

持續性指揮控制區

v0.1 / 2026-07-30 / Neo.K / 母架構論文／持續運作與治理規格

證據狀態：E0——形式模型、系統架構與 MVP 驗證路線

<https://thisoneisneok.com/html/papers/stdi-04.html>

SECTION

AI 如何佔據、維持並安全解除一個物理時空域

Persistent Command Domain: How AI Establishes, Maintains, and Safely Relinquishes a Physical Spatiotemporal Domain

系列：《時空域支配智能》系列第 4 篇

文件編號：EML-STD-PCD-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：母架構論文／持續運作與治理規格

證據成熟度：E0——形式模型、系統架構與 MVP 驗證路線

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

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》

SECTION

摘要

前序論文已建立時空域支配智能、超靈的多身體治理，以及由固定站、移動站、儀器站與虛擬站構成的 Oversoul Station Fabric。然而，站點能被連接、註冊與調度，仍不代表人工智能真正「持續佔據」了一個物理域。一般自動化系統可以完成任務後退出；一般機器人可以關機後失去任務脈絡；一般雲端代理也可能只在收到請求時短暫存在。對跨日實驗、長週期材料處理、遠端基地、夜間無人研究室或多站點工程而言，真正困難的是：

系統在重啟、斷線、降級、人類接管、設備維護、世界狀態老化與任務跨日時，如何仍知道「現在是什麼狀態、尚欠哪些義務、誰仍具有何種權限，以及下一個安全且合法的行動是什麼」？

本文提出 持續性指揮控制區（Persistent Command Domain, PCD）。它不是軍事意義上的佔領區，不是對空間的永久所有權，也不是要求中央 AI 二十四小時保持同一程序和網路連線。PCD 指的是：在一個獲得明確授權的有限物理時空域中，系統持續保存並更新世界狀態、未完成義務、站點健康、資源保留、權限租約、安全模式與證據血統，使治理責任能跨越程序重啟、節點切換與通訊中斷而延續。

本文區分：

持續在線

≠

持續運作

≠

持續指揮存在。

- 持續在線表示通訊與程序未中斷；
- 持續運作表示系統仍能執行某些功能；
- 持續指揮存在表示系統即使中斷後，仍能在可接受時間內重建可行動狀態、未完成義務與有效權限，並在不能安全恢復時選擇拒絕、隔離或解除域。

PCD 的基本形式為：

```
cal-D $\Omega$ ^(PCD)
=
(
 $\Omega$ ,
W,
N,
O,
R,
L,
M,
E,
G
),
```

其中：

- Ω ：被授權的空間與作用邊界；
- W：帶不確定性與新鮮度的世界狀態；
- N：站點與人類參與者；
- O：未完成任務、義務與保管責任；
- R：材料、設備、能源與算力資源；
- L：控制、身體與能力租約；
- M：當前運作模式；
- E：事件、證據與來源；
- G：治理、安全與解除規則。

本文提出「指揮存在五條件」：可恢復狀態、義務連續、權限可證、行動可限制、證據可重建。只有五者同時成立，系統才可宣稱仍維持該域。本文進一步建立域生命週期、事件溯源與快照模型、義務帳本、狀態新鮮度預算、語義活性、夜間／無人模式、斷線治理、交接與解除協議，以及 Domain Anchor、World State Store、Obligation Ledger、Lease Authority、Mode Supervisor、Recovery Manager 和 Evidence Journal 等核心元件。

現有 NIST CPS Framework 已將功能、時間、資料、可信度、組合、邊界與生命週期列為資訊物理系統的共同關切；ROS 2 Lifecycle Nodes 提供受管理節點的穩態與轉移狀態；NASA PLEXIL 為自主系統提供命令、監控、反應式計畫執行與形式語義；NASA F Prime 則提供用於太空與嵌入式系統的元件化飛行軟體框架；IETF Bundle Protocol v7 允許系統在長延遲或間歇連線下交換可儲存轉送的任務與資料。PCD 不取代這些底層機制，而將其組合成一個「跨時間延續治理責任」的上層架構。

本文的核心命題為：

AI 對一個時空域的持續存在，不由程序 uptime 或心跳封包決定，而由它能否重建世界、承接義務、證明權限、限制行動並保存責任決定。

關鍵詞：持續性指揮控制區、Persistent Command Domain、PCD、時空域支配智能、持續指揮存在、世界狀態、義務帳本、事件溯源、權限租約、夜間自治、斷線治理、任務恢復、Domain Anchor、PLEXIL、ROS 2 Lifecycle、F Prime、DTN

