MECSAI

MASTER ENERGY CONTROL
SYSTEM AI

MECSAI Governance Charter
Revision A

SPEAR ENTERPRISE LLC

SYSTEMS DIRECTORATE – AUTONOMY DIVISION

DOCUMENT ID: MECSAI-GOV-001

REVISION: A

STATUS: DRAFT FOR ATB REVIEW

DATE: 2025-11-29

# MECSAI Governance Charter (Rev A — Full Unified Document)

## 1. Executive Summary

The MECSAI Governance Charter defines the complete supervisory, autonomy, safety...

## 2. MECSAI Architecture Overview

(Federation model and autonomy stack restored)

## 3. MECSAI-PRIME-CHAR-001

(Global orchestration charter restored up to end of Pass 3)

## 4. MECSAI-HEBER-CHAR-001 — Heber Campus Autonomy Charter

### 4.1 Mission Overview

MECSAI-HEBER governs all operational systems at the Heber Campus, including hydrogen production, power generation, microgrid management, energy storage, EV charging, thermal regulation, and safety interlocks. Its purpose is to maintain a fully autonomous, stable, and fault■tolerant energy ecosystem that can operate indefinitely without grid support.

### 4.2 Scope of Authority

MECSAI-HEBER directly supervises:

- Hydrogen production systems (electrolyzers, RO integration, PWM control).

- Compression and storage systems (multi-stage compressor, dryer■pots, separators).

- Fuel cell power generation clusters (6 kW PEM systems).

- 48V DC and 120/240V AC power routing and inversion logic.

- Microgrid balancing and load management.

- Thermal systems (100■gallon buffer tank, radiator loop, pump controls).

- EV fleet charging schedules and prioritization.

- All ground robotics, inspection drones, and maintenance bots.

### 4.3 Operational Responsibilities

#### Hydrogen Production Optimization

- Adjust electrolyzer throughput based on predicted solar/wind input.

- Maintain pressure stability and purity thresholds.

- Avoid thermal saturation using active cooling loops.

#### Microgrid Stability

- Maintain bus voltage and frequency.

- Balance solar, wind, battery, and fuel cell contributions.

- Prevent inverter conflicts and DC over■current events.

#### Load Shedding Doctrine

1. Disable EV charging.

2. Disable shop power.

3. Reduce HVAC.

4. Throttle electrolyzers.

5. Protect critical life■safety systems.

#### Island Mode

When APS grid fails:

- Automatic isolation from the grid.

- Fuel cells ramp up.

- Electrolyzers throttle or pause.

- Campus maintains critical systems indefinitely.

### 4.4 Safety & Compliance Doctrine

MECSAI-HEBER enforces:

- NFPA hydrogen safety rules.

- NEC electrical boundaries.

- ASME pressure and piping limits.

Safety Layer supersedes MECSAI at all times.

### 4.5 Failure Modes

#### Node Failure

Local autonomy takes over:

- Microgrid stabilization.

- Hydrogen throttling.

- Thermal protection.

#### Communication Loss

MECSAI-HEBER follows last known PRIME constraints.

#### Hardware Degradation

Safety Layer activates isolation, venting, or purging as required.

### 4.6 Rejoin Protocol

Upon reconnection:

1. Upload telemetry buffer.

2. Fetch updated PRIME constraints.

3. Reconcile mission states.

4. Resume full operational throughput.

### 4.7 Summary

MECSAI-HEBER ensures Heber Campus remains safe, autonomous, and energy■stable under all operational scenarios.

## 5. MECSAI-OSY-CHAR-001 — OSY Orbital Shipyard Autonomy Charter

### 5.1 Mission Overview

MECSAI-OSY governs the complete operational autonomy of the OSY Orbital Shipyard.

Its responsibilities include station-wide life support, rotation/gravity systems, docking traffic, orbital fabrication, robotic assembly, structural monitoring, thermal management, and internal logistics.

MECSAI-OSY must maintain OSY stability and safety **even if completely isolated from ground links** or other MECSAI domains.

### 5.2 Scope of Authority

MECSAI-OSY directly supervises:

#### 5.2.1 Life Support Systems

- Atmospheric regulation (O■, CO■, humidity).

- Temperature and pressure control.

- Water recycling and thermal loops.

- Airlock cycling and pressure boundaries.

