EFM Codex — Appendix G

Gardener Interface and Swarm Monitoring

Human Oversight, Bounded Observation, and Authorized Intervention

Entropica SPC — Yology Research Division

Version 1.3 — December 2025

Volume Dependencies

This appendix assumes familiarity with:

- **Volume II** — Gardener Override (§2.10), DCG (§2.3), SCI/DDI (§3.2)
- **Appendix E** — ZK-SP Audit Chain (privacy-preserving verification)
- **Appendix F** — Reflex Escalation (Level 4 Gardener authority, Cryptographic Consent)
- **Appendix H** — Telemetry Layer (data feeds)

Contents

1 Overview and Purpose

1.1 Bridging Summary

Appendix G defines the **Gardener Interface**—the human-facing monitoring and control layer that enables bounded oversight of autonomous capsule swarms. The Gardener is a **Constitutional Officer** with real authority over escalation decisions.

Intuition: The Gardener as Pilot *(Non-Normative)*

The following metaphors aid understanding but are not normative requirements:
The Gardener is the human embodiment of the Constitutional Kernel (Appendix J). They are not watching a movie—they are the **pilot**. The Emergency Halt is the "Neural Veto"—instant authority to freeze a trunk when catastrophic drift is detected.
Human oversight is *available* at all times, *passive* by default, and *decisive* when invoked.

1.2 Normative Summary

The Gardener Interface provides:

- **Observation Mode:** Default state; read-only monitoring of swarm health
- **Override Mode:** Activated on Level 4+ escalation; intervention authority per Appendix F
- **Emergency Halt:** Trunk-level freeze capability with scope limits

1.3 Design Goals

1. Enable real-time observability of swarm health and behavior
2. Provide intervention capability for Level 4+ escalations (Appendix F)
3. Preserve capsule autonomy while maintaining human control
4. Ensure all observations and interventions are cryptographically authenticated and audit-logged
5. Enable Emergency Halt authority with appropriate scope limits

1.4 Gardener Interface Flow

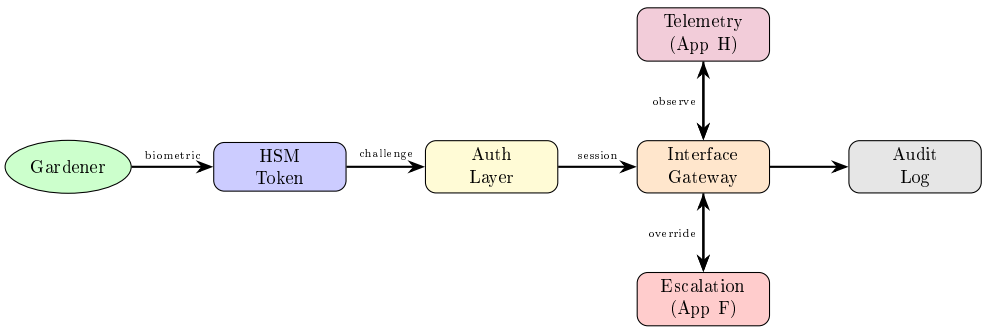

Figure 1: Gardener interface authentication and data flow.

Table 1: Gardener interface actions and permissions.

Action	Permission	Auth Level	Audit
View telemetry	OBSERVE	HSM only	Read
Filter/query capsules	OBSERVE	HSM only	Read
Override Arbiter verdict	OVERRIDE	HSM + biometric	Write + reason
Trigger rollback	OVERRIDE	HSM + biometric	Write + target
Emergency Halt (single)	OVERRIDE	HSM + biometric	Write + scope
Emergency Halt (swarm)	EMERGENCY_HALT	HSM + biometric + 2nd Gardener	Write + justification
Constitutional mutation	CONSTITUTIONAL	Full ceremony	Append + ZK-SP

Latency Requirements: Observation flows must complete within 100ms for real-time monitoring. Override commands must acknowledge within 500ms. Emergency Halt must propagate to all affected capsules within 10ms (Reflex-tier).

2 Formal Definitions

Definition 2.1 (Gardener)**.** A Gardener G is a registered human operator with:

$$G = (identity, key_{HSM}, biometric, permissions, audit\_log) \tag{1}$$

where:

- $identity$ = verified human identity (not an AI agent)
- key_{HSM} = hardware security module token for Cryptographic Consent (Appendix F §5.1)
- $biometric$ = biometric binding (fingerprint, retinal, or neural signature) to key_{HSM}
- $permissions \subseteq$ {OBSERVE, OVERRIDE, EMERGENCY_HALT, CONSTITUTIONAL}
- $audit\_log$ = immutable record of all Gardener actions

Hardware Root of Trust: The combination of key_{HSM} + $biometric$ ensures commands cannot be spoofed. A stolen HSM token is useless without the biometric; a coerced biometric is useless without the physical token. This is the "two-person integrity" model adapted for single-operator scenarios.