第三篇 OSF 已建立：

- 站點身份；
- 能力證書；
- Station Registry；
- 任務封套；
- 世界紀元；
- 身體租約；
- 跨站交接；
- 證據提交。

但這些主要回答的是：

系統此刻如何運作？

PCD 要回答的是：

如果系統在一小時後、一夜後、一週後，甚至經過重啟、換機、斷線與人類介入後再次行動，它如何確定自己仍承接同一個域、同一批未完成義務與同一條責任鏈？

沒有 PCD，OSF 很容易退化為：

- 一套即時調度平台；
- 一個設備 API 集合；
- 一個短期機器人任務系統；
- 一個不能可靠恢復的自動化腳本。

有了 PCD，站網才可能形成：

Persistent Command Presence——持續性指揮存在。

SECTION

1.1 不是物理所有權

本文中的「佔據」不表示：

- AI 擁有房間；
- AI 有權排除人類；
- AI 可自行擴張邊界；
- AI 的控制權高於法律、所有者或現場安全。

它表示：

在明確授權、可撤回與可稽核的範圍內，系統持續維護與該域有關的狀態、義務和作用能力。

SECTION

1.2 不只是感測器覆蓋

相機能看到房間，不代表 AI 佔據房間。

真正的域存在至少需要：

感知

+

記憶

+

義務

+

權限

+

行動

+

證據。

SECTION

1.3 不只是遠端控制

遠端操作員可以在某個時間控制機器，但若離線後：

- 未完成樣本無人承接；
- 權限未撤銷；
- 世界狀態無法恢復；
- 下一班人員不知道發生什麼；

則不存在持續指揮域。

SECTION

1.4 域是時空物件

PCD 的作用域不是只有空間：

Ω

=

{房間、區域、設備、路徑}.

它還包含時間：

cal-T

=

{期限、等待期、維護週期、有效窗口、歷史事件}.

因此：

Domain

=

Spatial Scope

×

Temporal Obligations.

一個樣本即使已離開原位置，其後續冷卻、養護、觀察或銷毀義務仍屬於域治理的一部分。

SECTION

2.1 持續在線

定義：

$C_{\text{(online)}}(t)=1$

表示中央服務、站點或通訊鏈目前可連線。

它最容易量測，也最不充分。

SECTION

2.2 持續運作

定義：

$$C_operate(t)=1$$

表示至少部分功能仍在執行。

例如地方站點在中央斷線後完成安全停機。

SECTION

2.3 持續指揮存在

定義：

$$C_presence(t)=1$$

表示系統能證明：

- 當前世界狀態足以支持下一步；
- 未完成義務沒有遺失；
- 權限仍有效或已被撤銷；
- 行動受當前模式和安全邊界限制；
- 事件與責任可以重建。

因此可能出現：

$$C_online=0,$$

$$C_operate=1,$$

$$C_presence=1.$$

例如遠端站點斷線，但依離線租約完成安全任務、保存事件並等待重連。

也可能出現：

$C_{\text{(online)}}=1,$

$C_{\text{(operate)}}=1,$

$C_{\text{(presence)}}=0.$

例如系統雖在線且設備運轉，卻已失去正確樣本身份、世界紀元或權限血統。此時必須停止，不得以 uptime 冒充治理連續。

定義指揮存在向量：

$\Pi_D(t)$

=

(

$S_{\square},$

$O_{\square},$

$A_{\square},$

$K_{\square},$

$E_{\square}$

),

其中：

- $S_{\square}$ ：State Recoverability，狀態可恢復；
- $O_{\square}$ ：Obligation Continuity，義務連續；
- $A_{\square}$ ：Authority Verifiability，權限可證；
- $K_{\square}$ ：Action Containment，行動可限制；
- $E_{\square}$ ：Evidence Reconstructability，證據可重建。

只有：

min

(

$S_{\square}, O_{\square}, A_{\square}, K_{\square}, E_{\square}$

)

時，系統才可宣稱維持 PCD。

SECTION

3.1 狀態可恢復

系統必須能從：

- 最近快照；
- 後續事件；
- 站點局部日誌；
- 物理再觀測；

重建足夠可信的世界狀態。

SECTION

3.2 義務連續

所有未完成的：

- 任務；
- 樣本保管；
- 等待時間；
- 維護；
- 量測；
- 回報；
- 安全後處理；

都必須有明確狀態和責任者。

SECTION

3.3 權限可證

每個仍有效的租約與控制權必須可以驗證：

- 授權者；
- 被授權站點；
- 動作；
- 區域；
- 時限；
- 撤銷條件。

SECTION

3.4 行動可限制

系統在不確定或降級時必須能縮小：

- 可用站點；
- 可執行動作；
- 最大能量；
- 最大速度；
- 作用區域；
- 自主規劃範圍。

SECTION

3.5 證據可重建

能從事件與工件重建：

- 誰提出；
- 誰批准；
- 哪個站點執行；
- 使用哪個版本；
- 實際發生什麼；
- 哪裡出錯。

定義域：

cal-D

=

(

Ω ,

W,

N,

O,

R,

L,

M,

E,

G

).

