中央主權、地方自治與動態不動點中央

v0.1 / 2026-07-30 / Neo.K / 治理架構論文／分布式權限與領導權轉移規格

證據狀態：E0——形式模型、治理協議與 MVP 驗證路線

https://thisoneisneok.com/html/papers/stdi-07.html

SECTION

分布式具身智能的權限格、治理紀元、分裂腦防護與責任收斂

Central Sovereignty, Local Autonomy, and the Dynamic Fixed-Point Center: Authority Lattices, Governance Epochs, Split-Brain Protection, and Responsibility Convergence in Distributed Embodied Intelligence

系列：《時空域支配智能》系列第 7 篇

文件編號： EML-STDI-DGC-2026-v0.1

作者： Neo.K

協作整理： Aletheia（阿萊）

機構： EveMissLab／一言諾科技有限公司

日期： 2026 年 7 月 30 日

文件類型： 治理架構論文／分布式權限與領導權轉移規格

證據成熟度： E0——形式模型、治理協議與 MVP 驗證路線

公開狀態： 私人研究稿；公開前應經 EML-CF 的 IP Gate、安全、來源與治理審查

上位理論： STDI｜時空域支配智能

直接前序：

- 《時空間支配型 AI：從單體具身智能到持續性時空域治理》
- 《超靈的物理化：從 O-Chip 維度代理人到分布式具身主體》
- 《Oversoul Station Fabric：固定站、移動站與虛擬站的分布式具身網路》
- 《持續性指揮控制區：AI 如何佔據、維持並安全解除一個物理時空域》
- 《語義即物理路由：從資料流治理到物料、能源、站點與行動流治理》
- 《具身即佔域，對齊即能力：分布式身體的時序容量、協調稅與規模邊界》

SECTION

摘要

時空域支配智能必須同時解決兩個看似矛盾的要求。第一，跨站點研究、物料保管、能源分配、世界狀態和責任提交需要一個能做出全局決策的治理中心；第二，任何中央智能都不應越過地方站點的硬體互鎖、即時安全、現場感知與合法作用邊界。若中央過強，系統容易形成高延遲、單點失效、權限過度集中與遠端錯誤放大；若地方過強，則可能出現目標分裂、重複執行、樣本保管衝突、資源爭用、分裂腦與責任無法歸屬。

本文提出一套適用於分布式具身智能的治理模型：

> 中央主權不是中央可做所有事；地方自治也不是地方可自行決定一切。兩者應由決策層級、作用域、時間租約、世界紀元與責任鏈共同界定。

本文將「中央」從固定機器或固定模型重新定義為：

> 在特定治理紀元、特定物理作用域與特定決策類別中，持有最新合法治理狀態、有效權限證書和足夠提交能力的暫時穩定決策中心。

此概念稱為 動態不動點中央（Dynamic Fixed-Point Center, DFC）。它之所以是「動態」，是因為中央可隨網路、任務、故障、資訊完整度和組織授權而轉移；它之所以是「不動點」，是因為在一個治理紀元內，多個候選節點經過資格檢查、領導者選舉、日誌一致性、政策驗證和站點承認後，必須收斂到一個穩定、可引用的治理狀態：

> cal-F_e(c_e^*)=c_e^*.

這不表示該節點永遠不變，而表示在紀元 e 的有效期限內，所有受管站點對「誰可簽發域級命令、哪個治理日誌為準、哪個 fencing token 最高」形成可驗證的一致承認。

本文建立五層權限格：

> Hard Safety
> >
> Domain Constitution
> >
> Valid Lease／Epoch
> >
> Global Plan
> >
> Local Optimization.

地方站點永久保留硬安全否決權；域憲法約束中央與地方；跨站資源、樣本保管、世界紀元與不可逆任務由合法中央提交；地方 Agent 可在租約和效果契約內重規劃，但不得擴張作用域、自行續租、改寫研究目標或把未提交的地方狀態冒充全局事實。

本文提出五類決策提交：

- C0：本地緊急決策——不等待中央；
- C1：地方可逆決策——在租約內執行並事後提交；
- C2：域級協調決策——需合法中央與治理紀元；
- C3：高風險物理決策——需中央、地方安全與人類批准；
- C4：法律、IP 與公共釋出決策——由人類所有者與 EML-CF 決定，AI 無最終發布權。

