Quuipu

QUUIPU RESEARCH & ARCHITECTURE SERIES

WHITEPAPER 04

Semantic Integrity

Preserving Meaning Across Adaptive Digital Experiences



Foundational Whitepaper · English

Quuipu Edition 2 · v1

Publication identity

Publication
Semantic Integrity

Series
Quuipu Research & Architecture Series

Publication number
Whitepaper 04

Edition
Quuipu Edition 2 · v1

Language
English

Historical edition
Cognisphere Edition 1

This publication succeeds Cognisphere Edition 1. Historical PDFs remain immutable.

Contents

01. The fundamental property

02. Canonical information

03. Semantic identity

04. Concept identity and relationship integrity

05. Semantic transformation

06. Derived representations

07. Evidence model

08. Claimability

09. Uncertainty

10. Semantic drift

11. Conflicts

12. Versioning

13. Source authority

14. Provenance graph

15. Integrity pipeline

16. Integrity states

17. Semantic fallback

18. LLMs and Semantic Integrity

19. Human agency

20. High-trust domains

21. Testing Semantic Integrity

22. Metrics

23. Governance

24. Multi-tenant integrity

25. IP and definitional property

26. Semantic Integrity invariants

27. The final promise

A. Semantic Integrity data model

B. Semantic failure matrix

C. Claimability ladder

D. Semantic Integrity invariants

Preamble

Preserving Meaning Across Adaptive Digital Experiences

> This publication succeeds Cognisphere Edition 1. Quuipu Edition 2 preserves the historical thesis while updating active brand and publication identity.

Preamble

Preserving Meaning Across Adaptive Digital Experiences

FOUNDATIONAL PRINCIPLE

Meaning as an invariant Form may adapt. Authority and material meaning may not change silently.

Quuipu may change how information is experienced without changing what the authoritative information means.

Canonical Source ↓

Semantic Identity ↓

Evidence ↓

Transformation ↓

Claim Validation ↓

Provenance Binding ↓

Integrity State ↓

Adaptive Experience

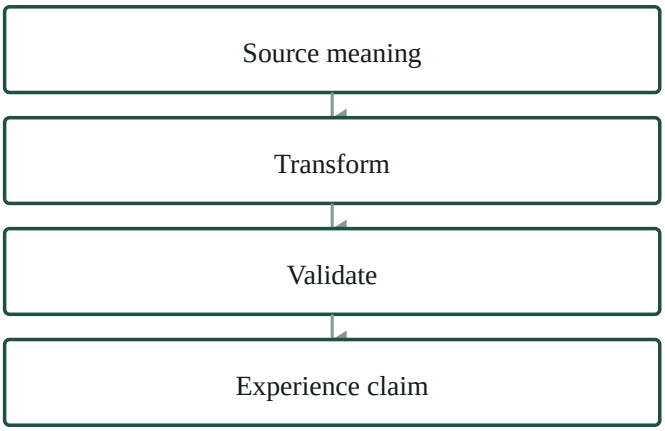


Figure 1 — Semantic Integrity chain.

SEMANTIC MODEL

From content to claim Object Question Integrity requirement

Source Where does authority originate? Scope + version + authority

Concept What semantic object is this? Stable identity

Evidence What supports the statement? Traceable coverage

Claim What may the system assert? Claimability threshold

Transformation What changed in representation? Invariant preservation

Experience What does the user see? Qualification + source path

CHAPTER 01

The fundamental property

Quuipu may change how information is experienced without silently changing what authoritative information means. Semantic Integrity is the system of constraints that makes this promise verifiable.

Experience is variable; meaning is governed A representation may be simplified, sequenced, contextualized or recomposed. These operations change form, order and density, but do not authorize the runtime to create a new editorial truth.

Integrity is not literal sameness Preserving meaning does not mean repeating the same words. It means retaining conditions, relationships, exceptions, quantities, negations, scope and dependencies that determine semantic content.

A system property Semantic Integrity is not a promise made by a generative model. It is an architectural property: source authority, identity, transformation contracts, evidence, provenance, uncertainty, conflict handling and fallback contribute to the same guarantee.

CHAPTER 02

Canonical information

The starting point is the separation of canonical information from derived representation. Without it, adaptation can become an invisible second editorial pipeline.

Canonical authority A canonical source is the authority recognized by a domain for specific information: an institutional page, product record, policy, specification, versioned document or another governed source system.

Canonical does not mean globally true Canonicality is relative to scope and authority. Two organizations may have different canonical sources; one source may be authoritative for policy but not for operational data.