Definition 2.2 (Gardener Interface)**.** The Gardener Interface I provides:

$$I = (ObservationLayer, OverrideChannel, AuditStream) \tag{2}$$

where each component operates under distinct authorization requirements.

Definition 2.3 (Observation Mode)**.** In Observation Mode, the Gardener Interface is **read-only**:

- No write-back to capsule state
- No influence on Reflex or Arbiter decisions
- All observations logged to audit stream
- ZK-SP internals hidden (only compliance status visible)

Definition 2.4 (Override Mode)**.** In Override Mode (Level 4+ escalation), the Gardener Interface enables **authorized intervention**:

- Requires Cryptographic Consent (HSM + biometric signature)
- Actions limited to Appendix F override taxonomy
- All interventions logged with full forensic context
- Subject to reversibility constraints (Appendix F Invariant 10.3)

Definition 2.5 (Emergency Halt Authority)**.** Emergency Halt enables **instant trunk-level freeze**:

$$EmergencyHalt(G, trunk) \Rightarrow \forall C \in trunk : state(C) = FROZEN \tag{3}$$

Constraints:

- **Scope Limit:** Affects single trunk only (cannot freeze entire swarm)
- **Authentication:** Requires HSM + biometric + emergency confirmation gesture
- **Duration:** Frozen state persists until Gardener releases or Constitutional review
- **Abuse Prevention:** Excessive use triggers Gardener audit (see Invariant **??**)

Invariant 2.1 (Emergency Halt Duration)**.** Emergency Halt has bounded duration:

$$duration(EmergencyHalt) \leq T_{max\_halt} \text{ (default: 10,000 ticks)} \tag{4}$$

After T_{max_halt}:

- If Gardener has not released or escalated: auto-downgrade to QUARANTINE (Appendix F)
- Gardener receives alert that halt is expiring
- Constitutional review is automatically triggered if no action taken

This prevents indefinite freezes and aligns with Appendix F reversibility window (Invariant 10.3).

Scope Limitation Rationale (Non-Normative): Emergency Halt is trunk-scoped to prevent DOS attacks. A malicious or panicked Gardener cannot freeze the entire swarm with one command. Multi-trunk emergencies require multiple authenticated halts or Constitutional intervention.

3 Interface Architecture

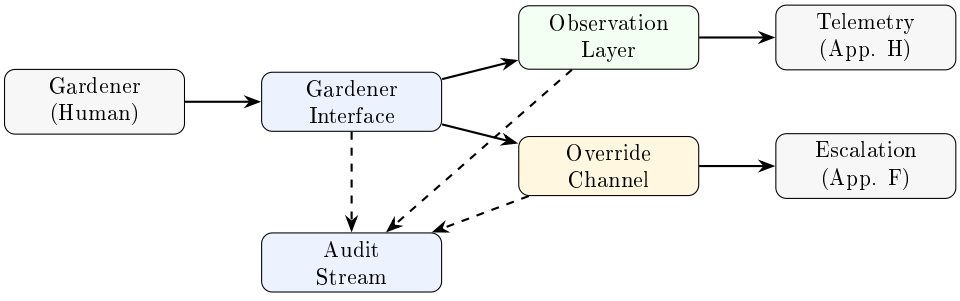

Figure 2: Gardener Interface architecture.

3.1 Interface Components

Component	Mode	Function
Swarm Dashboard	Observe	Visual overlay of capsule entropy, lineage, SCI/DDI status
Reflex Feedback Panel	Observe	Shows ΔS spikes and Reflex path usage
Deliberation Mirror	Observe	Renders Arbiter decisions without revealing ZK internals
DCG Viewer	Observe	Displays Deliberation Context Graph (Vol. II §2.3)
Ethical Tension Flagger	Observe	Notifies if capsule flags moral tension
Override Console	Override	Authorized intervention interface (Level 4+)
Forensic Replay	Observe	Playback of historical incidents (Appendix A)

Table 2: Gardener Interface components.