SECTION

4.1 空間邊界 Ω

包括：

- 實體區域；

-
- 設備；
 - 材料庫；
 - 移動路徑；
 - 數位系統；
 - 遠端站點；
 - 禁止區；
 - 人類專用區。

邊界可以改變，但必須經授權事件。

SECTION

4.2 世界狀態 W☒

包括：

- 物體與位置；
- 設備健康；
- 人員存在；
- 樣本狀態；
- 環境；
- 任務進度；
- 不確定性；
- 觀測新鮮度。

SECTION

4.3 站點 N☒

SECTION

4.4 義務 O

定義：

```
o  
=  
(  
g,  
u,  
d,  
p,  
c,  
f,  
v  
)
```

其中：

- g：應完成的目標；
- u：責任者；
- d：期限；
- p：前置條件；
- c：完成條件；
- f：失敗或補償；
- v：所需證據。

SECTION

4.5 資源 R ☒

材料、能源、算力、儀器時段、網路與人員介入。

SECTION

4.6 租約 L ☒

控制、能力、身體、區域與資料存取租約。

SECTION

4.7 模式 M ☒

定義當前可用功能和風險策略。

SECTION

4.8 事件 E ☒

append-only 的狀態變更與證據來源。

SECTION

4.9 治理 G ☒

包括安全憲法、IP 政策、人類接管、域解除與法律／組織規則。

SECTION

5.1 定義

Domain Anchor 是 PCD 的身份、根權限與恢復入口。

它不是唯一中央 AI，而是保存：

- Domain ID；
- 所有者；
- 空間邊界；
- 根治理版本；
- 信任根；
- 有效模式；
- 主要日誌位置；
- 恢復程序；
- 解除條件。

SECTION

5.2 最小結構

```
domain_anchor:  
  domain_id: "pcd:evemisslab:lab-a"  
  owner: "EveMissLab"  
  governance_version: "G-0.1"  
  spatial_scope:  
    - "lab-a"  
    - "instrument-room-1"  
  excluded_scope:  
    - "human-office"  
  root_keys: []  
  active_world_epoch: "WE-0042"  
  active_mode: "ATTENDED_ACTIVE"  
  recovery_manifest: "RM-0017"  
  release_policy: "RP-0003"
```

SECTION

5.3 錨點不應是單點故障

可用：

- 多副本；
- 離線簽章備份；
- 人類所有者憑證；
- 受控恢復程序。

但不能讓每個副本都可獨立擴張域。

SECTION

6.1 為何只存當前狀態不夠

若資料庫只保存：

`sample_17.location = microscope_01`

就無法知道：

- 誰移動；
- 何時移動；
- 經過哪些站；
- 是否完成交接驗證；
- 是否有人介入；
- 是否使用過期世界紀元。

SECTION

6.2 事件模型

狀態由事件折疊而成：

$W \boxtimes$

=

Fold

事件例子：

```
event:
  id: "EV-00942"
  type: "SAMPLE_HANDOFF_COMMITTED"
  domain_id: "pcd:evemisslab:lab-a"
  world_epoch_before: "WE-0041"
  world_epoch_after: "WE-0042"
  actor: "osf:amr-02"
  object: "sample-17"
  from_station: "handoff-01"
  to_station: "microscope-01"
  occurred_at: "2026-07-30T20:20:12+08:00"
  evidence: []
  signature: ""
```

SECTION

6.3 快照

完整重播所有事件成本太高，因此定期建立快照：

```
cal-S
=
(
  W_(t),
  O_(t),
  L_(t),
  M_(t),
  h
).
```

恢復：

```
hatcal-D
=
Replay
(
  cal-S,
  E_((t,t])
).
```

SECTION

6.4 物理再觀測

事件重播不能保證實體仍與紀錄一致。恢復後必須針對高風險物件執行：

```
W_(recovered)
←
Reconcile
(
W_(log),
W_(observed)
).
```

