

v3.4-EXE-003 – System Resilience & Self-Healing Patterns

Document Title	System Resilience & Self-Healing Patterns
Version	v3.4
Document ID	v3.4-EXE-003
Date	2025-03-22
Author	Take Back Your Data – Reliability Engineering Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the resilience principles and self-healing patterns implemented in MaxOneOpen environments. It ensures operational continuity, controlled fallback, and verifiable system recovery aligned with decentralized trust models.

2. Resilience Design Principles

- No single point of failure (SPOF)
- Decentralized control enforcement
- Containerized twins with isolation
- Real-time monitoring with trigger thresholds
- Edge-preferred fallback routing
- Signature-verified state restoration

3. Self-Healing Logic

Pattern	Trigger	Action
Twin Respawn	Unexpected termination or error exit	Clone from last valid checkpoint
Shadow Swap	Integrity alert or slow twin response	Replace with parallel shadow twin
Quota Drain Override	Overload + no active fallback	Temporary override with containment policy
Monitoring Escalation	Threshold breach or anomaly	Escalate to Control Layer for decision logic

4. Recovery Enforcement & Auditability

- All recovery actions are hashed and timestamped
- Shadow swaps must preserve role and quota state
- No rollback may reintroduce expired or invalid memory
- Control Layer must validate healing logic per instance
- Every recovery leaves an immutable log trace

5. Design Constraints

- Recovery may never bypass Zero-Trust boundaries
- Forks must define healing logic if diverging from default

- Resilience patterns must operate locally and autonomously
- Remote coordination is optional, never required

6. Certification Relevance

System resilience and healing behavior are core certification criteria. MaxOneOpen deployments must demonstrate autonomous fallback and role-consistent recovery under test conditions. Failure to do so invalidates compliance claims.