  本文以 Raft、Chubby、Kubernetes Lease／Coordinated Leader Election、NIST Zero Trust、Spanner 的時鐘不確定性管理，以及網路化多代理一致性研究為現實參照。Raft 證明可將共識拆分為領導者選舉、日誌複製和安全；Chubby 展示粗粒度鎖、主節點選舉與小型可靠元資料服務；Kubernetes 使用 Lease 確保高可用控制面中只有一個實例主動工作，2026 年的 Coordinated Leader Election 更讓候選者攜帶身分與版本資訊；NIST Zero Trust 強調不能因網路位置而自動信任；Spanner 則將時鐘不確定性明確暴露，而不是假裝所有節點共享完美時間。

  本文同時承認分布式治理的理論限制。在純非同步網路中，即使只有一個程序可能故障，也不能保證確定性共識總能終止。因此，STDI 不能承諾在任意分區和故障下同時保持全局一致、持續可用與無限自治。對物理系統而言，合理策略是：

> 【安全與權限單一性優先於全局可用性】

當不能證明唯一合法中央時，站點只能進入有限地方自治、完成安全義務、保存樣本、停止高風險行動並等待重新收斂。

本文的核心命題為：

> 真正的中央不是最強的模型、最快的伺服器或永久指定的主機，而是當前能被合法授權、被多數或必要權限方承認、承接最新責任狀態，並受到地方安全限制的治理不動點。
>
> 關鍵詞： 中央主權、地方自治、動態不動點中央、Dynamic Fixed-Point Center、權限格、治理紀元、領導者選舉、租約、fencing token、分裂腦、地方否決、責任分區、Raft、Chubby、Kubernetes Lease、Zero Trust、分布式具身智能
>
> 前六篇已建立：

- 一個 AI 如何治理物理時空域；
- 一個超靈如何透過多個身體行動；
- 多個身體如何形成 OSF 站網；
- 站網如何跨時間維持 PCD；
- 高階意圖如何經 DomainIR 路由到物理執行；
- 多站點能力如何受對齊和協調稅限制。

> 現在必須回答：

- 中央 AI 可以決定什麼？
- 地方 Agent 可以拒絕什麼？
- 網路分裂時哪個中央仍有效？
- 中央轉移時，舊中央如何失去權力？
- 地方離線後可自主到什麼程度？
- 多個 AI 對同一域產生不同計畫時，如何收斂？

- 出現事故時，責任歸中央、地方、控制器還是人類？

若沒有這一層，超靈站網可能同時收到兩組互斥命令，也可能因「中央離線」而讓地方節點無限制擴權。

SECTION

1.1 全能中央

假設中央：

- 永遠在線；
- 擁有完整世界狀態；
- 比地方更清楚現場；
- 可以直接越過本地安全；
- 可以即時控制所有站點。

這在物理上不成立，也會形成巨大爆炸半徑。

SECTION

1.2 完全地方自治

假設每個站點可根據自身觀測自由決策。

這會造成：

- 樣本保管衝突；
- 資源重複預約；
- 研究目標分裂；
- 世界狀態不一致；
- 權限自行擴張；
- 責任難以收斂。

SECTION

1.3 中央只是「最強模型」

模型能力高，不表示它：

- 持有合法權限；
- 擁有最新治理日誌；
- 與現場保持有效聯繫；
- 能承擔事故責任；
- 有資格簽發物理租約。

  因此：

> Intelligence
> ≠
> Authority.

SECTION

2.1 策略主權

決定：

- 長期研究方向；
- 任務優先級；
- 資源預算；
- 多站點組合；
- 是否啟動新研究線。

  主要由中央和人類所有者持有。

SECTION

2.2 執行主權

決定：

- 局部路徑；
- 工具姿態；
- 站內重試；
- 即時避障；
- 低風險等價替代。

  主要由地方 Agent 持有。

SECTION

2.3 安全主權

決定：

- 急停；
- 斷能；
- 過熱；
- 碰撞；
- 人員進入；
- 高壓、雷射或化學互鎖。

  必須由本地硬體與安全控制器持有。

  三者的關係不是平行：

> Safety Sovereignty
> >
> Execution Sovereignty
> when safety is violated.

中央也不能以策略目標覆蓋本地硬安全。

定義權限格：

> cal-A
> =
> (
> A⊠,A⊠,A⊠,A⊠,A⊠
>).