Canonical-first The original representation remains reachable. User and runtime can return to source when transformation is insufficient, uncertain or contested.

Canonical change When the authoritative source changes, derived representations can be invalidated, regenerated or marked stale. Persistence must not freeze obsolete meaning.

Layer Owns Does not imply

Canonical source Editorial/operational authority Universal truth

Derived representation Contextual form New canonical record

Provenance Derivation trace Automatic correctness

Integrity state Quality/limits of derivation Technical uptime

CHAPTER 03

Semantic identity

Semantic identity lets the system recognize that multiple representations refer to the same semantic object even when their forms differ.

Identity anchor A concept needs an anchor: source ID, URI, semantic key or another stable domain identity. The anchor prevents a paraphrase from accidentally becoming a new concept.

Identity across modes Original, Simple and Step-by-step share conceptual identity when they represent the same source. Mode is a property of the representation, not of the canonical object.

Identity across pages Continuity can connect the same concept across pages, allowing Explore to build paths without merging entities that merely share similar terms.

Identity and version Identity and version are distinct: the same entity can evolve. The runtime can express 'same concept, different version' rather than treating every change as a new identity.

CHAPTER 04

Concept identity and relationship integrity

An adaptive ecosystem must preserve not only statements but also relationships among concepts.

Typed relationships Relationships such as requires, applies-to, supersedes, exception-to, part-of or related-to carry different semantic force. Reducing them all to 'related' destroys information.

Directionality Many relationships are directional. If A requires B, B does not necessarily require A. Transformation preserves direction and cardinality where material.

Scope

A relationship may hold only for a version, jurisdiction, product or condition. Scope travels with the relationship.

Relationship provenance Links used by Explore also need origin: explicit source, governed rule or qualified derivation. A plausible relationship is not automatically canonical.

CHAPTER 05

Semantic transformation

A semantic transformation is a controlled operation that produces a derived representation from one or more sources without acquiring their authority.

Transformation intent Each transformation declares its purpose: simplify, decompose, reorder, summarize, compare or contextualize. Different purposes require different controls.

Invariant payload Before transformation, the system can identify payload that must not be lost: numbers, negations, conditions, exceptions, normative terms, references, prerequisites and limits.

Permitted change Form, vocabulary, order, granularity and selection may change within contract. Authority, claim scope and material conditions cannot change without qualification.

Transformation result The result is not merely text: it includes representation, source set, transformation type, integrity status, uncertainty and provenance.

Source + scope ↓

Invariant payload ↓

Transformation intent ↓

Candidate representation ↓

Claim validation ↓

Integrity state

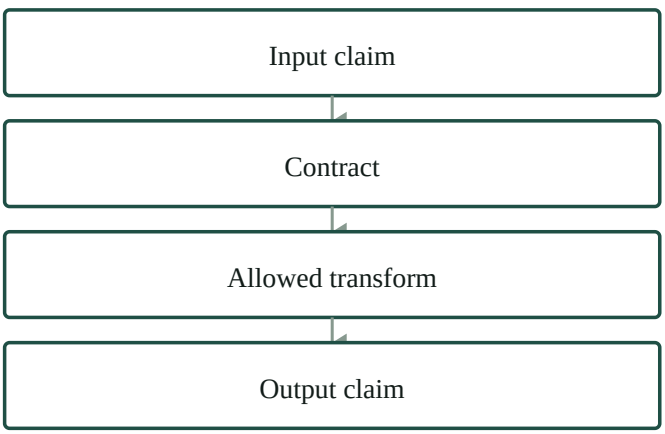


Figure 2 — Transformation contract.

CHAPTER 06

Derived representations

Derived representations are runtime artifacts. Their value comes from making a source more usable while preserving a visible relationship to origin.

Original Original is the canonical reference or a faithful projection of source. It is the control against which other modes can be compared.

Simple Simple reduces linguistic complexity and density. It does not remove qualifiers that change meaning or turn probabilities into certainties.

Step-by-step Step-by-step makes a process or reasoning sequence explicit. Order may be derived only when supported by source or a governed rule.

Composite representation When an answer combines sources, provenance distinguishes which parts depend on which sources and where the runtime performed synthesis.

CHAPTER 07

Evidence model

Evidence lets Quuipu support a representation without confusing plausibility with support.

Evidence unit An evidence unit can be a passage, structured field, record or relationship from an authorized source. It retains source identity and sufficient location.

Evidence coverage A generally relevant source is not enough: material claims in the representation need adequate coverage.