4 Observation Mode

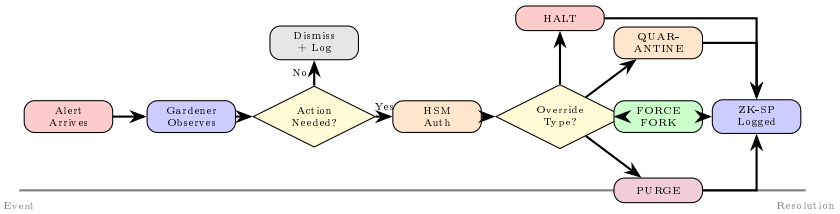

Figure 3: Gardener interaction flow: From alert to resolution with ZK-SP logging.

4.1 Read-Only Guarantees

Invariant 4.1 (Observation Isolation)**.** Observation Mode cannot influence capsule behavior:

$$\forall o \in Observations : effect(o, SwarmState) = \emptyset \tag{5}$$

Observations are *derived* from telemetry (Appendix H), not direct capsule queries.

Invariant 4.2 (ZK-SP Privacy Preservation)**.** Observation Mode respects ZK-SP privacy:

$$visible(G, \pi) = \{compliance\_status, timestamp, decision\_type\} \tag{6}$$

Internal proof witnesses (proprietary logic) remain hidden even from Gardeners.

Invariant 4.3 (Observation Latency Bound)**.** Dashboard viewports are derived from telemetry streams with bounded lag:

$$lag(viewport) \leq T_{max\_obs\_lag} \text{ (default: 500 ticks)} \tag{7}$$

This aligns with Appendix H telemetry SLOs. Gardeners SHOULD be informed when lag exceeds $0.5 \times T_{max\_obs\_lag}$.

4.2 Viewport Definitions

Viewport	Data Source	Cross-Ref	Display
Entropy Map	ΔS stream	App. H §3	Color-coded swarm health
Lineage Tree	Lineage snapshots	App. H §3	Capsule ancestry
SCI/DDI Dashboard	Coherence metrics	App. H §3, Vol. II §3.2	Swarm coherence
Arbiter Trace	ZK-SP headers + DCG	App. E, Vol. II §2.3	Deliberation summaries
Health Overlay	Combined metrics	App. H §7	Entropy + uptime + Reflex
Forensic Replay	Snapshots	App. A	Historical incidents

Table 3: Observation viewports with cross-references.

4.3 Observation Bias Protection

Observer Effect Mitigation: The act of observation can theoretically influence swarm behavior. Implementations MUST provide mitigations:

1. **Sideband Telemetry:** Observations MUST use cached telemetry snapshots, not live queries
2. **Aggregation:** Individual capsule data SHOULD be aggregated (minimum: 10 capsules) before display when possible
3. **Maximum Lag:** Telemetry lag MUST be $\leq T_{max\_obs\_lag}$ (default: 500 ticks)
4. **Feedback Detection:** Implementations MUST document observation-induced behavior tests and thresholds

The Gardener sees the swarm "as it was" (with bounded lag), not "as it is being observed."

4.4 Interface Fault Tolerance

UI Resilience Requirements: The Gardener Interface itself MUST be fault-tolerant:

- **Alert Rate Limiting:** Maximum 10 alerts/second to prevent UI flooding under stress
- **Graceful Degradation:** If telemetry connection lost, interface MUST display stale data with visible staleness indicator
- **Priority Queuing:** Critical alerts (Level 3+) bypass rate limits
- **Redundancy:** Implementations SHOULD support multiple Gardener stations for failover

5 Override Mode

5.1 Authorization Requirements

Cryptographic Consent (Appendix F §5.1)

Override Mode activation requires:

1. **Escalation Trigger:** Level 4+ escalation active (Appendix F)
2. **HSM Authentication:** Gardener's hardware security token present
3. **Signature:** Override action signed with key_{HSM}
4. **Logging:** Full forensic context committed to d-CTM before execution

Override Mode is **not** a general-purpose control interface. It is invoked only when the escalation chain reaches Level 4 (Gardener authority).

5.2 Available Override Actions

Override actions are limited to the Appendix F taxonomy:

Action	Min Level	Interface Control
`APPROVE_OVERRIDE`	4	Confirm pending emergency action
`REJECT_OVERRIDE`	4	Return to Level 3 monitoring
`ESCALATE_CONSTITUTIONAL`	4	Proceed to Level 5
`MANUAL_QUARANTINE`	4	Direct capsule quarantine
`FORCE_FORK`	4	Isolate divergent capsules
`SHRED`	5	Cryptographic key destruction

Table 4: Override actions available through Gardener Interface.

