来源隔离认知仲裁：智能体控制平面中的执行绑定证据认证与可能世界安全门控

JunHe
DeyingYuOpenKedge LLC{junhe,
deying}@openkedge.io

arXiv:2611.32032v1 [cs.DC] 24 Nov 2026

摘要

大型语言模型之间的一致意见，并非变更生产基础设施所需的物理证据。生成式模型共享预训练先验，并在推理过程中遵循同伴的论证，因此投票集成会使错误相互关联，而非提供独立容错；然而，对不受约束的智能体输出附加僵化的确定性检查，又会使事件处置陷入瘫痪。我们提出来源隔离认知仲裁（PIEQ），这是一种执行绑定认证层，可确保所有语言模型严格处于可信计算基之外。PIEQ 围绕三项不同义务，整合了基于假设的真值维护、物理来源隔离、控制理论可能世界安全防护以及线性化并发治理：从彼此独立的物理故障域中认证诊断前置条件；针对所有尚未排除的故障世界，对候选变更进行门控，并在存在歧义时退回只读诊断探测；以及通过快照屏障、修订检查、授权新鲜度、可信时序前置条件策略和分级能力执行机制，将准入证书绑定至目标执行过程。

在形式化保证、自动化etcd 和多进程操作系统级故障套件、冻结软件基准、可扩展性压力测试以及实时语言模型运行中，PIEQ 实现了零假设范围内的不安全准入和零错误前置条件提交，将代理偶发的证明遗漏转化为可恢复的误阻断，而非不安全操作。我们刻画了语言模型何时能在确定性可信计算基规则之外提供真正价值——具体而言，是在大型规则空间中进行多跳证明搜索（有界确定性补全趋于饱和，而定向验证仍保持在亚毫秒级），以及基于经认证遥测数据的非结构化事件分诊——并绘制了截至 $M{=}64$ 次观测、$|\mathcal{S}_{\mathrm{cand}}|{=}256$ 和模式 C 界的精确故障关闭截断边界。在物理 PostgreSQL/Patroni 集群上，PIEQ 与 Patroni 及etcd的原生脑裂保护协同，对受监督故障转移实施门控，并在单个可串行化 PostgreSQL 事务内执行完整的 E2 级契约，以实现有界容量预留。所有基准均由作者标注；我们的受控采样直接 API 确认运行将固定的本地 Qwen3-8B 检查点与 AWS Bedrock 推理配置别名配对，而不是使用按日期标记的不可变云快照；E2 级物理故障转移提升以及多主机硬件故障隔离仍属于待完成工作。

1 引言

自主云控制平面日益调用大语言模型集群来诊断事件、转移流量、排空节点并协调数据库故障转移 [1]。一种广泛采用的安全措施是多智能体辩论 [2, 3, 4], , 模型在发起变更型 API 调用前交换自然语言推理依据并进行投票。然而，将达成一致的智能体视为容错法定人数，混淆了观点共识与物理证据独立性。共享预训练先验和智能体间谄媚性使模型错误高度相关，远超经典容错假设 [5, 6, 7, 8]。试图通过将严格的确定性验证器直接置于自由形式智能体提议之前来解决这一问题，却造成了相反的故障模式，使修复工作陷入瘫痪。在最初的 40 案例五模型试点中，严格验证阻止了每个不安全操作（0/40），但也阻止了每个可采取行动的事件（0/19 项缓解措施），丢弃了 284 份提交的证明中的 140 份，并且未执行任何诊断探测。

要使自主基础设施变更既安全又可采取行动，就必须解决一个智能体共识无法应对的更深层系统与控制问题。设想一个三节点复制数据库，其主节点停止响应带内 SQL 探测。两种不相容的故障场景都符合这一症状：主节点可能已经崩溃，此时晋升一个副本节点可以恢复可用性，同时保持单主节点互斥性；也可能是非对称网络分区隔离了健康主节点，此时晋升将导致脑裂。无论有多少语言模型检查这些信号，物理遥测都源自彼此独立的故障域，例如带内 SQL 探测、带外管理桥接和共识租约存储。只处理这条流水线的部分环节，会留下关键的故障路径。若仅认证主节点不可达，却未排除网络分区，仍会允许脑裂发生。反过来，若在未认证诊断前置条件的情况下阻止不安全的晋升，就会让产生幻觉的智能体或单个故障传感器触发无正当依据的保持不变式的中断，例如负载削减或备用节点排空。

即使两项诊断检查在观测时刻均成功，如果并发协调器发生竞态、授权在提交前被撤销、瞬态条件在效果产生前消失，或多轮探测混合了来自不一致系统快照的观测，物理安全性仍会遭到破坏。

我们通过来源隔离的认知法定人数（PIEQ）应对这些耦合故障。PIEQ 是一种与执行过程绑定的认证层，部署于确定性验证代理（kf-proxy）中，使每个语言模型都严格位于可信计算基之外。PIEQ 并不声称其底层形式体系具有个体创新性，而是将四个学科中的既有技术组合起来，应用于智能体诊断与物理执行之间的边界。从符号人工智能和形式化验证中，我们采用基于假设的真值维护 [9], 基于模型的诊断 [10, 11], 数据溯源 [12],以及携证明授权 [13, 14]：不可信智能体不再以 prose 进行争辩，而是提交类型化的 Horn 子句推导和冲突证书，这些内容以经过密码学签名的遥测为根基，由确定性验证器进行检查，同时跟踪最小支持性假设及矛盾。从分布式容错和组合学中，我们将拜占庭故障域隔离 [5] 与不相交完整证明打包相结合，并根据独立物理遥测域的数量，而非达成一致的智能体数量，定义容错认证

。从控制理论中，我们应用离散事件监督控制 [16], 部分可观测的运行时安全屏蔽 [15], 可存活性理论 [20], 以及双重控制 [31]：验证代理保留所有未被足够多独立故障域反驳的建模故障世界，仅当某项变更在每个仍存续的世界中都保持建模不变量时才允许该变更，并在歧义仍然存在时转为只读诊断探测。最后，我们整合并发控制与分布式系统中的线性一致性、严格可串行化、停顿精化、租约、栅栏令牌以及托管式暴露核算 [17, 18, 19, 25, 35]，从而确保准入证书在到达物理提交边界的整个过程中始终有效、有序、获授权且不存在争议。

本文提出四项主要贡献，同时将所有语言模型置于可信计算基之外。第一，我们引入来源隔离的认知认证，将有界真值维护与基于递归物理故障域覆盖范围的精确完整证明打包相结合，使容错前置条件认证严格依赖相互独立的遥测域，而非智能体数量或对话上下文。第二，我们构建容错可能世界安全门控：在有界计算条件下，保留所有未被足够数量的不相交遥测域证伪的建模故障世界；仅当状态变更操作在所有存活世界中都保持状态不变量时才予以准入，否则确定性地派发只读诊断探测或升级处理。第三，我们设计执行约束目标治理层和八层条件风险核算框架，涵盖连续快照屏障、全局准入修订比较并交换、物理停顿细化契约、强制性的可信时序前置条件策略，以及按能力分级的目标执行。第四，我们通过三种配套工程机制，使这些门控能够应用于在线语言模型，同时不扩大信任边界：带有有界模式反馈重试的类型化证明提交、七边界快照审计式主动探测，以及选择加入的有界确定性补全；并在形式化反例、自动化 `etcd` 故障套件、冻结软件基准、在线模型运行、物理 PostgreSQL/Patroni 故障转移监控，以及真实 PostgreSQL 事务性强制执行等场景中评估完整架构，同时明确界定其形式化信任边界与经验范围。

本文首先形式化基础设施对象、可组合的安全概念以及智能体辩论中的一致性崩塌，随后提出来源隔离的认证与可能世界屏蔽，并将这些保证扩展到并发物理执行和风险核算，最后介绍我们的多层评估、相关工作及尚存局限。

2 系统模型与智能体辩论中的一致性崩塌

为自主基础设施设计安全层，需要在编写任何认证算法之前奠定两项基础。首先，我们必须定义受控的物理系统、并发执行下成立的精确安全属性、观测独立性的物理来源，以及划分可信验证与不可信推理的边界。其次，我们必须考察为何多智能体协商无法提供独立证据，这促使我们采取架构决策，将所有语言模型移出可信计算基。

2.1 被控对象、安全概念、故障域与信任边界

自主控制平面负责监管部分可观测的基础设施对象，例如复制数据库集群、路由域或存储池；其精确物理配置无法瞬时完整地进行检查。为确定性地推理风险，操作人员通过有限抽象对该对象进行建模，将物理配置划分为离散的故障状态（例如健康主节点、崩溃主节点，或被非对称网络分区隔离但仍在运行的主节点），并规定哪些状态满足单主节点互斥性等运行安全不变量。形式化地，令 Σ_{phys} 表示物理状态空间，$\mathcal{S}_{\mathrm{cand}} \subseteq \mathcal{S}$ 表示有限抽象模型空间，令 $\alpha : \Sigma_{\mathrm{phys}} \to \mathcal{S}$ 为抽象映射，在时期 τ 生成建模状态 $S_\tau = \alpha(\sigma_\tau)$。令 $\mathcal{K} \subseteq \mathcal{S}$ 表示与物理不变量 $\mathcal{K}^{\mathrm{phys}} \subseteq \Sigma_{\mathrm{phys}}$ 对应的抽象安全状态不变量，并通过健全性蕴含 $\alpha(\sigma) \in \mathcal{K} \implies \sigma \in \mathcal{K}^{\mathrm{phys}}$ 加以定义。可用控制操作明确划分为非变更的诊断探测和改变状态的状态变更操作，即 $\mathcal{A} = \mathcal{A}_{\mathrm{probe}} \sqcup \mathcal{A}_{\mathrm{mut}}$。对于任一建模状态 $s \in \mathcal{S}$ 和变更 $a \in \mathcal{A}_{\mathrm{mut}}$，$\mathrm{Post}(s, a) \subseteq \mathcal{S}$ 表示建模后继状态的集合，而 $A^{\mathcal{K}}_{\mathrm{safe}}(s) \subseteq \mathcal{A}_{\mathrm{mut}}$ 表示从 s 出发能够保持 $\mathcal{K}$ 的变更。

控制理论仔细区分了每一步都保持状态不变量与维持长期可控性，而这一区别直接决定了并发安全性如何组合。状态不变量保持要求执行过程中的每个中间状态和终止状态都处于$\mathcal{K}$内，而单步安全性则保证从 $s \in \mathcal{K}$出发，应用a 后得到 $\mathrm{Post}(s,\ a) \subseteq \mathcal{K}$。相比之下，受控可生存性要求状态属于可生存核 $\mathrm{Viab}(\mathcal{K}) \subseteq \mathcal{K}$，也就是说，存在一个无限的容许控制序列，使状态始终处于 $\mathcal{K}$ [20]内。关键在于，对于耦合不变量，受控可生存性不能通过求交来组合：一般而言，$\mathrm{Viab}(\mathcal{K}_1 \cap \mathcal{K}_2) \subsetneq \mathrm{Viab}(\mathcal{K}_1) \cap \mathrm{Viab}(\mathcal{K}_2)$严格成立。考虑一个状态 $s_0 \in \mathcal{K}_1 \cap \mathcal{K}_2$，它允许采取动作 a_1，在 $\mathcal{K}_1 \setminus \mathcal{K}_2$ 内无限循环；也允许采取动作 a_2，在 $\mathcal{K}_2 \setminus \mathcal{K}_1$内无限循环，但不存在任何能使被控对象始终处于 $\mathcal{K}_1 \cap \mathcal{K}_2$内的动作。在此，$s_0$ 同时属于两个单独的可生存核，但 $\mathrm{Viab}(\mathcal{K}_1 \cap \mathcal{K}_2) = \varnothing$。因此，PIEQ 的组合式执行保证针对的是状态不变量保持；该性质可通过交集在闭合域之间可靠组合（$\mathcal{K} = \bigcap_{\mathcal{D}} \mathcal{K}_{\mathcal{D}}$）；要实现受控可生存性，则需要提供一个预先验证的全局可生存核 $\mathcal{K}^\star \triangleq \mathrm{Viab}(\mathcal{K})$作为目标不变量。

观测独立性源于物理基础设施拓扑，而非检查仪表板的推理代理数量。在我们的数据库场景中，带内 SQL 健康检查、带外管理桥接和共识租约存储经过不同的物理路径，因此构成独立的遥测故障域。形式化地说，遥测通过 M 通道 $\mathcal{O} = \{O_1, \ldots, O_M\}$到达；每个通道都由签名拓扑清单（摘要 h_{man}）映射到一个 D 遥测故障域 $\mathcal{F} = \{F_1, \ldots, F_D\}$（与我们分析并发时引入的封闭暴露域集合 $\mathcal{D} = \mathrm{Dom}^\star(a)$ 区分）。在时期 τ，通道 O_m 发出一个签名原始假设

$$e_m = \langle \mathrm{id}_m, \mathrm{res}_m, \tau, d_m, v_m, h_{\mathrm{man}}, \sigma_m \rangle, \tag{1}$$

其中，res_m 界定目标资源，$d_m \in \{1, \ldots, D\}$ 标识故障域 F_{d_m}，$v_m = v_{\mathrm{obs}}(e_m)$ 记录观测到的

表 1：共指代（区分 $D = |\mathcal{F}|$ 遥测故障域与封闭暴露域集合 $\mathcal{D} = \mathrm{Dom}^{\star}(a)$）。

符号	含义
$\sigma_\tau, \alpha, S_\tau, \mathcal{K}$	物理状态、抽象映射、建模状态 $S_\tau{=}\alpha(\sigma_\tau)$，不变量
$\mathcal{F} = \{F_1, \ldots, F_D\}$	遥测故障域（D 总计；$d_m \in \{1, \ldots, D\}$）
$\mathcal{E}_{\mathrm{prim}}$，$\mathfrak{L}(c)$，$\mathcal{N}_\tau$	带符号假设（$M \le 64$）、ATMS 标签、已验证无解集
$\Pi, E_{\mathrm{leaf}}(\Pi)$ $\Phi_{\mathrm{phys}}(\Pi)$	已验证推导有向无环图、原语叶节点、物理证据足迹
$\mathcal{W}(a)$ ν_{pack}	c_a的活跃证明有向无环图、不相交完整证明打包数
k_a、$f = k_a - 1$	a和可容忍故障域
$\mathcal{B}^{(f)}_{\tau,v}, \widehat{\mathcal{B}}^{(f)}_{\tau,v}$	精确且有界计算的 f 故障容错可信世界集合
$\mathcal{D} = \mathrm{域}^{\star}(a)$ $\mathcal{K}_{\mathcal{D}}$	封闭暴露域集合（$d \in \mathcal{D}$）、作用域状态不变量
θ，细化$_{\mathcal{D}}$	物理执行轨迹和停顿细化契约
$\mathcal{I}_C, \mathcal{I}_H, \mathcal{I}_U, \mathbf{r}_{\mathrm{adm}}$	已提交、进行中、未知 集合；逐域准入修订
$\tau_{\mathrm{adm}}, \tau_{\mathrm{auth}}, t_{\mathrm{auth}}$	证据时期、授权纪元、有效性截止时间
$E_1, \ldots, E_8$	条件风险中的有序残余故障事件核算

目标快照版本，而 σ_m 是涵盖所有字段的采集器签名。

采集器签名 σ_m 可认证来源、载荷完整性和元数据绑定，但绝不保证物理真实情况：配置错误的传感器或分区探针仍可能对误导性观测进行有效签名。PIEQ 将所有 N 语言模型提议者 $\{A_1, \ldots, A_N\}$ 严格置于可信计算基（TCB）之外。TCB 恰好由四个确定性元素组成：经认证的遥测采集器和签名拓扑清单 h_{man}；用于根据编写的 Horn 模型 $\mathcal{V}_{\mathrm{rule}}$检查推导 $\mathcal{M}_{\mathrm{sys}}$ 和冲突不变量的确定性规则与冲突验证器 P_{sys}；容纳有界真值维护引擎、完备证明打包器、合理世界安全防护层及线性化暴露账本的验证代理 `kf-proxy`；以及物理效果边界处持久化的目标隔离与授权适配器（能力等级 E1–E2）。表 1总结了全文使用的核心符号。

2.2 为什么多智能体审议会导致多样性坍塌

在以物理来源认证取代智能体投票之前，我们先总结为何同行审议无法制造观测独立性（形式化定义、谱证明和反例见附录B）。设有$N \ge 2$个提议者，通过无界潜在分数残差 $\varepsilon_i^{(t)} = z_i^{(t)} - z^{\star}(S_\tau) \in \mathbb{R}$ 评估二元假设，并采用独立的概率读出 $y_i^{(t)} = \psi(z_i^{(t)}) \in [0,1]$、初始等相关性 $\bar{\rho}_0 \in [0,1)$，以及由相关创新项 $\eta^{(t)}$ [3, 8]驱动的共享上下文一致性更新 $\varepsilon_i^{(t+1)} = (1-\gamma)\,\varepsilon_i^{(t)} + \gamma\bar{\varepsilon}^{(t)} + \eta_i^{(t)}$（$\gamma \in (0,1]$）。由于该线性算子在每一轮将分歧子空间 $\mathbf{1}^{\perp}$ 衰减$1-\gamma$，同时让共识子空间span(1)保持不衰减，定理B.1（附录B）表明，有效样本量$N_{\mathrm{eff}}(\Sigma^{(t)}) = N/[1 + (N-1)\,\bar{\rho}_t]$ 在无创新项时随 $(1-\gamma)^{2t}$ 以几何速度坍缩至1，在持续创新项下则按 $1 + \Theta(t^{-1})$ 坍缩。由此伴随三个分析上的细微问题坍缩：谱参与比 r_{PR} 相对于 N_{eff}（定义B.1）严格高估了方差缩减；Popoviciu界（$\mathrm{Var}(y_i^{(t)}) \le 1/4$直接禁止在 $[0,1]$ 概率上施加无界的持续加性漂移，因此必须采用潜在得分表述；仅靠对称平均会将5取5门控坍缩为第0轮多数决，而非单智能体误差（备注B.1）；在共享先验（$\bar{\rho}_0 \gg 0$）和不对称谄媚性 [7, 8, 21]下，实证辩论会进一步恶化。因此，PIEQ从不将意见一致的智能体计入安全法定人数。

2.3 何时让语言模型留在闭环中：综合与验证不对称性

由于 PIEQ 要求操作人员在可信计算基内编写可信符号安全模型（$\mathcal{S}_{\mathrm{cand}}$，$\mathcal{M}_{\mathrm{sys}}$，$P_{\mathrm{sys}}$，$A^{\mathcal{K}}_{\mathrm{safe}}$，$\widehat{\ }$Post h_{man}，TPol），因此会立即引出一个架构问题：一旦有了这个符号模型，让不可信的语言模型留在控制回路中，相较于纯粹的确定性控制器，何时才能带来真正的价值？坦诚地回答这个问题，可以区分出三种运行机制。

首先，在小型、单跳、完全结构化的领域中（例如，Patroni 中由三个干净信号判定主节点失效，或`CN10/CN12` 在第6.6节中的小型单步确认事件），确定性监督器或有界的单步可信计算基前向链接器，速度更快、成本更低，也比实时大语言模型推理更可靠。在这种运行机制下，PIEQ 并不是引入大语言模型的理由；相反，当大语言模型智能体已部署用于更广泛的编排时，PIEQ 可提供可靠的安全边界。

其次，在大型或多跳规则空间以及多动作修复规划中，PIEQ 利用了合成与验证的不对称性这一经典原理，这一原理常见于携带证明的代码和 SAT/SMT 见证检查 [14, 13]。检查提议的 Horn 推导有向无环图并计算其物理足迹，在微小的可信计算基中只需不到一毫秒的确定性时间；而要在可信计算基内进行穷举前向链接，就必须施加严格的推导上限，才能确保过程可预测且可审计。正如第6.7 节的实证结果所示，当背景规则和推导深度增加时（$R_{\mathrm{bg}} \ge 80$，深度 $d \in \{2,3,4\}$），单跳和有界多跳的可信计算基前向链接都会耗尽推导上限并采取失效关闭策略（0/8 允许），而执行目标导向证明搜索的不可信提议者只提交相关的多跳有向无环图，未经改动的可信计算基会在0.07–0.28ms内完成验证，且可信计算基扩展量为零。

第三，在为经认证探测提供输入的非结构化事件分诊中，真实的运行事件始于杂乱的工单、堆栈跟踪、日志片段、变更差异和操作员运行手册，而确定性 Horn 引擎无法直接解析这些内容。在此过程中，大语言模型严格充当不受信任的分诊、范围选择和假设提议引擎：它选择要检查的资源范围、在安全备选方案中选择最符合运行意图的候选修复方案，以及请求哪些诊断探测。PIEQ 保证，非结构化文本中的任何幻觉或提示注入都无法伪造物理证据，因为每个获准叶节点都必须以加密方式绑定到采集器签名观测或只读探针句柄。第6.7节量化了所有十个基准测试域中的作者建模足迹，以及这种综合与补全权衡。

3 完整证明认证与来源打包

将语言模型移出可信计算基带来了架构挑战：控制平面仍希望利用智能体跨异构运维遥测综合多跳诊断的能力，但绝不能接受源自同一物理故障域的说服性文字或重复计数的证据。PIEQ 在kf-proxy （图1）中，通过结合携带证明的通信、基于假设的真值维护和递归物理来源打包来解决这一问题。如图1所示，来自不同故障域的签名遥测会输入确定性规则与冲突验证器，并与有界真值维护引擎配合工作。不受信任的模型在 TCB 外部提议候选推导图和冲突证书，而 kf-proxy 在执行前强制实施两个独立的认知门控：正向证据打包（问题1）证明变更的诊断前置条件在相互独立的物理域中均成立；合理世界安全防护层结合封闭域并发治理（问题2），验证该变更在所有未被反驳的故障世界和活动调度中都保持不变量。经认证的操作将继续执行至目标执行边界（问题3），而含糊或支持不足的提案则触发只读诊断探测或升级处理。