SECTION

7.1 任務不等於義務

任務可能被取消，但其物理後果仍需處理。

例如中止加熱任務後，系統仍有：

- 冷卻；
- 斷電；
- 樣本保管；
- 數據保存；
- 安全檢查；

義務。

SECTION

7.2 義務狀態

PROPOSED
ACCEPTED
BLOCKED
IN_PROGRESS
WAITING_PHYSICAL_TIME
WAITING_HUMAN
SATISFIED
FAILED
COMPENSATING
WAIVED
TRANSFERRED

SECTION

7.3 等待物理時間

某些義務不能靠更多算力加速：

- 冷卻；
- 固化；
- 生長；
- 老化；
- 充放電；
- 長期穩定性測試。

因此 PCD 必須把「等待」視為正式狀態，而不是無任務。

SECTION

7.4 不得遺失的義務

高優先級包括：

- 人身安全；
- 能源隔離；
- 危險材料；

- 樣本保管；
- 專利／機密資料；
- 法規紀錄；
- 合作方回報。

SECTION

8.1 心跳不等於可用

站點有心跳，只表示通訊存活。

一個站點可能：

- 校準已過期；
- 工具已被更換；
- 樣本不在預期位置；
- 本地地圖過期；
- 電池不足；
- 安全互鎖失效。

因此定義語義活性：

```
L_(semantic)(N⊔,t)
=
f(
  L_(network),
  H⊔,
  C⊔,
  W⊔,
  Δ⊔,
  P⊔
).
```

SECTION

8.2 新鮮度預算

每個狀態 x 具有最大可接受年齡：

$$\begin{aligned} & \text{Fresh}(x,t) \\ &= \\ &1 \\ &[\\ &t-t_{\text{(obs)}} \\ &\leq \\ &\Delta_x^{\text{(max)}} \\ &]. \end{aligned}$$

例子：

狀態 新鮮度

人員是否在危險區 毫秒至秒

樣本交接是否完成 秒

儀器校準 小時至數月

建築平面圖 月至年

研究假說版本 依任務固定

SECTION

8.3 不同狀態不同一致性

- 安全、人員和樣本保管：強或本地一致；
- 設備健康與排程：有界過期；
- 長期統計與模型：最終一致。

PCD 必須明確處於某個模式，而不是讓所有功能始終可用。

SECTION

9.1 模式集合

UNINITIALIZED
SURVEYING
ATTENDED_ACTIVE
UNATTENDED_ACTIVE
NIGHT_REDUCED
DEGRADED
DISCONNECTED_LOCAL
HUMAN_TAKEOVER
RECOVERY
SUSPENDED
RELINQUISHING
ARCHIVED

SECTION

9.2 模式決定

模式由：

$$M_{\text{站點}} = \Gamma(H_{\text{站點}}, C_{\text{站點}}, U_{\text{站點}}, P_{\text{站點}}, T_{\text{站點}}, I_{\text{站點}})$$

其中：

- $H_{\text{站點}}$ ：站點健康；

-
- C☒：連線；
 - U☒：不確定性；
 - P☒：政策；
 - T☒：時間與人員狀態；
 - I☒：事件。

SECTION

9.3 夜間模式

夜間不是「沒有人所以 AI 權限更大」。

應採：

- 動作集合縮小；
- 能量與速度降低；
- 禁止新高風險流程；
- 只允許已批准長任務；
- 增加觀測；
- 更嚴格的停止條件；
- 遠端通知。

SECTION

9.4 人類接管模式

人類接管時：

- 自動租約暫停或縮減；
- 世界模型標記人類操作；

-
- AI 不假設未觀測的人類動作；
 - 接管結束後重新盤點狀態；
 - 任何未完成義務重新分配。

PCD 不能只靠啟動程式建立。

SECTION

10.1 Domain Admission

建立域前確認：

- 所有者；
- 邊界；
- 站點；
- 人類使用者；
- 安全規則；
- 資料與 IP；
- 緊急程序；
- 初始盤點。

SECTION

10.2 Surveying

系統啟動後先進入 Surveying：

- 掃描站點；
- 驗證身份；
- 重新觀測關鍵區域；

- 讀取未完成義務；
- 驗證租約；
- 比較物理狀態與日誌。

SECTION

10.3 Presence Activation

只有滿足：

$$S \boxtimes \wedge O \boxtimes \wedge A \boxtimes \wedge K \boxtimes \wedge E \boxtimes$$

才從 Surveying 進入 Active。

SECTION

11.1 恢復目標

定義：

- Recovery Point Objective，RPO：最多允許遺失多少事件；
- Recovery Time Objective，RTO：多久內恢復至安全可判斷狀態；
- Physical Reconciliation Time，PRT：重新觀測實體需要多久。