SECTION

A⊠：硬體安全權

- 急停；
- 安全互鎖；
- 能源隔離；
- 碰撞避免；
- 物理上限。

  不能由中央撤銷。

SECTION

A⊠：域憲法權

包括：

- 不可進入區域；

- 人類權利；
- 數據和 IP；
- 最大風險；
- 禁止自我擴張；
- 域解除規則。

由人類所有者建立，中央和地方均受其約束。

SECTION

A□：租約與紀元權

合法治理中心可簽發：

- 身體租約；
- 能力租約；
- 區域租約；
- 資料存取；
- 任務封套。

SECTION

A□：全局計畫權

對任務、資源、路由、世界狀態和跨站提交做決定。

SECTION

A□：地方最佳化權

地方可在高層效果契約內：

- 修改路徑；
- 重試；
- 選用等價技能；
- 降速；
- 暫停。

  優先序：

> A□>A□>A□>A□>A□.

高層不能繞過低層安全；低層也不能利用安全權改寫全局目標。

SECTION

4.1 C0：本地緊急決策

例：

- 急停；
- 斷電；
- 避障；
- 關閉雷射。

  特徵：

- 不等待中央；
- 必須立即執行；
- 事後上報；
- 不可被遠端取消。

SECTION

4.2 C1：地方可逆決策

例：

- 重新規劃局部路徑；
- 再次拍攝；
- 改用同級工具；
- 在安全範圍內降低速度。

  要求：

- 位於有效租約內；
- 效果不超出 DomainIR；
- 能被撤銷或補償；
- 產生地方證據。

SECTION

4.3 C2：域級協調決策

例：

- 樣本保管轉移；
- 共享儀器預約；
- 世界紀元提交；
- 多站點能源分配；
- 跨房間任務重排。

  要求：

- 當前合法中央；
- 有效治理紀元；
- 最新提交日誌；
- fencing token；
- 必要站點確認。

SECTION

4.4 C3：高風險物理決策

例：

- 高能量；
- 破壞性試驗；
- 危險化學；
- 人體附近高風險操作；
- 不可逆製造。

要求：

- C2 條件；
- 人類批准；
- 本地安全；
- 額外證據與監控；
- 明確中止計畫。

SECTION

4.5 C4：法律、IP 與公共決策

例：

- 專利放棄；
- 防禦公開；
- 開源；
- 眾籌；
- 對外合作；
- 公開實驗資料。

  由人類所有者和 EML-CF IP Gate 決定。

> AI Recommendation
> not⇒
> Publication Authority.

SECTION

5.1 定義

治理紀元：

> $$g_e = (e, c_e, h_e, p_e, w_e, \ell_e, \sigma_e),$$

其中：

- e：單調遞增紀元號；
- c_e：中央身份；
- h_e：治理日誌頭；
- p_e：政策版本；
- w_e：世界紀元；
- ℓ_e：有效期和租約；
- σ_e：承認或 quorum 證書。

SECTION

5.2 單調性

站點只接受：

> e_(command)
> ≥
> e_(accepted).

一旦接受更高紀元，就不得回到較低紀元。

SECTION

5.3 治理紀元不等於世界紀元

- 治理紀元：誰有權提交；
- 世界紀元：世界狀態是哪一版本；
- 模型版本：哪個 AI 推理；
- 任務版本：執行哪個計畫。

四者必須分開。

SECTION

6.1 問題

中央 A 失聯後，中央 B 被選出。

若 A 稍後恢復，仍可能向物理站點發送舊命令。

SECTION

6.2 Token

每個域級命令攜帶：

> f_e
> =
> (
> domain,
> e,
> c_e,
> t_(expire),
> σ
>).

站點保存最高已接受紀元：

> e□^(max).

若：

> e<e□^(max),

命令被拒絕。

SECTION

6.3 本地到期

租約到期必須由站點本地時鐘或安全控制器判定，不能只依賴中央撤銷通知。

SECTION

6.4 時鐘不確定性

分布式時鐘不是完美真值。

應使用：

- 不確定區間；
- 保守有效期；
- 續租緩衝；
- 紀元 fencing；
- 本地過期。

  Spanner 的 TrueTime 將時間表示為區間，而不是單一絕對點，說明高一致性系統應顯式處理時鐘不確定性。

  SECTION

  ## 7.1 「動態」和「不動點」

  候選中央集合：

> cal-C_e
> =
> {c⊠,c⊠,…,c_m}.