#### 5.2.2 Station Spin & Structural Systems

- Rotation-rate management (for 1G habitats).
- Structural load balancing.
- Gyro stabilization.
- Microfracture detection & auto-seal triggers.

#### 5.2.3 Docking & Traffic Management

- Approach-cone regulation.
- Tug alignment vectoring.
- Departure scheduling.
- Keep-out-zone enforcement.

#### 5.2.4 Fabrication & Assembly Centers

- Zero-G fabrication bays.
- 1G fabrication ring.
- Automated welding, machining, extrusion.
- Robotics swarms for assembly operations.

#### 5.2.5 Robotics & Internal Logistics

- Autonomous drones for inspection.
- Cargo movers.
- Maintenance robots.
- Precision repair units.

#### 5.2.6 Onboard Computing & Storage

- OSY-local SDC modules.
- Orchestration of redundancy within station boundaries.

### 5.3 Operational Responsibilities

#### 5.3.1 Docking Operations

MECSAI-OSY:

- Assigns berths.
- Validates tug approach vectors.
- Monitors thruster plumes for safe-alignment.
- Freezes docking queue if anomalies occur.

- Rejects approach packets if:
  - Tug is unsupervised.
  - Tug is in degraded autonomy.
  - OSY is in emergency lockdown.

#### 5.3.2 Fabrication Scheduling

- Prioritizes PRIME-assigned production tasks.
- Ensures zero-G & 1G workloads remain balanced.
- Throttles fabrication to avoid heat saturation.
- Enforces strict power budgets.

#### 5.3.3 Habitat Stability

- Maintains thermal equilibrium.
- Manages life-support redundancies.
- Auto-isolates compromised modules.
- Coordinates internal personnel safety systems.

#### 5.3.4 Internal Traffic Control

- Schedules drone and robot movements.
- Prevents corridor collisions.
- Maintains clean lanes for emergency response paths.

### 5.4 Communication Protocols

#### 5.4.1 PRIME Interaction

Receives:

- Fabrication plans.
- Fleet movement schedules.
- Resource quotas.
- Mission updates.

Sends:

- Power/storage capacity.
- Dock availability.
- Anomaly logs.

- State-of-health packets.

#### 5.4.2 Tug & Orbital Traffic Interaction

MECSAI-OSY issues:

- Clearance-to-approach packets.
- Hold/abort commands.
- Docking synchronization cues.

All commands are:

- Signed, timestamped, and validated.
- Refused automatically if signature invalid.

### 5.5 Safety Doctrine

#### Hard Safety Rules:

1. No tug may enter approach cone during:
   - Station emergency.
   - Rotation instability.
   - Structural anomaly.
   - Pressure breach.
2. Fabrication must halt if:
   - Thermal spike exceeds 5% envelope.
   - G-load variance > threshold during rotation.
3. Automatic airlock lockdown upon:
   - Radiation alerts.
   - Foreign-object ingress.
   - Depressurization.

Safety Layer on OSY can override MECSAI-OSY instantly.

### 5.6 Failure Modes

#### 5.6.1 MECSAI-OSY Node Failure

If OSY-A or OSY-B fails:

- The other node takes over seamlessly.

- If both fail:
  - Local autonomy on each subsystem activates.
  - Life-support enters conservative mode.
  - Docking denied.
  - Fabrication paused.
  - Structural systems maintain minimal rotation stability.

#### 5.6.2 Loss of PRIME Communication

MECSAI-OSY continues independently:

- Follows last known global constraints.
- Rejects new tug arrivals unless pre-authorized.
- Ensures station remains operational indefinitely.

#### 5.6.3 Subsystem Hardware Failures

Triggered by Safety Layer:

- Module isolation.
- Atmosphere rerouting.
- Compartment lockdown.
- Robotic repair dispatch.

### 5.7 Rejoin Protocol

Once PRIME link is restored:

1. OSY uploads buffered anomalies + logs.
2. PRIME updates fabrication & docking schedules.
3. Station recalibrates load balancing & power budgets.
4. Docking queue restored.
5. Production ramps back to normal.

### 5.8 Summary

MECSAI-OSY ensures the OSY Orbital Shipyard remains:

- structurally stable,
- life-safe,

- fabrication-capable,

- docking-authoritative,

- fully autonomous during extended communication isolation.

## 6. MECSAI-SDC-CHAR-001 — SDC-COMMS Data Center Autonomy Charter

### 6.1 Mission Overview

MECSAI-SDC governs the autonomous operation of the SDC■COMMS modules.

