SISMIQ Continuity Requirements (SCR)

Identity Continuity Under Interruption

1. Scope and Intent

This document defines architectural continuity requirements for systems that must preserve identity continuity under interruption.

It applies to distributed, spatial, cyber-physical, and hybrid systems operating under conditions where continuous observation, sensing, or telemetry cannot be assumed.

These requirements are architectural in nature. They do not prescribe specific implementation techniques, inference algorithms, sensor modalities, data formats, or system topologies. Conformance may be achieved through a variety of technical approaches, provided the required behaviors are satisfied.

The purpose of this document is to define the minimum system-level behaviors necessary to prevent identity collapse, duplication, drift, or reset cascades when interruption occurs.

2. Definitions

For the purposes of this document:

Interruption
A condition in which telemetry associated with an entity is degraded, delayed, reordered, partially unavailable, unreliable, or otherwise insufficient to maintain identity association based on observation alone.

Identity
A stable referential designation used by a system to associate state, history, and behavior with an entity across time.

Identity Authority
The system-level designation of which identity instance is authoritative for an entity at a given time.

Persistent Internal State
An internal system representation of an entity that remains addressable independent of continuous external observation.

Identity Authority Association
The maintained association between an entity's identity and its persistent internal state, including during interruption.

Validated Re-Association
A gated process by which restored telemetry is evaluated against preserved internal state before identity authority is resumed.

Reinitialization
Destruction or replacement of an identity instance. Reinitialization is considered an external failure handling action, not a continuity mechanism.

3. Identity Failure Chain Under Interruption

In systems that rely primarily on continuous observation, interruption commonly produces the following failure sequence:

- Telemetry becomes degraded, delayed, reordered, or unavailable
- Observation-based identity inference fails
- Identity ambiguity emerges
- One or more of the following occur:
    - Duplicate identity instantiation
    - Identity drift
    - Incorrect re-association
    - Distributed state divergence
    - Reset cascades
- Downstream system correctness degrades

As systems scale across distributed components, heterogeneous compute environments, and asynchronous execution domains, these failure modes compound and become increasingly difficult to correct manually.

4. Required Architectural Behaviors

Systems claiming interruption-resilient identity continuity **shall** satisfy the following requirements.

4.1 Preservation of Identity Authority Across Interruption

The system shall preserve identity authority across interruption conditions without requiring reinitialization of the identity or its associated internal state.

Loss of telemetry alone shall not be sufficient cause to revoke identity authority.

4.2 Persistent Internal Identity Representation

The system shall maintain a persistent internal state for each entity that remains addressable independent of continuous external observation.

This internal state shall serve as the basis for identity continuity during interruption.

4.3 Downstream Identity Creation Inhibition

During interruption, the system shall inhibit downstream subsystems from creating new identity instances for an entity unless identity authority is explicitly revoked.

This requirement applies across distributed components and execution domains.

4.4 Validated Re-Association Upon Recovery

Upon restoration of telemetry, the system shall perform validated re-association before resuming identity authority.

Restored telemetry shall not automatically overwrite, replace, or supersede preserved internal state without validation.

4.5 Continuity Across Distributed Execution

The required behaviors above shall apply across distributed and heterogeneous compute environments, including edge, cloud, and hybrid execution domains.

Transitions of execution or authority between domains shall not require identity reinitialization.

5. Explicit Non-Requirements

The following are **not** required for conformance:

- Deterministic behavior
- Any specific inference, estimation, or prediction method
- Continuous sensing or uninterrupted telemetry
- Machine learning or artificial intelligence
- Centralized control or global synchronization

- Any specific sensor modality or data format

Architectural continuity may be achieved through deterministic, probabilistic, hybrid, or heuristic techniques.

6. Conformance Statement

A system may claim conformance with SISMIQ Continuity Requirements only if all required architectural behaviors defined in Section 4 are satisfied.

Implementation details are intentionally unspecified to allow adaptation across domains, technologies, and evolving system architectures. Interpretation of these requirements may depend on system architecture, operating environment, and interruption characteristics.

Related Reference Material

Identity Failure Chain Under Interruption
Explanatory overview of common identity failure modes in interruption-prone systems.

Architectural Note: Identity Continuity Under Interruption
Contextual discussion of architectural implications and design tradeoffs.

Continuity Compliance Checklist
Self-assessment tool mapping system behavior to continuity requirements.

Procurement / RFP Language Pack
Specification-ready language for solicitations and contracts.

For architecture or specification discussion:

contact@sismiq.io