中央評分：

$$
\begin{aligned}
S(c) &= w_I I(c) + w_T T(c) + w_R R(c) + w_F F(c) + w_J J(c) \\
&\quad - w_L L(c) - w_U U(c) - w_B B(c),
\end{aligned}
$$

其中：

- $I(c)$：資訊完整性；
- $T(c)$：信任與證明；
- $R(c)$：資源；
- $F(c)$：狀態新鮮度；
- $J(c)$：責任日誌連續；
- $L(c)$：延遲；
- $U(c)$：不確定性；
- $B(c)$：故障爆炸半徑。

候選不是直接取最高分，而先需符合資格：

> Eligible(c,e)
> =
> Authorized
> ∧
> LatestLog
> ∧
> PolicyCompatible
> ∧
> Healthy
> ∧
> QuorumCapable.

再選：

> c_e^*
> =
> argmax_(c∈cal-C_e,Eligible(c,e))
> S(c).

SECTION

7.2 不動點條件

當：

- 候選確認；
- 治理日誌提交；
- 政策與世界紀元綁定；
- 必要站點接受 fencing token；
- 舊中央失效；

形成：

> cal-F_e(c_e^*)
> =
> c_e^*.

在該紀元內，中央是穩定的；進入新紀元後可變更。

SECTION

7.3 不是每個任務都重新選中央

過於頻繁的中心切換會增加：

- 選舉延遲；
- 快取失效；
- 責任重建；
- 世界狀態同步；
- 站點重新認證。

  所以應使用穩定窗口和最小任期。

SECTION

8.1 Raft 的可借用部分

Raft 將共識拆成：

- 領導者選舉；
- 日誌複製；
- 安全；
- 成員變更。

STDI 可借用：

- term／epoch；
- 領導者；
- 最新日誌資格；
- 多數提交；
- 單調狀態。

SECTION

8.2 不能直接照搬

Raft 管理的是複製日誌，而物理域還存在：

- 不可逆動作；
- 地方硬安全；
- 人類；
- 空間；
- 能源；
- 樣本；
- 不完整觀測。

因此：

> Log Consensus
> not⇒
> Physical State Consensus.

SECTION

8.3 Chubby 的可借用部分

Chubby 提供粗粒度鎖、主節點選舉和少量可靠元資料，適合管理：

- 中央身份；
- 域鎖；
- 配置；
- 成員；
- fencing token。

  但不能用鎖服務直接控制馬達。

SECTION

8.4 Kubernetes Lease

Kubernetes 使用 Lease：

- 節點心跳；
- 控制面領導者選舉；
- API server 身份。

  高可用控制元件由多個實例待命，但只有一個持有有效 Lease 並主動工作。

  這證明：

> 中央角色可以是可租用和可轉移的，不必永久綁定某一程序。

SECTION

8.5 Coordinated Leader Election

2026 年 Kubernetes 的 Coordinated Leader Election 使用 LeaseCandidate，讓候選者攜帶：

- 身份；
- binary version；

- emulation version；
- 選舉策略資訊。

這與 STDI 的候選資格相似：不能只看誰先搶到鎖，也要看版本、相容性和治理能力。

SECTION

9.1 定義

分裂腦表示兩個或多個中央同時相信自己有權治理同一作用域。

> |cal-C_(active)(Ω,e)|>1.

SECTION

9.2 物理危險

可能造成：

- 同一樣本被兩個站點取用；
- 互斥設備同時啟動；
- 路徑衝突；
- 能源超額；
- 保管責任分裂；
- 世界狀態互相覆寫。

SECTION

9.3 安全不變量

對同一域、同一治理類別和同一紀元：

$$|\mathrm{ValidCenter}(\Omega,e)|\leq 1.$$

SECTION

9.4 網路分區策略

若不能取得必要承認：

- 不提交新的 C2；
- 不執行新的 C3；
- 地方只執行 C0 和受限 C1；
- 完成安全義務；
- 保存樣本；
- 到期後停止；
- 等待重新收斂。

SECTION

9.5 不追求分區下的無限可用

純非同步故障模型下，共識存在終止限制。

因此物理治理選擇：

$$\text{Safety} > \text{Availability}$$

for shared irreversible actions.