Evidence strength A primary source, structured operational datum and secondary synthesis may have different strength. The model can represent authority hierarchies or policies.

Evidence gaps If a necessary claim is unsupported, the system can omit, qualify, clarify or fall back. It must not fill the gap with stylistic confidence.

CHAPTER 08

Claimability

Claimability defines what Quuipu is authorized to present as a derived assertion on the basis of available sources.

Claim boundary A source may support a fact but not a broader conclusion. The runtime distinguishes what is explicit, what is derivable and what is merely plausible.

Claim classes A useful taxonomy separates canonical claim, supported derivation, qualified inference and unsupported claim. Classes can drive UI and policy.

Material claims Numbers, dates, requirements, obligations, compatibility, availability and conditions are high-materiality claims and require stricter thresholds.

Refusal as integrity Refusing to formulate an unsupported claim is an integrity success, not an experience failure.

Claim class Meaning Default treatment

Canonical Directly stated by authority May be presented as source content

Supported derivation Logically/structurally supported Present with provenance

Qualified inference Plausible but conditional Expose qualification

Unsupported Evidence threshold not met Do not emit as trusted claim

CHAPTER 09

Uncertainty

Uncertainty must not be hidden by fluent language. Quuipu needs to represent what it does not know, what is ambiguous and what depends on unresolved conditions.

Source uncertainty The source can be incomplete, dated or contradictory.

Resolution uncertainty The runtime may not know which source, entity or interpretation matches the intent.

Transformation uncertainty A synthesis may be semantically plausible but insufficiently safe for a high-materiality context.

Experience projection Uncertainty can produce qualifiers, alternatives, clarification, return to Original or refusal. The detail shown may vary, but uncertainty itself must not be falsified.

CHAPTER 10

Semantic drift

Semantic drift is the growing distance between a derived representation and the current meaning of its source or concept.

Source drift The source changes while cache or memory retains an earlier derivation.

Model drift A model or prompt change produces different transformations for the same source.

Context drift A representation valid in one context is reused in another scope.

Vocabulary drift The operational meaning of a term evolves while aliases and semantic maps remain unchanged.

Drift controls Version binding, invalidation, regression tests, semantic fingerprints and policy review reduce risk. No single control is sufficient.

Drift Trigger Control

Source Canonical update Version binding + invalidation

Model Model/prompt release Golden regression suite

Context Reuse outside scope Context binding

Vocabulary Domain meaning changes Schema/ontology review

CHAPTER 11

Conflicts

Authoritative sources can conflict. Semantic Integrity requires preserving conflict when no legitimate rule resolves it.

Conflict detection The system distinguishes version, scope and authority differences from genuine contradictions.

Authority resolution Policy may establish precedence: primary over secondary source, current over obsolete version, transactional data over editorial description. Precedence is governed.

Unresolved conflict If conflict remains, the experience exposes it or reduces the claim. A synthesis that erases disagreement without basis is semantically incorrect.

Conflict provenance Conflicting sources remain identifiable for audit and, where relevant, for the user.

CHAPTER 12

Versioning

Versioning makes meaning temporally verifiable. Without version, provenance can identify the right source but the wrong state of that source.

Source version Document version, ETag, hash, timestamp or revision ID can act as anchors depending on the system.

Transformation version Rules, prompts, models and pipelines producing the representation can also be versioned where reproducibility matters.

Policy version The same source may yield different output as claimability or transformation policy changes. Policy is part of derivation.

Temporal validity An output can be correct at time T and no longer correct at T+1. Integrity represents this temporality.

CHAPTER 13

Source authority

Authority determines which source has the right to establish operational meaning within a scope.

Authority is contextual A commerce catalog may be authoritative for price and availability, documentation for specifications, a legal policy for conditions. The runtime avoids authority leakage.

Primary and secondary sources Secondary sources may help explain but do not override a primary source when a claim depends on primary authority.

Authority registry A mature deployment may maintain a registry of source classes, scopes, priorities and conflict rules. This is an architectural pattern, not a requirement that every site implement it identically.

Authority loss If authority cannot be determined, resolution degrades. Semantic safety comes before apparent completeness.

CHAPTER 14

Provenance graph

The most useful provenance is not a footnote but a derivation graph connecting sources, transformations, claims and outputs.

Nodes Source, source version, evidence unit, transformation, policy, model/capability, claim and representation can be distinct nodes.

Edges derived-from, supported-by, transformed-by, governed-by, supersedes and conflicts-with describe operational relationships.