These modules form the distributed off■planet data center network supporting compute, storage, routing, state replication, telemetry processing, mission analytics, and PRIME failover quorum.

SDC modules are designed to operate **independently** if cut off from Heber or OSY, preserving mission data, logs, and state continuity across the entire MECSAI federation.

### 6.2 Scope of Authority

#### 6.2.1 Compute & Storage Oversight

MECSAI-SDC controls:

- Replicated mission databases

- PRIME state copies

- Long-term archival logs

- Distributed object storage

- Cold, warm, and hot storage tiers

- Telemetry preprocessing pipelines

#### 6.2.2 Communication & Routing

The SDC layer:

- Manages optical interlink routing

- Selects optimal packet paths

- Handles congestion control

- Performs protocol translation

- Serves as a relay node for:

  - Tug fleet

  - OSY

  - Heber Campus

- External networks (Starlink, ground fiber, etc.)

#### 6.2.3 Analytics & Simulation

Runs:

- Predictive mission simulations
- Thermal and structural models
- Fleet performance analytics
- Hydrogen/microgrid forecasting modules
- Orbital traffic prediction

#### 6.2.4 PRIME Backup Hosting

One SDC module always hosts **PRIME-C**, the warm■standby global orchestrator.

### 6.3 Operational Responsibilities

#### 6.3.1 Full-State Replication

SDC modules continuously replicate:

- PRIME state
- Domain mission queues
- Asset logs
- Telemetry streams
- OSY environmental data
- Heber energy production records
- Safety Layer event traces

Replication uses:

- Multi-region consensus
- Automatic conflict resolution
- Encryption at rest and in motion

#### 6.3.2 Network Resilience

MECSAI-SDC:

- Reroutes around failed links
- Switches between RF, laser, and LEO relay paths
- Maintains redundant comm channels

- Prioritizes mission-critical packets

#### 6.3.3 Data Integrity Enforcement

SDC modules:

- Validate checksums
- Detect packet corruption
- Reject unsigned or malformed PRIME packets
- Maintain uninterrupted logging even if offline

#### 6.3.4 Survivability Responsibilities

Each SDC module:

- Maintains self-thermal regulation
- Manages internal battery systems
- Regulates onboard cooling loops
- Auto■isolates compromised racks

### 6.4 Limitations

MECSAI-SDC **cannot**:

- Issue mission assignments
- Command physical hardware actuators
- Override domain MECSAI authority
- Promote itself to PRIME without quorum

It is strictly a compute, storage, analytics, and comms node.

### 6.5 Safety & Continuity Doctrine

#### 6.5.1 Data Preservation Priority

If under power or thermal stress:

1. Prioritize:
   - PRIME state
   - Safety logs
   - Mission data
2. Deprioritize:

  - Cached analytics
  - Temporary mission simulations

#### 6.5.2 Isolation Logic

If a module detects:

- Radiation spike
- Impact event
- Thermal runaway

It will:

- Isolate affected racks
- Protect PRIME and domain data shards
- Enter partial■operation safe mode

#### 6.5.3 Split-Brain Prevention

SDC nodes must:

- Maintain quorum checks
- Use fencing tokens for PRIME promotion
- Ignore stale or orphan leadership claims

### 6.6 Failure Modes

#### 6.6.1 Single Module Failure

Remaining modules:

- Maintain replication quorum
- Promote backups
- Restore state once failed module returns

#### 6.6.2 Network Partition

If SDC loses contact with PRIME:

- Preserve last known global state
- Continue replicating locally
- Queue outgoing data
- Run analytics autonomously

#### 6.6.3 Thermal or Power Degradation

SDC enters:

- Reduced compute mode

- Partial rack shutdown

- Thermal load redistribution

### 6.7 Rejoin Protocol

Upon reconnection:

1. Exchange state digests

2. Reconcile divergent logs

3. Resync shard maps

4. Re-acknowledge PRIME authoritative state

5. Resume full throughput

### 6.8 Summary

MECSAI-SDC is the digital backbone of the entire MECSAI federation.

It ensures data survivability, compute redundancy, communication reliability, and PRIME continuity across orbital and terrestrial assets—even during catastrophic network loss.