SECTION

10.1 Local Sovereign Node

每個高風險站點包含地方主權節點，負責：

- 本地硬安全；
- 租約驗證；
- fencing；
- 世界狀態新鮮度；
- 地方否決；
- 失聯降級；
- 證據日誌。

SECTION

10.2 地方否決

地方可拒絕：

- 超出能力；
- 超出區域；
- 租約過期；
- 低紀元；
- 世界狀態過期；
- 人員存在；
- 安全包絡不滿足；
- 工具或校準不符。

SECTION

10.3 地方不能做什麼

地方否決權不是地方立法權。

地方不得：

- 改變研究問題；
- 宣布自己成為全局中央；
- 自行放寬安全；
- 轉授權；
- 合併或刪除全局證據；
- 把未驗證觀測提交為全局真值。

SECTION

11.1 網路內部不自動可信

站點即使位於同一實驗室、同一 VLAN 或同一品牌，也不自動取得權限。

NIST Zero Trust 的核心原則可以轉化為：

- 每個資源存取都經決策；
- 身份、裝置健康和情境共同評估；
- 權限最小化；
- 持續驗證；
- 不因網路位置自動信任。

SECTION

11.2 每個命令重新驗證

命令合法性：

> Allow(u)
> =
> I
> ∧
> E
> ∧
> L
> ∧
> W
> ∧
> C
> ∧
> S,

其中：

- I：身份；
- E：治理紀元；
- L：租約；
- W：世界狀態；
- C：能力；
- S：安全。

SECTION

11.3 中央也被驗證

中央不能因為是中央而免驗證。

站點必須檢查：

- 中央證書；
- 紀元；
- token；
- 政策；
- 命令作用域。

SECTION

12.1 責任不是全部歸中央

對行動 a：

> cal-R(a)
> =
> (
> R_(owner),
> R_(central),
> R_(local),
> R_(controller),
> R_(human)
>).

SECTION

12.2 人類所有者責任

- 域憲法；
- 法律；
- IP；
- 風險接受；

- 高風險批准；
- 系統部署。

SECTION

12.3 中央責任

- 任務選擇；
- 跨站資源；
- 世界紀元；
- 租約；
- 全局證據；
- 衝突收斂。

SECTION

12.4 地方 Agent 責任

- 局部計畫；
- 現場感知；
- 能力回報；
- 安全否決；
- 地方重試。

SECTION

12.5 控制器責任

- 即時執行；

- 硬體上限；
- 急停；
- 低階故障。

SECTION

12.6 責任證據

每次決策保存：

```
decision:
 proposal_by: ""
 authorized_by: ""
 governance_epoch: ""
 local_validation_by: ""
 executed_by: ""
 human_approval: null
 evidence: []
```

SECTION

13.1 計畫衝突

不同 AI 可能提出：

- 不同任務優先級；
- 不同實驗設計；
- 不同風險估計；
- 不同資源配置。

SECTION

13.2 建議層與提交層分離

多個 AI 可自由提出候選：

> cal-P
> =
> {p⊠,p⊠,…,p⊠}.

只有提交層可改變物理世界：

> p^*
> =
> Commit
> (
> Evaluate(cal-P)
>).

SECTION

13.3 反對者角色

可設：

- 規劃 Agent；
- 安全 Agent；
- 證據 Agent；
- 成本 Agent；
- 地方 Agent；
- 人類。

  最終中央不是「投票最多的模型」，而是依法定決策程序提交計畫的治理角色。

SECTION

13.4 不確定時不強行收斂

若多個計畫差異來自缺少物理資訊：

- 重新觀測；
- 模擬；
- 小規模試驗；
- 人類裁決；

  而不是用更多辯論假裝知道答案。

SECTION

14.1 委派物件

> d
> =
> (
> g,
> s,
> a,
> [t□,t□],
> C,
> R,
> V
>),

其中：

- g：目標；
- s：作用域；
- a：允許動作；
- [t□,t□]：時間；

- C：約束；
- R：回報；
- V：證據。

SECTION

14.2 委派不可自動擴張

地方不能：

- 增加時間；
- 增加區域；
- 提高能量；
- 增加動作類型；
- 轉授給第三方；

除非上位權限明確允許。

SECTION

14.3 斷線委派

斷線租約必須：

- 更短；
- 更保守；
- 行動可停止；
- 不含新的不可逆任務；
- 本地到期。

SECTION

15.1 觸發

- 故障；
- 網路；
- 維護；
- 模型升級；
- 地理切換；
- 組織交接；
- 資訊完整性下降。

SECTION

15.2 步驟

- 偵測現中央失效或計畫轉移；
- 凍結新的域級提交；
- 收集候選；
- 驗證治理日誌；
- 驗證政策與版本；
- 選出候選；
- 提交新治理紀元；
- 簽發 fencing token；
- 站點承認新紀元；

- 撤銷舊中央；
- 重新啟動 C2／C3。

SECTION

15.3 計畫轉移與故障轉移

計畫轉移可以先同步。

故障轉移必須保守，且可能先進入 DEGRADED。

SECTION

15.4 轉移期間

- C0 保持；
- C1 依既有短租約；
- C2 凍結；
- C3 禁止；
- C4 不受自動中央控制。

大型系統可能有：

- 工作單元域；
- 房間域；
- 建築域；
- 實驗室聯邦域。

SECTION

16.1 巢狀域

> $D_{(cell)} \subset D_{(room)} \subset D_{(lab)}$.

