# Module XX – Test Runtime & Capsule Verification Layer

Version: 4.1 | Classification: CTO Mandatory (Engineering Support Layer)

Scope: Simulation layer for capsule validation, trust enforcement tests, and replay chain coverage

## 0. Purpose & Engineering Requirement

This module defines a formal test runtime and capsule verification layer that enables engineers and CTOs to validate the actual enforceability of MaxOneOpen v4.1 capsule logic. It provides mock capsule structures, replay attack simulation paths, trust escalation emulation, and runtime rule response validation. It is required to ensure implementation traceability and verification depth across all trust tiers.

## 1. Test Capsule Format & Mock Execution Engine

Test Capsules (TC) follow the full execution and ledger submission flow, but are isolated from production trust environments. Each includes:  
`{ capsule\_type, payload\_mock[], trust\_tier\_sim, hash\_seed, rule\_trigger[], expected\_response }`  
The Test Runtime emulates:  
- capsule registration  
- signature binding  
- rule injection and conflict path  
- replay defense (via fake timestamps and ID collisions)

## 2. Verification Coverage & Failure Mapping

Each test case must validate:  
- Replay detection logic (hash/time overlap)  
- Trust tier enforcement and execution lockout  
- Signature chain mismatch response  
- Add-on boundary containment  
Failures are mapped into:  
- `TVC`, `RBC`, `ASC`, `FAC`, or `CRC` capsules  
- Simulation logs with trigger path and resolved logic tree

## 3. Integration Points & Capsule Injection API

The Test Runtime can be integrated into:  
- Manifest Engine prevalidation (Module 06)  
- Replay Handler (Module 13)  
- Audit Capsule Inspector (Module 14)  
- Certification flow precheck (Module 17)  
Capsules can be injected via `TEST\_INJECT(capsule\_object)` or loaded from `.mocapsim` formats.

## 4. Role-Specific Simulation Profiles

Simulation profiles may be defined for:  
- Sovereign CTOs (ledger replay, fork stress tests)  
- Operator roles (rule injection scenarios, audit divergence)  
- Policy agents (validation scope tests, trust recovery chains)

## 5. Output Artifacts & Certification Linkage

All simulation outputs must be logged, signed, and optionally submitted to the ledger test overlay. Valid outputs include:  
- `Verification Summary Capsule (VSC)`  
- `Failure Simulation Capsule (FSC)`  
- `Injection Replay Path Snapshot (IRPS)`  
Module 17 must reference successful capsule simulation coverage before full certification approval.