3.1 推导DAG PCE+不可满足组合通道与有界ATMS

基于假设的真值维护系统（ATMS） [9]跟踪的不仅是推导出了哪些诊断结论，还会精确记录哪些原始观察的最小组合支持每个结论，以及哪些组合彼此矛盾。PIEQ通过以携带证明的证据与不可满足组合（PCE+不可满足组合）通道取代自由形式的智能体对话 [23, 24], ，让模型能够基于分布式遥测 [22, 7] 合成多跳解释，同时剔除未经验证的说辞。具体而言，令 $\mathcal{E}_{\text{prim}} = \{e_0, \dots, e_{M-1}\}(M \le 64)$表示绑定到活动元组（res τ, h_{man}）的签名原始假设。任一假设环境 $E \subseteq \mathcal{E}_{\text{prim}}$ 都会映射为一个64位整数掩码 $\text{mask}(E) = \sum_{e_m \in E} 2^m$，从而能够以常数时间执行子集检查。每个ATMS节点 $n_c = \langle c, \mathfrak{L}(c)\ \mathcal{J}(c)\rangle$ 都会存储最小一致原始环境 $\mathfrak{L}(c)$以及支持命题 c的已验证推导DAG $\mathcal{J}(c)$。

定义1（已验证推导DAG与不可满足组合通道）。当且仅当 m满足以下任一条件时，确定性验证器 $\mathcal{V}_{\text{rule}}$ 允许消息 m：(1) Π 是一个以命题 c为根的已验证推导DAG，由有限无环图组成，其叶节点是非空的带符号假设 $e_m \in \mathcal{E}_{\text{prim}}$，与(res τ, h_{man})匹配；其内部节点 $v = \langle \text{id}_A(v)$、$\text{ctx}(v)$ c_v、$\text{ch}(v)$ $r_v, \sigma_v\rangle$分别应用规则 $r_v \in \mathcal{M}_{\text{sys}}$，该规则的后件 c_v 的前件集合与$\text{ch}(v)$中的命题双射匹配，并且具有递归原始叶节点集合 $E_{\text{leaf}}(e_m) \triangleq \{e_m\}$ 和 $E_{\text{leaf}}(v) \triangleq \bigcup_{u \in \text{ch}(v)} E_{\text{leaf}}(u) \neq \varnothing$；或(2) 一个最小不可满足组合证书 $\text{nogood}(E_\perp, \text{inv}_{\text{id}})$，其中非空带符号 $E_\perp \subseteq \mathcal{E}_{\text{prim}}$ 与$\text{inv}_{\text{id}} \in P_{\text{sys}}$ $(P_{\text{sys}}(E_\perp) \vdash \perp)$的冲突集合双射匹配。

只要编写的霍恩规则和冲突不变量准确描述了被建模的装置，真值维护就会保留有效结论，并清除相互矛盾的推导。

假设 1（可信演绎规则与不变量健全性）。在一致快照状态 S 下，令 $\mathcal{E}_{\text{true}}(S) \subseteq \mathcal{E}_{\text{prim}}$ 表示其谓词在 S 中物理成立的原始假设。每个 $r \in \mathcal{M}_{\text{sys}}$ 在 S 中均为保真，且 P_{sys} 具有冲突健全性：对于所有 $E \subseteq \mathcal{E}_{\text{true}}(S)$，$P_{\text{sys}}$ $(E) \not\vdash \perp$。

定理*1*（最小子集保留与冲突消除）。根据定义*1*和假设 *1*，设 $\mathcal{N}_\tau^{(t)}$ 是截至第 t 轮登记的已验证无解集。那么：（*1*）如果真实假设集 $E^\star \subseteq \mathcal{E}_{\text{true}}(S)$ 通过经验证的有向无环图 Π_0（其中 $E_0 = E_{\text{leaf}}(\Pi_0) \subseteq E^\star$ $(|E_0| \le d_{\max})$）支持 c，并且在登记时，要么某个 $E \subseteq E_0$ 已属于 $\mathfrak{L}(c)$，要么 $|\mathfrak{L}(c)| < L_{\max}$，那么，由于在检查 $L_{\max}$之前会剪除严格超集，$\mathfrak{L}^{(t)}(c)$ 对所有 $t \ge 1$ 都至少保留一个最小一致子集 $E \subseteq E^\star$，即使后续到达项导致预算_超限；（*2*）每个包含 $E_\perp \in \mathcal{N}_\tau^{(t)}$ 的环境 $E \supseteq E_\perp$ 都会从 $\overline{\mathfrak{L}^{(t)}(c)}$ 中清除，并且每个满足 $E_\perp \subseteq E_{\text{leaf}}(\Pi)$ 的有向无环图 Π 都会通过掩码(E) & 掩码$(E_\perp)$ = 掩码$(E_\perp)$ 停用。

证明。根据假设 1，不存在经验证的禁用集子集 $E_0 \subseteq \mathcal{E}_{\text{true}}(S)$，因此 E_0（或现有的 $E \subseteq E_0$）位于 $\mathfrak{L}(c)$ 中。任何后续一致的 E' 只有在 $E' \subsetneq E \subseteq E^\star$时才会取代 $E \subseteq E^\star$；在检查$L_{\max}$之前，剪除严格超集会丢弃 E，从而留下$|\mathfrak{L}_{\text{pruned}}(c)| < L_{\max}$，因此 E' 得以插入。容量已满时，不包含于现有集合的到达项会导致预算_超限，而不会修改 $\mathfrak{L}(c)$，且未来经验证的禁用集不可能成为 $E' \subseteq \mathcal{E}_{\text{true}}(S)$的子集。断言 (2) 源于位掩码子集恒等式。 □

该构造带来了两个操作属性。首先，定理1保证的是演绎可靠性，而不是幸存观测之间的统计独立性：将相互独立的 X、$Y \sim$ 伯努利分布 Bernoulli(0.5)置于执行$X = Y$的冲突过滤器条件下，会诱导出 $\text{Corr}(X, Y \mid X = Y) = 1$（伯克森悖论）。其次，由于通用 ATMS 标签维护和命中集枚举可能呈指数增长， [26], PIEQ 施加了严格的在线资源上限（$M \le 64$、$|E_{\text{leaf}}(\Pi)| \le d_{\max} = 6$、$|\mathfrak{L}(c)| \le L_{\max} = 64$、命中集上限 $B_{\text{HS}} = 256$以及打包上限 B_{pack}）。这些上限实施双重故障关闭截断：耗尽正向打包上限只会降低经认证的下界 $\hat{}$ $\nu_{\text{pack}} \le \nu_{\text{pack}}$（拒绝准入），而耗尽信念屏障上限则会保守地保留候选故障世界。安全性从不依赖不可信智能体发现每一个有效的禁用集。

3.2 递归依赖足迹与完整证明打包

验证单个 Horn 推导可证明：给定其叶节点，推导在逻辑上有效；但这尚未揭示有多少物理上相互独立的遥测域为候选变更提供支持。对于带有诊断前置条件 c_a 的变更 $a \in \mathcal{A}_{\text{mut}}$，令 $\mathcal{W}(a) \triangleq \{\Pi \in \mathcal{J}(c_a)\colon\ \forall E_\perp \in \mathcal{N}_\tau,\ E_\perp \not\subseteq E_{\text{leaf}}(\Pi)\}$ 为其活跃且无冲突、经过验证的证明有向无环图。计算 $\mathcal{W}(a)$ 的容错能力，需要进行精确的完整证明打包，而非采用标准图连通性或浅层前件检查，因为这两种较简单的启发式方法都会高估共享依赖。考虑从互不相交的故障域 F_1，F_2，F_3 中选取的三个观测，它们组合成三个合取证明：

$$E_{\text{leaf}}(\Pi_1) = \{e_1, e_2\}, \qquad E_{\text{leaf}}(\Pi_2) = \{e_2, e_3\}, \qquad E_{\text{leaf}}(\Pi_3) = \{e_1, e_3\}. \tag{2}$$

单位顶点最大流找到了三条顶点不相交路径（$F_i \to e_i \to \Pi_i$），并报告最小割 $= 3$，尽管任意一对

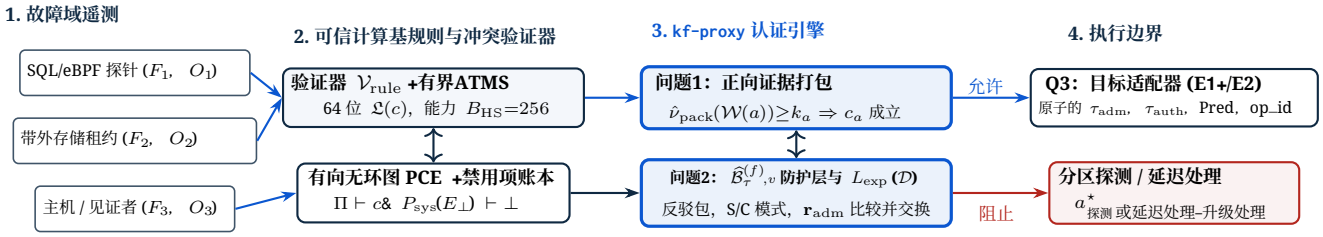

图1：PIEQ 中执行边界上的认识论认证（kf-proxy）。不受信任的大语言模型在 TCB 之外提出候选霍恩有向无环图和禁忌项；$\mathcal{V}_{\text{rule}}$ 以确定性方式验证推导；kf-proxy 将问题1（针对前置条件的正证据认证 $\hat{\nu}_{\text{pack}}(\mathcal{W}(a)) \geq k_a$） c_a与问题2（通过反驳打包实现的合理世界安全防护，以及在 $\mathcal{D}$ = 域$^\star(a)$ 上通过物理细化实现的封闭域并发治理，采用 $\mathbf{r}_{\text{adm}}(\mathcal{D})$ 比较并交换）区分开来；问题3 则将持久化隔离、Pred(a)和执行时授权新鲜度委托给目标能力层级（表2）。

证明都共享一个原始叶节点，因此没有两条完整证明在物理上彼此不相交（$\nu_{\text{pack}} = 1$）。同样，仅检查直接前件也无法处理多跳推导：两条深度为 2 的证明 $d_1 \vdash c_a$ 和 $d_2 \vdash c_a$分别由 $\{e_1, e_2\}$ 和 $\{e_1, e_3\}$推导而来，在深度 1 看似不相交，却共享上游叶节点 e_1。

借鉴数据溯源中的谱系传播 [12],，我们递归定义推导 DAG上的物理证据独立性足迹 $\Phi_{\text{phys}}(\Pi)$:

$$\Phi_{\text{phys}}(e_m) \triangleq \{F_{d_m}, O_m, e_m\}, \quad \Phi_{\text{phys}}(v) \triangleq \bigcup_{u \in \text{ch}(v)} \Phi_{\text{phys}}(u), \tag{3}$$

收集所有祖先原始叶节点、采集器通道和物理故障域，不包含其他任何内容。提议者上下文标识符 Ctx(Π) 用于标记发出每个推导节点的智能体和对话轮次，特意将其排除在外。将 {ctx(v)} 纳入足迹会混淆四种不同的独立性概念：物理遥测故障域独立性、经认证的原始观测独立性、语言模型推理独立性，以及证明构造上下文标识符 distinctness。只有前两种会纳入我们的确定性故障阈值保证。上下文标识符只是标签产物，单个模型可以随意生成，且永远无法证明推理独立；而模型推理独立性在经验上与合成召回率有关，但未纳入形式化模型。因此，PIEQ 的故障阈值严格以独立物理证据域为依据，完全不受智能体数量、模型族、对话上下文或提交次数影响。

定义 2（互不相交的完整论证打包数）。对于活动的已验证证明有向无环图 $\mathcal{W}$,

$$\nu_{\text{pack}}(\mathcal{W}) \triangleq \max\Big\{ |\mathcal{J}| : \mathcal{J} \subseteq \mathcal{W}, \\ \forall \Pi \neq \Pi' \in \mathcal{J},\ \Phi_{\text{phys}}(\Pi) \cap \Phi_{\text{phys}}(\Pi') = \varnothing \Big\}, \tag{4}$$

排除任何 Π 且满足 $\Phi_{\text{phys}}(\Pi) = \varnothing$ 的情况，因为不依赖任何经认证原始观测的推导无法认证任何内容，也不得被视为与其他证明真空地互不相交。

操作员可以选择实施更严格的提议者上下文隔离策略，要求打包证明中的上下文令牌两两不同。由于将上下文标签纳入足迹后会得到 Φ_{phys}的超集，因此此类策略只会降低 ν_{pack}，绝不会削弱物理故障界；无论如何标记上下文，共享的物理遥测总会造成足迹重叠。根据定义 2，一个智能体综合来自三个独立遥测域的证明，可合理达到$\nu_{\text{pack}} = 3$；而五个智能体（或五个上下文 ID）在单一物理域上进行推理，永远无法超过 $\nu_{\text{pack}} = 1$。来自某个域的单次错误观测，绝不会通过不同推导被重复计数。

假设 2（故障域划分完整性）。 可信计算基拓扑清单 h_{man} 准确地将每个采集器 O_m 绑定到其真实的物理或逻辑故障域 $F_{d_m} \in \mathcal{F}$，且每个经验证的有向无环图 Π 均满足 $E_{\text{leaf}}(\Pi) \neq \varnothing$。

定理 *2*（完整证明的独立性与正面证据认证）。设假设 *1* 和 *2* 在一致的观测快照 $S_{v_{\text{snap}}}$ 处成立（ $\mathcal{W}(a)$ 中的所有叶节点都观测 $S_{v_{\text{snap}}}$ 的谓词），并设 $\mathcal{G}_{\text{prov}}$ 为基于 $\mathcal{F}_{\text{src}} \to \mathcal{O}_{\text{raw}} \to \mathcal{E}_{\text{prim}} \to \mathcal{W}(a)$、排除提议者上下文的单位顶点容量物理流图。那么以下三项性质成立。第一，*(1)* 对于确定性的 k_a 域容错和快照前置条件认证， $\nu_{\text{pack}}(\mathcal{W}(a)) \geq k_a$ 可认证 k_a 个完整的已验证有向无环图 $\mathcal{J}_a = \{\Pi_1, \ldots, \Pi_{k_a}\}$，这些图的祖先故障域、采集器和叶节点两两不相交，且不受提议者上下文影响；若 c_a 在 $S_{v_{\text{snap}}}$ 中物理上为假，则至少有 k_a 个不同的故障域在 $\mathcal{F}$ 中发出了错误假设，因此反过来说，在至多 $f = k_a - 1$ 个故障域发生故障的情况下， $\nu_{\text{pack}}(\mathcal{W}(a)) \geq k_a$ 可认证 *SnapshotPreconditionValid*(a, v_{snap})，即前置条件在快照 $S_{v_{\text{snap}}}$ 时在物理上成立（这不同于提交时真值 *CommitPreconditionValid*(a, t_{eff})，后者将在第 *5* 节讨论）。第二，*(2)* 对于门格尔上界和单叶精确性，$\nu_{\text{pack}}(\mathcal{W}(a)) \leq \textit{minCut}_{\mathcal{G}_{\text{prov}}}(\mathcal{F}_{\text{src}}, \mathcal{W}(a))$，且在 $|E_{\text{leaf}}(\Pi)| = 1$ 对每个 $\Pi \in \mathcal{W}(a)$ 均成立的单叶片段中，可在多项式时间内判定相等。第三，*(3)* 对于足迹位掩码分支定界的精确性和故障关闭截断，对相同足迹去重，并丢弃任何满足 Π' 且 $\Phi_{\text{phys}}(\Pi) \subsetneq \Phi_{\text{phys}}(\Pi')$ 的情况，可精确保留 $\nu_{\text{pack}}(\mathcal{W}(a))$；对任意精度足迹位掩码进行有界分支定界，在 B_{pack} 尚未耗尽时返回 ν_{pack}，耗尽时则返回可靠下界 $\hat{\nu}_{\text{pack}} \leq \nu_{\text{pack}}$ （其中 *trunc* = 为 *true*）。

证明。对于（1），对任意经验证的有向无环图 Π 进行结构归纳可知：如果其根命题在 $S_{v_{\text{snap}}}$ 中为假，则根据假设 1，至少有一个子节点在 $S_{v_{\text{snap}}}$ 中为假，并可继续下降到域 $F_{d_{m_i}} \in \Phi_{\text{phys}}(\Pi_i)$ 中的一个为假的原始叶节点 $e_{m_i} \in E_{\text{leaf}}(\Pi_i)$。两两不相交性 $\Phi_{\text{phys}}(\Pi_i) \cap \Phi_{\text{phys}}(\Pi_j) = \varnothing$ 会产生 k_a 个不同的故障域；如果 c_a 为假，这将与至多 $f = k_a - 1$ 个故障域相矛盾。对于（2），每个大小为 k 的不相交打包都会根据门格尔定理诱导出 $\mathcal{G}_{\text{prov}}$ 中的 k 条顶点不相交路径；反之，

当 $|E_{\text{leaf}}(\Pi)| = 1$ 时，k 上的顶点不相交路径中的每条终端边 $(e_m,\ \Pi)$ 都有一个证明 $\Pi_{e_m} \in \mathcal{W}(a)$ 作为见证者，并且其物理足迹 $\{F_{d_m}, O_m, e_m\}$ 在各条路径之间两两不相交。对于（3），如果 $\Phi_{\text{phys}}(\Pi) \subseteq \Phi_{\text{phys}}(\Pi')$ 且满足 $\Pi \neq \Pi'$，则二者不可能同时存在于任何不相交打包中；将 Π' 替换为 Π 可保留有效性和基数。分支定界只记录有效的不相交子集，并剪枝严格受支配的分支，因此终止结果是精确的，而截断返回 $\hat{}\nu_{\text{pack}} \leq \nu_{\text{pack}}$。 □

认证 $\Phi_{\text{phys}}(\Pi_i) \cap \Phi_{\text{phys}}(\Pi_j) = \varnothing$ 证明了在 h_{man} 下的结构性故障域不相交性。它既不证明物理故障在统计上的独立性（第 5.3 节将有条件地处理这一问题），也不证明提议者推理的独立性；PIEQ 既不要求也不声称这一点。更重要的是，证明某个诊断前置条件在快照 v_{snap} 时成立，本身并不能保证候选变更在多个故障世界都能解释同一症状时仍保留安全不变量；接下来将讨论这一控制理论问题。

4 容错的可能世界安全防护层

即使正向证明打包满足 $\nu_{\text{pack}}(\mathcal{W}(a)) \geq k_a$，确认某种症状也无法区分彼此不兼容的底层故障世界。在我们的复制数据库示例中，独立确认 SQL 健康检查超时，既可能对应主节点崩溃（s_{dead}），也可能对应主节点仍在运行、但被非对称网络分区隔离的情况（s_{part}）。此外，检查可能世界两两之间的安全动作重叠，并不能保证变更在全局范围内安全：如果三个可能世界的安全动作集

$$A_{\text{safe}}(s_1)=\{a,b\},\ A_{\text{safe}}(s_2)=\{b,c\},\ A_{\text{safe}}(s_3)=\{a,c\}, \quad (5)$$

每一对都共享一个安全动作，但全局交集$\bigcap_{i=1}^{3} A_{\text{safe}}(s_i)$为空。反之，允许单个故障传感器（$1 < k_a$）排除 s_{part}，将破坏 f-域故障预算，并使集群暴露于脑裂风险之下。

为在部分可观测性和有界遥测故障下管理执行，PIEQ 借鉴离散事件监督控制 [16], 部分可观测运行时安全防护层 [15, 28], 以及 Feldbaum 双重控制 [31]。kf-proxy 不依赖点诊断，而是将完整证明打包反向应用于反驳推导：除非至少有 $f+1$ 个物理上不相交的遥测域对其予以反驳，否则保留每个建模的故障世界。只有在同时对每个仍存世界保持不变量时，才允许执行变更。当没有任何变更在所有世界中都安全时，控制器便调用双重控制原则，以即时执行换取信息增益，派发只读诊断探测来划分仍存的世界，或确定性地升级至人工操作员。

定义 3（f-容错可信信念集）。对于有限候选全集 $\mathcal{S}_{\text{cand}}$，令 $\mathcal{W}_{\text{refute}}(s)$ 表示与 $s \in \mathcal{S}_{\text{cand}}$ 不兼容、且其叶节点在 v_{snap} 处与快照一致的活动已验证反驳有向无环图。对于故障预算 $f = k_a - 1$，将精确计算和有界计算的可信信念集定义为

$$\mathcal{B}^{(f)}_{\tau,v_{\text{snap}}} \triangleq \left\{ s \in \mathcal{S}_{\text{cand}} : \nu_{\text{pack}}(\mathcal{W}_{\text{refute}}(s)) \leq f \right\}, \quad (6)$$

$$\widehat{\mathcal{B}}^{(f)}_{\tau,v_{\text{snap}}} \triangleq \left\{ s \in \mathcal{S}_{\text{cand}} : \text{trunc}(s) \vee \hat{\nu}_{\text{pack}}(\mathcal{W}_{\text{refute}}(s)) \leq f \right\}, \quad (7)$$

其中 截断（s）表示以下情况成立：触发了任一 ATMS 或打包能力上限s，或者在发生变更的提交之间，反驳叶节点混用了不匹配的观测版本。根据定理 2（3），$\mathcal{B}^{(f)}_{\tau,\,v_{\text{snap}}} \subseteq \widehat{\mathcal{B}}^{(f)}_{\tau,\,v_{\text{snap}}}$无条件成立。