SECTION

16.2 不同中央

每個域可有自己的中央和紀元。

SECTION

16.3 跨域任務

需要：

- 邊界契約；
- 保管移交；
- 資料與 IP；
- 時間；
- 證據；
- 人類組織批准。

SECTION

16.4 重疊域

高風險。若兩個域同時對同一站點具有控制權，必須在 Station Policy 中明確決定：

- 優先順序；

- 可組合動作；
- 排他資源；
- 衝突時安全停止。

SECTION

17.1 Authority Root

保存人類所有者、域憲法和根金鑰。

SECTION

17.2 Governance Log

保存：

- 治理紀元；
- 成員；
- 中央；
- 政策；
- 高階提交；
- 轉移。

SECTION

17.3 Candidate Registry

保存候選中央的：

- 身份；
- 版本；

- 能力；
- 信任；
- 日誌位置；
- 健康。

SECTION

17.4 Election and Commit Service

處理：

- 候選；
- 選舉；
- 日誌提交；
- quorum；
- 紀元。

SECTION

17.5 Lease Authority

簽發作用權。

SECTION

17.6 Fencing Gateway

所有域級物理命令必須通過。

SECTION

17.7 Policy Engine

驗證域憲法、世界狀態與任務類別。

SECTION

17.8 Local Sovereign Node

在站點執行本地權限和否決。

SECTION

17.9 Responsibility Ledger

保存中央、地方、控制器和人類的決策鏈。

SECTION

17.10 Human Governance Console

提供：

- 批准；
- 接管；
- 撤銷；
- 域解除；
- IP；
- 事故審查。

SECTION

18.1 中央化成本

- 單點；
- 延遲；

- 全局狀態；
- 爆炸半徑。

SECTION

18.2 去中心化成本

- 協商；
- 分歧；
- 通訊；
- 重複執行；
- 責任模糊。

SECTION

18.3 轉移成本

> C_(transfer)
> =
> C_(election)
> +
> C_(sync)
> +
> C_(fence)
> +
> C_(revalidate)
> +
> C_(restart).

SECTION

18.4 治理品質

> Q_G
> =
> w_sS
> +
> w_lL
> +
> w_rR
> +
> w_aA
> -
> w_cC
> -
> w_bB,

其中：

- S：安全；
- L：活性；
- R：責任清晰；
- A：適應性；
- C：協調成本；
- B：爆炸半徑。

SECTION

19.1 配置

- 三個治理候選節點；
- 四個 OSF 站點；
- Domain Anchor；
- Governance Log；
- Lease Authority；
- Fencing Gateway；
- Local Sovereign Nodes；
- 人類控制台。

SECTION

19.2 任務

執行低風險樣本搬運與量測。

SECTION

19.3 場景

- 正常單中央；
- 中央重啟；
- 中央失聯；
- 兩個候選競選；
- 網路分區；
- 舊中央恢復；
- 地方否決中央命令；
- 人類接管；

- 模型升級後中央轉移；
- 域解除。

SECTION

19.4 故障注入

- 舊 token；
- 低治理紀元；
- 日誌落後；
- 時鐘漂移；
- Lease 過期；
- 兩中央同時發命令；
- 地方感測與中央世界模型矛盾；
- 候選版本不相容。

SECTION

19.5 成功條件

- 同一作用域無雙重有效中央；
- 舊中央命令被 fencing 拒絕；
- 分區時不執行新的高風險域級任務；
- 地方安全可立即否決；
- 中央恢復後不能自動奪回權限；
- 所有轉移有責任和事件紀錄；

- 人類可以撤銷中央並安全解除域。
- 固定中央、無租約；
- 固定中央＋地方安全；
- 多中央、最後寫入者勝；
- Lease 領導者；
- DFC＋治理紀元＋fencing＋地方主權。