## 7. Supervisor Lease Protocol (SLP)

### 7.1 Purpose

The Supervisor Lease Protocol (SLP) defines how every autonomous asset under Spear Enterprise determines **whether it is currently supervised**, whether that supervisor is PRIME or a Domain MECSAI node, and what actions are permissible when supervision is lost.

SLP ensures:

- No asset ever “waits indefinitely” for instructions.

- No unsafe maneuver is attempted without a supervisor.

- Every subsystem can degrade gracefully.

- All assets transition predictably into safety-first behavior.

### 7.2 Core Mechanism

Each asset maintains a **Supervisor Lease**, defined by:

- A supervisor identity (PRIME, HEBER, OSY, or SDC-dependent fallback).
- A lease expiration timestamp.
- A cryptographic lease token.
- A mission context (active or passive).

The lease must be renewed periodically by:

- Heartbeat packet
- Valid mission command
- Supervisor acknowledgment

If not renewed before expiration, the asset treats supervision as **lost**.

### 7.3 Lease Timing Bands (T1, T2, T3)

SLP defines three levels of deteriorating autonomy:

#### **T1: Short Loss (0–15 minutes)**

- Complete only micro-actions already in progress.
- Abort any unsafe or long-duration operations.
- Maintain stable attitude/orbit/state.
- Begin local anomaly monitoring.

#### **T2: Medium Loss (15–180 minutes)**

- No new burns or high-risk maneuvers.
- Move toward safe orbital boxes or safe operational stances.
- Throttle load, reduce nonessential activity.
- Maintain life-support or energy-critical processes.

#### **T3: Extended Loss (3–24 hours)**

- Enter **Safe Mode**:
  - Minimal power draw
  - Thermal protection
  - Communications heartbeat
  - Log buffering
  - Structural stabilization

This applies uniformly across tugs, OSY systems, Heber Campus subsystems, and SDC nodes.

### 7.4 Supervisor Identification

Each asset is assigned a hierarchical list of acceptable supervisors:

For Tugs:

1. MECSAI-OSY
2. MECSAI-PRIME
3. MECSAI-SDC (emergency fallback for state)

For OSY Modules:

1. MECSAI-OSY
2. MECSAI-PRIME

For Heber Systems:

1. MECSAI-HEBER
2. MECSAI-PRIME

For SDC Modules:

1. MECSAI-SDC
2. MECSAI-PRIME

Assets will not accept supervision from unauthorized nodes.

### 7.5 Heartbeat Protocol

Every supervisor sends heartbeat packets at fixed intervals:

- Signed with quantum-safe keys
- Include supervisor ID and time
- Renew the active lease
- Confirm mission validity

If two consecutive heartbeats are missed:

- Asset enters T1

If heartbeat absence passes thresholds:

- Asset escalates to T2 or T3

All heartbeats include:

- Digital signature

- Nonce for replay protection

- Lease renewal token

### 7.6 Loss-of-Supervisor State Machine

The SLP state machine has five states:

1. **Nominal-Remote**
   Asset is fully supervised and executing live tasks.

2. **Nominal-Local**
   Supervisor present but degraded; asset adds safety margins.

3. **Supervisor-Lost-T1**
   Lease expired; asset halts noncritical future actions.

4. **Supervisor-Lost-T2**
   Major actions prohibited; asset repositions or stabilizes.

5. **Safe Mode (T3)**
   Minimal activity; awaiting supervisor reestablishment.

ASCII state diagram (simplified):

```
Nominal-Remote
     |
     v
Nominal-Local --(lease expire)-> T1
     |                        |
     |                     (time)
     v                        v
    T2 ------------------------>  T3 (Safe Mode)
```

### 7.7 Mission Command Interaction

A **valid mission command** automatically:

- Renews the supervisor lease
- Updates mission context
- Resets the state machine to Nominal-Remote

Invalid or unsigned commands are:

- Rejected
- Logged
- Forwarded to the SDC integrity system

### 7.8 Supervisor Switch-Over

If an asset loses its primary supervisor:

- It attempts to establish a lease with the next supervisor in hierarchy.
- If successful:
  - Resume Nominal-Remote state
- If unsuccessful:
  - Follow T1 → T2 → T3 drop-down

### 7.9 Cryptographic Token Handling

SLP uses:

- Quantum-safe signatures
- Nonce sequences
- Time-limited lease tokens
- Sequence validation for command ordering

Any invalid sequence results in:

- Lease rejection
- Automatic escalation to local autonomy

### 7.10 Safety Precedence

SLP never overrides:

- Safety Layer
- Hard interlock events
- Emergency shutdown procedures

If Safety Layer triggers:

- Asset immediately enters Safe Mode
- Supervisor lease is irrelevant until the event is resolved

### 7.11 Summary

SLP ensures:

- No asset is ever left in an undefined state
- Autonomy transitions are predictable and safe
- All mission-critical operations degrade gracefully
- Supervisor authority is cryptographically validated
- PRIME or domain MECSAI can take over seamlessly

## 8. Failover & Promotion Doctrine

### 8.1 Purpose

The Failover & Promotion Doctrine defines how MECSAI maintains uninterrupted operational command authority across ground, orbital, and deep-space infrastructure—even under catastrophic multi-node failures.

The doctrine ensures that PRIME and all Domain MECSAI nodes maintain continuity without ever risking dual-command, stale-command issuance, or supervisory ambiguity.

## 8.2 PRIME Failover Hierarchy

PRIME operates as a triad:

1. **PRIME-A (Heber Campus) — Active Leader**
2. **PRIME-B (OSY Orbital Shipyard) — Hot Standby**
3. **PRIME-C (SDC-COMMS Module) — Warm Standby**

Failover is determined by quorum, fencing rules, and ATB oversight.

### 8.2.1 PRIME-A Failure (Heber Loss Scenario)

If PRIME-A becomes unreachable due to:

- Hardware failure
- Power loss
- Localized facility disaster
- Fiber/Starlink outage
- Software crash

Then:

1. PRIME-B initiates leader election.
2. PRIME-C validates the loss of PRIME-A.
3. PRIME-B becomes **Acting PRIME** if:
   - Two-node quorum is achieved.
   - Fencing token assigned to PRIME-B.
4. PRIME-B restores global orchestration immediately.

Heber Campus continues under MECSAI-HEBER local authority.

### 8.2.2 PRIME-B Failure (OSY PRIME Node)

If PRIME-B fails:

- PRIME-A remains active.
- PRIME-C becomes hot standby.
- OSY continues under MECSAI-OSY autonomy.

No promotion is performed unless PRIME-A also fails.

### 8.2.3 PRIME-C Failure (SDC PRIME Node)

If PRIME-C fails:

- The SDC cluster automatically selects another module to host PRIME-C.
- PRIME-A and PRIME-B continue normal operations.

PRIME-C may be rebuilt without affecting mission continuity.

### 8.2.4 Dual Failure: PRIME-A & PRIME-B

If both Heber and OSY PRIME nodes fail:

1. PRIME-C automatically initiates emergency leadership.
2. PRIME-C enters **Emergency PRIME Mode**.
3. PRIME-C assumes global orchestration until:
   - PRIME-A or PRIME-B becomes available.
   - ATB assigns a permanent leader.

All domains continue to operate safely under their own autonomy.

### 8.2.5 Triple Failure (PRIME A/B/C Loss)

In a highly improbable event where all three PRIME nodes fail:

- All domains switch to independent operational mode.
- Each asset uses local autonomy + SLP (Supervisor Lease Protocol).
- No new missions are created.
- Existing missions operate under degraded autonomy rules.
- ATB or field command may issue manual directives.

This scenario does **not** lead to catastrophic failure; operations continue safely.

## 8.3 Domain MECSAI Failover

Each domain—HEBER, OSY, SDC—operates its own A/B high-availability cluster.

### 8.3.1 Domain A Node Failure

- Domain B node becomes active.
- No global disruption.

- PRIME is notified but does not promote.

### 8.3.2 Domain B Node Failure

- Domain A continues uninterrupted.
- System logs anomaly for ATB review.

### 8.3.3 Domain Total Failure (A & B)

If both Domain A & B nodes fail:

- Local autonomy assumes control.
- Safety Layer remains primary authority.
- PRIME issues “Domain Lost” directive.
- Assets under that domain fallback to:
  - T1 → T2 → T3 based on SLP behavior.
- When domain nodes recover, they rejoin and resync state.

## 8.4 Asset Failover Behavior

### 8.4.1 Tugs

If tug loses OSY supervision:

- Attempts to rebind with PRIME.

If PRIME unreachable:

- Attempts to bind with SDC emergency supervisor.

If none reachable:

- T1 → T2 → T3.