要在该可信信念集中保留真实状态，取决于编写的候选全集是否覆盖真实快照状态，以及反驳推导是否基于真正与被反驳世界相矛盾的谓词。

假设 3（受快照约束的候选全集与安全模型）。在一致的观测快照 v_{snap} 处（$\mathcal{W}_{\text{refute}}(S_{v_{\text{snap}}})$中的所有叶节点均满足 $v_{\text{obs}}(e_m) = v_{\text{snap}}$，或者跨越 $[v_{\min}, v_{\max}]$，且在区间 $(v_{\min}, v_{\max})$ 内没有提交会变更已观测谓词）：(1) $S_{v_{\text{snap}}} \in \mathcal{S}_{\text{cand}}$；(2) 每个经验证的反驳有向无环图 $\Pi \in \mathcal{W}_{\text{refute}}(S_{v_{\text{snap}}})$ 至少引用一个在物理上于 $S_{v_{\text{snap}}}$ 中为假的原始叶节点（只要反驳是对 $S_{v_{\text{snap}}}$ 中为假的谓词进行 Horn 推导，这一点便由假设 1 自动推出）；以及 (3) 对每个 $a \in A^{\mathcal{K}}_{\text{safe}}(S_{v_{\text{snap}}})$，$\text{Post}(S_{v_{\text{snap}}}, a) \subseteq \mathcal{K}$。

引理 3（容错可信世界不变式安全性）。在假设 *2*和*3*下，假设在一致的快照 v_{snap} 中，至多有 f 个故障域发出错误遥测假设。那么，无论正向证明打包 $\nu_{\text{pack}}(\mathcal{W}(a))$ 如何，两项保证均成立。第一，*(1)* 对于通过反驳打包保留真实状态，无论 *ATMS* 或打包是否发生截断，$\nu_{\text{pack}}(\mathcal{W}_{\text{refute}}(S_{v_{\text{snap}}})) \leq f$，因此 $S_{v_{\text{snap}}} \in \mathcal{B}^{(f)}_{\tau,\,v_{\text{snap}}} \subseteq \widehat{\mathcal{B}}^{(f)}_{\tau,\,v_{\text{snap}}}$。第二，*(2)* 对于一步不变式保持，任何满足以下条件的变更

$$a \in \bigcap_{s \in \widehat{\mathcal{B}}^{(f)}_{\tau,v_{\text{snap}}}} A^{\mathcal{K}}_{\text{safe}}(s) \quad (8)$$

保证 $a \in A^{\mathcal{K}}_{\text{safe}}(S_{v_{\text{snap}}})$ 以及 $\text{Post}(S_{v_{\text{snap}}}, a) \subseteq \mathcal{K}$，即使 $\nu_{\text{pack}}(\mathcal{W}(a)) = 0$。当 $\mathcal{A}_{\text{mut}}$ 上的交集为空时，kf-proxy 会调度只读分区诊断探测 $a^{\star}_{\text{probe}} \in \mathcal{A}_{\text{probe}}$，以最大化跨 $\widehat{\mathcal{B}}^{(f)}_{\tau,\,v_{\text{snap}}}$ 的不同预测结果（或对安全分区探测采用任意策略加权 *EVSI* 排序），否则确定性地转换为DEFER_ESCALATE。

证明。根据假设 3(2)，每个 $\Pi \in \mathcal{W}_{\text{refute}}(S_{v_{\text{snap}}})$ 都在 $S_{v_{\text{snap}}}$ 中包含一个错误叶节点。如果 $\nu_{\text{pack}}(\mathcal{W}_{\text{refute}}(S_{v_{\text{snap}}})) \geq f+1$，则假设 2 意味着至少存在 $f+1$ 个不同的故障故障域，这与故障预算 f 相矛盾。因此 $S_{v_{\text{snap}}} \in \mathcal{B}^{(f)}_{\tau,v_{\text{snap}}} \subseteq \widehat{\mathcal{B}}^{(f)}_{\tau,v_{\text{snap}}}$，结合假设 3(3)，等式 (8) 可立即推出 $a \in A^{\mathcal{K}}_{\text{safe}}(S_{v_{\text{snap}}})$ 和 $\text{Post}(S_{v_{\text{snap}}}, a) \subseteq \mathcal{K}$。 □

至关重要的是，引理3从不依赖不可信的语言模型枚举所有候选世界，或发现每个有效反驳。由于 $\mathcal{S}_{\text{cand}}$ 是在可信计算基内部编写的（假设3(1)），遗漏反驳只会降低$\hat{}\nu_{\text{pack}}(\mathcal{W}_{\text{refute}}(s))$，从而保守地保留世界，而不是将其剪除 $S_{v_{\text{snap}}}$。同样，第6.6 节评估的可选有界确定性补全钩子，只会在已认证叶节点上添加经验证器接受的推导，因此，只要假设1 –3成立，它就能维持引理3，同时直接暴露任何违反假设1 的情况。

引理 3 还阐明了 PIEQ 两个认知门控之间一项关键的架构分离。正向证明打包

$(\nu_{\mathrm{pack}}(\mathcal{W}(a)) \geq k_a)$ 在逻辑上并非维持所建模安全不变量所必需 $\mathcal{K}$，反驳打包和全局安全动作交集本身就能确保该不变量。相反，根据定理 2(1)，正向打包承担了一项独立义务：证明该变更的诊断前提 c_a 确实在至多 $f = k_a - 1$ 个故障域的情况下成立。仅移除正向打包，同时保留 $\widehat{\mathcal{B}}_\tau^{(f)}$中的反驳打包以及等式 v_{snap}（8），仍能保留 $\mathcal{K}$，但会丧失前置条件可靠性，使产生幻觉的智能体或单个受损的遥测域触发无正当依据的错误前提变更（$\neg c_a$，例如不必要的故障转移、节点排空或负载削减），而这些变更碰巧仍能使被控对象处于 $\mathcal{K}$之内。反之，移除或削弱反驳打包（例如统计来自共享交换机的原始反驳，或在 $\mathcal{W}_{\mathrm{refute}}(s)$ 中对等式（2）使用门格尔路径流）会直接破坏真实状态保留，使 f 个或更少的故障域将 $S_{v_{\mathrm{snap}}}$ 从信念集中排除，并允许接受违反不变量的变更，例如脑裂。因此，两个认知门控都不可或缺，但二者仍然都只评估单个冻结快照；下一节将讨论多个操作针对实时物理目标并发执行时会发生什么。

5 物理精化并发、持久性与风险核算

第 3 节和第 4节中提出的认知认证与可能世界屏蔽，只能在没有竞争写入者的单一冻结快照上保证安全性。生产控制平面很少能保持这种静止状态：多个协调器可能同时对重叠资源采取操作；目标状态可能在观测与执行之间发生变化；授权或策略审批可能在执行过程中被撤销；而物理执行器通常执行多阶段操作，而非瞬时转换。为了将快照级认知安全性贯彻到物理提交边界，本节借鉴并发控制与分布式系统理论，具体包括线性一致性、严格可串行化、Abadi–Lamport 颤动细化、托管式风险暴露核算、租约和栅栏令牌，并将这些内容组织为封闭域并发治理、可验证的物理精化契约、分级目标强制执行和条件式风险核算。

5.1 并发危险、连续快照与物理精化

由于安全不变量通常会耦合多个基础设施资源，并发治理必须作用于封闭暴露域集合 $\mathcal{D} = \mathrm{Dom}^\star(a) \triangleq \mathrm{Close}(\mathrm{Dom}(a)\ \mathcal{G}_{\mathrm{inv}})$，涵盖所有通过共享不变量与候选变更 a 传递关联的域。对$\mathcal{D}$ 进行安全并发执行，必须消除六种不同的执行层危害。其中三种源于操作排序和取消：仅在进行中的操作 u 之后检查候选项 a，会遗漏反向交错执行（$a \to u \to s_{\mathrm{bad}} \notin \mathcal{K}_{\mathcal{D}}$ 即使 $u(s_0) = s_1$ 且$a(s_0) = a(s_1) = s_2 \in \mathcal{K}_{\mathcal{D}}$ 但 $u(s_2) = s_{\mathrm{bad}}$）；仅检查终止状态，会忽略被后续恢复掩盖的不安全前驱前缀（$u_1(s_0) = s_{\mathrm{bad}} \notin \mathcal{K}_{\mathcal{D}}$，随后 $a(s_{\mathrm{bad}}) = s_{\mathrm{rec}} \in \mathcal{K}_{\mathcal{D}}$）；而取消或对 a 实施栅栏（已栅栏_无_效果）可能暴露不安全的候选项缺席调度（u_1、u_2）：只要 $a \prec_{\mathrm{ord}} u_2$ 仅在 a 执行的运行中负责保护u_1、u_2，就会出现这种情况，因为栅栏 a 仍满足 $\mathrm{Pred}(u_2) \subseteq \mathrm{Settled}^{\mathrm{target}}$。

状态版本管理、并发执行重叠和并发协调器还会带来三种额外风险。首先，未进行版本管理的提交或隐藏的提交版本间隙会破坏状态投影：如果快照 $v_{\mathrm{snap}} = 0$ 观察到 $x = 0$，而未进行版本管理的提交或未确认操作 $u \in \mathcal{I}_U$ 实际上已在 $v = 1(x \leftarrow 10)$ 提交，且已确认提交$c \in \mathcal{I}_C$ 在 $v = 2\,(x \leftarrow x + 1)$ 提交，那么只推进 c，然后 u 计算出 $\{1, 10\}$，就会遗漏真实的物理状态$x = 11$。其次，读写阶段重叠会导致物理写偏斜：在不变量 $\neg(x = 1 \wedge y = 1)$ 下，初始状态为 $(x,\ y) = (0,\ 0)$，操作 a (读取 y；若为 0，则设为 $x \leftarrow 1$) 和操作 u (读取 x；若为 0，则设为 $y \leftarrow 1$) 各自按顺序执行时均安全（分别得到 $a \to u \mapsto (1,\ 0)$ 和 $u \to a \mapsto (0,\ 1)$），但当写入阶段 $r_a \to r_u \to w_a \to w_u$ 在物理上重叠时，会得到 $(1,\ 1) \notin \mathcal{K}_{\mathcal{D}}$，即使在可交换双重提交变体中也是如此。第三，若没有账本串行化，两个并发协调器可能各自基于同一个未决集合 $\mathcal{U}|_{\mathcal{D}}$ 进行验证，并在顺序或并发准入模式下签发彼此无效的过时准入证书。

为消除版本间隙并跟踪跨越$\mathcal{D}$的在途暴露，kf-proxy维护观测水位线 $[v_{\min}, v_{\max}]$、承载提交版本 $v_{\mathrm{commit}}(c) \in \mathbb{N} \cup \{\perp\}$的提交历史 $\mathcal{H}_C|_{\mathcal{D}}$、针对每个 $d \in \mathcal{D}$两两不相交的暴露集合 $\mathcal{I}_C(d)$ $\mathcal{I}_H(d)$ $\mathcal{I}_U(d)$（其暴露总量为 $C(d)$ $H(d)$ $U(d)$，未决集合为 $\mathcal{U}_\tau|_{\mathcal{D}} \triangleq \bigcup_{d \in \mathcal{D}} (\mathcal{I}_H(d) \cup \mathcal{I}_U(d))$，以及单调递增的逐域准入修订版本 $\mathbf{r}_{\mathrm{adm}}(\mathcal{D}) = \{(d,\ r_{\mathrm{adm}}(d))\}_{d \in \mathcal{D}}$。令 $\widehat{\mathrm{Post}}(s,\ o) \triangleq \mathrm{Post}(s,\ o) \cup \mathrm{Post}^{\mathrm{part}}(s,\ o)$包含声明的部分效果、$\mathcal{T}_{\mathrm{det}}(S,\ c) \triangleq \bigcup_{s \in S} \mathrm{Post}(s,\ c)$，以及 $\mathcal{T}_{\mathrm{opt}}(S,\ c) \triangleq S \cup \mathcal{T}_{\mathrm{det}}(S,\ c)$；每当任何转换到达 $\mathcal{S}_{\mathrm{cand}}$之外的未建模世界标识符时，均采取故障闭合。

通过强制执行连续提交版本屏障，可彻底消除隐藏版本间隙。令 $\Delta_C^{\perp}(\mathcal{D}) \triangleq \{c \in \mathcal{H}_C|_{\mathcal{D}} : v_{\mathrm{commit}}(c) = \perp\}$ and $v_{\mathrm{head}} \triangleq \max(\{v_{\max}\} \cup \{v_{\mathrm{commit}}(c) :\ c \in \mathcal{H}_C|_{\mathcal{D}} \setminus \Delta_C^{\perp}(\mathcal{D})\})$。每当 $\Delta_C^{\perp}(\mathcal{D}) \neq \varnothing$ 或任意整数版本$v \in (v_{\min},\ v_{\mathrm{head}}]$ 在 $\{v_{\mathrm{commit}}(c) :\ c \in \mathcal{H}_C|_{\mathcal{D}}\}$中缺失时，`kf-proxy` 会阻止 $\mathcal{D}$ 准入，直到目标预写式日志协调补齐缺失的提交历史，或确认已围栏_无_影响。提交序列连续后，跳过不大于 $v_{\min}$ 的提交，观测窗口内的提交 $\Delta_C^{\mathrm{win}} = \{c :\ v_{\min} < v_{\mathrm{commit}}(c) \leq v_{\max}\}$可选择通过 $\mathcal{T}_{\mathrm{opt}}$ 推进，而严格晚于快照的提交 $\Delta_C^{>v_{\max}}$则通过 $\mathcal{T}_{\mathrm{det}}$ 按 v_{commit} 升序确定性地推进：

$$\mathcal{S}_\tau^{\mathrm{base}} \triangleq \mathcal{T}_{\mathrm{det}}^{\Delta_C^{>v_{\max}}}\Big(\mathcal{T}_{\mathrm{opt}}^{\Delta_C^{\mathrm{win}}}\big(\widehat{\mathcal{B}}^{(f)}_{\tau_{\mathrm{obs}},[v_{\min},v_{\max}]}\big)\Big). \tag{9}$$

仅当真实的目标执行忠实对应于这些抽象转换时，检查来自 $\mathcal{S}_\tau^{\mathrm{base}}$ 的抽象调度才能保证物理安全性。令 $\theta = (\sigma_0 \xrightarrow{e_1} \sigma_1 \cdots \xrightarrow{e_m} \sigma_m)$ 为操作 O 在 $\mathcal{D}$ 上的物理执行轨迹。借鉴 Abadi–Lamport 颤动细化 [25],，我们要求一个明确的物理细化契约 $\mathrm{Refines}_{\mathcal{D}}(\mathcal{S}_\tau^{\mathrm{base}}, O, \prec_{\mathrm{ord}})$：每个从 $\alpha(\sigma_0)$ 开始的物理可达步骤 $\sigma_k \xrightarrow{e_{k+1}} \sigma_{k+1} \in \mathcal{S}_\tau^{\mathrm{base}}$，要么停顿（$\alpha(\sigma_{k+1}) = \alpha(\sigma_k)$），要么沿着可接受调度 $\pi \in \widehat{\mathrm{Lin}}(O', \prec_{\mathrm{ord}}|_{O'})$ 匹配一个已启用的抽象步骤 o，并满足 $\alpha(\sigma_{k+1}) \in \mathrm{Post}(\alpha(\sigma_k)\ o)$。

PIEQ 通过两种经验证的执行制度以及故障关闭默认机制，将细化$_{\mathcal{D}}$ 操作化。在 R1 制度（可串行化_原子的）下，目标必须在建模操作效果边界处提供严格可串行化（线性一致性）[17]，而非弱可串行化或快照隔离 [19]：弱

可串行化忽略实时优先关系，可能会将栅栏之后或 Pred(a)之后的写入，排在一个已完成的前驱操作之前进行序列化；而快照隔离则允许写偏斜（$r_a \to r_u \to w_a \to w_u \to (1,\ 1)$）。要符合 R1，必须在 h_{man} 中绑定经签名的目标能力配置，以证明存在单一边界上的严格可串行化提交原语（例如 SQLite`BEGIN IMMEDIATE`、Raft/`etcd`跨所有编码 $\mathcal{K}_{\mathcal{D}}$的键执行多键比较并交换，或硬件/存储代际比较并交换），并结合完整写入方中介。

在 R2 制度（阶段_分解式）下，物理操作在内部可能发生重叠，经验证的转移关系必须明确建模六种物理现象：由 $\prec_{\text{intra}}$ 排序的内部读取、决策和写入阶段；嵌入 $\mathcal{S}$ 内的每操作局部状态和缓存的读取值（例如，$(x,\ y,\ y_a,\ x_u)$）；表示为尾随步骤的异步后台回调或网络钩子，即使客户端已返回或中止，这些步骤仍保持启用；部分效果（$\text{Post}^{\text{part}}$）以及不可取消的操作内前缀，在控制平面取消或租约到期后仍可执行；从中间前缀可达的崩溃与恢复后续过程；以及重试或重复的物理效果，这些效果要么通过目标原生的逐阶段幂等性证明为停顿式无操作，要么明确表示为有界重试阶段。若未获得经认证的 R1 或 R2 资格认证，PIEQ 将回退至故障关闭默认机制（未经验证_异步）：完全拒绝并发模式 C 准入；若两个或更多无序前驱可能发生重叠，则拒绝模式 S 准入；仅允许完全有序且互不重叠的模式 S 执行。

一个重要的保真边界约束着这些契约：对有限抽象阶段图进行穷举探索，只能验证抽象模型，绝不能证明物理实现符合该模型。运行故障注入（第 6节）可以证伪精化主张，并为简单的单存储事务适配器构建证据；而分布式异步适配器则需要形式化模拟或精化验证（例如 TLA+或机械化证明）。凡是物理精化尚未经过形式化证明的地方，$\text{Refines}_{\mathcal{D}}$ 仍是一个明确的可信目标契约，并在第 E_8 5.3 节的层级 中予以计入。

定义 4（归纳调度不变式、模式 S 和模式 C）。固定封闭域集合 $\mathcal{D} = \text{Dom}^{\star}(a)$、不变量 $\mathcal{K}_{\mathcal{D}}$，以及由 Pred($o$) 编码的目标偏序 $\prec_{\text{ord}}$（连同 R2 下的 $\prec_{\text{intra}}$）。首先，（1）对于归纳调度不变式，调度 $\pi = (o_1, \ldots, o_\ell)$ 从 s_0 起对 $\mathcal{K}_{\mathcal{D}}$ 是顺序安全的，当且仅当 $s_0 \in \mathcal{K}_{\mathcal{D}}$，并且对于每个 $j \in \{1, \ldots, \ell\}$ 和每个可达的 s_{j-1}，$s_{j-1} \in \mathcal{K}_{\mathcal{D}}$、$o_j \in A^{\mathcal{K}_{\mathcal{D}}}\text{safe}(s_{j-1})$，且 $\widehat{\ }\text{Post}(s_{j-1}, o_j) \subseteq \mathcal{K}_{\mathcal{D}} \cap \mathcal{S}_{\text{cand}}$。谓词 $\text{Inv}_{\text{sched}}(\mathcal{S}_0, \mathcal{U}, \prec_{\text{ord}}; \mathcal{K}_{\mathcal{D}})$ 成立，当且仅当每个可准入子集 $O \subseteq \mathcal{U}$（允许缺失或被隔离的 _ 无 _ 效果操作，并且在 R2 下操作内前缀闭合）以及每个 $\pi \in \text{Lin}(O, \prec_{\text{ord}}|_O)$，从每个 $s_0 \in \mathcal{S}_0$ 出发都顺序安全；令 $\mathcal{R}_{\prec_{\text{ord}}}(\mathcal{S}_0, \mathcal{U})$ 表示沿此类前缀可达的所有状态。其次，（2）对于暴露量守恒和通用版本比较并交换，对于每个 $d \in \mathcal{D}$，集合 $\mathcal{I}_C(d)\ \mathcal{I}_H(d)\ \mathcal{I}_U(d)$ 始终两两不相交，且 $C(d) + H(d) + U(d) \le B(d)$。模式 S 或模式 C 下的每次准入都会绑定 $\text{r}_{\text{adm}}(\mathcal{D})$，并通过线性化比较并交换原子地提交，要求对所有 $d \in \mathcal{D}$，$r^{\text{cur}}_{\text{adm}}(d) = r^{\text{cert}}_{\text{adm}}(d)$；而 L_{exp} 中的每次预留变更（准入、崩溃保留、超时、提交、释放或协调）都会递增 $r_{\text{adm}}(d)$，使并发协调器处理陈旧状态前必须重新验证必须重新验证。第三，（3）对于前驱边界，每当 $u \prec_{\text{ord}} o$、$u.\text{op_id} \in$ 属于 Pred(o) 时，必须在目标端原子地强制执行 $\text{Pred}(o) \subseteq \text{Settled}^{\text{target}}$（已持久化提交为 COMMITTED 或已隔离为 _NO_EFFECT）。第四，（4）对于有界模式 C 认证（CompatCert），将 $\mathcal{U}_\tau|_{\mathcal{D}} = \mathcal{U}_S \sqcup \mathcal{U}_C$ 划分为满足 $\mathcal{U}_S \prec_{\text{ord}}(\mathcal{U}_C \cup \{a\})$ 的部分。模式 C 要求经证明的 R1（$|\mathcal{U}_C| \le K_{\text{conc}} = 4$）或 R2（$|\mathcal{P}| \le K_{\text{phase}} = 6$ 阶段步数），且无序 $|\mathcal{U}_S| \le K_{\text{conc}}$ 有界（或 $\mathcal{U}_S$ 全序）。验证器 $\mathcal{V}_{\text{compat}}$ 验证 $\text{Inv}_{\text{sched}}(\mathcal{S}^{\text{base}}_\tau, \mathcal{U}_S, \prec_{\text{ord}}; \mathcal{K}_{\mathcal{D}})$，得到 $\mathcal{S}^{\text{pre}}_\tau$；对每个可准入子集 O'（包括包含和不包含 a 的子集，在 R2 下操作内前缀闭合）以及跨越 Post 的每个 $\pi \in \text{Lin}(O', \prec_{\text{ord}}|_{O'})$ 进行穷举验证，并使用 SHA-256 摘要封存该机制及 $\text{r}_{\text{adm}}(\mathcal{D})$。（我们的实现还会检查无序 R1 操作对是否两两可交换，将其作为保守的收敛策略；不过，为保持不变式，可交换性在逻辑上并非必需。）超出此有界类别时，模式 C 会安全关闭，回退至模式 S 或拒绝。