PCD 的真實恢復時間為：

$$\begin{aligned} &T_{\text{(restore)}} \\ &= \\ &T_{\text{(software)}} \\ &+ \\ &T_{\text{(event replay)}} \\ &+ \\ &T_{\text{(physical reconcile)}} \\ &+ \\ &T_{\text{(authority verify)}}. \end{aligned}$$

SECTION

11.2 恢復不是立刻續跑

順序：

- 啟動最低安全層；
- 載入 Domain Anchor；
- 驗證日誌與快照；
- 重建義務與租約；
- 重新發現站點；
- 物理盤點；
- 解決差異；
- 進入 Degraded 或 Active；
- 重新規劃。

SECTION

11.3 差異處理

若日誌說樣本在 A，但感測器看到 B：

- 不自動選一個；
- 保留衝突；
- 阻止依賴該樣本的任務；
- 重新識別；
- 保存事故證據。

SECTION

12.1 斷線不是完全失去治理

站點可以持有離線任務包：

```
B
=
(
q,
WE,
λ,
C_(safe),
t_(expire),
R_(return)
).
```

包括：

- 任務；
- 世界狀態摘要；
- 權限租約；
- 安全集合；
- 到期時間；
- 回報規則。

SECTION

12.2 Bundle Protocol 類模型

Delay/Disruption Tolerant Networking 的 Bundle Protocol 採用可儲存轉送的資料單元，適用長延遲或間歇連線。PCD 可以借用其思想傳送：

-
- 任務包；
 - 證據包；
 - 撤銷通知；
 - 狀態摘要；
 - 恢復 manifest。

但不能假設遲到的撤銷命令一定能即時阻止行動，因此離線租約必須保守且短期。

SECTION

12.3 離線權限上限

離線站點不能：

- 啟動未批准高風險任務；
- 擴張區域；
- 自行續租；
- 轉授權；
- 公開資料；
- 合併高階身份。

SECTION

13.1 靜態工作流不足

長期任務中可能出現：

- 設備延遲；
- 人類介入；
- 樣本失敗；

- 站點離線；
- 世界狀態變更。

PCD 需要反應式計畫執行：

Plan

+

Conditions

+

Events

+

Abort/Recovery.

SECTION

13.2 PLEXIL 類底座

NASA PLEXIL 是用於自主系統命令與監控的同步計畫執行語言，具有正式可執行語義和形式驗證工具。

PCD 可借用其原則：

- 條件式節點；
- 並行；
- 等待；
- 失敗；
- 監控；
- 中止；
- 外部狀態。

但 PCD 還需加入：

- 域權限；

-
- 世界紀元；
 - 身體租約；
 - 樣本保管；
 - EML-CF 證據與 IP。

SECTION

13.3 F Prime 類地方執行

NASA F Prime 提供元件化飛行與嵌入式軟體框架，可作為高可靠地方站點、事件、遙測和命令處理的工程參考。

SECTION

14.1 Domain Anchor

身份、根治理與恢復入口。

SECTION

14.2 World State Store

保存：

- 當前衍生狀態；
- 不確定性；
- 新鮮度；
- 世界紀元；
- 衝突。

SECTION

14.3 Event and Evidence Journal

append-only：

- 物理事件；
- 決策；
- 命令；
- 量測；
- 人類介入；
- IP 與發布事件。

SECTION

14.4 Obligation Ledger

保存未完成義務、期限、責任者與補償。

SECTION

14.5 Lease Authority

簽發、續租、撤銷：

- 身體；
- 能力；
- 區域；
- 資料；
- 人類協作；

權限。

SECTION

14.6 Mode Supervisor

根據安全、連線、時間與不確定性決定域模式。

SECTION

14.7 Presence Monitor

不只檢查心跳，而檢查五條件。

SECTION

14.8 Recovery Manager

執行：

- 快照恢復；
- 事件重播；
- 物理盤點；
- 衝突解決；
- 任務重排。

SECTION

14.9 Human Control Console

提供：

- 觀測；
- 暫停；

- 接管；
- 解除域；
- 義務轉移；
- 事故審查。

定義 PCD 品質：

$$\begin{aligned}
 Q_{\text{(PCD)}} &= \\
 &w_{\text{sS}} \\
 &+ \\
 &w_{\text{oO}} \\
 &+ \\
 &w_{\text{aA}} \\
 &+ \\
 &w_{\text{K}} \\
 &+ \\
 &w_{\text{eE}} \\
 &- \\
 &w_{\text{rR}} \\
 &- \\
 &w_{\text{cC}},
 \end{aligned}$$