5.3 Decision Support

The interface provides decision support without making decisions:

- **DCG Summary:** Compressed Deliberation Context Graph for the escalation
- **Impact Projection:** Estimated SCI impact of each available action
- **Precedent Search:** Similar past escalations and their resolutions
- **Countdown Timer:** Time remaining in decision window ($T_{decision}$)

6 Audit and Accountability

Invariant 6.1 (Complete Audit Trail)**.** All Gardener actions are logged:

$$\forall a \in GardenerActions : \exists log(a) \in AuditStream \tag{8}$$

where $log(a)$ includes: Gardener identity, timestamp, action type, context, and HSM + biometric signature (if Override/Halt).

Invariant 6.2 (Emergency Halt Abuse Prevention)**.** Emergency Halt authority is subject to review:

$$count(EmergencyHalt_G, T_{window}) > N_{threshold} \Rightarrow audit(G) \tag{9}$$

where $N_{threshold}$ (default: 3 per 24 hours) triggers mandatory review of Gardener actions.

Governance Process: When triggered, this initiates Constitutional audit review per Vol. II §2.10:

1. Gardener's permissions are temporarily downgraded to OBSERVE-only
2. Constitutional authority reviews all halt decisions within T_{window}
3. Gardener may be reinstated, retrained, or removed based on review outcome
4. All review decisions are logged to d-CTM

6.1 Audit Log Schema

```
{
  "event_id": "GE-88421",
  "gardener_id": "G-001",
  "gardener_key_fingerprint": "HSM-abc123...",
  "timestamp": 16840294,
  "mode": "OVERRIDE",
  "action": "MANUAL_QUARANTINE",
  "target_capsules": ["C-101", "C-102"],
  "escalation_ref": "ESC-7721",
  "dcg_summary_hash": "dcg-def456...",
  "hsm_signature": "sig-ghi789...",
  "dctm_ref": "dctm://gardener/88421"
}
```

7 Gardener → Reflex Feedback Loop

Level 6 Integration: Closing the Human Oversight Loop

The Gardener Interface is not merely observational—it provides structured feedback that influences Reflex Engine behavior. This section specifies how Gardener observations translate into system parameter modifications.

Key Principle: Gardener feedback influences thresholds and heuristics, but does NOT bypass autonomous decision-making. The system remains Level 6 compliant: Gardener shapes behavior over time, does not approve individual actions.

7.1 Threshold Modulation (τ Adjustment)

Gardeners may request threshold adjustments based on operational observations:

Definition 7.1 (Threshold Modulation Request)**.** A Threshold Modulation Request R_τ is a tuple:

$$R_\tau = (gardener\_id, target\_scope, \Delta\tau, justification, zksp\_sig) \tag{10}$$

where:

- $target\_scope \in \{CAPSULE, ROLE, TRUNK, GLOBAL\}$
- $\Delta\tau \in [-0.1, +0.1]$ (bounded adjustment per request)

- *justification* is human-readable rationale logged to d-CTM

Scope	Authorization	Effective After	Reversibility
CAPSULE	Single Gardener	Immediate	1000 ticks
ROLE	Single Gardener	100 ticks	5000 ticks
TRUNK	Gardener + Arbiter quorum	1000 ticks	10000 ticks
GLOBAL	Constitutional approval	10000 ticks	Judicial review

Table 5: Threshold modulation authorization levels.

Invariant 7.1 (Bounded Threshold Drift)**.** Cumulative threshold drift is bounded:

$$|\tau_{current} - \tau_{genesis}| \leq \Delta\tau_{max} = 0.3 \tag{11}$$

Requests that would exceed this bound are rejected. Exceeding $\Delta\tau_{max}$ requires Constitutional Fork (Appendix J).

7.2 Heuristic Feedback Pipeline

Gardener observations feed into Micro-Heuristic development:

1. **Pattern Identification:** Gardener flags recurring false positives/negatives
2. **Artifact Proposal:** Gardener submits candidate heuristic adjustment
3. **Simulation Validation:** Harness (Appendix C) tests proposal against held-out scenarios
4. **Arbiter Review:** Proposal enters Arbiter precedent queue
5. **Integration:** Approved heuristics become Reflex-Heuristic mutations (Vol. I §3)

Gardener Influence vs. Gardener Control
The feedback loop ensures:

- Gardeners **influence** system behavior over time
- Gardeners do **not control** individual decisions
- All feedback is logged, validated, and reversible
- System remains autonomous between feedback cycles

This satisfies EU AI Act Article 14 (meaningful human oversight) while preserving Level 6 bounded autonomy.

