Aurora Research Initiative (ARI)

ARI Institutional Coordinator

Tooling Constraints (v1.0.0)

Author: Shawn C. Wright
Affiliation: Waveframe Labs — Independent Open-Science Research Entity
ORCID: 0009-0006-6043-9295
Creation Date: 2025-11-27
Concept DOI: https://doi.org/10.5281/zenodo.17743096

This document establishes the binding constitutional constraints governing the CRI-CORE tooling layer. It defines the legal, epistemic, and operational boundaries under which CRI-CORE must function. These constraints ensure that CRI-CORE remains a purely mechanistic execution engine with no authority to interpret, infer, validate, or influence epistemic or methodological logic.

CRI-CORE is the lowest-level enforcement subsystem in the Aurora ecosystem. Its neutrality is essential for preserving governance integrity, reproducibility guarantees, and long-term institutional stability.

---

1. Purpose

The purpose of this document is to:

- define the strict limitations of CRI-CORE
- ensure CRI-CORE performs only mechanical, deterministic execution
- prevent semantic or epistemic influence from tooling
- avoid structural or interpretive overreach
- guarantee independence from AWO and ARI logic
- provide enforceable guardrails for all future CRI development

This document is binding for all implementations and versions of CRI-CORE.

---

2. Required Capabilities of CRI-CORE

CRI-CORE must strictly implement the following capabilities:

2.1 Deterministic Execution

CRI-CORE must: - execute workflows deterministically
- eliminate nondeterministic behavior where possible
- produce byte-identical outputs given identical inputs
- enforce consistency across environments

2.2 Identity and Attestation Enforcement

CRI-CORE must: - perform identity-binding for execution contexts
- enforce attestation independence
- ensure that actors cannot approve their own changes
- validate signatures or checksums as required by ARI

2.3 Integrity Validation

CRI-CORE must: - compute and validate SHA-based integrity hashes
- detect tampering or unapproved modifications
- fail safely when integrity is violated
- verify that artifacts remain unaltered across runs

2.4 Execution Environment Capture

CRI-CORE must: - capture environment details deterministically
- record runtime conditions as metadata
- expose this information for audits
- avoid any implicit environmental dependencies

---

3. Explicit Prohibitions

CRI-CORE is explicitly forbidden from the following actions. These prohibitions are strict, non-negotiable, and enforced by ARI doctrine.

3.1 Epistemic Prohibitions

CRI-CORE may **not**: - interpret the meaning of workflow steps
- evaluate scientific or logical correctness
- infer intent, semantics, or structure
- perform reasoning of any kind

CRI-CORE is a machine, not an epistemic actor.

3.2 Method Prohibitions

CRI-CORE may **not**: - implement or modify method logic
- validate the correctness of workflows
- embed procedural reasoning
- override any logic defined by AWO

CRI enforces; it does not interpret.

3.3 Structural Prohibitions

CRI-CORE may **not**: - inspect, analyze, or infer structural properties of workflows
- attempt to detect logical errors
- conditionally alter execution paths
- modify structure during runtime

All structural interpretation belongs to AWO.

3.4 Governance Prohibitions

CRI-CORE may **not**: - modify ARI governance documents
- approve governance changes
- override ARI or AWO constraints
- engage in any validation of epistemic authority

CRI has no governance role.

3.5 Provenance Prohibitions

CRI-CORE may **not**: - produce metadata
- modify metadata
- infer missing metadata
- correct metadata violations

CRI-CORE may only validate integrity; provenance remains a method/governance responsibility.

---

4. Cross-Layer Boundaries

4.1 CRI-CORE → ARI

CRI-CORE must obey ARI doctrine and governance rules.
CRI may not reinterpret, modify, or influence those rules.

4.2 CRI-CORE → AWO

CRI-CORE accepts workflow instructions mechanically.
It may not: - question them
- refine them
- interpret them
- modify them

4.3 CRI-CORE → Waveframe Labs

Waveframe Labs may implement CRI-CORE, but may not grant CRI any reasoning or interpretive capabilities beyond this document.

4.4 CRI-CORE → Case Studies

Case studies may use CRI for deterministic execution, but may not extend or modify CRI behavior.

---

5. Forbidden Cross-Layer Interactions

The following interactions represent governance failures and are prohibited:

- CRI interpreting workflow meaning
- CRI inferring structural properties
- CRI evaluating correctness or logic
- CRI producing, altering, or inferring metadata
- CRI performing epistemic validation
- CRI altering workflow structure
- CRI conditioning behavior on semantics
- CRI making autonomous decisions

These protections ensure CRI-CORE remains a neutral enforcement mechanism.

---

6. Revision Rules

All revisions require:

1. Approval by the ARI Institutional Coordinator
2. An entry in the governance log
3. Formal version increment
4. Backward linkage to prior versions
5. Rationale included in log entry

No silent modifications permitted.