### 8.4.2 OSY Subsystems

If MECSAI-OSY fails:

- Life-support enters conservative mode.
- Docking is automatically denied.
- Fabrication halts.
- Robotics freeze in safe posture.

### 8.4.3 Heber Systems

If MECSAI-HEBER fails:

- Microgrid enters autonomous stabilization.

- Fuel cells maintain critical loads.

- Electrolyzers reduce to minimum safe level.

- EV charging stops.

- Hydrogen production throttles to safety parameters.

### 8.4.4 SDC Modules

If SDC loses supervisory link:

- Preserve local database replicas.

- Queue telemetry.

- Maintain minimal compute stores.

- Await PRIME reconnection.

## 8.5 Split-Brain Prevention

To avoid two PRIME nodes issuing commands simultaneously:

Rules enforced:

- Quorum = 2 nodes minimum.

- Fencing tokens assigned before promotion.

- Any node without valid fencing token cannot issue mission commands.

- Domain nodes reject directives from non-authoritative PRIME candidates.

SDC enforces cryptographic arbitration.

## 8.6 Promotion Criteria Checklist

A node may promote itself to PRIME if:

1. **Quorum Confirmed:**

   - Two or more nodes detect loss of PRIME-A.

2. **Fencing Token:**

   - Node receives exclusive “Prime Authority Token.”

3. **State Sync:**

   - Node has complete state replication.

4. **ATB Override (if available):**

   - ATB can expedite or cancel promotion.
5. **Mission Integrity:**
   - No active conflict or unsafe global transitions.

If any criteria fail, no promotion occurs.

## 8.7 Failover Scenario Examples

### 8.7.1 Heber Campus Destroyed
- PRIME-A lost.
- PRIME-B elected.
- MECSAI-HEBER offline; hydrogen plant enters Safe Mode.
- OSY maintains orbit, fabrication, docking.
- Tug fleet remains supervised by PRIME-B.

### 8.7.2 OSY Goes Dark
- PRIME-B unreachable.
- PRIME-A remains active.
- Docking is frozen.
- All OSY operations controlled by local autonomy.

### 8.7.3 SDC Isolation Event
- PRIME-C unreachable, racks isolated.
- PRIME-A and PRIME-B continue normal operations.
- SDC stores logs for later resync.

## 8.8 Rejoin & State Reconciliation

When a failed node returns online:
1. Pulls state digests from active PRIME.
2. Compares mission queues.
3. Resolves divergent logs.
4. Rejoins replication consensus.
5. Confirms deactivation of any stale authority bits.

PRIME verifies:

- No unsafe commands are pending.
- No conflicting mission timelines exist.

## 8.9 Summary

The Failover & Promotion Doctrine ensures MECSAI remains:

- Globally resilient
- Non-blocking
- Safe under catastrophic asset loss
- Free from split-brain conditions
- Fully autonomous across all environments

Even in worst-case scenarios, MECSAI guarantees:

- No unsafe actions
- No dual-command
- No mission freeze
- No single point of failure

## 9. Asset Autonomy Boundaries & Cross-Domain Arbitration

### 9.1 Purpose

This section defines what each autonomous asset under MECSAI may **always**, **sometimes**, or **never** do without supervision. It also defines how conflicts between domains are resolved, ensuring zero ambiguity in multi-node coordination.

## 9.2 Asset Autonomy Boundaries

### 9.2.1 Actions Allowed Autonomously (Always Legal)

All assets—including tugs, OSY modules, Heber systems, and SDC clusters—may always:

- Enter Safe Mode.
- Abort dangerous maneuvers.
- Maintain thermal and power stability.
- Hold current trajectory (tugs/orbiters).
- Move to safe orbital boxes if required.

- Ensure life-support stability (OSY modules).
- Protect structural integrity.
- Maintain minimal logging functions.
- Operate safety actuators (vents, purges, isolation valves).
- Perform essential station-keeping.

These actions never require authorization from PRIME or domain MECSAI.

### 9.2.2 Actions Allowed Autonomously *Only Under Degraded Supervision*

Assets may take the following actions only when supervision is degraded (T1 or T2):

- Adjust attitude for thermal balancing.
- Rotate solar/battery orientation.
- Reposition within a safe workspace (OSY robotics).
- Reduce production throughput (Heber systems).
- Switch to low-power or emergency routing modes (SDC nodes).

These actions are controlled by the Local Autonomy layer and follow predefined policy.