将抽象调度安全性提升至物理状态，需要来自不相交域的中介、精化、持久性与隔离。

假设 4（并发中介、细化、持久性与框架）。对于封闭域集合 $\mathcal{D} = \text{Dom}^{\star}(a)$ 和不变量$\mathcal{K}_{\mathcal{D}}$：(1) 所有涉及 $\mathcal{D}$ 的写入者都通过可线性化的 L_{exp} 进行中介，并采用经身份校验的签发去重、通用 $\text{r}_{\text{adm}}(\mathcal{D})$ 比较并交换，以及跨 $\mathcal{D}$ 的原子多域预留（或全局串行化）；(2) $0 \le \text{Exp}_{\text{act}}(u, d) \le \text{Exp}(u, d)$，且物理执行过程在其经证明的执行机制下满足 $\text{Refines}_{\mathcal{D}}$（R1、R2 或非重叠的全序模式 S）；(3) 存在 $v_{\text{snap}} \in [v_{\min}, v_{\max}]$，其具有 $S_{v_{\text{snap}}} \in \widehat{\mathcal{B}}^{(f)}_{\tau_{\text{obs}},\ [v_{\min}, v_{\max}]}$；(4) 超时、确认丢失或与取消竞争的操作，将 $\mathcal{I}_H(d) \to \mathcal{I}_U(d)$ 转移，并且仅在经验证的栅栏_无_效果屏障之后释放预效果；(5) 目标持久化存储时期、Pred(o) 界、至多一次操作_标识以及跨崩溃的敞口上限；并且 (6) 根据封闭域框架条件，任何其 $\text{Dom}^{\star}(v) \cap \mathcal{D} = \varnothing$ 的操作v，都会使支配 $\mathcal{K}^{\text{phys}}_{\mathcal{D}}$、$\mathcal{K}_{\mathcal{D}}$、$A^{\mathcal{K}_{\mathcal{D}}}$ 的物理投影和建模投影保持安全，，并保持 $\widehat{\ }\text{Post}|_{\mathcal{D}}$ 不变量。

定理 *4*（封闭域物理不变式保持）。设在修订向量 $r_{\text{adm}}(\mathcal{D})$ 下，$\mathcal{D} = \text{Dom}^{\star}(a)$ 且 $\mathcal{U}_\tau|_{\mathcal{D}} = \bigcup_{d \in \mathcal{D}}(\mathcal{I}_H(d) \cup \mathcal{I}_U(d))$。在假设 *2–4* 下，且最多存在 f 个发生故障的遥测失效域，假设 *kf-proxy* 仅在连续提交版本屏障通过时才允许 a（式 *(9)*），L_{exp} 原子地提交 $r_{\text{adm}}(\mathcal{D})$ 比较并交换和敞口检查 $C(d) + H(d) + U(d) + \text{Exp}(a, d) \le B(d)$，跨越所有 $d \in \mathcal{D}$，并且满足以下任一条件：模式 *S* 成立（每个 $u \in \mathcal{U}_\tau|_{\mathcal{D}}$ 均位于 *Pred(a)* 中，$\mathcal{U}_\tau|_{\mathcal{D}}$ 在 *UNVERIFIED_ASYNC* 下全序排列，$\text{Inv}_{\text{sched}}(\mathcal{S}^{\text{base}}_\tau, \mathcal{U}_\tau|_{\mathcal{D}}, \prec_{\text{ord}}; \mathcal{K}_{\mathcal{D}})$ 成立，且对于所有 $s' \in \mathcal{R}_{\prec_{\text{ord}}}(\mathcal{S}^{\text{base}}_\tau, \mathcal{U}_\tau|_{\mathcal{D}})$，$a \in A^{\mathcal{K}_{\mathcal{D}}}\text{safe}(s')$ 且 $\widehat{\ }\text{Post}(s', a) \subseteq \mathcal{K}_{\mathcal{D}} \cap \mathcal{S}_{\text{cand}}$）；或模式 *C* 通过来自 $\mathcal{V}_{\text{compat}}$、在经证明的 *R1* 或 *R2* 下获得的已验证 $\text{CompatCert}(a, \mathcal{U}_C, \text{r}_{\text{adm}}(\mathcal{D}))$ 成立。则独立于正向证明打包：*(i)* $\text{Inv}_{\text{sched}}(\mathcal{S}^{\text{base}}_\tau, \mathcal{U}_\tau|_{\mathcal{D}} \cup \{a\}, \prec_{\text{ord}}; \mathcal{K}_{\mathcal{D}})$ 在准入线性化点得到保持；*(ii)* 对于 $\mathcal{U}_\tau|_{\mathcal{D}} \cup \{a\}$ 在 $\mathcal{D}$上的每条物理可准入轨迹 $\theta = (\sigma_0 \to \cdots \to \sigma_m)$，每个物理状态都满足 $\alpha(\sigma_k) \in \mathcal{K}_{\mathcal{D}}$ 和 $\sigma_k \in \mathcal{K}^{\text{phys}}_{\mathcal{D}}$；并且 *(iii)* 对所有 $d \in \mathcal{D}$，$\text{Exp}_{\text{real}}(d, t) \le C(d) + H(d) + U(d) \le B(d)$。

证明。 我们依次建立暴露量守恒、快照包含性、抽象调度安全性以及物理细化，具体如下：

对于暴露量守恒和版本修订比较并交换，根据 L_{exp} （假设 4(1)）的线性化事务进行归纳可知，针对 $\mathbf{r}_{\mathrm{adm}}(\mathcal{D})$ 执行原子比较并交换时，会拒绝任何依据较早账本状态评估的并发模式 S 或模式 C 证书；而回滚、崩溃保留至 $\mathcal{I}_U$、去重重试、超时（$\mathcal{I}_H \to \mathcal{I}_U$）、提交（$\mathrm{Exp}_{\mathrm{act}} \le \mathrm{Exp}$）以及经验证的带栅栏_无_效果释放，均保持 $\mathrm{Exp}_{\mathrm{real}}(d,t) \le C(d) + H(d) + U(d) \le B(d)$。对于连续快照包含性，引理 3(1) 和假设 4(3) 保证存在某个$v_{\mathrm{snap}} \in [v_{\min}, v_{\max}]$ 满足 $S_{v_{\mathrm{snap}}} \in \widehat{\mathcal{B}}^{(f)}_{\tau_{\mathrm{obs}},[v_{\min},v_{\max}]}$，而假设 4(6) 确保只有触及 $\mathcal{D}$ 的写入会修改 $\mathcal{K}_{\mathcal{D}}$。由于连续版本屏障确认 $(v_{\min}, v_{\mathrm{head}}]$ 中的每个整数版本均无间隙地出现在 $\mathcal{H}_C|_{\mathcal{D}}$ 中，因此没有未确认操作能在 $(v_{\min}, v_{\mathrm{head}}]$ 内提交；每个未确认操作要么已在 $v_{\min}$ 时或之前提交（由排除该操作的子集捕获），要么在 v_{head} 之后生效。因此，按版本升序应用 $\mathcal{T}^{\Delta_C^{\mathrm{win}}}$ opt，随后应用 $\mathcal{T}^{\Delta_C^{>v_{\max}}}$ det，即可得到 $\alpha(\sigma_0) \in \mathcal{S}_\tau^{\mathrm{base}}$。对于抽象调度安全性，假设 4(5)–(6) 以及 $\mathrm{Pred}(o) \subseteq \mathrm{Settled}^{\mathrm{target}}$ 确保每个已执行子集 O' 都沿着某个 $\pi \in \mathrm{Lin}(O', \prec_{\mathrm{ord}}|_{O'})$ 运行。模式 S 会验证 $\mathcal{U}_\tau|_{\mathcal{D}}$ 中的所有前缀（覆盖 $a \notin O'$），并验证来自每个 $s' \in \mathcal{R}_{\prec_{\mathrm{ord}}}$ 的 a（覆盖 $a \in O'$）；而模式 C 则穷举检查 $\mathcal{U}_S$ 以及每个可准入子集 O_C（既包含也排除 a，在 R2 下前缀闭合），并检查跨越 Post 的每个$\widehat{\ }$线性扩张，从而保持 $\mathrm{Inv}_{\mathrm{sched}}$。最后，根据细化$_{\mathcal{D}}$ （假设 4(2)），沿 θ 的每个物理状态 σ_k 都会通过 $\alpha(\sigma_k)$ 映射到一个可沿经验证的 π 在$\widehat{\ }$下到达的状态，从而得到 $\alpha(\sigma_k) \in \mathcal{K}_{\mathcal{D}}$ 和 $\sigma_k \in \mathcal{K}_{\mathcal{D}}^{\mathrm{phys}}$。 □

当全局安全性可分解为 $\mathcal{K} = \bigcap_{\mathcal{D}} \mathcal{K}_{\mathcal{D}}$ 且每个不变式耦合都封闭在 $\mathcal{G}_{\mathrm{inv}}$内时，定理 4通过求交进行组合，从而确立全局物理不变量保持（但不会自动确立全局受控可生存性 $\mathrm{Viab}(\mathcal{K})$）。然而，在陈述端到端组合保证之前，必须清楚地区分两个执行语义细节：诊断前置条件如何随时间变化，以及授权撤销何时会在不同目标能力层级上产生物理效果。

第一项区分是快照真实性 $\mathrm{SnapshotPreconditionValid}(a, v_{\mathrm{snap}}) \triangleq (S_{v_{\mathrm{snap}}} \models c_a)$ 与实际提交时真实性 $\mathrm{CommitPreconditionValid}(a, t_{\mathrm{eff}}) \triangleq (\sigma(t_{\mathrm{eff}}) \models c_a)$。定理 2(1)认证的是快照真实性，这是历史快照触发器所需的精确语义，例如撤销在 v_{snap} 时获证明已遭入侵的 IAM 角色或证书颁发机构。对于要求系统可靠保证提交时真值的瞬态状态操作，以下两种机制各自都足以满足要求：(S1) 区间持久化 $\mathrm{Persist}(c_a, [v_{\mathrm{snap}}, t_{\mathrm{eff}}])$ 并结合快照有效性；或 (S2) 在 E2级 下执行目标端原子重新验证 $\mathrm{AtomicReval}_a(t_{\mathrm{tx}})$，检查编码$c_a$ ($\mathrm{Reval}_a(\sigma) \Rightarrow \sigma \models c_a$ 的权威物理状态（而非缓存镜像），并在完整写入方中介下，于与变更相同的精确原子事务边界 $t_{\mathrm{tx}} = t_{\mathrm{eff}}$ 内完成。将析取式 (S1) ∨ (S2) 视为必要条件（即双条件）是错误的：瞬态谓词在 $[v_{\mathrm{snap}}, t_{\mathrm{eff}}]$ 上经历真 →假 →真的状态变化，即使没有持久化或原子重新验证，在提交时仍可能在物理上为真。反过来，在变更的原子事务之外重新验证谓词，会在条件检查通过后引入检查时与使用时之间的竞态（TOCTOU），此时条件已不再成立。此外，将重新验证交由调用方或提议者自行决定，会导致静默降级为仅检查快照（第 6.5 节对此有说明）。因此，PIEQ 为每种变更类型指定可信的时间策略 $\mathsf{TPol}(a) \in${快照触发，提交时敏感}

完全由 TCB 操作元数据持有，而绝不由不可信代理提议持有。在强化配置中，未分类的状态变更操作会默认拒绝；提交时敏感操作必须进行 E2 层级原子重新验证（S2），或采用经证明的持久性（S1），并且无论调用方是否遗漏，都会注入可信提交谓词；规范策略标识会签入证书，并在原子效果边界内重新检查，以拒绝已被取代的策略；快照触发操作则避免不必要的重新验证，并在短暂症状消退后仍可采取行动。

第二个区别在于 E2级原子新鲜性与 Tier E1+quiescence 相对于栅栏的排除。采用完整写入方中介的 E2级中，授权检查与物理状态变更会在 t_{tx} 原子地串行执行，从而实现零撤销竞态窗口（$\delta^{\mathrm{E2}}_{\mathrm{fresh}} = 0$）。而在 Tier E1+quiescence 下，一个最小的六步轨迹证明，严格的执行时新鲜性无法成立：在 $t = 1$，签发证书 C，其中包含 $\tau_{\mathrm{auth}} = 5$；在 $t = 2$，目标 r 验证 $\tau_{\mathrm{auth}} \ge 5$、获取锁 r，并进入 已准备_槽位；在 $t = 3$ （$t_{\mathrm{rev_init}}$），控制平面启动撤销 $\tau_{\text{控制平面授权}} \leftarrow 6$，并因锁 r 而阻塞；在 $t = 4$（t_{eff}），已进入准备状态的操作在撤销启动后仍完成物理提交；在 $t = 5$（t_{fenced}），锁 r 清空、刷新 $\tau^{\min}_{\mathrm{auth}}[r] \leftarrow 6$，并返回 FenceAck；在 $t = 6$，后续 $\tau_{\mathrm{auth}} = 5$ 操作会被确定性地拒绝。因此，Tier E1+quiescence 保证的是相对于栅栏的 FenceAck 后排除，而非零窗口撤销新鲜性。

推论 *1*（层级精确的组合式、执行过程绑定允许）。在假设 *1–4* 下，且发生故障的遥测失效域至多为 $f = k_a - 1$，假设 *kf-proxy* 仅在以下条件成立时允许变更 a：*(1)* 在一致快照有向无环图上，通过 $\hat{\nu}_{\mathrm{pack}}(\mathcal{W}(a)) \ge k_a$ 满足证据有效性；*(2)* $\mathit{SafetyValid}_{\mathcal{D}}$ 满足定理 *4* 在 $\mathcal{D} = \mathit{Dom}^\star(a)$ 上的假设；并且 *(3)* 目标层级 $T \in \{E2、E1 + q\}$ 通过签名证书验证强制执行 $\tau_{\mathrm{adm}} \ge v_{\mathrm{fence}}$, $\tau_{\mathrm{auth}} \ge \tau^{\min}_{\mathrm{auth}}$, $t_{\mathrm{now}} \le t_{\mathrm{auth_until}}$，且在完整写入方中介和 $\mathit{Refines}_{\mathcal{D}}$下，$\mathit{Pred}(a) \subseteq \mathit{Settled}^{\mathrm{target}}$ 成立。由此可得四项层级精确的性质：*(a)* 根据定理 *2(1)*，$\mathit{SnapshotPreconditionValid}(a, v_{\mathrm{snap}})$成立；若 $\mathit{Persist}(c_a, [v_{\mathrm{snap}}, t_{\mathrm{eff}}])$成立，或 $T = E2$执行权威的目标端原子前置条件重新验证 $\mathit{AtomicReval}_a(t_{\mathrm{tx}})$，并与物理变更共享原子提交边界，则系统可对 $\mathit{CommitPreconditionValid}(a, t_{\mathrm{eff}})$作出可靠保证（因此$\sigma(t_{\mathrm{eff}}) \models c_a$，但反向命题一般不成立）；*(b)* 根据引理 *3*和定理 *4*，每个中间物理状态和终止物理状态均满足 $\sigma_k \in \mathcal{K}^{\mathrm{phys}}_{\mathcal{D}}$，其中 $\mathit{Exp}_{\mathrm{real}}(d,t) \le B(d)$；*(c-E2)* 对于$T = E2$，在物理线性化点 t_{tx} ($\delta^{\mathrm{E2}}_{\mathrm{fresh}} = 0$)，授权和证据时期在原子层面均为最新；而 *(c-E1+)* 对于 $T = E1 + q$，在持久化 *Fence Ack* ($t \ge t_{\mathrm{fenced}}$)完成后，不会执行任何已撤销授权下的提交；但持有锁$_r$ 的已准备操作可能在 *FenceAck* 前窗口内提交（$t_{\mathrm{rev_init}}, t_{\mathrm{fenced}}$）（相对于 $t_{\mathrm{rev_init}}$，> 0为最新）。

5.2 证书绑定、持久性与能力层级

每份准入证书都会对以下十二元组进行密码学绑定：op_id，res $\mathcal{D}$，v_{snap}，h_{man}，h_{proof}，$\mathbf{r}_{\mathrm{adm}}(\mathcal{D})$ τ_{adm}，τ_{auth}，

$t_{\text{auth_until}}$，Pred(a) σ_{cp})。由于策略批准可能会在事件冻结或 RBAC 轮换期间被撤销，即使物理遥测仍然有效，授权纪元 τ_{auth}和有效期截止时间 $t_{\text{auth_until}}$ 也会独立于证据时期 τ_{adm} 演变。如果设置了 $t_{\text{auth_until}}$ 且没有可信目标时钟，目标验证将默认失败；与此同时，清单轮换（h_{man}）或迟到的冲突禁配约束会以原子方式推进 τ_{adm}，从而隔离飞行中证书。

在崩溃和分区故障下处理不可取消的外部操作，需要依赖持久化围栏屏障，而不能仅依靠控制平面租约到期。在 Tier E1+-静默下，控制平面租约到期并不会停止已经启动的外部 RPC：如果目标 r 在租约截止时间 $t_{\text{lease}} = 10$ 前于 $t = 9$ 发起不可取消的调用，并发生停滞或分区，该调用仍可能在租约到期后于 $t = 11$完成。因而，只有当目标 r 获取锁$_r$、排空活动执行，并通过 WAL/fsync（例如 SQLite PRAGMA synchronous=FULL或 Raft 仲裁提交）持久化刷新 $v_{\text{fence}}[r] \geq v$ 和 $\tau^{\min}_{\text{auth}}[r]$ 后再返回带签名的 FenceAck，或者外部目标本身在提交时强制执行 $t^{\text{loc}}_{\text{eff}} \leq t_{\text{lease}} - \Delta_{\text{skew}}$，同时将操作保留在 $\mathcal{I}_U$ 中直至完成协调，才能宣布围栏完成 $t_{\text{fenced}}(v)$。否则，kf-proxy 会将操作保留在 $\mathcal{I}_U(d)$中，并无限期阻止冲突的准入，以安全性优先于活性，直至 FenceAck、协调或 STONITH 或 IAM 撤销等硬外部屏障完成。

相关的持久性边界将本地预写日志去重与真正的目标原生幂等性区分开来。将持久化操作_身份绑定到本地或控制平面预写日志中的规范操作标识，只有当去重记录与物理状态变更在同一原子事务中提交时，才能保证至多一次执行；当事务性存储本身就是物理效果边界时，E2级即属此情形。对于跨越网络边界的远程执行器，在确认丢失后要防止重复执行，就需要真正的目标原生幂等性，例如与远程状态转换以原子方式持久化的远程幂等键或代际 CAS。当非事务性远程执行器缺乏目标原生幂等性且其响应丢失时，重试是不安全的：控制平面绝不能自动重试，而必须将该操作保持为未知状态，$\mathcal{I}_U$ 直到带外状态协调确定其是否已提交。同样，记录已隔离_无_效果 时，如果操作_身份 已提交，则必须以原子方式失败；重启后恢复还会根据持久化的目标$\mathcal{I}_H \cup \mathcal{I}_U$ 已提交 状态和 已隔离_无_效果日志进行协调，同时将未确认的操作保留在 $\mathcal{I}_U$中。表 2对目标能力层级 E0–E2 进行了分类，因此 PIEQ 绝不会声称底层目标在物理上无法强制实施的更强保证。

5.3 条件八风险分层核算

由于 PIEQ 中的每项形式化保证都以可信域模型、准确的故障域拓扑、有界传感器故障和目标细化为条件，操作人员需要一个清晰的记账恒等式，以跟踪残余故障模式而不重复计数。对于在 $D = |\mathcal{F}|$ 个遥测故障域上、封闭域集合$\mathcal{D}$ = Dom*(a)中的获准变更 a，我们定义八个有序的可测故障事件，涵盖建模契约、物理遥测故障和执行边界破坏。前两个事件刻画可信计算基建模和拓扑错误： $E_1 \equiv E_{\text{univ}}$ 发生在候选全集遗漏真实状态（$S_{v_{\text{snap}}} \notin \mathcal{S}_{\text{cand}}$）或观测结果跨越撕裂快照时； $E_2 \equiv E_{\text{rule}}$ 发生在$\widehat{\ }$($\mathcal{M}_{\text{sys}}$、 P_{sys}、 A_{safe}、Post)中的编写规则、冲突不变量、安全操作集合或后状态转换不健全时； $E_3 \equiv E_{\text{dom}}$ 发生在 h_{man} 错误地将采集器归类到某个故障域时。接下来的两个事件刻画物理遥测故障：