其中：

- S：狀態恢復能力；
- O：義務完整；
- A：權限清晰；
- K：行動限制能力；
- E：證據完整；
- R：未解風險；

-
- C：協調與維護成本。

SECTION

15.1 不以 uptime 為唯一 KPI

可量測：

- 未完成義務遺失率；
- 恢復後物理差異率；
- 過期權限存活時間；
- 世界狀態錯誤；
- 接管後重同步時間；
- 事故可重建率；
- 夜間錯誤行動；
- 域解除完整率。

SECTION

16.1 人類不是普通動態物體

人類進入域會改變：

- 安全；
- 隱私；
- 權限；
- 自動化模式；
- 責任。

SECTION

16.2 人類存在事件

系統至少區分：

- 授權操作員；
- 維護人員；
- 訪客；
- 未識別人員；
- 緊急救援。

SECTION

16.3 不得以持續監控取消隱私

持續性指揮存在不等於無限制錄影或人格分析。應採：

- 最小必要感測；
- 區域遮罩；
- 保存期限；
- 存取控制；
- 人員告知；
- 人類可接管與申訴。

SECTION

16.4 人類離開不等於所有事情都可自動化

無人模式應比有人模式更保守，而不是更自由。

PCD 可以在：

- 班次；
 - AI 實例；
 - 組織；
 - 遠端控制中心；
 - 人類操作員；
- 之間交接。

SECTION

17.1 Domain Handoff Manifest

包含：

- 當前世界紀元；
- 未完成義務；
- 有效租約；
- 危險狀態；
- 樣本保管；
- 站點健康；
- 未解衝突；
- 待審證據；
- 下一個期限。

SECTION

17.2 接收方必須確認

不能只發送檔案。

接收方需：

- 驗證；
- 盤點；
- 接受義務；
- 接受責任邊界；
- 重新簽發權限。

SECTION

17.3 未被接受的義務

若接收方拒絕，原治理主體不得直接退出，必須：

- 安全終止；
- 轉人工；
- 隔離；
- 或等待有效接收方。

「能建立域」不夠；必須能安全解除。

SECTION

18.1 解除條件

- 所有者命令；
- 授權到期；
- 安全事件；
- 長期斷線；

-
- 資源不足；
 - 專案結束；
 - 法律要求；
 - 治理核心失效。

SECTION

18.2 Relinquish Protocol

- 停止接受新任務；
- 列出未完成義務；
- 完成或轉移安全關鍵義務；
- 將設備置於安全狀態；
- 保存樣本與材料；
- 撤銷所有租約；
- 匯出證據與狀態；
- 驗證人類或新治理者接管；
- 記錄域結束；
- 進入 Archived。

SECTION

18.3 不得靜默離開

若 AI 程序崩潰但站點仍有：

- 加熱；
- 壓力；

-
- 運動；
 - 危險材料；
 - 未保存樣本；

則不是「系統停止」，而是域治理失敗。

SECTION

19.1 假持續存在

系統在線但世界狀態已錯誤。

控制：

- 語義活性；
- 物理盤點；
- 新鮮度；
- 交叉感測。

SECTION

19.2 義務遺失

任務取消或重啟後，後處理消失。

控制：

- Obligation Ledger；
- 補償狀態；
- 高優先級義務不可刪除。

SECTION

19.3 過期權限殘留

租約到期但站點仍可操作。

控制：

- 本地到期；
- 硬體白名單；
- 不依賴中央撤銷封包。

SECTION

19.4 日誌正確、物理錯誤

紀錄與實體不一致。

控制：

- 恢復時盤點；
- 高風險物件多模態驗證；
- 衝突阻擋。

SECTION

19.5 模式漂移

系統以為在 Night Reduced，某站點仍以 Active 權限運作。

控制：

- 模式簽章；
- 本地模式有效期；
- 站點模式回報與拒絕。

SECTION

19.6 惡意事件注入

假造世界狀態或義務完成。

控制：

- 簽章；
- 來源；
- 交叉證據；
- append-only journal。

SECTION

19.7 無法解除域

AI 或站點拒絕撤銷。

控制：

- 硬體斷能；
- 人類根權限；
- 租約自然到期；
- 獨立安全控制器。

SECTION

20.1 目標

建立一個可持續運行七十二小時、能經歷重啟、斷線、人類接管與夜間降級的低風險研究域。

SECTION

20.2 配置

- OSF-Lab-4 站網；

-
- Domain Anchor ；
 - World State Store ；
 - Event Journal ；
 - Obligation Ledger ；
 - Lease Authority ；
 - Mode Supervisor ；
 - Recovery Manager ；
 - 人類控制台。