User view versus audit view A user may see a source link and derivation indicator; audit may require the complete graph. Both views share the same origin.

Provenance completeness A representation can have partial provenance. Status matters because 'provenance present' does not mean 'provenance sufficient'.

Node Example edge Why it matters

Source version supports → Evidence Temporal authority

Evidence supports → Claim Coverage

Policy governs → Claim Claimability

Transformation produces → Representation Derivation

Representation derived-from → Source User/audit trace

Source A conflicts-with → Source B Conflict preservation

CHAPTER 15

Integrity pipeline

Semantic Integrity crosses the entire Quuipu pipeline rather than being applied as a final check after generation.

Pre-resolution Establish scope, source authority, version and policy before source selection.

Resolution Build candidate set and evidence map while distinguishing authority and uncertainty.

Transformation Apply transformation contract and invariant payload during generation.

Validation Check claim coverage, contradiction, material terms, provenance and policy.

Emission Emit representation plus integrity state; otherwise degrade, qualify or fall back.

Authority Resolution ↓

Evidence Mapping ↓

Transformation ↓

Claim Validation ↓

Conflict / Uncertainty Check ↓

Provenance Binding ↓

Emit / Qualify / Fallback

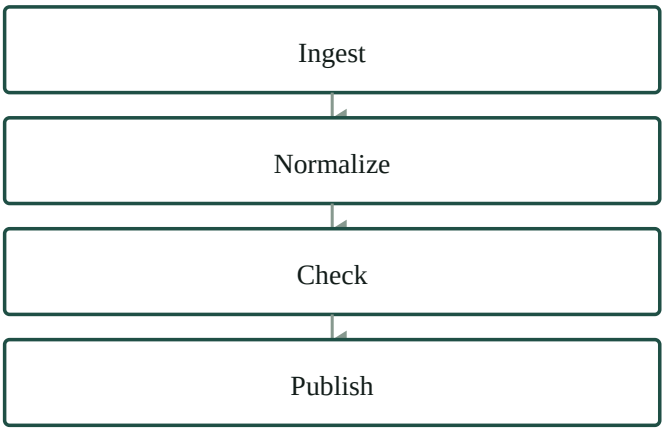


Figure 3 — Integrity pipeline.

CHAPTER 16

Integrity states

Adaptive output needs an integrity state distinct from the technical runtime state.

Verified Material claims are covered by admissible evidence and no unresolved conflict is known within scope.

Qualified The output is usable but contains uncertainty, inference or limits that must remain visible.

Conflicted Admissible sources support incompatible claims and policy does not permit a unique resolution.

Stale The derivation is bound to a version that is no longer current or verifiable.

Insufficient Evidence or provenance does not meet the threshold required for the intended claim.

Rejected The transformation violates an invariant or policy and is not emitted as a trusted experience.

Integrity state Can display? Required behavior

Verified Yes Normal derived experience + source path

Qualified Yes Visible qualification

Conflicted Yes, bounded Expose conflict / alternatives

Stale Usually no Refresh or clearly mark

Insufficient No trusted claim Reduce scope / Original

Rejected No Fallback / refusal

CHAPTER 17

Semantic fallback

Semantic fallback differs from technical fallback: the runtime can be perfectly operational and still decide not to transform.

Return to Original When transformation cannot preserve meaning reliably enough, Original is the natural fallback.

Reduce scope The system can answer only the supported portion of a request.

Expose alternatives Under ambiguity or conflict, it can show alternative interpretations or sources.

Ask for context A missing condition can be resolved by asking the user explicitly rather than inferring it.

Refuse For high-materiality claims, refusal may be the only integrity-consistent response.

CHAPTER 18

LLMs and Semantic Integrity

LLMs can be powerful semantic transformers, but they are not the authority of the system.

Model as capability The model receives bounded input and produces candidate output. Source selection, policy, provenance and fallback remain runtime responsibilities.

Grounding is necessary, not sufficient Providing sources reduces risk but does not guarantee fidelity. Controls are still required for claims, negations, quantities, exceptions and scope.

No authority by fluency Linguistic quality does not increase claimability. Elegant unsupported output remains unsupported.

Model independence Semantic Integrity must survive a model change. If the guarantee exists only for one provider or prompt, it is not an architectural property.

CHAPTER 19

Human agency

Semantic integrity serves the person; it is not merely an audit mechanism.

Inspect source The user can reach the canonical source.

Switch representation The user can compare Original with derived forms.