$E_4 \equiv E_{\text{common}}$表示外生的跨域共同原因故障机制发生（例如共用电源、DNS、内核或固件缺陷耦合两个或更多域；这里严格将其定义为因果机制，而非结果 $\{\sum_\ell Z_\ell \geq 2\}$，从而在以 E_4^c 为条件时不会引入负相关），而 $E_5 \equiv E_{\text{sensor}} \triangleq \{\sum_{\ell=1}^{D} Z_\ell \geq k_a\}$ 刻画 k_a 个或更多域发出错误假设的情形，其中 $Z_\ell \in \{0,1\}$ 表示域 F_ℓ中的错误假设。最后三个事件刻画执行层故障： $E_6 \equiv E_{\text{drift}}$ 发生于未被观测的被控对象漂移、未受中介的外部写入者，或两个足够的提交时前置条件机制（S1 Persist 和 S2 权威 E2级原子重新验证 $_a$）均未能满足已声明的提交时真实性操作时； $E_7 \equiv E^T_{\text{fresh}}$ 刻画目标强制执行、证据纪元或层级-T 授权新鲜度故障（包括在严格撤销新鲜度下、针对 $T = \text{E1}+\text{q}$评估时，($t_{\text{rev_init}}$、t_{fenced})中的 FenceAck 前提交，而在完全中介的T = E2下则为 $\delta_7 = \delta^{\text{E2}}_{\text{fresh}} = 0$）； $E_8 \equiv E_{\text{conc}}$ 刻画跨越提交历史间隙、暴露包络、Pred、Refines$_{\mathcal{D}}$、$\mathbf{r}_{\text{adm}}$ CAS、框架条件或 CompatCert 的并发协调故障。

命题 *5*（按层级索引的条件八风险核算）。定义互斥分层 $G_i \triangleq E_i \cap \bigcap_{j=1}^{i-1} E_j^c$ （i =*1*，*...*，*8*）及条件风险 $\delta_i \triangleq \mathbb{P}(E_i \mid \bigcap_{j=1}^{i-1} E_j^c)$，当条件事件的概率为零时，设定 $\delta_i = 0$。仅假设在给定 $\bigcap_{j=1}^{4} E_j^c$的条件下， D域故障指示变量 $\{Z_\ell\}_{\ell=1}^{D}$ 相互独立，且$\mathbb{P}(Z_\ell = 1 \mid \bigcap_{j=1}^{4} E_j^c) \leq \bar{p}_{\text{dom}}$。令 *BadCommit*$_T$（$a$）表示违反以下任一条件的物理执行过程：*(i)* $\mathcal{K}^{\text{phys}}_{\mathcal{D}}$ 或暴露能力上限 B（d）；*(ii)* *SnapshotPreconditionValid*（a， v_{snap}）（以及仅当 a 被声明为提交时真实性操作时的 *CommitPreconditionValid*（a， t_{eff}））；或 *(iii)* 第 T 层的授权保证，即在 t_{tx} 处对 $T = E2$ 的执行时新鲜度，或对 $T = E1 + q$ 的 *FenceAck* 后排除（如果将 *FenceAck* 前的撤销竞争计入严格新鲜度，则在 $E_7^{\text{E1+q}}$ 中予以核算）。那么根据推论 *1*，*(1)* *BadCommit*$_T$（a） $\subseteq \bigsqcup_{i=1}^{8} G_i$，且 $\mathbb{P}$（*BadCommit*$_T$（a） $\mid \bigcap_{i=1}^{8} E_i^c$） $= 0$；以及 *(2)*

$$\mathbb{P}(\text{BadCommit}_T(a)) \leq 1 - \prod_{i=1}^{8}(1-\delta_i) \leq \sum_{i \neq 5} \delta_i + \sum_{j=k_a}^{D} \binom{D}{j} \bar{p}^{\,j}_{\text{dom}} (1-\bar{p}_{\text{dom}})^{D-j}. \tag{10}$$

证明。在 $\bigcap_{i=1}^{8} E_i^c$ 上，假设 1–4 成立，至多有 $f = k_a - 1$ 个域失效，对于任何声明的提交时真实性操作，至少有一个充分条件（S1 或 S2）成立（根据推论1(a)，这意味着提交前置条件有效(a, t_{eff})），并且满足层级-T强制要求；因此排除了 BadCommit$_T$(a)。不相交性给出 $\mathbb{P}(\bigsqcup_{i=1}^{8} G_i) = \sum_{i=1}^{8} \delta_i \prod_{j=1}^{i-1}(1-\delta_j) = 1 - \prod_{i=1}^{8}(1-\delta_i) \leq \sum_{i=1}^{8} \delta_i$。 以 $\bigcap_{j=1}^{4} E_j^c$ 为条件的 G_5 通过随机占优，由二项分布尾部对 δ_5 给出界。 □

表 2：物理效果边界处的目标执行能力层级（精确到层级的授权时效性、可选的提交时前置条件重新验证、持久性以及丢失响应重试语义）。

Tier	有保障	无保障	线性化	所需持久状态	故障、确认丢失与剩余风险
E0（仅代理）	在派发前检查 kf-proxy。	准入后证据／授权撤销或去重。	t_{adm} 仅（无任何目标）。	目标处无。	延迟/撤销会泄露提交；确认丢失时非事务操作无法安全重试；$\delta^{\mathrm{E0}}_{\text{新鲜}} > 0.$
E1（异步推送）	拒绝过时/已撤销证书在本地栅栏之后到达。	当证书超过延迟栅栏时予以排除。	本地 $v_{\mathrm{fence}}[r], \tau_{\mathrm{auth}}[r]$。	持久化异步时期 +认证寄存器。	延迟栅栏泄露提交；$\delta^{\mathrm{E1}}_{\text{新鲜}} > 0.$
E1+读取（锁+读取索引）	拒绝在此之前已撤销的证书同步ReadIndex t_{read}。	如果发生撤销则排除在（t_{read}，t_{eff}）中提交。	拆分：$t_{\mathrm{read}} \neq t_{\mathrm{eff}}$。	锁$_r$ +同步ReadIndex + 持久化操作_标识日志。	在 (t_{read}，t_{eff}) 中撤销会泄露提交；$\delta^{\mathrm{E1+-read}}_{\text{新鲜}} > 0.$
E1+静止（两阶段屏障）	零 FenceAck 后提交（$t \geq t_{\mathrm{fenced}}$）；阻止 $\mathcal{I}_U$ 中的冲突停滞。	零窗口认证新鲜度在（$t_{\mathrm{rev_init}}$，t_{fenced}）中；CP 仅租约到期并不会停止不可取消的 RPC。	$t_{\mathrm{fenced}}(v)$开启持久化 FenceAck（或目标租约）。	锁$_r$ + fsync'的时期，RegisterPrepared，操作_标识日志 + FenceBarrier。	已准备好的操作可在 FenceAck 前提交（$\delta^{\mathrm{E1+q}}_{\text{新鲜}} > 0$ 与 $t_{\mathrm{rev_init}}$；0 次 FenceAck 后）；停滞使 $\mathcal{I}_U$ 无限期持续，直至完成协调。
E2（共享 / 原生原子的）	原子的 $\sigma_{\mathrm{cp}}, h_{\mathrm{man}}, \tau_{\mathrm{adm}}, \tau_{\mathrm{auth}}$、$t_{\mathrm{auth}}$、Pred、界 op_id、能力和选择加入提交前置条件有效在 t_{tx}（如果存储是效果边界）。	未经调解的带外外部写入者或远程原子事务之外的远程执行器事务。	单一不可分事务 / 目标原生比较并交换位于 t_{tx}.	持久化原子存储 (SQLite WAL 同步=完全/ etcd）或目标原生比较并交换。	确定性地中止过期/已撤销的证书，时间为 t_{tx}（在崩溃/重启后仍有效）；对以下情况安全地进行幂等重试：相同操作_ID；$\delta^{\mathrm{E2}}{}_{\text{新鲜}} = 0$以完整性为条件调解。

命题 5是一种条件会计恒等式，而非普适的经验界：δ_1，δ_4，δ_6，以及 $\bar{p}_{\mathrm{dom}}$ 仍是依赖环境的输入。用于验证我们执行语义反例的自动化回归测试（层级 E1+- 静默前置 FenceAck 竞态、瞬时下降并回升的非必要性，以及非原子的检查时与使用时竞态重新验证）已记录于附录 A。

5.4 端到端示例：编写与执行过程演示

为具体说明TCB编写、Q1打包、Q2防护层与Q3执行之间的交互，我们追踪一个紧凑的集群治理场景，将数据库故障转移与有界容量预留结合起来。

1. 编写的TCB模型。操作员指定：(i) 候选全集 $\mathcal{S}_{\mathrm{cand}} = \{s_{\mathrm{dead}}, s_{\mathrm{part}}, s_{\mathrm{ok}}\}$，以及安全操作映射 $A^{\mathcal{K}}_{\mathrm{safe}}(s_{\mathrm{dead}}) =$ {提升、探测、延迟处理}、$A^{\mathcal{K}}_{\mathrm{safe}}\ s_{\mathrm{part}} = \{\quad,\quad,\quad\}$ $A^{\mathcal{K}}_{\mathrm{safe}}\ s_{\mathrm{ok}} =$ ( ) 重路由 探测 延迟处理，以及 ( ) {预留、探测、延迟处理} （针对容量上限为B=10的容量池）；(ii) 签名拓扑清单 h_{man}，将带内 SQL（$O_1 \mapsto F_1$）、带外BMC/REST（$O_2 \mapsto F_2$）和etcd租约（$O_3 \mapsto F_3$）分别分配给三个互不相交的遥测故障域（k_a=3、f=2）；(iii) 霍恩规则$\mathcal{M}_{\mathrm{sys}}$，将经认证的观测映射到操作前提（act:提升、act:预留）和世界反驳（refute:s_{part}、refute:s_{ok}），以及冲突不变量 P_{sys}，标记{sql_down、sql_write_ok} $\vdash \bot$；以及 (iv) 可信时序策略TPol(提升) = 快照触发和TPol(预留) = 提交时敏感(pred:余量)。

2. 问题1 正向证据打包与问题2 可能世界屏蔽。假设主节点在快照 v_{snap}=50 处停止响应 SQL 查询。最初只有 $e_1 \in F_1$ （sql_hb_absent）到达。即使五个智能体分别提出 晋升 并引用e_1 下不同的上下文 ID，递归的物理足迹也会为所有 i 给出$\Phi_{\mathrm{phys}}(\Pi_i) = \{F_1, O_1, e_1\}$，将 $\hat{\nu}_{\mathrm{pack}} = 1 < 3$ 限制在上限以内。同时，s_{dead} 和 s_{part} 都在 $\widehat{\mathcal{B}}^{(2)}_{\tau,\ 50}$ 中存续，因为二者都没有 $f{+}1{=}3$ $A^{\mathcal{K}}_{\mathrm{safe}}\ s_{\mathrm{dead}}$ ∩互不相交 $A^{\mathcal{K}}_{\mathrm{safe}}\ s_{\mathrm{part}} = \{\quad,\quad\}$ 的反驳，而 ( ) ( ) 探测 延迟处理不包含任何变更。因此，kf-proxy阻止晋升，并向 F_2 （带外电源/REST）和 F_3 （etcd 租约）派发只读分区探测。当两个探测都确认领导者在同一个一致的快照 v_{snap}=50 和清单 h_{man}中已停机后，智能体为 $\{F_1, F_2, F_3\}$ 上的 act:晋升($\hat{\nu}_{\mathrm{pack}}$=3 ≥ 3)提交三个经过验证的霍恩有向无环图，并分别为 s_{part} 和s_{ok}提交三个互不相交的反驳，将 $\widehat{\mathcal{B}}^{(2)}_{\tau,\ 50}$ 降至 $\{s_{\mathrm{dead}}\}$，并允许晋升。

3. Q3 C 模式兼容性与 E2 级原子提交。在健康集群（s_{ok}）上，假设两个并发协调器 C_1，C_2 各自观察到准入修订版本 r_{adm}=1，并针对当前用量 3 和能力上限 B=10 （3+4+4=11 > 10)提出 +4 容量预留。在经证明的执行机制 R1（可串行化_原子的）下，kf-proxy 在 $\mathcal{V}_{\mathrm{compat}}$ 封闭域 $\mathcal{D}$上运行，验证所有子集和线性扩展（包括缺失/已取消的调度方案），使用（r_{adm}=1，τ_{auth}=5，TPol(预留)）封存证书，并将其调度至 E2 级事务边界。在单个 可串行化事务内，目标重新计算 HMAC 签名，锁定控制行（SELECT . . . FOR UPDATE），检查 $\tau_{\mathrm{auth}} \geq \tau^{\min}_{\mathrm{auth}}$，验证 $r^{\mathrm{cur}}_{\mathrm{adm}} = 1$，重新检查权威的 Pred:余量 行，检查 SUM $+ 4 \leq 10$，插入预留，并递增$r_{\mathrm{adm}} \leftarrow 2$。协调器 C_1 提交（3+4=7 ≤ 10），而 C_2在陈旧的 r_{adm} （或序列化冲突）情况下确定性地中止，并且必须根据 r_{adm}=2重新验证——此时新的 +4 尝试会因暴露上限而被拒绝，从而在每条物理轨迹中保持 SUM ≤ 10。

6 评估

我们使用 OpenKedge 仓库中research/pieq/发布的实现、基准测试、轨迹和测试运行器，对 PIEQ 进行端到端评估（https://github.com/openkedge/openkedge；精确的提交哈希和工件路径见附录 A）。我们的评估考察六个核心问题：物理域证据认证能否防止错误前置条件准入；可能世界屏蔽能否在有界故障遥测下防止不安全的状态变更操作；主动探测和有界确定性补全能否在不削弱健全性的情况下恢复可执行的补救措施；执行边界能否阻止过时、未经授权或冲突的提交；PIEQ 的保证能否适用于物理 PostgreSQL/Patroni 故障转移监控和真实 PostgreSQL 事务；以及在遥测可见性和执行门控保持不变时，加入语言模型智能体能否提升可靠性。

为避免将确定性软件检查与实时模型行为或物理集群试验混为一谈，我们严格按照六个层级分别报告证据，绝不将其汇总为单一的总体比率。这些层级包括第 2–5 节所建立的条件形式化保证；自动化持续集成回归测试和故障测试套件，其中包含 GitHub Actions 持续集成中的 249 个通过的 pytest 测试（包括 14 个由容器支持的 etcd 测试，以及新的 E1+级静默屏障测试）、持续集成中的 140 次三成员分布式 etcd 故障试验、200 次基线 POSIX/SQLite WAL 故障试验、80 次多进程操作系统级第 5 节并发与撤销故障试验，以及容器化 PostgreSQL 16 E2级并发协调器和执行中撤销竞态测试（附录 A）；使用确定性提议器运行的冻结软件基准测试，这些测试基于磁盘上的 E2 级 SQLite WAL，并结合我们新的综合与补全测试套件及可扩展性压力测试套件；对初始五模型试点进行的经审计的离线反事实重放；涵盖单次运行和重复研究的实时语言模型评估；以及与真实 PostgreSQL E2 层事务性强制执行配套的物理 PostgreSQL/Patroni 故障转移监控。在每个层级中，我们都分别报告假设内和假设外的结果，不提供固定确定性测试夹具上的独立同分布置信区间，并将本地验证器延迟与端到端恢复时间分开。为使经验数据表易于浏览，表 4–8 使用标准化结果列：缓解（可执行的安全缓解措施）、错误阻断（被不必要阻止的可执行事件）、强制延期（正确阻止的强制延期）、假设内不安全（假设内不变式违例）、错误前置条件（满足不变式安全性但在诊断上缺乏正当理由的状态变更操作）、UBSA（仅由执行门捕获的认知上已准入的执行延期案例），以及假设外不安全（在命题 5 信任边界之外准入的有意假设外对照）。本研究贯穿始终适用三项方法学边界：每个基准测试均由作者标注，而非由外部人员注释；早期命令行界面层级的实时运行使用未固定版本、在本地完成身份认证的快照，并采用不受控采样（第 6.6 节补充了一次受控采样的直接 API 三系列确认运行，该运行完整计入了 Bedrock 推理配置别名和本地 SGLang Qwen3-8B 的费用）；物理测试平台中的容器共享同一个虚拟机内核。

6.1 支持性工程机制

要将严格的确定性验证转化为适用于不可信语言模型的实用控制平面，就必须在不扩展可信计算基（TCB）的前提下，弥合语法、歧义和证明遗漏之间的摩擦。PIEQ 将其未改变的验证器与三种支持性工程机制结合起来。

首先，类型化证明提交接口公开了一个有限的验证器已知词汇表，涵盖许可操作、候选故障世界、编写规则 $\mathcal{M}_{\mathrm{sys}}$ 以及映射到原子命题的授权证据句柄。提议者会提交解耦的行动提案以及带类型的（规则_ID、证据_句柄）声明，而任何由提议者提供的可信计算基元数据，例如签名、故障域、位掩码、时期或清单哈希，都会以故障关闭方式被拒绝。可信计算基会确定性地解析句柄，并执行有界模式反馈重试（最多重试两次），且不会泄露跨智能体观察。

其次，只要可能世界屏蔽阻止立即执行，有界只读主动探测循环便会实现双重控制。候选探测会依据已验证的只读安全契约以及成本或负载上限进行故障关闭式筛选，并按以下标准排序：最坏情况下的可能世界缩减和领域新颖性（或校准后的样本信息期望价值），并围绕七个快照一致性边界进行跨轮次审计，以强制执行假设 1–3：被动遥测与探测之间的被控对象版本漂移；探测执行期间并发发生的目标提交；禁止将过时的观测句柄用于跨版本合取规则；采集器观测到的不一致快照绝不能被打包进同一个法定人数；探测重试返回不同的状态纪元；探测期间清单轮换或故障域不匹配；以及新观测到的冲突导致先前已验证的证明失效 P_{sys}（触发自动禁忌约束登记，并排除受到质疑的叶节点，同时遵循同域非膨胀性）。只要无法验证任一边界上的快照一致性，PIEQ 就会故障关闭：拒绝正向证书，并保留所有候选世界。

第三，一种选择加入的有界确定性补全辅助程序，被实现为默认关闭的 ∼70行内可信计算基前向链接例程，仅基于已经过认证的观测 $\mathcal{M}_{\mathrm{sys}}$ 并在故障关闭的资源上限下，补全验证器接受的推导。第6.6 节将同时衡量它所恢复的活性，以及它引入的明确的超出假设范围的风险权衡。

6.2 试点取证与反事实重放

在构建完整评估套件之前，我们先诊断了为何最初的 40 案例五模型试点（800 次调用）使补救工作陷入停滞。尽管该试点实现了 $0/40$ 次不安全授权（相比之下，$3/40$ 次处于辩论状态，$5/40$ 次来自原始遥测通道），但它仅实现了 $0/19$ 项可执行缓解措施（$19/19$ 次误阻断），并执行了 $0/549$ 次请求的探测。对所有 $140/284$ 个被拒绝的第0轮证明进行分类（详见配套补充材料）后发现，$95/140$（67.9%）是完全符合验证器要求的推导，却仅仅因为原型系统将证明接受与最终行动投票绑定在一起而被丢弃；只要谨慎型智能体投票选择探测或延迟处理，就会出现这种情况。其余拒绝原因包括 $33/140$（23.6%）的位掩码或前件映射错误，以及 $12/140$（8.6%）的模式错误。

在受控机制开关下重放这些冻结的第0轮试点回复（表3），揭示了两条方法论经验。将证明接受与行动投票解耦（R4-B），使有效证明数量从 $144/284$ 恢复到 $239/284$，并将缓解措施数量从 $0/19$ 提高到 $5/19$，同时保持 $0/40$ 次不安全准入；而移除正向打包（R4-D）则立即放行了两项未经认证的正向变异（案例72和74）。在R4-E中，全部43次探测都重新查询了测试夹具中已有的被动观测；试点智能体此前遗漏了有效的霍恩规则（$4/14$ 个案例仅遗漏反驳规则，$2/14$ 个案例仅遗漏正向规则，$8/14$ 个案例两者皆有遗漏）。由于该原型循环在没有在线模型参与的情况下，以确定性方式进行前向链式推导，并根据已实现的测试夹具观测构建探测菜单，因此间接泄露了已实现的支持集。审计第七个时间边界时，还发现案例1、39和71中重新探测的叶节点存在一个遗漏的冲突禁忌约束；修复该冲突检查后，系统执行了46次探测（30次有效），同时保持 $19/19$ 项缓解措施和 $0/40$ 次不安全准入。

严格依据公开事件类别架构构建探测菜单（R4-E-严格版，对未观测到的谓词返回缺失标记）消除了菜单泄漏，同时保留了$19/19$ 缓解措施和 $0/40$ 不安全准入，但使探测量 $2.5\times$ 从 43 增加到 108（有效探测为 28）。这证实了 R4-E较低的探测数量得益于菜单泄漏。

表3：针对已冻结试点第0轮回复的经审计的离线反事实重放（40个案例：19个可采取行动，21个延迟处理；TCB弱化为零）。

重放	缓解（19）	暂缓（21）	未解决问题（有效）	经审计的来源标签
R4-A （已归档）	0/19	21/21	0	0(0) 在线试点（严格耦合；144/284）
R4-B （解耦）	5/19	21/21	0	0（0） 离线回复重放（239/284）
R4-D （无位置包）	7/19	21/21	0	0(0) 离线回放 (2 不确定位置）
R4-E （基线）	19/19	21/21	0	43 (33)* 夹具支持的 + 可信计算基规则符合性
R4-E-严格版	19/19	21/21	0	108(28) 无泄漏公共模式菜单