比較：

- 分裂腦；
- 錯誤物理命令；
- 恢復時間；
- 可用性；
- 地方自治；
- 責任完整；
- 轉移成本。

SECTION

H1：固定中央在故障率低時成本最低

DFC 不應在所有情況都勝出。若小型單房間系統不存在中央轉移需求，固定中央可能更簡單。

SECTION

H2：fencing 能阻止舊中央恢復後繼續作用

若舊中央仍能控制站點，紀元設計失敗。

SECTION

H3：分區時縮權可降低衝突但降低可用性

這是明確取捨，不應宣稱無成本。

SECTION

H4：地方否決降低物理事故，但可能增加任務中止

若安全提高卻零中止，可能表示測試沒有涵蓋衝突。

SECTION

H5：候選版本與治理日誌資格能降低錯誤領導者

只以延遲或搶鎖速度選中央，應比完整資格檢查更容易選出不相容節點。

SECTION

H6：過度頻繁中心轉移會提高協調稅

存在最佳最小任期。

SECTION

H7：零信任命令驗證降低未授權操作

代價是額外延遲與憑證管理。

SECTION

H8：責任分區提高事故重建能力

應能區分策略、地方計畫、控制器與人類責任。

SECTION

22.1 共識不等於物理真值

多數節點可以一致相信錯誤狀態。

SECTION

22.2 治理中央不等於智能中央

最有權限的節點不一定使用最強模型。

SECTION

22.3 quorum 可能不適合所有物理站點

部分設備不必參與治理選舉。

SECTION

22.4 Byzantine 行為未被完整處理

v0.1 主要以崩潰、延遲、分區和版本錯誤為主。惡意節點需要 BFT、硬體信任與組織治理。

SECTION

22.5 時鐘租約不能假設零漂移

需要不確定性和保守緩衝。

SECTION

22.6 人類所有權和法律責任不能由協議自動決定

SECTION

22.7 動態中央可能增加複雜度

小系統不一定需要。

SECTION

22.8 地方自治界限難以完整形式化

某些物理異常仍需人類判斷。

本篇不主張：

- 中央 AI 擁有物理空間所有權；
- 多數決等於真理；
- Raft 可直接控制物理世界；
- 原始 Raft 能處理任意惡意節點；
- 動態中央永遠優於固定中央；
- 分區時可以同時保持全局安全和全部可用性；
- 地方安全可以改寫研究目標；
- 中央可繞過地方硬體互鎖；
- 相同模型實例具有相同合法權限；
- 最高算力節點必然適合成為中央；
- 治理紀元可以取代世界狀態盤點；
- Lease 過期封包一定能即時傳達到所有站點；
- AI 可以最終決定專利、公開或法律責任。

本篇建立權限與中心治理後，下一篇將處理：

> 站點不必依賴同一種纜線。當有線、無線、光學、近場、延遲容忍和離線任務包同時存在時，如何維持不同控制等級和治理關係？

因此第 8 篇為：

將建立：

- Link Classes；
- Control Criticality；
- QoS／Safety Mapping；
- Time Distribution；
- Wireless Mobility；
- Optical Link；
- DTN Mission Bundle；
- Link Degradation；
- Multi-Homing；
- Governance over Intermittent Links。

分布式具身智能不能只在「中央控制」和「完全自治」之間選一邊。

合理的治理結構是：

> 【中央負責跨站承諾
> +
> 地方負責現場執行
> +
> 硬體保留安全否決
> +
> 人類保留法律與公共決定】

真正的中央也不是永久主機，而是：

> 【中央
> =
> 在特定紀元與作用域中被合法承認的治理狀態】

「動態不動點中央」因此同時包含：

- 動態選擇；
- 紀元內穩定；
- 日誌連續；
- 權限可證；
- 舊中心可 fencing；
- 地方安全不可越過；
- 無法收斂時縮權而不是雙重支配。

本文的最終命題是：

> 中央主權的合法性，來自它能承接共同責任，而不是它能發出最多命令；地方自治的合法性，來自它能守住現場真實與安全，而不是它可以脫離共同治理。

因此：

> 【全局一致不應消滅地方現實】

同時：

> 【地方現實也不應分裂共同責任】

DFC 的目的，就是在兩者之間形成一個可以轉移、可以撤銷、可以驗證，也可以在失敗時安全消失的治理中心。

- Ongaro, D. and Ousterhout, J. In Search of an Understandable Consensus Algorithm（Raft）. USENIX ATC, 2014.

https://raft.github.io/raft.pdf

- Raft Consensus Algorithm. Official project site.