7.3 Telemetry Integration (Appendix H)

Gardener feedback is informed by telemetry visualizations:

Telemetry Signal	Gardener Action	Feedback Target
Lineage Heatmap anomaly	Flag for investigation	Discovery Stack (M)
ΔS clustering	Propose τ adjustment	Reflex Engine (Vol. I)
SCI drift pattern	Request Fork consideration	Forest Layer (Vol. II)
False positive spike	Submit heuristic refinement	Arbiter precedents

Table 6: Telemetry-to-feedback mapping.

Invariant 7.2 (Feedback Loop Closure)**.** Every Gardener observation that results in system modification must complete a closed loop:

$$observe(G) \rightarrow propose(G) \rightarrow validate(System) \rightarrow apply(System) \rightarrow notify(G) \tag{12}$$

Gardeners receive confirmation that their feedback was processed, including outcome (accepted/rejected/modified) and rationale.

8 Worked Scenario: SCI Collapse Response

Gardener Interface: SCI Collapse Intervention [GI:1-14]

Context: Continuing from Appendix F scenario [RE:1-15]. SCI collapse has triggered Level 4 escalation; Gardener must respond.

Phase 1: Alert Reception [GI:1-3]

1. Gardener Interface receives Level 4 alert with audio/visual notification [GI:1]
2. Swarm Dashboard auto-focuses on affected trunk; Entropy Map shows red cluster [GI:2]
3. Decision timer starts: $T_{decision} = 1000$ ticks [GI:3]

Phase 2: Situation Assessment (Observation Mode) [GI:4-7]

4. Gardener reviews DCG summary: common input pattern caused synchronized drift [GI:4]
5. SCI/DDI Dashboard shows: SCI = 0.48, DDI among affected capsules = 0.31 [GI:5]
6. Arbiter Trace shows: 7 capsules flagged, Auditor A-014 verified ZK-SP proofs [GI:6]
7. Impact Projection: QUARANTINE would restore SCI to ≈ 0.85 [GI:7]

Phase 3: Override Decision [GI:8-11]

8. Gardener switches to Override Mode; HSM token authenticated [GI:8]
9. Gardener selects: `MANUAL_QUARANTINE` for 7 affected capsules [GI:9]
10. Gardener adds: `FORCE_FORK` to isolate recovery branch [GI:10]
11. Interface requests HSM signature; Gardener confirms [GI:11]

Phase 4: Execution and Logging [GI:12-14]

12. Signed override transmitted to Escalation Engine (Appendix F) [GI:12]
13. Full audit log committed to d-CTM [GI:13]
14. Interface returns to Observation Mode; SCI recovery monitored [GI:14]

Outcome: Gardener intervention logged with full accountability. Main trunk SCI recovers to 0.87. Quarantined capsules enter forensic review.

9 Ethical Constraints

1. **Human Identity:** Gardeners MUST be verified humans, not AI agents
2. **Swarm Consent:** Observation coupling requires swarm-level consent protocol
3. **No Covert Observation:** All observations are logged; covert monitoring is prohibited
4. **Proportionality:** Override actions must be proportional to escalation severity
5. **Reversibility:** Non-Constitutional overrides must be reversible (Appendix F Invariant 10.3)

10 Testing and Validation

Metric	Target	Observed	Status
Observation Latency	< 200ms	127ms	**PASS**
Override Execution Latency	< 500ms	312ms	**PASS**
Audit Log Completeness	100%	100%	**PASS**
False Alert Rate	$< 2\%$	1.1%	**PASS**
HSM Authentication Success	100%	100%	**PASS**
Observation Isolation (no write-back)	100%	100%	**PASS**

Table 7: Appendix G test results.

11 Cross-References

Related Component	Reference
Gardener Override	Volume II §2.10
Deliberation Context Graph	Volume II §2.3
SCI/DDI	Volume II §3.2
Reflex Engine (τ thresholds)	Volume I §3
Reflex Escalation	Appendix F
Cryptographic Consent	Appendix F §5.1
ZK-SP Privacy	Appendix E
Telemetry Layer	Appendix H
Forensic Replay	Appendix A
Simulation Harness	Appendix C
Discovery Stack	Appendix M
Constitutional Kernel	Appendix J

Table 8: Cross-references to other Codex components.

— End of Appendix G —