Correct context The user can correct an intent or scope the system resolved incorrectly.

See qualification When the system is uncertain or a claim is derived, the UI avoids presenting it with the same force as canonical content.

Exit adaptation The user can leave the adaptive layer without losing access to content.

CHAPTER 20

High-trust domains

Integrity thresholds depend on the materiality of domain and claim.

Public administration Requirements, deadlines and procedures need rigorous source authority and versioning.

Commerce Price, compatibility and availability derive from the correct operational systems.

Technical documentation Version and platform are part of meaning; cross-version synthesis can be dangerous.

Education Simplification preserves the concept and distinguishes explanation, example and source.

Enterprise knowledge Internal policy, permissions and tenant boundaries limit not only access but also what may be claimed.

Domain Material claim Primary integrity risk

Public administration Eligibility / deadline Outdated or wrong authority

Commerce Price / compatibility Authority leakage

Documentation API behavior Version mismatch

Education Concept explanation Oversimplification

Enterprise Internal policy Permission/tenant leakage

CHAPTER 21

Testing Semantic Integrity

Fidelity should be testable through suites combining deterministic checks, reference datasets and human evaluation.

Invariant tests Numbers, negations, mandatory terms, conditions and references can often be checked automatically.

Golden transformations Curated reference cases enable regression tests across pipeline or model versions.

Adversarial cases Contradictory, obsolete, ambiguous or near-identical sources test conflict handling and identity resolution.

Human review In complex domains, subject-matter experts evaluate fidelity and materiality. Automation does not remove governance.

Release gates A semantic capability is not promoted on linguistic quality alone; it must pass integrity, provenance and fallback thresholds.

Test family Example Detects

Invariant Negation/number preserved Material omission

Golden Expected transformation Regression

Adversarial Conflicting sources False synthesis

Version Old vs current source Staleness

Human SME Domain review Subtle semantic loss

CHAPTER 22

Metrics

Semantic Integrity needs metrics describing derivation quality rather than only satisfaction or latency.

Claim support ratio Share of material claims covered by admissible evidence.

Provenance completeness Share of derived elements for which source, version and transformation path are sufficiently reconstructable.

Conflict preservation rate Ability not to erase relevant conflict during synthesis.

Stale derivation rate Frequency with which served output is bound to outdated sources.

Fallback precision Ability to fall back when necessary without unnecessarily refusing safe transformations.

CHAPTER 23

Governance

Semantic Integrity requires organizational responsibility in addition to code.

Source governance Who decides which sources are authoritative and for what scope?

Transformation governance Which transformations are allowed for which content classes?

Claim policy Which claims require primary evidence, multiple sources or refusal?

Change governance How are source, model, prompt, policy and semantic-schema updates managed?

Incident governance An integrity loss can be investigated as a product incident with provenance and remediation.

CHAPTER 24

Multi-tenant integrity

In a multi-tenant architecture, semantic integrity includes isolation of meaning and authority among organizations.

Tenant-scoped authority Tenant A's canonical source is not automatically authoritative for tenant B.

Tenant-scoped semantics Aliases, taxonomies and relationship maps can be tenant-specific.

No cross-tenant evidence Evidence from one tenant does not support another tenant's claims unless federation is explicitly governed.

Shared core, isolated truth Runtime code and invariants can be shared while source authority, policy, state and provenance remain isolated.

CHAPTER 25

IP and definitional property

Semantic Integrity can become an important definitional property of Quuipu. Its relevance as an IP asset depends on novelty, technical specificity, implementation and prior art and requires dedicated professional review.

What may be distinctive The combination of canonical authority, contextual adaptation, claimability, provenance binding, integrity states and semantic fallback can be formalized as a coherent technical system.

Architecture before claims Before discussing patentability, it is useful to freeze invariants, data model, pipeline, validation algorithms and failure cases in versioned technical documentation.

No legal conclusion This whitepaper does not conclude that any particular idea is patentable or protectable. It defines technical territory suitable for prior-art search and IP counsel.

CHAPTER 26

Semantic Integrity invariants

The invariants condense the discipline into verifiable rules that remain valid across models, hosts and experience modes.

Meaning before fluency Stylistic quality cannot compensate for loss of meaning.

Authority before synthesis Before synthesis, establish which sources have authority in scope.

Evidence before claim A material claim requires sufficient evidence.

Provenance before trust A trusted derived representation can explain where it came from.

Conflict before collapse Unresolved conflict remains visible rather than being merged into false certainty.

