

## AGI-COS v2.2 (部署验证与技术接口版)

基于 v2.1 完整版的架构，v2.2 应重点解决“技术接口标准化”与“本地化部署验证”的问题，使其成为可直接调用的 API 接口与操作手册。

---

### AGI-COS v2.2

Civilizational Operating System

Deployment & Interface Standard Edition

(部署验证与接口标准版)

---

#### 一、版本声明

Version: v2.2

Status: Technical Implementation Standard

Purpose: Define Technical Interfaces & Verification Protocols for AGI-COS 2.1

AGI-COS v2.2 translates the "Seven-Layer Architecture" into executable code, APIs, and legal templates, enabling institutions to "plug in" to the global stability infrastructure.

---

#### 二、技术接口标准

##### 2.1 Sensing API (感知接口)

用于连接各国/机构的数据源与 AGI-COS 感知层。

Input Format: Standardized JSON streams for SSI/CI indicators.

Privacy Protocol: Zero-Knowledge Proof (零知识证明). Local nodes can submit data status (e.g., "High Stress") without revealing raw sensitive data (e.g., specific military movements).

Latency Requirement: < 100ms for IRI alerts.

##### 2.2 Intervention API (干预接口)

用于接收 AGI 建议并执行微干预。

Action Format: Structured Command Packages (SCP).

Human-in-the-Loop Requirement: Every SCP must carry a digital signature from a Human Authority key. Unsigned packages are rejected by local execution systems.

---

#### 三、微干预伦理审查协议

针对 v2.1 Layer 3 的落地细化：

##### 3.1 Intervention Classification (干预分级)

Type A (Invisible): Algorithmic parameter tuning. (Requires: Automatic Log).

Type B (Soft): Resource reallocation. (Requires: Department Head Approval).

Type C (Visible): Public guidance. (Requires: Public Announcement).

##### 3.2 Mandatory Sunset Clause (强制日落条款)

All Micro-Interventions must have an expiration time (default: 72 hours).

Extension requires a new round of human authorization.

If the network is down, interventions automatically expire to prevent permanent automated control.

---

#### 四、先行者架构实施细节

##### 4.1 托管协议

v2.1 提到的“中立机构托管文件”，v2.2 定义其技术实现：

Repository: Distributed Ledger (e.g., IPFS + Permissioned Blockchain).

Release Logic: "Dead Man's Switch". If X number of key nations deposit ratification documents, the system remains armed. Once threshold N is reached, the "Activation Block" is mined, and all deposited documents are simultaneously revealed.

#### 4.2 验证节点

Major AI labs and neutral states run "Verification Nodes" to confirm that no participant has secretly activated early.

---

### 五、文明学习层防篡改机制

#### 5.1 Immutability Standard

Critical incident reports stored in the Global Civilization Learning Archive are hashed and anchored to a public blockchain.

Conflict Resolution: If multiple nodes report conflicting narratives of an event, all versions are preserved but tagged with "Source Confidence".

#### 5.2 Dark Archive

A backup of the learning archive stored in offline, air-gapped facilities to survive systemic digital collapse.

---

### 六、系统隔离协议

应对极端情况（如某节点失控）：

#### 6.1 Contagion Detection

If Node A reports "Normal" but neighboring Nodes B, C, D report "Anomalous Input from A", Node A is flagged as "Compromised".

#### 6.2 Firewall Activation

The Coordination Secretariat (or automated consensus) issues a "Block Command".

Nodes B, C, D sever non-essential links with Node A to prevent cascade failure, while maintaining minimal humanitarian channels.

---

### 七、部署成熟度模型

定义组织采用 AGI-COS 的等级：

Level 1 (Observer): Subscribe to public indicators (SSI/CTI).

Level 2 (Compatible): Implement Perception Audit Layer.

Level 3 (Integrated): Connect to Intervention API, participate in MEU pilots.

Level 4 (Guardian): Host a Verification Node, contribute to Learning Archive.

---

### 八、最终声明

AGI-COS v2.2 bridges the gap between governance philosophy and engineering reality.

It ensures that as complexity accelerates, our ability to coordinate remains robust, verifiable, and secure.

---

End of Release