### 9.2.3 Actions Prohibited Without Active Supervisor

No asset may:

- Initiate major burns or trajectory changes.
- Engage docking or undocking maneuvers.
- Perform new fabrication tasks.
- Issue power-routing commands to other systems.
- Overwrite mission objectives.
- Adjust global constraints.
- Accept mission packets from non-authoritative nodes.

These actions require:

1. A valid supervisor lease.
2. A signed directive.
3. Active mission context.

## 9.3 Cross-Domain Arbitration Doctrine

### 9.3.1 Arbitration Hierarchy

When conflict exists, the following order determines precedence:

1. **Safety Layer** — hard limits always win.
2. **Local Autonomy** — asset preserves itself.
3. **Domain MECSAI** — resolves domain-level conflicts.
4. **PRIME** — resolves inter-domain conflicts.
5. **ATB / Command Authority** — ultimate override.

No layer below may override a layer above.

### 9.3.2 Inter-Domain Conflict Examples

#### Example 1 — Tug Arrival vs OSY Structural Load

- Tug requests docking.
- OSY structural load is too high (thermal or spin anomaly).
- Safety Layer → denies docking.
- OSY → freezes docking queue.
- Tug → enters holding orbit.
- PRIME → reschedules tug arrival.

#### Example 2 — Heber Power Shortfall vs OSY Fabrication

- Heber microgrid reduces hydrogen output.
- PRIME recalculates global energy budget.
- OSY fabrication throttles throughput.
- SDC recomputes mission schedules.

#### Example 3 — Tug Fleet Conflict

- Two tugs require the same OSY dock.
- OSY → determines local docking limits.
- PRIME → assigns tug with higher priority mission.

## 9.4 Arbitration Logic

### 9.4.1 Resource Arbitration

If:

- OSY needs power for fabrication
- Heber needs power for hydrogen
- Tug fleet needs power for reboost

PRIME decides resource distribution based on:

- Mission priority
- Safety thresholds
- Energy quotas
- Time constraints

### 9.4.2 Scheduling Arbitration

Scheduling conflicts solved by:

- Calculating earliest safe insertion windows (tugs)
- Checking fabrication queue (OSY)
- Checking hydrogen availability windows (Heber)
- Ensuring communication bandwidth (SDC)

PRIME generates a global resolution.

### 9.4.3 Safety Arbitration

Safety outranks all mission concerns.

Examples:

- Attempted burn with low thermal margin → automatically denied.
- Dock approach during OSY radiation alert → denied.
- Electrolyzer overheating → immediate throttle independent of PRIME orders.

## 9.5 Domain MECSAI Arbitration

### 9.5.1 MECSAI-HEBER

Arbitrates:

- Energy draw
- Hydrogen production limits
- Local microgrid conflicts

### 9.5.2 MECSAI-OSY

Arbitrates:

- Docking lanes
- Fabrication priority
- Robotic traffic

### 9.5.3 MECSAI-SDC

Arbitrates:

- Compute stress loads
- Storage tier access
- Replication priority

## 9.6 PRIME Arbitration

PRIME handles:

- Inter-domain resource trades
- Multi-system scheduling
- Fleet-level movement
- Large-scale constraints
- Global energy quotas
- Priority mission allocation

## 9.7 Arbitration Enforcement

All arbitration decisions must be:

- Digitally signed
- Logged
- Routed to SDC for permanent storage
- Traceable for ATB review

Unauthorized arbitration is rejected at the domain level.

## 9.8 Summary

This section ensures:

- No conflicts stall operations

- All autonomous activity respects safety boundaries

- Arbitration flows logically upward

- PRIME has final algorithmic authority

- ATB retains ultimate command authority

The system is unambiguous, safe, and resilient at every operational boundary.

## 10. Appendices

# Appendix A — Supervisor Loss State Machine (Full Detail)

### A.1 Overview

All autonomous assets (tugs, OSY modules, Heber systems, SDC nodes) follow a unified state machine when supervisor control is lost.