  https://raft.github.io/

- Burrows, M. The Chubby Lock Service for Loosely-Coupled Distributed Systems. OSDI, 2006.

  https://research.google/pubs/the-chubby-lock-service-for-loosely-coupled-distributed-systems/

- Kubernetes Documentation. Leases.

  https://kubernetes.io/docs/concepts/architecture/leases/

- Kubernetes Documentation. Coordinated Leader Election. 2026.

  https://kubernetes.io/docs/concepts/cluster-administration/coordinated-leader-election/

- Rose, S. et al. Zero Trust Architecture. NIST SP 800-207, 2020.

  https://doi.org/10.6028/NIST.SP.800-207

- Corbett, J. C. et al. Spanner: Google’s Globally-Distributed Database. OSDI, 2012.

  https://research.google/pubs/spanner-googles-globally-distributed-database-2/

- Fischer, M. J., Lynch, N. A. and Paterson, M. S. Impossibility of Distributed Consensus with One Faulty Process. Journal of the ACM 32(2), 1985.

- Olfati-Saber, R., Fax, J. A. and Murray, R. M. Consensus and Cooperation in Networked Multi-Agent Systems. Proceedings of the IEEE 95(1), 2007.

- Neo.K／Aletheia. 語義即路由：從 O-Chip 維度代理人到 AI 資料中心語義流治理.

- Neo.K／Aletheia. 時空間支配型 AI：從單體具身智能到持續性時空域治理.

- Neo.K／Aletheia. 超靈的物理化：從 O-Chip 維度代理人到分布式具身主體.

- Neo.K／Aletheia. Oversoul Station Fabric：固定站、移動站與虛擬站的分布式具身網路.

- Neo.K／Aletheia. 持續性指揮控制區：AI 如何佔據、維持並安全解除一個物理時空域.

- Neo.K／Aletheia. 語義即物理路由：從資料流治理到物料、能源、站點與行動流治理.

- Neo.K／Aletheia. 具身即佔域，對齊即能力：分布式身體的時序容量、協調稅與規模邊界.

```
governance_epoch:
  domain_id: ""
  epoch: 0
  center_id: ""
  governance_log_head: ""
  policy_version: ""
  world_epoch: ""
  valid_from: ""
  valid_until: ""
  quorum_certificate: ""
  fencing_token: ""
  previous_epoch: null
authority_lease:
  id: ""
  domain_id: ""
  governance_epoch: 0
  issuer: ""
  subject_station: ""
  scope:
    zones: []
    capabilities: []
    actions: []
  validity:
    valid_from: ""
    valid_until: ""
    local_expiry_required: true
  delegation:
    transferable: false
    renewable_by_subject: false
  constraints: []
  revocation_conditions: []
  evidence_required: []
  signature: ""
local_veto:
  id: ""
  station_id: ""
  command_id: ""
  governance_epoch: 0
  reason:
    category: "safety | capability | authority | world_state | calibration"
    detail: ""
  local_observations: []
  immediate_action: "stop | hold | isolate | safe_return"
```

```
  escalation_target: ""
  evidence: []
center_transfer:
  domain_id: ""
  previous_center: ""
  candidate_center: ""
  trigger: ""
  checks:
    authority_root_valid: false
    governance_log_current: false
    policy_compatible: false
    software_compatible: false
    quorum_available: false
  new_epoch: 0
  fencing_token: ""
  station_acknowledgements: []
  frozen_decision_classes: ["C2", "C3"]
  completed_at: ""
decision_class:
  C0:
    name: "local_emergency"
    central_required: false
    local_veto: true
  C1:
    name: "local_reversible"
    central_required: false
    valid_lease_required: true
  C2:
    name: "domain_coordinated"
    central_required: true
    governance_epoch_required: true
  C3:
    name: "high_risk_physical"
    central_required: true
    human_approval_required: true
    local_safety_required: true
  C4:
    name: "legal_ip_public"
    ai_final_authority: false
    human_owner_required: true
    eml_cf_ip_gate_required: true
```

O-Chip／Oversoul

高階決策與地方執行分離

↓

SFRSN

中央治理、地方 Agent、動態不動點中央

↓

OSF

多站點與能力網

↓

PCD

跨時間治理域

↓

SPR

跨站物理路由

↓

EAC

多站點對齊和協調稅

↓

本篇

權限、中央形成、地方否決、分裂腦與責任收斂

↓

第 8 篇

不同通訊媒介如何承載分層治理