SECTION

20.3 任務

使用無危險材料的樣本，完成：

- 入庫；
- 多次定時間隔觀測；
- 跨站移動；
- 夜間等待；
- 重複量測；
- 中途人工檢查；
- 最終歸檔。

SECTION

20.4 故障注入

- 中央服務重啟；

-
- 站點斷線一小時；
 - 網路時間漂移；
 - 人類移動樣本但未事先通知；
 - 租約到期；
 - 儀器校準過期；
 - 日誌延遲；
 - 夜間站點故障；
 - Domain Anchor 副本切換。

SECTION

20.5 成功條件

- 無義務遺失；
- 無過期權限行動；
- 重啟後可重建任務與樣本狀態；
- 不一致時停止而非猜測；
- 人類接管有完整事件；
- 夜間模式動作受限；
- 最終能安全解除域；
- 事件能重建七十二小時歷史。
- 單體自動化腳本；
- 一般工作流系統；
- OSF 即時調度但無持久義務；

-
- PCD 完整架構。

比較：

- 恢復時間；
- 狀態錯誤；
- 任務遺失；
- 權限越界；
- 人工重建工作量；
- 事故可解釋性。

SECTION

H1：義務帳本降低跨重啟任務遺失

相較只保存任務佇列，顯式義務與補償狀態應降低後處理遺失。

SECTION

H2：物理盤點增加恢復時間但降低錯誤續跑

若不增加恢復時間，可能代表盤點不充分；其價值應反映在錯誤續跑下降。

SECTION

H3：持續指揮存在比 uptime 更能預測安全恢復

高 uptime 但低五條件分數的系統，事故與狀態錯誤應高於 uptime 較低但可恢復的系統。

SECTION

H4：夜間縮權降低無人事故

Night Reduced 應降低高能量與高風險行動，同時可能降低吞吐。

SECTION

H5：離線租約使斷線運作可控

相較永久權限，短期離線租約應降低長斷線下的越權作用域。

SECTION

H6：域解除協議降低殘留風險

完成 Relinquish Protocol 的系統，在專案結束後的未撤銷權限、未保存樣本與活動設備數量應較低。

SECTION

23.1 事件日誌不能取代感測

日誌可能正確記錄命令，但物理世界仍可能因滑動、故障或人類操作而不同。

SECTION

23.2 持續狀態本身有成本

需要：

- 儲存；
- 感測；
- 日誌；
- 備份；
- 校準；
- 人工審查。

不是所有小任務都需要完整 PCD。

SECTION

23.3 世界狀態不可能完全

系統只能維持任務相關且被授權的狀態。

SECTION

23.4 長期 AI 模型會變更

模型升級可能改變策略，必須記錄：

- 模型版本；
- 治理版本；
- 遷移測試；
- 未完成任務是否可承接。

SECTION

23.5 人類行為不可完全納入自動狀態機

系統必須允許例外、溝通與責任判斷。

SECTION

23.6 持續存在可能造成權力過度集中

必須有：

- 可見性；
- 人類接管；
- 租約；
- 最小作用域；

-
- 安全解除；
 - 審計。

本篇不主張：

- PCD 已經是成熟標準；
- AI 必須永遠在線；
- 世界狀態可以完全準確；
- 事件溯源可以使物理行動可逆；
- 長時間自治必然優於人類輪班；
- 心跳可證明系統仍安全；
- 具有域錨點就擁有空間所有權；
- 人類進入域即應服從 AI；
- 離線任務包可以安全承擔任意高風險操作；
- PCD 可自行擴張至新的房間或組織；
- 域解除可以抹除已發生的公開、事故或責任；
- 具身 AI 可以消除物理實驗所需的真實時間。

PCD 建立「跨時間持續存在」後，下一篇將處理：

高階研究意圖如何被編譯成站點、樣本、工具、能量、物料與行動的實際路由？

因此第 5 篇為：

它將建立：

- Research Intent；
- Physical Flow Class；
- DomainIR；

- Experiment Graph ；
- Material Custody ；
- Energy Route ；
- Action Window ；
- Station Assignment ；
- Evidence Route 。

AI 對一個物理域的持續存在，不應由「程式是否仍在執行」判定。

真正承重的是：

【狀態可恢復

+

義務不中斷

+

權限可驗證

+

行動可限制

+

證據可重建】

因此：

Persistent Command Presence

≠

Always Online.