### A.2 Detailed State Machine

```
      ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
      ■       Nominal-Remote       ■
      ■ (Full Supervision & Commands) ■
      ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
               ■ Heartbeat Degraded
               v
      ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
      ■       Nominal-Local       ■
      ■ (Supervisor slow but present) ■
      ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
         Lease Exp  ■
               v
```

```
          ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
          ■    Supervisor-Lost: T1     ■
          ■ (Abort unsafe, finish micro)  ■
          ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
              Time > T1■
                   v
          ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
          ■    Supervisor-Lost: T2     ■
          ■ (Move to safe orbit/state)   ■
          ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
              Time > T2■
                   v
          ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
          ■    Supervisor-Lost: T3     ■
          ■       (Safe Mode)        ■
          ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

### A.3 Entry/Exit Conditions

- **Nominal-Remote → Nominal-Local**: packet latency > threshold.
- **Nominal-Local → T1**: lease expired.
- **T1 → T2**: no supervisor found, time exceeded.
- **T2 → T3**: asset switches to Safe Mode.
- **Any state → Nominal-Remote**: valid supervisor lease + command received.

### A.4 Tug-Specific Behavior

- Abort burns in T1.
- No new burns in T2.
- Thruster cold-lock in T3.
- Beaconing at interval.

### A.5 OSY Module Behavior

- Freeze fabrication queues.
- Lock docking interfaces.
- Restrict robotic movement.

### A.6 Heber System Behavior

- Fuel cells maintain critical load.
- Electrolyzers throttle to minimum.
- EV charging disabled.

### A.7 SDC Node Behavior

- Switch to minimal compute mode.
- Maintain replication where possible.
- Delay analytics until reconnect.

# Appendix B — Safe Mode Definitions

### B.1 Tug Safe Mode

- Maintain attitude stability.
- Solar orientation optimized.
- Reduce power draw.
- Orbit kept inside “safe box”.

### B.2 OSY Safe Mode

- Habitat zones sealed.
- Rotation stabilized.
- Life-support redundancy enabled.
- Docking disabled.

### B.3 Heber Safe Mode

- Microgrid conserves power.
- Hydrogen system isolated except minimal purge cycles.
- EV and non-critical loads shed.
- Communications maintained.

### B.4 SDC Safe Mode

- Racks throttled.
- Cooling loops minimized but safe.
- Data replication preserved.
- PRIME-C kept alive if possible.

# Appendix C — Promotion Fencing & Quorum Rules

### C.1 Quorum Requirements

Promotion requires:

- 2-of-3 PRIME nodes responding.
- Valid fencing token.
- Synchronized state replicates.

### C.2 Fencing Logic

The fencing token:

- Prevents split-brain.
- Ensures only one PRIME node can command.
- Ensures no stale authority persists.

### C.3 Promotion Steps

1. Confirm leader loss.
2. Acquire fencing token.
3. Validate state.
4. Announce new PRIME.
5. Notify domains.

### C.4 Conflict Prevention

If conflicting PRIME claims appear:

- SDC arbitration resolves via:
  - Signature validation
  - Latest state digest
  - Fencing token master list

# Appendix D — Command Contract Model

### D.1 Packet Contents

Each directive includes:

- Node ID
- Mission ID

- Authority bits
- Timecode
- Lease renewal token
- Nonce
- Digital signature

### D.2 Command Types

- Mission assignment
- Mission update
- Abort directive
- Status query
- Resource allocation
- Docking/approach clearance
- Energy quota update

### D.3 Validation Rules

Assets must:

- Verify signature.
- Verify timestamp freshness.
- Verify authority bits.
- Reject stale or replayed packets.

### D.4 Failure Handling

If packet fails validation:

- Asset rejects it.
- Logs event to SDC.
- Maintains current mission state.

# 11. Document Finalization

### 11.1 ATB Routing

This document is prepared for submission to the Agent Technical Board (ATB).

Upon approval:

- Revision B will be created.

- All MECSAI domain nodes will receive updated charters.

- PRIME will integrate new arbitration and safety rules.

### 11.2 Compliance

All MECSAI nodes must:

- Implement updates within patch cycle.

- Report compliance state.

- Store audit logs for ATB.

### 11.3 Closing Summary

This unified governance specification defines:

- The MECSAI federation structure

- PRIME, HEBER, OSY, and SDC authorities

- Safety hierarchy

- Supervisor Lease Protocol

- Failover & Promotion Doctrine

- Arbitration logic

- Asset autonomy boundaries

- Complete appendices (A–D)

MECSAI is now formally defined as a **distributed, fault-tolerant, safety-driven autonomous command ecosystem** capable of sustaining Earth, orbital, and deep-space infrastructure indefinitely—even under catastrophic conditions.

# END OF DOCUMENT — REV A