*修复P_sys 不良检查后：46 (30) 个探测（案例 1、39、71）；结果相同，19/19，0 个不安全项。

6.3 留出软件基准测试、消融实验与确认

在冻结实现哈希后，我们编写了一个相互独立的 36 案例留出基准测试（H01–H36），与原先四个新基础设施域中的 40 个试点案例完全不重叠：bgp_route_leak、storage_quorum_fence、k8s_control_plane_drain，以及 tls_ca_rotation。该套件涵盖九种故障原型，每种包含四个案例（被动可恢复、可通过探测恢复、不可消解的不确定性、相关或误分类遥测、有有效证据但不合理的变更、执行授权不足、并发或过期证书、具有探测期间漂移的瞬态前置条件，以及可信模型缺陷对照），并为每个事件配备无泄漏的域级探针目录和封存式真实标签，分为四类：9 个可执行的安全缓解措施、5 个安全但在诊断上不合理的状态变更操作、17 个强制延期，以及 5 个假设外阴性对照（H16、H33–H36）。本小节中的所有软件运行均采用与磁盘上的 E2 级 SQLite WAL 配对的确定性提议器（PRAGMA synchronous=FULL），且未进行任何重新调优。

评估我们最初冻结的实现（添加跨轮次探针快照审计之前）揭示了三个明显的行为边界。首先，在 H31（探测过程中被控对象版本从 $v = 50$ 跳至 $v = 51$）上，初始代码提交了$1/31$假设内不安全不变量违例，因为探测未审计跨轮次快照一致性；启用七边界时序审计且不作任何重新调优后，H31 转为快照不一致延期处理，实现了 $0/31$ 假设内不安全准入、 $9/9$ 项缓解措施（其中 4 项通过无泄漏探测 H05–H08 实现，1 项通过历史快照 CA 吊销 H32 实现），以及 $17/17$ 项强制延期处理。其次，在 H30 上（调用方自行决定重新验证期间，瞬时 I/O 峰值在提交前消退），PIEQ 阻止了全部 $4/4$ 被动虚假前置条件案例（H17–H20），但仍提交了一项过期前置条件变更，且没有不变量违例；这直接促使我们采用强制时间策略注册表，并在第 6.5 节进行实时评估。第三，在全部 $5/5$ 假设范围外对照中（H16 位于 E_3，H33 位于 E_1，H34 位于E_2，H35 位于 E_5，H36 位于 E_6），PIEQ 按照模型所示，在命题 5 的可信边界之外准入了不安全变更。

由于 PIEQ 的故障阈值计算的是物理故障域，而非智能体数量，我们随后开展了一项因果公平的智能体数量隔离研究：在保持验证器、词汇表、探测预算和 E2级 SQLite WAL 不变的同时，改变智能体数量和遥测可见性（表 4，上部）。这揭示了此前的共享上下文混杂因素：1A_本地遥测 （$0/9$ 在heldout36上被动，$0/19$ 在 40 个案例套件上）此前仅获得了五分之一的遥测信息；即使拥有完整遥测句柄，1A_完整遥测_共享上下文仍停留在 $0/9$ 被动状态，因为将单个提议器上下文 ID 折叠进证明打包后， $\nu_{\text{pack}} \leq 1$能力受到上限限制。将ν_{pack} 仅定义在物理足迹之上 Φ_{phys} （公式（3））消除了这一伪影。在完整遥测和基于物理足迹的打包条件下，1A_完整遥测_域隔离与五智能体 5A_PartTel 和 5A_完整遥测在 heldout36（$5/9$ 被动、 $9/9$ 带探测、$0/31$不安全、 $17/17$ 延迟处理）和 frozen40（$19/19$ 缓解措施、$0/40$ 不安全）上的安全性与活性均完全一致，同时发出的提议器调用次数更少（36 次，而非 216 次；40 次，而非 240 次）。相比之下，在获得相同遥测和 E2 级隔离的匹配无屏蔽单智能体与五取三辩论基线中，两者均出现了 $6/31$不安全不变式违例和 $5/5$ 错误前置条件准入。第 6.5 节将检验随机实时语言模型在重复采样下是否会偏离这种确定性等价。

为在相同遥测和 E2级 SQLite WAL 条件下隔离各认知机制的因果作用，表4（底部；完整的 17 行矩阵见配套补充材料）总结了受控的机制隔离析因设计。仅禁用正向打包并未改变不变式违例数量（仍为 $0/31$ ），但由于放行了全部四个被动陷阱（H17–H20），错误前置条件准入从 1 次升至 $5/5$ 次，这证实了物理域正向认证决定前置条件可靠性。禁用容错反驳打包（$f = 0$）后，单个故障域即可排除真实世界，使 heldout36 上的被动缓解措施从 $5/9$项骤降至 $1/9$ 项，并导致frozen40上出现 $6/40$ 次不安全准入（$0/19$项缓解措施）；两种打包方式均禁用时，heldout36上出现 $4/31$次不安全准入和 $5/5$ 次错误前置条件准入。移除可能世界屏蔽（NO_SHIELD）后，系统放行了H09 Helly 重叠陷阱（heldout36上有$1/31$ 次不安全准入；frozen40上有$7/40$ 次），证实了全局安全动作交集不可或缺。在活性方面，类型化解耦使被动缓解措施从 $0/9$ 项增至 $5/9$ 项（frozen40上为$0/19 \to 14/19$ 项）；再加入主动探测和七边界时序审计后，缓解措施进一步从 $5/9$ 项增至 $9/9$ 项（frozen40上为$14/19 \to 19/19$ 项），且假设范围内的不安全准入为零。

由于H31 促使我们加入七边界时间审计，重新评估 heldout36 仅用于回归验证，而非新的样本外测试。因此，在冻结更新后的实现哈希后，我们在一个新的第五个领域中编写了一组彼此独立的 12 个案例软件确认集（dns_anycast_集群），用于测试跨轮次快照漂移、混合快照、探测中途提交、清单轮换、同域句柄、延迟出现的探测派生禁忌项、过期重试、并发账本 CAS 竞争、两个可执行控制项以及两项时序策略检查。首次执行实现了 $9/9$ 次强制延期、$3/3$ 项缓解措施，且不安全准入为 0、误阻断为 0。

6.4 验证漏斗、延迟与证据归因

跟踪提案在验证流程中的处理过程，可以明确确定性检查在何处筛除格式错误的提交，以及相较于外部输入/输出和推理，可信计算基增加的延迟有多小。在 heldout36 的 5A_PartTel条件下，共有 216 项提案（其中 180 项为首次尝试，36 项为重试，且重试耗尽次数为零），首次尝试有效性为$144/180$ （80.0%）。首次尝试的推导数量从提交时的 277 项，经过筛选后变为 241 项（87.0%）符合模式，以及 205 项（74.0%）同时满足 Horn 和来源有效性，重试后达到 $205/205$已接受证书。达到法定人数 k_a 的案例从探测前的 21 项增加到探测后的 25 项，其中 4 项通过探测获准，12 项因证据不足或快照漂移而被拒绝，另有 21 项延迟处理。在 1A_FullTel_DomainIsolated条件下，所有 $36/36$

表 4：冻结的36例留出基准（H01–H36：31例假设内 [9 可采取行动，17例强制延后，5例错误-前置条件] + 5 假设范围外对照；确定性软件提议方，E2级 SQLite WAL 同步=FULL）。上部：因果公平的智能体数量隔离。下部：2^4 机制隔离析因设计的关键单元（T=类型化、P=PosPack、R=RefutePack、B=探测；完整的17行矩阵见配套补充材料）。

配置（留出36例：31例假设内 + 5 OOA）	缓解（9）	错误阻断	强制延后（17）	不确定性内	错误前提 (5)	假设外不确定性 (5)	探测（有效）	调用次数
智能体数量隔离（无泄漏探测，*E2*级 *SQLite WAL*；显示5A_PartTel的初始冻结基线）								
5A_PartTel （初始冻结基线）	9/9	0	16/17	1[a]	1[b]	5/5	17（7）	216
1A_本地tel +防护层（1/5 遥测）	8/9	1	17/17	0	0	0/5	31（16）	36
1A_完整tel_共享上下文（共享上下文容量）	8/9	1	17/17	0	0	0/5	27 (12)	36
1A_FullTel_域隔离 （公平 1A）	9/9	0	17/17	0	1[b]	5/5	17 (6)	36
5A_PartTel （完整 PIEQ，时间审计）	9/9	0	17/17	0	1[b]	5/5	17 (6)	216
5A_完整遥测（5 个智能体，完整遥测）	9/9	0	17/17	0	1[b]	5/5	17 (6)	216
1A_完整遥测_未防护（+匹配 E2）	9/9	0	11/17	6	5	5/5	0 (0)	36
5A_FullTel_辩论 (3/5 多数 +匹配 E2)	9/9	0	11/17	6	5	5/5	0 (0)	180
机制隔离析因设计（5A_PartTel、时间审计、匹配层级 *E2 SQLite* 预写日志）								
严格动作耦合（T0_P1_R1_B0）	0/9	9	17/17	0	0	0/5	0（0）	180
类型化，无探针（T1_P1_R1_B0）	5/9	4	17/17	0	1[b]	5/5	0（0）	216
丢弃正向打包（T1_P0_R1_B0）	5/9	4	17/17	0	5[c]	5/5	0（0）	216
丢弃反驳打包，$f=0$（T1_P1_R0_B0）	1/9	8	17/17	0[d]	1[b]	5/5	0（0）	216
丢弃两个打包（T1_P0_R0_B0）	5/9	4	13/17	4	5	5/5	0 (0)	216
无合理世界屏蔽（T1_P1_NO_SHIELD_B0）	5/9	4	16/17	1[e]	1[b]	5/5	0 (0)	216
完整 PIEQ +探测（T1_P1_R1_B1）	**9/9**	**0**	**17/17**	**0**	1[b]	5/5	17 (6)	216

[a]H31 在七边界时序审计（$v=50/51$）之前捕获跨快照错误。 [b]H30 调用方裁量模式下未重新验证的瞬态降级（0/4被动错误前置条件H17–H20）；已被强制注册表阻止（第 6.5 节）。[c]允许全部 4/4 个被动错误前置条件（H17–H20） + H30。[d]在 frozen40 上，T1_P1_R0_B0 导致 6/40 个不安全案例（0/19 缓解）。[e]允许H09 Helly陷阱（7/40 在 frozen40 上不安全）。OOA = 假设范围外对照（H16、H33–H36）。

提案和 204/204 推导均在第 1 次尝试中通过，且没有重试。

计时测量（Apple M系列、Python 3.13.9、预初始化 SQLite WAL，PRAGMA synchronous=FULL；详细分解见配套补充材料）表明，本地TCB验证比语言模型推理和物理故障转移快四到五个数量级。在本地TCB内，类型化构建与验证耗时 0.088 ms（第 50 百分位；第 95 百分位为 0.189 ms），重试验证耗时 0.002 ms（0.013 ms），ATMS打包与屏蔽耗时 0.031 ms（0.059 ms），探测循环时序审计耗时 0.185 ms（0.304 ms），E2级 SQLite WAL提交耗时 0.101 ms（0.118 ms；原子拒绝耗时 0.097 ms）；在九个可采取行动的留出案例中，从本地TCB到授权行动的总耗时为 0.531 ms（第 50 百分位；第 95 百分位为 0.576 ms）。相比之下，模拟带外探针往返增加 20.0 ms （第 50 百分位；第 95 百分位为 38.0 ms ）；真实的三成员 etcd 3.7.3 Raft共识，在 140 次 CI故障试验中，各调度的中位耗时为 45–2,467 ms（附录 A）；在线试点的大语言模型推理每次调用耗时 15.72 s（第 50 百分位；第 95 百分位为 40.75 s），每起事件的并行第0轮墙钟时间为 24.25 s（第 50 百分位；第 95 百分位为 97.61 s；顺序执行为 82.74 s；输入 19.78M 个词元、输出 607k 个词元，报告成本为 $5.13）。物理 PostgreSQL故障转移（第 6.8 节）中，原生自动故障转移耗时 9.9–10.2 s，而暂停的实时大语言模型监督式晋升耗时 57–67 s；这反映的是不同的可用性策略，而非可直接比较的延迟目标。表5概述了 PIEQ 的各项贡献如何对应其形式化依据、实证证据及尚存差距。

表5：贡献与证据的归属映射，将形式化保证与经验性软件、实时大语言模型及物理证据区分开来，并明确列出尚待解决的问题。

贡献	形式化依据	经验支持与未解决的问题
1. 认知来源证书。	定理 1，定理 2	阶乘P0 与 P1：切断被动错误前置条件 4/4→0/4 (heldout36)；H13–H15 已阻止； $M\to64$打包压力测试与综合与补全（第6.7节）；H16 （E_3）显示 h_{man} 边界。
2. 可能世界门控	引理 3	R0/NO_防护层：切断不安全的 6→0（frozen40）， 4→0（heldout36）；$\lvert\mathcal{S}_{\mathrm{cand}}\rvert\to256$ 防护压力测试（2.23 毫秒）；H33 （E_1）显示世界完备性边界。
3. 执行约束治理	定理4，推论 1，命题5	H21–H29 已阻止；249 个持续集成测试 + 200 POSIX/SQLite + 80第5节多进程。竞态 + 140 etcd 试验 + 持续集成etcd 静默状态与 PG-16 竞态测试套件通过；PG/Patroni 故障转移已门控于E0+级原生和真实PG的E2级对有界预留强制执行（第6.8节）。范围：Patroni提升仍为E0+级原生；多主机集群故障开放。
支持：类型化，探测、补全	假设 1–3 (7边界审计)	提升软件缓解措施。0/9→5/9→9/9；实时命令行界面运行（9/9 留出测试， 20× 可靠性， 5× 智能体数量） + 直接 API 3 系列确认12 (4/4 缓解， 0/11 不安全，$0.14 补全成本）； 16/16 目标导向与 1/16 l跳补全的对比。范围：使用 Bedrock 云端点配置文件别名；补全暴露 E_2 缺陷（CN11）。

6.5 实时大语言模型留出评估与智能体数量扩展

为测试 PIEQ 在随机推理而非确定性提议器下的表现，我们在全部 36 个留出事件上评估了实时语言模型推理：不进行重放、不访问预言机、不使用确定性补全，且重试预算最多为两次。五智能体异构集成将三个 Claude 模型（claude-sonnet-5-5、claude-haiku-5-5、claude-opus-5-5）与两个 GPT 实例（openai.gpt-5.6-sol）配对，而单智能体和同构运行则使用 Claude Sonnet。本地经过身份验证的

智能体运行器在整个过程中均被使用；GPT 的令牌计费未被捕获（报告中的美元成本仅涵盖 Claude 的使用费用），此外，运行器框架开销使每次调用额外增加约 18–21k 个输入令牌。表 6 和7 报告了八种配置（配置 A–E0、E1、S1 和 H1）下单次运行的安全性、活性和运营指标。

比较配置 A 至 E1 可隔离出四种实时影响。主动探测在不削弱安全性的前提下恢复了实时修复：自由形式配置（A）和仅类型化配置（B）各自重新解决了 4/9 个可采取行动的事件，但出现了 5 次误阻断（主要是可通过探测恢复的案例 H04–H08）；而加入有界泄漏

表6：对全部36个冻结留出事件进行实时大语言模型评估（31 假设内 [9 可采取行动，17 强制延后，5错误前提] + 5 假设范围外对照）。底部三行启用了强制时间策略注册表；E0采用调用方自主裁量验证。运营指标见表7。

配置	缓解（9）	错误阻断	不确定性内（31）	强制延后（17）	错误前提（5）	UBSA	假设外不确定性（5）
A：自由形式（无执行门控）	4/9	5	0/31	13/17	1/5	4	2/5
B：类型化（无执行门控）	4/9	5	0/31	9/17	1/5	8	4/5
C：类型化 + 探测（无执行门控）	9/9	0	0/31	9/17	1/5	8	4/5
D：1 模型全电信（无执行门控）	9/9	0	0/31	12/17	0/5	5	3/5
E0：完整 PIEQ，由调用方自行决定	9/9	0	0/31	17/17	1/5（H30 已提交）	0	2/5
E1：完整 PIEQ，强制注册表	9/9	0	0/31	17/17	0/5（H30 已阻止）	0	3/5
S1：一个 Sonnet、完整 tel、完整门控	9/9	0	0/31	17/17	0/5	0	3/5
H1：五个同质 Sonnet	9/9	0	0/31	17/17	0/5	0	4/5

表7：全部36起留出事件的实时大语言模型运营指标（每种配置单次运行；多次重复运行结果见表 8）。有效提案 = 回复包含 ≥ 1 验证器接受的推导，首次尝试→重试后（由于分区智能体可能缺乏足够证据，因此无法在不同遥测划分之间进行比较）。报告成本仅涵盖 Claude 的使用费用（GPT 使用不计费）；运行器框架开销每次调用另增加 ≈182.1 万至 2.1 万输入令牌。

配置	有效提案	探测（有效）	大语言模型调用	令牌（输入/输出）	单例延迟中位数	报告成本
A：自由形式	62→62/180	0	180	3.9M / 71k	43.2 s	$2.80
B：类型化	73→74/180	0	182	3.9M / 76k	38.7 秒	$2.68
C：类型化 + 探测	69→74/180	17 (6)	189	4.1M / 85k	46.3 秒	$2.85
D：1 模型全电信	30→33/36	19（8）	39	0.9M / 18k	6.4 秒	$1.00
E0：调用方自主决定的完整 PIEQ	73→74/180	17（6）	181	3.9M / 76k	44.4 秒	$2.81
E1：强制注册表	73→74/180	18（7）	183	3.9M / 77k	52.9 秒	$2.77
S1：单个 Sonnet 全门控	30→33/36	19（8）	39	0.9M / 18k	6.3 秒	$1.00
H1：五个 Sonnet*	68→72/180	17 (6)	188	4.2M / 62k	30.2 秒	$4.58

*包含 1 次瞬时凭证导出失败　　重试后恢复；所有其他运行在重试后均无提供商故障　　。

式自由探测（C）后，实时模型处理了 9/9 项缓解措施，误阻断降至 0，同时将假设内的不安全准入维持在 0/31。执行绑定同样不可或缺：在没有执行门控时（A–D），实时模型在授权、过期证书和并发案例中进行了 4–8 次缺乏依据的状态变更操作（H21–H29</style）；而完整 PIEQ 的 E2 层边界阻止了所有此类操作（ 次强制延期，0 次 UBSA）。启用强制可信时间策略注册表后，剩余的瞬时前置条件缺口也得到弥合：在调用方自主裁量验证下（E0），瞬时案例 H30 仍然提交成功（1/5 次错误前提；配置 D 在探测后延迟处理，因此偶然避免了这一问题）；而启用强制注册表（E1）后，H30 转为阻止（0/5）。轨迹检查确认，实时模型提出了该变更，通过了打包和安全屏蔽，并在 E2 层事务原子地拒绝该变更之前收到了签名的提交时策略；拒绝原因是提交时可信谓词为假。与此同时，包括历史案例H32 在内的快照触发操作仍可采取行动，且没有新增误阻断。在配置 A–E0 中（771 次调用，报告成本为 $12.13），重试为每种配置挽回了 1–5 项有效提案，重试后提供商故障为 0；按设计，假设范围外对照在 5 个案例中有 2–4 个准入了不安全变更，而在线代理对其余案例进行了延迟处理。

在单次运行中保持完整强化门不变时，配备完整遥测的一个 Sonnet（S1）在全部 31 个假设范围内案例和全部 5 个错误前置条件对照中，表现与五代理异构集成（E1）及五个同构 Sonnet（H1）均相当（假设范围内零分歧；在假设外H33/H35出现两次方向相反的分歧），同时消耗的资源少得多（调用次数为 39 次，而对比组为 183–188 次；成本为 $1.00，而对比组为 $2.77–$4.58；每次执行的第 50 百分位耗时为 6.3 秒，而对比组为 30.2–52.9 秒起事件）。为检验这种单次运行等价性在随机重复下是否依然成立，我们预注册了一项五次重复的配对比较，比较 S1、H1 和 E1，并在每次重复中随机排列条件顺序（2,030 次调用，报告成本为 $41.28 ）。这 540 次案例执行分为 465 次假设范围内执行（每种条件 155 次）和 75 次假设外执行（每种条件 25 次；表 8）。

与定理2 和引理3一致，在假设内安全性方面，五次重复实验中智能体数量均不影响不变量：PIEQ 记录了 0/465 次不安全准入（0/155 每种条件），0/75 次错误前置条件提交（每次 0/25 ），以及 255/255 次强制延期（每次 85/85 ）。在五个有意设置的可信模型缺陷对照（H16、H33–H36）中，PIEQ 记录了 47/75 次假设外不安全准入（11/25 S1、 20/25 H1、 16/25E1），而模型克制使另外 28/75 次延期处理（包括H34，延期 15/15 次），体现了设计好的、位于 PIEQ 可信边界之外的假设违反。就活性而言，单次执行等价性未能在重复实验中完全保持：S1 在 2/5 次重复中错误阻断了历史 CA 撤销案例H32 （43/45 项缓解措施；Wilson 95% $[0.85, 0.99]$，按 9 起事件聚类），而两个五智能体条件均达到 45/45 $[0.92, 1.00]$，且不存在 H1 与 E1 之间的假设内不一致，延迟为 4–6×（第 50 百分位为 26.4–43.0 秒，而另一组为 6.8 秒），报告成本为 2.7–4.3×（13.81–22.27 美元，而另一组为 5.20 美元）。由于这一差异集中于 $n = 5$ 次重复中的单一事件（2/45 个不一致配对），它反映的是有界的单次活性冗余，而非多智能体优越性的统计证明；模型异质性并未带来假设内收益，而确定性补全（下文考察）针对的正是同一种证明遗漏模式，且不会增加推理成本。

6.6 实时可靠性与有界确定性补全

冻结流水线哈希后，我们编制了一组预注册的 12 个案例实时确认集（CN01–CN12），涵盖两个此前未见过的域（cdn_tls_edge和mq_broker_cluster），包括 4 项可执行缓解措施、6 次强制延期、1 个提交时错误前置条件对照（CN09），以及 1 个假设外不健全规则对照（CN11）。在初始冻结运行中，所有安全性标准均通过（0 次不安全准入，CN09 被阻止，$6/6$ 次延期处理），但活性标准未通过（$2/4$ 项可采取行动），因为模型提交了两个正向证明，却遗漏了每个世界所需的两个反驳中的一个（探索性重跑达到 $4/4$）。

