 Governance & Control	Governance & Control addresses slower-than-execution timing; this family focuses on immediate seam execution.	Do not absorb governance tempo or control-path latency into tool-boundary doctrine.

X. Future Research

Expansion of this family is restricted to established structural mechanisms:

- Accepted Expansion Mechanisms: Refinement is permitted only through engineering-principle expansion under AI-DL-018, supporting principle refinement under AI-DL-013, and narrow operational guidance at consequence seams.
- Preserved Unresolved Questions:
 - Does future autonomous tool-planning material justify promoting a theorem beneath AI-DL-018 about delegated tool-chain depth?
 - Should context-validation-state material remain in this family or migrate into a later AI continuity-runtime subfamily?
- Prohibited Scope: Implied answers to these questions, new independent roots, or unsupported tool taxonomies remain strictly out of bounds.

XI. Conclusion

The Tool Use & Boundaries family does not establish a new authority architecture. Instead, it explains how consequence-bearing interactions at tool boundaries remain governed by AI-DL-018 Bounded Local Evaluation. By restricting evaluation to the immediate conditions necessary for realization, while relying on AI-DL-013 to preserve the integrity of the state history feeding that evaluation, the family extends the AI Foundations architecture without introducing a new independent architectural root.