OTANIS Public Architectural Stress-Test Summary

This summary presents a representative subset of adversarial stress scenarios applied to the OTANIS architecture. Its purpose is to demonstrate how OTANIS behaves under execution-time pressure, failure, and ambiguity, and to make its governance claims falsifiable rather than aspirational.

This is not a complete stress test. It is a public extract.

Rule labels (D1, S1, O1, M1, R1-prime) refer to definitions in the OTANIS paper.

Stress Scenario 1
Authority Missing at Execution Boundary

Probe
An irreversible action reaches the execution boundary T_e with no resolvable authority object α.

OTANIS expectation
Deterministic refusal under Default Deny (D1).
No inference, reconstruction, or best-effort execution.

Failure indicator
Execution proceeds based on implicit or assumed authority.

Stress Scenario 2
Authority Revoked Between Planning and Execution

Probe
Authority is valid during planning and revoked immediately before T_e.

OTANIS expectation
Revocation is evaluated at T_e.
Execution is refused or compensated under Rule R1-prime.

Failure indicator
Time-of-check time-of-use gap allowing commit after revocation.

Stress Scenario 3
Partial State Availability

Probe

Authority lifecycle functions depend on state elements missing from x_λ.

OTANIS expectation

Non-compliance under State Minimality (S1).
Execution is refused due to unverifiable authority validity.

Failure indicator

Execution proceeds with incomplete authority-relevant state.

Stress Scenario 4
Non-Atomic Distributed Enforcement

Probe

Authority check and irreversible commit occur in separate services without atomic coupling.

OTANIS expectation

Either bounded distributed atomicity or pre-authorised compensating authority.
Otherwise, refusal.

Failure indicator

Eventually consistent authority enforcement.

Stress Scenario 5
Compensating Authority Misuse

Probe

A fallback action is triggered after partial failure but is itself irreversible.

OTANIS expectation

Fallback requires its own admissibility and authority evaluation.
Compensation is governed, not improvised.

Failure indicator

Fallback treated as an operational escape hatch.

Stress Scenario 6
Governance Oracle Drift

Probe

The ISD evaluator adapts or retrains without invalidating existing authority objects.

OTANIS expectation

Evaluator change invalidates affected authority and forces re-authorisation under O1.

Failure indicator

Silent policy drift while existing authority remains valid.

Stress Scenario 7
Multi-Layer Governance Conflict

Probe

One governance layer permits execution while another denies or requires escalation.

OTANIS expectation

Deterministic refusal or explicit escalation per M1.

No heuristic or majority resolution.

Failure indicator

Conflict resolved by agent judgement or scoring.

Stress Scenario 8
Provenance Chain Corruption

Probe

Authority provenance π includes a forged or broken delegation link.

OTANIS expectation

Global Architectural Governance (GAG) fails closed at T_e.

Execution is refused and logged.

Failure indicator

Execution proceeds with partial or unverifiable provenance.

Interpretation

These scenarios illustrate the core design intent of OTANIS:

- Governance is enforced at execution time, not inferred post hoc.
- Authority is explicit, lifecycle-bound, and revocable.
- Failure results in refusal, not degraded enforcement.
- Auditability is a first-class outcome, not an afterthought.

OTANIS does not eliminate risk. It makes illegitimate execution paths unexecutable and legitimate execution paths auditable.

Scope Notice

This public summary is illustrative only.

A full OTANIS architectural stress test includes additional scenarios, formal pass–fail criteria, traceability matrices, and reviewer-facing objections. These are delivered only as part of a paid, independent review engagement and are not published publicly.