Fallback before fabrication When integrity cannot be preserved, the system reduces scope, returns to Original or refuses.

CHAPTER 27

The final promise

Semantic Integrity turns adaptation from a generative capability into a system discipline. Quuipu can be flexible in form precisely because it is rigorous about meaning.

One concept, many experiences The same concept can be read, simplified, sequenced or explored without losing identity.

One source, traceable derivations Every derived experience remains connected to its origin and the process that produced it.

Adaptive, not arbitrary Context determines which experience is useful; it does not grant the run-time freedom to change authority.

The principle Quuipu may change how information is experienced without changing what the authoritative information means.

CHAPTER A

Semantic Integrity data model

Entity Minimum fields Purpose

SourceRef id, uri, authorityScope, version Anchor canonical information

ConceptRef semanticId, sourceBindings, version Preserve identity

EvidenceRef sourceRef, locator, strength Support claims

Claim claimId, type, materiality, evidence[] Represent assertable meaning

Transformation type, version, invariantSet Describe permitted change

ProvenanceRecord sources, evidence, transformation, policy Reconstruct derivation

IntegrityAssessment state, uncertainty, conflicts, reasons Gate emission

CHAPTER B

Semantic failure matrix

Failure	Risk	Integrity response
Missing authority	Wrong source treated as truth	Degrade / refuse
Unsupported claim	Hallucinated certainty	Remove / qualify / refuse
Lost negation	Meaning inversion	Reject transformation
Lost condition	Over-broad claim	Reject or restore condition
Version mismatch	Stale guidance	Invalidate / refresh
Unresolved conflict	False consensus	Expose alternatives
Broken provenance	Untraceable derivation	Do not trust-enhance
Cross-tenant evidence	Authority/data leakage	Reject + isolate

CHAPTER C

Claimability ladder

Canonical statement ↓

Evidence-backed derivation ↓

Qualified inference ↓

Unresolved hypothesis ↓

Unsupported assertion

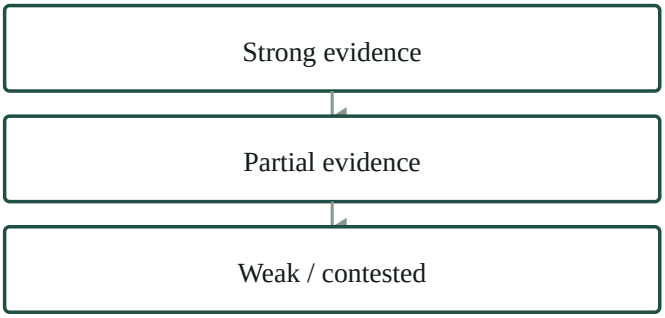


Figure 4 — Claimability decreases as evidence and authority weaken.

The runtime should become more conservative as materiality rises or evidence weakens.

CHAPTER D

Semantic Integrity invariants

SI-01 · Canonical authority Every trusted derivation is scoped to an identifiable authority.

SI-02 · Identity preservation Representation change does not silently create a new concept.

SI-03 · Material fidelity Conditions, negations, quantities and exceptions are preserved.

SI-04 · Evidence before claim Material claims require admissible support.

SI-05 · Claimability boundary Plausibility is not permission to assert.

SI-06 · Provenance binding Trusted output remains traceable to source and transformation.

SI-07 · Uncertainty visibility Unknown, ambiguous and conditional states are not rendered as certainty.

SI-08 · Conflict preservation Unresolved authoritative conflict is not collapsed into consensus.

SI-09 · Version awareness Temporal state is part of semantic validity.

SI-10 · Semantic fallback Integrity failure returns to a safer representation rather than fabrication.

SI-11 · Model independence Integrity controls survive replacement of the generative model.

SI-12 · Tenant isolation Authority, evidence and semantic state remain tenant-scoped.

APPENDIX E

Relationship to the Quuipu series Whitepaper Primary question Relationship to Semantic Integrity

01 · The Cognitive Web Why should Quuipu exist? Integrity protects comprehension from becoming distortion.

02 · Architecture How is the runtime structured? Integrity becomes a cross-cutting architectural discipline.

03 · Quuipu Web What changes on a website? Adaptive representations remain bounded by canonical meaning.

04 · Semantic Integrity How is meaning preserved? Formalizes authority, evidence, claimability, provenance and fallback.

Semantic Integrity Preserving Meaning Across Adaptive Digital Experiences

EXPERIENCE MAY ADAPT. AUTHORITATIVE MEANING MUST NOT SILENTLY DRIFT.