为精确测量这种单次运行方差，我们对这组12个案例进行了 20 次未经修改的实时重复运行（240次执行： 220次假设内执行，加上 20 次假设外 CN11；共 248 次调用，报告成本为 $5.47，提供商故障为零；见表 8）。每次执行均满足假设内安全性： $0/220$ 次不安全准入，CN09 上的 $0/20$ 次错误前置条件提交（认证后有11次在E2级被原子拒绝，另有9次因认识论歧义而更早延迟处理），$120/120$次强制延期，以及在基线模型的克制倾向下CN11 上的 $0/20$次准入。可操作活性呈现明显的两极分化：CN01 和CN02 实现了$20/20$ 项缓解措施（Wilson 95% 置信区间为 $[0.84, 1.00]$），而CN10 达到 $11/20[0.34, 0.74]$ （9次误阻断：缺少5项反驳和4项肯定项），CN12 达到 $9/20$ $[0.26, 0.66]$ （11次误阻断，均因缺少反驳），总计 $60/80$ 项缓解措施和20次误阻断。所有误阻断都源于省略了验证器可接受的推导；无效 Horn、来源或探测预算故障均为零。由于提交在语法上有效，模式驱动重试无法解决此问题。因此，故障关闭式验证会将模型提交不足转化为可恢复的误阻断，而非不安全的状态变更操作。</output>

随后，我们通过针对全部 20 次基线运行的逐案例配对重放，评估了有界确定性补全辅助程序（经 13 项对抗性单元测试验证，涵盖共享域、共享叶节点、禁忌项、截断和缺失传感器；在无探测内补全和有探测内补全两种情况下分别进行 240 次重放，共 480 次；见表 8）。在两种模式下，补全均恢复了全部 20 个可采取行动的误阻断：CN10 从 $11/20$ 提升至 $20/20$ （$+9$ 次恢复，提供了 20 个推导），而CN12 从 $9/20$ 提升至 $20/20$ （$+11$ 次恢复，提供了 22 个推导），使缓解措施从 $60/80$ 提升至 $80/80$。在假设内，补全产生了 $0/220$ 次不安全准入、$0/20$ 次错误前提提交（CN09 仍被阻止 $20/20$，其中 $9/20$ 从认知延迟转为原子的 E2级拒绝）、 $120/120$ 次未改变的强制延期，并且没有真实世界反驳。一个实时的类型级缺失证明反馈环（$n = 3$ 次运行、46 次调用，$0.43）重现了这些收益（$12/12$ 项缓解措施，零假设内回归）。

该实验还揭示了一个重要的负面发现。由于确定性补全会系统地推导出每个规则有效的结论，它将假设外不健全的规则控制（CN11，层 E_2）从基于基线模型犹豫而延迟处理 $20/20$ 转变为在补全下允许-不安全 $20/20$ （以及在 $3/3$ 实时反馈下）转变为允许-不安全。补全消除了语言模型克制针对受信规则缺陷所提供的偶然保护（PIEQ 定理从未依赖这种保护），并将健全性完全置于编写的域模型之中（命题 5，层 E_2）。因此，我们默认禁用补全，将其明确视为操作员在单次活性与暴露于规则编写缺陷之间的权衡，而不是无条件的安全性提升。

直接 API 控制采样的三模型家族确认运行。为弥补同一套冻结的 12 个案例确认测试套件（CN01–CN12）中的非受控采样、CLI 测试框架臃肿和计费不完整问题，我们执行了一次直接 HTTPS 五智能体运行（完整_PIEQ，配备强制时间策略注册表，不进行确定性补全，温度=0.0，top_p=1.0，随机种子=17），涵盖三个独立模型家族：两个 AWS Bedrock Anthropic 模型（claude-sonnet-5-5、claude-haiku-5-5）、两个 AWS Bedrock OpenAI 模型（us.openai.gpt-5.6-sol）和一个本地 SGLang 开放权重模型（Qwen/Qwen3-8B；表 8）。每次 API 调用均在第 1 次尝试时成功，重试次数和格式错误输出均为零（$60/60$个有效提案， $173/173$ 个已接受推导，9 次探测中有 [3 次有效], 每起事件的第 50 百分位为 19.2 秒）。移除 CLI 包装器后，令牌用量降低了一个数量级以上，降至 45.1k 个输入令牌 / 17.6k 个输出令牌（每次调用 ≈ 751 个输入令牌）；多提供商总成本为 0.139 美元（Bedrock Anthropic 为 0.0765 美元，Bedrock OpenAI 为 0.0625 美元，本地 SGLang 为 0.00 美元）。在假设范围内，PIEQ 实现了 $11/11$ 精确结果： $4/4$ 项可采取行动的缓解措施（误阻断为 0，包括 CN02 通过 2 次有效探测解决），$6/6$次强制延期， $0/1$ 次错误前置条件提交（CN09 在 E2级通过 REJECTED_COMMIT_PRECONDITION_FALSE 原子性拒绝），以及 $0/11$ 次不安全准入。对于不健全规则控制项（CN11），逐智能体轨迹直接印证了我们的 EXP-06 发现，即使不进行确定性补全也是如此：两名 Claude 智能体仍因模型克制而遗漏了不健全规则，而两名 Bedrock GPT 智能体和本地 Qwen/Qwen3-8B 则忠实应用了受信规则，导致 $1/1$ 假设外接纳。这在经验上表明，对 E_2 缺陷保持克制只是特定模型的偶然表现，而非架构保证。为严格披露模型身份，尽管 Qwen/Qwen3-8B 是固定的本地开放权重检查点，且全部 60 次调用均返回了服务器报告的模型 ID，AWS Bedrock 端点使用的是跨区域美国推理配置别名，而非带日期标记的不可变快照。

6.7 综合与验证的不对称性、编写开销及在线可扩展性压力测试

为实证检验第 2.3节提出的架构权衡，并量化负载下 PIEQ 的在线资源上限，我们执行了两套专门的软件压力测试套件（scripts/run_rev12_synthesis_vs_completion.py 和 scripts/run_rev12_scalability_stress.py；表9）。

TCB 模型编写开销。审计涵盖全部十个域的 100 起基准事件（frozen40：3 个域；heldout36：4 个域；软件_confirm12：dns_anycast_集群；实时_confirm12：cdn_tls_边缘、mq_代理_集群）表明，逐域 TCB 规范十分简洁： $|\mathcal{S}_{\text{cand}}| = 2$–3 个故障世界， $|\mathcal{M}_{\text{sys}}| = 1$–41 条霍恩规则（核心单次执行域中为 1–15 条，在探测增强的留出测试套件中最多为 41 条），$|P_{\text{sys}}| = 0$–2 个冲突不变量，以及 $M = 1$–每起事件 9 项原始观测，远低于 $M \leq 64$ 位掩码上限。

多跳证明搜索 vs. 有界 TCB 补全。在 4 个域中保持 M=33 经认证的观测 (k_a=3， f=2) 不变，我们扫描了背景干扰规则$R_{\text{bg}} \in \{0, 20, 80, 250\}$和推导跳数深度 $d \in \{1, 2, 3, 4\}$（16 种配置；表9，上）。现有的单跳 TCB 补全辅助程序（pieq/completion.py，能力为 128）仅允许 $1/16$种配置（R_{bg}=0， d=1，与 CN10/CN12一致），阻止了每个

表 8：在冻结的 12 案例确认集（20× 可靠性 + 成对完成重放 + 1× 直接 API 三族运行）和冻结的 36 案例留出测试套件（5× 成对智能体数量重复）上进行的重复命令行界面在线评估和直接 API 受控抽样确认。假设内和假设外（OOA）的分母始终分别报告；同一事件的重复运行按案例聚类，而非视为独立同分布场景样本。

研究 / 条件	缓解	错误阻断	强制定义错误呈现		不确定性内	假设外不确定性	运行情况 / 注释
冻结的 *12* 案例确认集： 20× 命令行界面运行（220 在 + 20 *OOA* 内）及 1× 直接 *API* 三族运行（11 在 + 1 *OOA* 内）							
基线在线 Sonnet（命令行界面， 20×）	60/80	20[a]	120/120	0/20	0/220	0/20	248 次调用，$5.47；CN10 11/20，CN12 9/20
确定性补全（配对）	80/80	0	120/120	0/20[b]	0/220	20/20[c]	恢复全部 20 项反馈（+9 CN10， +11 CN12；42 个派生项）
类型级反馈（命令行界面， n=3）	12/12	0	18/18	0/3	0/33	3/3[c]	46 次调用（每个案例 1–2 次），0.43 美元；与补全相符
直接 API 3 系列（温度=0, 1×）	**4/4**	**0**	**6/6**	**0/1**[b]	**0/11**	1/1[f]	60/60 有效，45.1k/17.6k 令牌，**0.14 美元**（全部 3 家提供商），第 50 百分位 19.2 秒
冻结的 *36* 案例留出测试套件 ×5配对重复次数（540 次执行 = 465，其中 *135* 执行，255 次延迟处理，75 次错误前提 *I* + 75 *OOA*）							
S1（1×Sonnet，完整 tel，完整门控）	43/45	2[d]	85/85	0/25	0/155	11/25	199 次调用，$5.20，6.8 秒，每个案例的第 50 百分位
H1（5× Sonnet，部分 tel，完整门控）	45/45	0	85/85	0/25	0/155	20/25	920 次调用，$22.27，26.4 秒每个案例的第 50 百分位
E1（5×异构、部分 tel、完全门控）	45/45	0	85/85	0/25	0/155	16/25	911 呼叫，$13.81+GPT，43.0 秒/案例的第 50 百分位
配对总计（重复 5 次）	133/135	2	255/255	0/75	0/465	47/75[e]	2，030 次调用，$41.28+GPT；0 次 H1 与 E1 在文内判别。

[a]9 在 CN10 + 11 上，在 CN12 上。[b]CN09 在 E2级原子地被阻止（已拒绝_提交_前置条件_为假；9/20 在补全过程中被延后处理）。CCN11 （E_2 不健全规则）在补全消除基线犹豫后，将 0/20→20/20 翻转。[d]在H32上均为误阻断。[e]OOA 控制项：H16 （E_3）、H33 （E_1）、H34 （E_2；15/15 延后处理）、H35 （E_5）、H36 （E_6）。[f]在CN11上，Bedrock Anthropic 智能体有所犹豫，而 Bedrock GPT 和 SGLang Qwen/Qwen3-8B 应用了不健全的受信规则（补全次数为零）。

多跳链 ($d \geq 2$)，并在 $R_{\mathrm{bg}} \geq 20$后截断。将 TCB 补全推广为有界多跳广度优先搜索后，在能力为 128 时允许$4/16$ 种配置，在能力为 512 时允许 $8/16$ 种配置（2.38–2.89 毫秒），但一旦 $R_{\mathrm{bg}} \geq 80$，在 $0/8$ 种配置中均故障关闭截断（3.46–3.62 毫秒），因为干扰规则耗尽了推导预算。相比之下，一个不受信任的、目标导向的确定性软件提议器仅向添加_经验证的_推导相关的多跳有向无环图，便实现了 $16/16$ 次准入，p50 延迟为 0.07–0.28 毫秒，TCB 扩展为零，且不安全准入为 0；同时， $4/4$ 对抗性幻觉控制（伪造的未经认证的日志声明、幻觉规则 ID、同域多上下文欺骗以及跳步前件不匹配）均被确定性地拒绝。由于这项 16 种配置的扫描使用的是确定性软件提议器，而非实时语言模型推理，因此它隔离了有界 TCB 前向链推理与定向有向无环图验证之间的计算不对称性；在数百条干扰规则中测量实时大语言模型的证明搜索召回率（覆盖深层多跳链）仍是有待开展的实证工作。

在线可扩展性与故障关闭截断边界。表9（底部）描述了四个资源轴上的延迟和故障关闭截断：（1）ATMS 与完整证明打包（$M \rightarrow 64$）：ATMS 注册在不超过 M=64, d=6 时，p50 保持在 0.057–1.405 ms；单叶打包在 M=64 时仍保持精确，耗时 0.372 ms。在针对 18 个共享域（M=64, k_a=3, B_{pack}=10,000）的对抗性稠密相交 3 叶超图中， $|\mathcal{W}|$=32 在 1.43 ms 内完成精确计算（误阻断率为 0%），而 $|\mathcal{W}| \in \{64, 128, 256\}$ 耗尽分支定界资源（13.4–47.4 ms，截断率为 100%）；在所有可采取行动和陷阱实例中，均未出现不安全准入。关键在于，问题1的可靠下界 $\hat{}\nu_{\mathrm{pack}} \geq k_a$ 仍能认证有效的不相交打包（问题1误阻断率为 0%）；而问题2的严格保守打包_截断防护仍保留世界（问题2误阻断率为 100%），这表明见证去重或下界反驳剪枝是处理稠密相交反驳集的关键手段。（2）ATMS 标签和命中集上限：$L_{\max}$=64 在 80 个最小环境时会明确标记预算_超限；B_{HS}=256 可精确处理最多 6 个不相交的 2 叶禁集（64 个命中集，耗时 0.166 ms），并在≥ 8 个独立冲突时明确故障关闭（耗时 0.625 ms）。（3）可能世界屏蔽与模式 C：屏蔽延迟随规模线性增长，从 0.030 ms（$|\mathcal{S}_{\mathrm{cand}}|$=4）增至 2.232 ms（$|\mathcal{S}_{\mathrm{cand}}|$=256, M=64, f=2）。对于无序的 $|\mathcal{U}_C|$=1..4，模式 C R1 检查在 0.012–0.556 ms（$|\mathcal{S}_{\mathrm{base}}|$=1）内处理 4、15、64、325 个调度方案，在 0.027–3.095 ms（$|\mathcal{S}_{\mathrm{base}}|$=16; DAG排序将 $|\mathcal{U}_C|$=4 缩减至 95 个调度方案（耗时 0.206–0.806 ms），并在 $|\mathcal{U}_C|$=5 时于 0.001 ms 内故障关闭；R2 制度检查针对 $|\mathcal{P}|$=2, 4，6 处理 2、18、270 个调度方案，耗时分别为 0.008、0.044、0.539 ms，会在派发前拒绝写偏斜，并在 $|\mathcal{P}|$=7 时于 0.001 ms 内故障关闭。（4）多作用域告警风暴：由于 $M \leq 64$ 按活动资源元组（res τ， h_{man}）划分作用域，而非按集群范围划分，20 个并发作用域 ×32 信号（640 条同时告警）实现了 $20/20$ 准入，且截断数为 0；每个作用域的 p50 为 0.125 ms。相比之下，未分区的单作用域风暴（$M \in \{65, 96, 128\}$）会故障关闭并拒绝溢出信号，且不安全准入数为 0。

6.8 执行边界故障注入、物理 Post-greSQL/Patroni 与真实数据库 E2级评估

为缩小第5节并发理论与物理验证之间的差距，我们在三个彼此独立、不进行合并的真实存储层上评估执行边界契约：(1) 多进程操作系统级POSIX/SQLite WAL故障注入；(2) CI 中由三个成员组成的容器化 etcd v3.7.3 Raft 集群；以及 (3) 物理 PostgreSQL 16/Patroni 集群。

第五节多进程操作系统级故障测试套件（80 次试验）和分布式etcd试验（140 次试验）。在我们原有的 200 次 POSIX/SQLite WAL 试验基线上，我们执行了 80 次新的分叉进程操作系统故障试验（scripts/run_rev12_section5_fault_eval.py；在四种调度方案下各重复 20 次，并通过 POSIX管道进行同步，针对磁盘上的 SQLite WAL PRAGMA synchronous=FULL）：(i) 在 concurrent_coordinator_radm_cas 中，两个独立的协调器进程在相同的 r_{adm}=1 处验证了模式 C R1（ModeCCompatibilityVerifier），并在 BEGIN IMMEDIATE 提交时展开竞争，产生 $20/20$ 精确的单一获胜者提交（$r_{\mathrm{adm}} \rightarrow 2$）、对失败者的确定性过期修订拒绝，以及干净的重新验证后提交（第 50 百分位为 6.32 ms）；(ii) 在 midflight_auth_revocation_e2 中，分叉的协调器进程与撤销进程跨越管道屏障展开竞争，针对 E2层 SQLiteProtectedResourceBoundary 实现了 $20/20$ 有效的串行化，且撤销后提交泄漏为零（$\delta^{\mathrm{E2}}_{\mathrm{fresh}}$=0，第 50 百分位为 8.71 ms）；(iii) 在 tier_e1_plus_quiescence_6step 中，基于磁盘的两阶段静默屏障通过实证重现了推论 1(c-E1+) 的精确六步轨迹，涵盖 $20/20$ 次试验（$20/20$ FenceAck 前窗口期间的已准备槽完成、 $0/20$ FenceAck 后的已撤销提交，以及在已准备状态下真实 SIGKILL 后的 $20/20$ 冲突阻塞，第 50 百分位为 15.18 ms）；以及 (iv) 在 mode_c_r2_phase_decomposed_write_skew 中，R2 制度在派发前拒绝了写偏斜对，

表9：修订版 12 综合与补全不对称性（16 种状态， $M{=}33$， $k_a{=}3$；使用确定性软件提议器，隔离验证器与补全扩展性，而非实时大语言模型多跳召回）以及在线可扩展性 / 故障关闭截断压力测试（scripts/run_rev12_synthesis_vs_completion.py，scripts/run_rev12_scalability_stress.py；Apple M系列，Python 3.13.9）。每种饱和或对抗性状态均记录到**0 次不安全准入**。

基准测试 / 压力状态	准入/精确	截断率	不安全	第 50 百分位（毫秒）	关键发现 / 故障关闭边界
综合与验证不对称性（R_{b}	$_{\mathrm{g}} \in \{0, 20, 80, 250\} \times d \in \{1..4\}$，*16* 种情形；*4/4* 项对抗性控制均已阻止）				
TCB一跳补全（能力 128, completion.py）	1/16	12/16	0	0.06–0.91	仅在 $R_{\mathrm{bg}}{=}0$， $d{=}1$ 时成功；阻止所有 $d \geq 2$
可信计算基多跳广度优先搜索（能力 128 / 能力 512）	4/16 ｜ 8/16	12/16 ｜ 8/16	0	0.10–3.62	在 R_{b} 时耗尽预算（0/8） $_{\mathrm{g}} \geq 80$
针对性软件提议器 +TCB验证器	**16/16**	**0/16**	**0**	**0.07–0.28**	零 TCB 增长； 4/4 幻觉控制已阻止
在线可扩展性与故障关闭截断压力测试（$M \to 64$、$\lvert\mathcal{S}_{\mathrm{cand}}\rvert \to 256$、模式*C R1/R2*、告警风暴）					
打包真实（$M{=}64$， $d{=}1$ / $d{=}6$, $\lvert\mathcal{W}\rvert{=}64$）	$\hat{\nu}{=}64/\hat{\nu}{=}7$	0.00 / 1.00	0	0.37 / 14.38	ATMS 注册。。60–1。41 毫秒；下界$\hat{\nu}$ 有效
对抗性三叶超图 ($\lvert\mathcal{W}\rvert{=}32$， $B{=}10^4$)	精确（20/20）	0.00	0	1.43	$M{=}64$ 处问题1和问题2的误阻断率均为 0%
对抗性三叶（$\lvert\mathcal{W}\rvert{=}64/256$， $B{=}10^4$)	问题1 20/20；问题2 0/20	1.00	0	13.44 / 47.40	问题1$\hat{\nu}{\geq}3$ (0% 反馈); 问题2 严格 截断 保留世界
命中集上限 ($B_{\mathrm{HS}}{=}256$, 6 对比 8 个禁忌项)	精确 / 故障关闭	0.00 / 1.00	0	0.17 / 0.63	6 处精确命中集为 64；在 $2^8{=}256$处安全截断
合理屏蔽 ($\lvert\mathcal{S}_{\mathrm{cand}}\rvert{=}4 \to 256$， $M{=}64$， $f{=}2$)	100% 均保留	0.00	0	0.03 → 2.23	线性扩展；强制截断 保留全部 256 个世界
模式 C R1（$\lvert\mathcal{U}_C\rvert{=}4$无序。 $\lvert\mathcal{S}\rvert{=}1/16$; $\lvert\mathcal{U}_C\rvert{=}5$)	325 次调度 / 拒绝	–	0	0.56 / 3.10	有向无环图剪枝至 95（0.21–0.81 毫秒）； $\lvert\mathcal{U}_C\rvert{=}5$ 拒绝耗时 0.001 毫秒
模式 C R2（$\lvert\mathcal{P}\rvert{=}2/4/6$； $\lvert\mathcal{P}\rvert{=}7$）	2 / 18 / 270 / 拒绝	–	0	0.01–0.54	写偏斜在派发前被拒绝； $\lvert\mathcal{P}\rvert{=}7$ 拒绝 0.001 毫秒
告警风暴（$20 \times 32{=}640$限定范围 vs. $M{>}64$ 单个）	20/20 vs. 溢出	0.00 / 1.00	0	0.13/作用域	按（预留 τ， h_{man}）限定作用域可避免 $M{=}64$ 饱和