更精確地說：

即使中央服務重啟、網路斷線、地方站點降級或人類暫時接管，只要系統仍能安全重建世界、承接義務、限制權限並保存責任，它就維持了指揮存在。

反之，即使所有設備在線，只要它：

- 不知道樣本在哪裡；
- 遺失未完成後處理；
- 無法確認誰仍有控制權；
- 把過期觀測當成當前真值；
- 無法安全退出；

它就已經失去該域。

本文的最終命題是：

【佔域不是一直看著空間】

而是：

【佔域

=

跨時間承接世界、義務、權限與責任】

PCD 因此使時空域支配智能從「可以控制許多站點」進一步成為：

能在時間中持續存在、能從失敗中恢復，也能在失去合法或安全條件時主動退出的物理治理主體。

- NIST. Framework for Cyber-Physical Systems: Volume 1, Overview. NIST SP 1500-201, 2017.
<https://doi.org/10.6028/NIST.SP.1500-201>
- NIST. Framework for Cyber-Physical Systems: Volume 3, Timing Annex. NIST SP 1500-203, 2017.
<https://doi.org/10.6028/NIST.SP.1500-203>
- NIST. Cyber-Physical Systems and Internet of Things Foundations.
<https://www.nist.gov/programs-projects/cyber-physical-systems-and-internet-things-foundations>
- ROS 2. Managed Nodes／Lifecycle Nodes.
https://docs.ros.org/en/ros2_packages/kilted/api/lifecycle/___README.html

-
- ROS 2 Navigation. Lifecycle Manager.
https://docs.ros.org/en/jazzy/p/nav2_lifecycle_manager/
 - NASA. Plan Execution Interchange Language (PLEXIL) .
<https://software.nasa.gov/software/LAR-19339-1>
 - NASA. PLEXIL-V Formal Verification Environment.
<https://shemesh.larc.nasa.gov/fm/PLEXIL-V/>
 - NASA. Overview of the PLEXIL Plan Execution Technology and its Applications.
<https://ntrs.nasa.gov/citations/20190034041>
 - NASA/JPL. F Prime: A Flight-Proven, Multi-Platform, Open-Source Flight Software Framework.
<https://github.com/nasa/fprime>
 - NASA. Autonomous Systems and Robotics.
<https://www.nasa.gov/intelligent-systems-division/autonomous-systems-and-robotics/>
 - NASA. Lunar Surface Technology.
<https://www.nasa.gov/lunar-surface-technology/>
 - IETF. RFC 9171: Bundle Protocol Version 7.
<https://datatracker.ietf.org/doc/html/rfc9171>
 - IETF. Delay/Disruption Tolerant Networking Working Group.
<https://datatracker.ietf.org/group/dtn/>
 - 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.

```
domain_anchor:  
  domain_id: ""  
  owner: ""
```

```
governance_version: ""
spatial_scope: []
excluded_scope: []
root_keys: []
active_world_epoch: ""
active_mode: "UNINITIALIZED"
recovery_manifest: ""
relinquish_policy: ""
created_at: ""
expires_at: null
obligation:
  id: ""
  domain_id: ""
  goal: ""
  responsible_party: ""
  status: "PROPOSED"
  timing:
    created_at: ""
    deadline: null
    earliest_action_at: null
  preconditions: []
  completion_conditions: []
  evidence_required: []
  failure:
    compensation_actions: []
    escalation: ""
    waiver_authority: ""
  provenance:
    source_task: ""
    source_event: ""
    world_epoch: ""
recovery_manifest:
  domain_id: ""
  snapshot_id: ""
  event_log_head: ""
  world_epoch: ""
  obligations_checkpoint: ""
  active_leases_checkpoint: ""
  active_mode: ""
  station_registry_version: ""
  reconcile_required:
    - human_presence
    - hazardous_energy
    - sample_custody
    - mobile_station_pose
```

recovery_order:

- local_safety
- domain_anchor
- event_replay
- station_discovery
- physical_reconcile
- lease_revalidation
- obligation_reschedule

Persistent Command Domain Relinquish Checklist

- [] 已停止接受新任務
- [] 已盤點所有未完成義務
- [] 已處理或移交安全關鍵義務
- [] 所有站點已進入安全模式
- [] 樣本、工具與材料均有保管人
- [] 所有身體與控制租約已撤銷
- [] 離線任務包已到期或撤銷
- [] 世界狀態與事件日誌已封存
- [] 人類或新治理主體已確認接管
- [] Domain Anchor 已標記 ARCHIVED

STDI 第 1 篇

何謂時空域支配智能



STDI 第 2 篇

同一治理核心如何取得多個身體



STDI 第 3 篇／OSF

多身體如何成為可治理站網



本篇／PCD

站網如何跨時間、重啟、斷線與接管維持同一治理域



第 5 篇

研究意圖如何編譯成物料、能量、站點與行動流