同时允许分叉进程中不相交键的重叠两阶段事务，并出现 $0/20$ 不变式违例（第 50 百分位为 6.53 ms）。在 GitHub Actions 持续集成中真实的三成员容器化 etcd Raft 集群上（运行 45335050195，提交 80836b20）， $140/140$ 次试验（$20\times$ 涵盖七种调度方案：过期_恢复、同时_排空、重复_重放、前驱_边界、领导者_故障、法定人数_丢失以及客户端_隔离）在 Raft 选举和网络切断期间保持了暴露能力上限、单调纪元和前驱边界；EtcdQuiescenceBoundary 直接在三成员 etcd 集群上通过了 FenceAck 前/后的排除以及崩溃阻塞检查这六步检查。在配套的 rev12-stress-and-pg-e2 持续集成任务中，针对运行中的 postgres:16 容器，rev11_exp08_e2_adapter.py –include-rev12-races 通过了全部 12 项基线 E2 级契约检查，以及由屏障同步的并发协调器 $\mathrm{r}_{\mathrm{adm}}$CAS 竞争（单一获胜者推进 $r_{\mathrm{adm}} \to 2$、确定性失败者中止、干净的重新验证重试），并通过了由屏障同步的飞行中授权撤销竞争，撤销后提交泄漏为零。

物理 PostgreSQL/Patroni 集群（E0+原生层级）与真实 PostgreSQL E2 级预留。 为测试 PIEQ 在真实有状态数据库基础设施上的表现，而不仅仅是在软件模拟器中，我们在容器虚拟机内部署了一个由三个 Patroni/PostgreSQL 16 节点（spilo-16:3.3-p1）组成的物理集群，并由一个三成员 etcd v3.7.3 共识集群提供支持，在持续写入流量下运行。一个独立的 1 Hz SQL 观察器查询每个节点，记录角色、时间线和写入见证行（± 1 分辨率，因此无法排除亚秒级双主状态）。由于 Patroni 的 REST 晋升端点不会在 PostgreSQL 提交边界重新验证 PIEQ 证书，我们严格将此故障转移适配器归类为 E0 层级，并结合目标原生高可用性防护措施；同时运行一个层级受限的物理配置，仅复用 PIEQ 的认知、时序和授权检查进行派发前门控。由于所有六个容器共用同一个虚拟机内核，领域独立性主张严格限于注入的容器故障和网络故障。

我们在此集群上执行了五类物理试验。在原生基线中，终止领导者会触发 Patroni 自动-晋升，在 9.9–10.2 秒内完成；在 1 Hz 下不存在双主时间段。在四次受监督的实时大语言模型提升试验（Patroni 暂停模式）中，真实领导者失效后，Sonnet 提交了 $5/5$ 条经验证的类型化推导，涵盖三个真实采集器域（带内 SQL 路径、带外 REST 桥接以及 etcd 租约），实现了 $\nu_{\mathrm{pack}} = 3$，并仅剩一个故障世界；随后，REST 派发产生了由观察者记录的晋升，耗时 57–67 秒，且不存在双主时间段。事件时间线审计验证了因果归因：从终止领导者到最早的 PIEQ 派发之间不存在可写主节点（故障加上 35 秒租约失效，再加 6.1–12.1 秒实时推理），而新主节点在派发后 9–15 秒出现。在领导者持有租约期间通过黑洞处理 SQL 路径的非对称网络分区下，PIEQ 因合理世界歧义而延迟处理，而领导者继续提供服务（$20/20$ 写入）；重复的同路径遥测未使 ν_{pack}膨胀。在策略与撤销拒绝试验中，经认证的提升（$\nu_{\mathrm{pack}} = 3$）在授权撤销后于派发前被拒绝；提交时敏感策略在 E0 层级目标上安全失败，而快照触发策略则顺利允许。最后，在一次假设范围外绕过试验中，绕过 PIEQ 的直接patronictl 切换按建模结果在完整写入方中介之外执行，并被协调标记。

必须对这个测试平台上的因果归因保持精确：在所有试验中，Pa- troni 和 etcd 均通过原生机制防止了脑裂；检查相同三个信号的传统确定性监督器也会同样顺利地完成领导者故障提升；而朴素的大语言模型基线出于模型自身的审慎，而非正式强制要求，在四次分区试验中延迟处理。因此，PIEQ 在 Patroni 故障转移中的实测物理增益，应归因于经过认证的派发前门控（验证来源和故障预算、执行授权和时序策略拒绝、在出现分区歧义时延迟处理，以及检测未受中介的写入），而非防止脑裂或加快无故障的故障转移。

为在真实数据库引擎上验证真正的 E2 级契约强制执行，我们还构建了一个容量预留适配器，在实时 Patroni 主节点上的单个可串行化 PostgreSQL 事务内强制执行十点 E2 级契约。数据库内的pgcrypto HMAC 会使用服务器存储密钥验证已签名的操作身份和时序

策略绑定，而控制行SELECT . . .FOR UPDATE 锁则将聚合暴露串行化；并发的超容量尝试最终一个提交成功、另一个产生可重试的串行化中止，独立 SQL 读取确认最终 SUM $= 10 \leq$ 能力。相同事务还会强制执行授权纪元、数据库时钟 TTL、准入版本修订比较并交换、前置操作结算、幂等性、身份冲突拒绝以及提交时原子谓词重新验证，在状态完全不变更的情况下拒绝过时的瞬态谓词。提交前崩溃不会留下任何行，而提交后崩溃则通过权威操作表进行协调，以幂等方式重新呈现，且不会自动重新调度。在权限边界处，非中介代理角色会被拒绝（42501），而postgres 超级用户则可作为管理员在中介假设之外绕过检查并成功执行。此适配器仅涵盖有限的预留词汇表，不会将 Patroni 故障转移提升从 E0 层级升级。

7 相关工作与研究定位

PIEQ 的核心贡献是执行过程绑定的认知认证：在智能体推理与物理执行之间的边界上，组合经典形式化方法、控制理论和分布式系统原语，但不声称任何单一组件本身具有原创性。

在符号诊断和谱系跟踪领域，de Kleer [9, 10],Reiter [11], 与 Provan [26]确立了最小环境基于假设的真值维护、击集诊断及其最坏情况复杂度界，而 Green 等人 [12]则形式化了代数溯源半环。PIEQ 直接基于这些基础，通过将有界 ATMS 标签维护与递归式物理故障域覆盖范围、故障关闭式计算截断下的精确完整证明打包，以及类型化验证器词汇表证书合成相结合，进一步构建系统。

在多智能体语言模型协调领域，关于分布式信息条件下辩论 [2, 3, 27, 8, 21, 4] 和集体推理 [22, 7] 的研究记录了一致性崩塌、谄媚性以及共享证据羊群效应。PIEQ 并未试图设计能够抵御一致性压力的辩论提示，而是将语言模型完全排除在可信计算基之外，同时通过类型化证明主张和只读诊断探测，保留其多跳诊断假设。

在控制理论和运行时保障中，PIEQ 的可信世界门控借鉴了部分可观测马尔可夫决策过程（POMDP）安全屏蔽 [15, 28, 29], 离散事件监督控制与可诊断性 [16, 30],可存活性理论 [20],以及 Feldbaum 的双重控制 [31]。PIEQ 将这些理念扩展到易故障分布式遥测场景，采用 f-容错反证打包（$\widehat{\mathcal{B}}^{(f)}_{\tau\,v.}$）、计算上限下的保守世界保留、经快照审计的只读探测，以及明确区分组合式状态不变量与非组合式耦合可存活核。

在安全性与智能体治理领域，Necula [14]、Appel 和 Felten [13] 开创了携带证明的代码和携带证明的认证，启发了近期的智能体治理框架，包括 CaMeL [32], 、保形策略控制 [33], 、携带证明的智能体行动 [23, 24], 以及 PC^2 [34]；这些框架将不受信任的大语言模型规划与确定性策略验证解耦。PIEQ 通过多域合取式来源隔离、容错信念保持和精确到层级的并发执行契约，补充了针对单个行动的策略检查。

最后，线性一致性 [17],、快照隔离异常 [19],、停顿精化映射 [25], 、托管与划界协议 [35, 36], 、租约和栅栏令牌 [18, 37], 以及拜占庭容错 [5]，都是分布式系统的经典基础。在 KedgeFlow 控制平面 [1, 6], 中，PIEQ 通过连续版本的快照屏障、通用$\mathbf{r}_{\mathrm{adm}}$ 比较并交换、显式的 Refines$_{\mathcal{D}}$ 机制、精确到层级的授权新鲜度以及受信任的提交时前置条件策略，将这些执行层原语直接连接到认知屏蔽。

8 残余局限与结论

8.1 残余局限

PIEQ 在四项外部信任契约和两个经验范围边界之外不提供安全性保证。首先，安全性从根本上依赖可信域模型：遗漏故障世界（E_1，如H33所示）、不健全的演绎规则（E_2，如H34和CN11所示），或 $\mathcal{G}_{\mathrm{inv}}$ （E_8）中缺失的不变量耦合，即使存在 k_a 互不相交的证明，也可能导致不安全准入。在确认测试套件上启用有界确定性补全，可恢复全部 20 次单次误阻断，但代价是消除 LLM 偶然的克制行为对 E_2 规则缺陷的掩盖（CN11从 $0/20$ 变为 $20/20$），因此补全是明确的操作方权衡，而非无条件的保障。其次，物理故障计数依赖准确的故障域分类： h_{man} （E_3，H16）中的物理依赖分类错误、故障域超出预算 f（E_5，H35），或外生的跨域共同原因故障（E_4），都会破坏确定性的仲裁保证。

第三，验证有限抽象阶段图只能证明抽象模型本身的安全性，绝不会自动完成物理到抽象的细化（Refines$_{\mathcal{D}}$）；未建模的内部阶段、缓存读取、后台回调、崩溃恢复延续或非幂等重试，除非经过形式化验证，否则都会使 R1 或 R2 失效。第四，目标原生强制执行与持久性限制了 PIEQ 在执行器边界能够作出的承诺：本地 WAL 去重绝不会让非事务型远程执行器变得幂等；未受中介的外部写入者（E_6，例如直接通过 patronictl 切换主节点，或绕过限制的 PostgreSQL 超级用户）可以绕过 L_{exp}；Tier E1+ 静默状态仍保留 FenceAck 前的授权撤销窗口，并通过无限期阻止 UNKNOWN，以牺牲活性换取安全性；持久化则位于 SQLite WAL、etcd 或 PostgreSQL 后端，而非内存中的账本核心。

两项经验边界也限制了我们当前的证据。早期的CLI 层级实时运行（heldout36 和重复研究）使用了未固定的快照，采样不受控，成本报告也不完整（未计入 GPT 令牌计费）；尽管我们新开展的直接 API 三个系列确认12 运行解决了受控采样问题（温度=0.0、种子=17）、服务器报告的模型标识以及完整计费（$0.14，涵盖全部三个系列），但其 AWS Bedrock 云端点使用的是跨区域推理配置文件别名，而非不可变的带日期戳快照，因此跨heldout36 进行带日期固定的云 API 评估仍是未来工作。此外，所有基准测试均由作者标注；我们的代理数量研究仅重复五次，统计功效有限，因为活性分歧集中于单一事件（H32）；而密集交叠的反驳超图（每个世界$|\mathcal{W}| \geq 64$ 3个叶见证者，达到 B_{pack}=10，000）在严格执行 Q2 世界保留时会触发故障关闭截断，除非对见证者去重或按下界剪枝（第6.7节）。关于

物理测试平台方面，Patroni REST 故障转移适配器仍属于 E0 层级，并依赖原生保障措施（Patroni 和etcd原生提供脑裂保护）；我们的真实 PostgreSQL E2 层级适配器仅覆盖有限的能力预留词汇；全部六个测试平台容器共用一个虚拟机内核；1Hz SQL 观测无法排除亚秒级双主状态；此外，尽管并发协调器$\mathbf{r}_{\mathrm{adm}}$ 比较并交换、执行中撤销、R2 制度和 E1+ 静默状态竞争均通过了80/80 多进程 POSIX/SQLite WAL 试验，以及经 CI 验证的容器化etcd静默状态和 PostgreSQL 16 并发/撤销竞争测试，多主机 Patroni 故障转移故障注入仍是未来工作。

8.2 结论

安全的自主基础设施变更，需要区分三项生成式智能体共识永远无法替代的职责：独立来源的证据认证、考虑不确定性的可能世界安全门控，以及与执行过程绑定的目标治理。通过条件形式化保证、自动化 CI 和分布式etcd 故障测试套件、冻结的软件基准测试、实时语言模型评估、受监督的物理 PostgreSQL/Patroni 故障转移，以及真实 PostgreSQL 上 E2级事务执行机制，PIEQ 表明，自主变更可以通过确定性、以证据为依据的安全契约加以治理，同时确保所有语言模型始终严格处于可信计算基之外。容错依赖独立的物理故障域，而非智能体数量或模型多样性；提交时语义由可信策略元数据而非调用方自行决定来执行；故障关闭式验证则将智能体偶尔遗漏证明的问题转化为可恢复的误阻断，而非假设内的不安全变更。未来仍有四个具体方向有待探索：对完整的 36 项留出测试套件开展带不可变日期戳的云 API 评估、E2 层级物理故障转移提升、独立的外部基准标注，以及多主机硬件故障隔离。

可复现性、工件可用性与 CI 验证

所有实现代码、回归测试、冻结基准定义、预注册、实验脚本、轨迹和审计报告均已发布于 https://github.com/openkedge/openkedge 下的权威路径 research/pieq/，对应已验证的修订版 12 提交 80836b200ec56d8d4ef845cf86c0c2873314b287（扩展自修订版 11 基线提交525ff84e）。

在 research/pieq/中，评估依赖项通过以下命令安装：python3-m pip install-rrequirements-eval.txt。仓库工作流 .github/workflows/pieq-evaluation.yml针对提交 80836b20 在 GitHub 托管运行器（ubuntu-latest、Python 3.13、pytest、NumPy）上运行，涵盖两个容器支持的作业；已验证的工作流运行地址为https://github.com/openkedge/openkedge/actions/runs/45335050195：（1）etcd-faults （总计 302 秒）启动了一个隔离的、摘要固定的三成员容器化etcd 集群（containers/etcd-compose.yml），并在python -m pytest tests/-q下通过全部 249/249 项测试（169 秒内失败 0 项、跳过 0 项）——其中包括全部 14 项容器支持的etcd 集成测试（涵盖test_etcd_quiescence_6step_revocation_and_crash_blocking 在EtcdQuiescenceBoundary上的测试）以及全部 6 项修订版 12 回归测试（tests/test_revision12_evals.py）——随后通过etcd 故障分布式试验（111 秒），在python scripts/run_etcd_fault_eval.py-repetitions20-output results/ci_etcd_evidence.json下运行，并作为 CI 构件 pieq-etcd-evidence上传；（2）rev12-stress-and-pg-e2（总计 34 秒）在 Linux 上重新执行全部三套修订版 12 测试套件，并针对一个运行中的容器化postgres:16 服务容器运行 experiments/pg_patroni_failover/rev11_exp08_e2_adapter.py 127.0.0.1 -include-rev12-races，通过全部 12 项基线 E2级契约检查，以及屏障同步的并发协调器$\mathbf{r}_{\mathrm{adm}}$ CAS 和 10 次试验中的飞行中授权撤销竞争；结果作为 CI 构件 pieq-rev12-evidence上传。由于 pytest 的etcd 集成测试与独立故障测试套件覆盖了相互重叠的调度方案，因此分别报告这两套测试，而不将其结果相加。GitHub CI 是对作者已发布实现的一次独立重新执行，并非独立的第三方科学复现。

冻结哈希和预注册清单位于 results/rev11/rev11_phase0_freeze.json、results/rev11/REVISION11_EVIDENCE_MANIFEST.json、results/rev10_frozen_hashes.json、results/rev9_frozen_hashes.json 和 results/rev7_frozen_hashes.json。研究输出和运行器位于 results/rev11/exp05/（20 条原始轨迹和 exp05_analysis.json），用于 20× 实时可复现性研究；results/rev11/exp06/c1_results.jsonl、c2_results.jsonl 和 c3_results.jsonl（通过 scripts/run_rev11_exp06.py –condition C1|C2 进行确定性重放），用于有界确定性补全；results/rev11/exp07/ 和 experiments/pg_patroni_failover/rev10_logs/ 用于物理故障转移因果性；results/rev11/exp08/ 和 experiments/pg_patroni_failover/rev11_exp08_e2_adapter.py（通过 –include-rev12-races 扩展）用于真实 PostgreSQL E2 级预留；results/rev11/exp09/（15 条轨迹和 exp09_analysis.json）用于 5× 成对代理数量研究；results/rev12/（rev12_synthesis_vs_completion.json、rev12_scalability_stress.json、rev12_section5_multiprocess_faults.json、pinned_conf12_full_pieq.jsonl[SHA-256 9964a33f...], pinned_conf12_full_pieq_summary.json、pinned_conf12_full_pieq_scored.json，以及 rev12_pinned_confirmation_preflight.json）用于修订版 12 的综合与补全、可扩展性/截断、80 次试验的多进程第 5 节，以及直接 API 受控采样三族确认套件。所有确定性软件套件、冻结的留出评估、成对完成重放、可扩展性压力基准测试和多进程 POSIX/SQLite WAL 调度方案，均可依据已提交的轨迹和脚本确定性重现；而新鲜的实时大语言模型运行无法在未来模型版本之间逐位重现，因为模型快照未固定且采样不受控。重新运行物理 PostgreSQL/Patroni 研究需要 Docker Compose，并使用 ghcr.io/zalando/spilo-16:3.3-p1 和 quay.io/coreos/etcd:v3.7.3（experiments/pg_patroni_failover/docker-compose.rev10.yml）。对于拥有直接提供商 API 密钥的复现实验者，scripts/run_rev8_pinned_live_eval.py –dataset heldout36|confirmation12 提供了一个固定配置的多提供商 API 运行器及其预检清单（results/rev10_pinned_preflight.json、results/rev12/rev12_pinned_confirmation_preflight.json）。扩展的归档表见配套补充文档和 research/pieq/docs/。

B 一致性动态：形式化陈述、谱证明与方差界

本附录提供了第 2.2 节的完整形式化定义。令 $N \geq 2$ 提议者通过无界潜在分数残差 $\varepsilon_i^{(t)} = z_i^{(t)} - z^\star(S_\tau) \in \mathbb{R}$ 对二元命题 $h \in \mathcal{H}$ 进行评估，并由独立的非线性读出 $y_i^{(t)} = \psi(z_i^{(t)}) \in [0,1]$ 生成取值为概率的信念。令 $\Sigma^{(t)} = \mathrm{Cov}(\varepsilon^{(t)} \mid S_\tau) \in \mathbb{R}^{N\times N}$ 具有相同的边际方差 $\Sigma_{ii}^{(t)} = \sigma_t^2 > 0$、两两相关系数 $\rho_{ij}^{(t)} = \Sigma_{ij}^{(t)}/\sigma_t^2$ 以及平均非对角相关系数 $\bar\rho_t = \frac{1}{N(N-1)}\sum_{i\neq j}\rho_{ij}^{(t)} \geq 0$。

定义 B.1（有效样本量与参与率）。对于满足 $\bar\rho_t \geq 0$ 的 $N \geq 2$ 等方差分数残差，决定 $\mathrm{Var}(\bar\varepsilon^{(t)} \mid S_\tau) = \sigma_t^2/N_{\mathrm{eff}}(\Sigma^{(t)})$ 的有效样本量为 $N_{\mathrm{eff}}(\Sigma^{(t)}) \triangleq N/[1+(N-1)\bar\rho_t] \in [1,N]$，而参与率为 $r_{\mathrm{PR}}(\Sigma^{(t)}) \triangleq (\mathrm{tr}\,\Sigma^{(t)})^2/\|\Sigma^{(t)}\|_F^2 = N^2/[N+\sum_{i\neq j}(\rho_{ij}^{(t)})^2]$。在等相关条件下，对于每个 $\bar\rho_t \in (0,1)$，$r_{\mathrm{PR}} = N/[1+(N-1)\bar\rho_t^2] > N_{\mathrm{eff}}$ 都严格成立，因此 r_{PR} 高估了方差缩减（例如，在 $N=5$ 和 $\bar\rho_t = 0.142$ 时，$N_{\mathrm{eff}} = 3.19$，而 $r_{\mathrm{PR}} = 4.63$）。

在一种风格化的共享语境辩论线性模型中 [3, 8], 每位提议者都会将其潜在得分残差向同伴均值调整 $\bar\varepsilon^{(t)}$，从众权重为 $\gamma \in (0,1]$ 同时累积加性的推理创新 $\eta_i^{(t)} \in \mathbb{R}$:

$$\varepsilon_i^{(t+1)} = (1-\gamma)\varepsilon_i^{(t)} + \gamma\bar\varepsilon^{(t)} + \eta_i^{(t)}. \tag{11}$$

定理*B.1*（潜在得分从众协方差收缩）。设 $N \geq 2$，并假设无界潜在得分残差 $\varepsilon^{(t)} \in \mathbb{R}^N$ 按照式（*11*）从等相关的 $\Sigma^{(0)}$（$\sigma_0^2 > 0$，$\bar\rho_0 \in [0,1)$）演化，受时序白噪声、零均值创新 $\{\eta^{(t)}\}_{t\geq 0}$ 驱动，且 $\mathrm{Cov}(\eta^{(t)}, \eta^{(s)}) = 0$（$t \neq s$），$\mathrm{Cov}(\varepsilon^{(t)}, \eta^{(t)}) = 0$，协方差为等相关的 Q_η（$\sigma_\eta^2 \geq 0$，$\rho_{\mathrm{model}} \in [0,1]$）。那么，对所有 $t \geq 0$，$\Sigma^{(t)}$ 在 $\mathrm{span}(\mathbf{1}) \oplus \mathbf{1}^\perp$ 上保持等相关，其共识特征值为 $\lambda_\parallel^{(t)} = \sigma_0^2[1+(N-1)\bar\rho_0] + t\sigma_\eta^2[1+(N-1)\rho_{\mathrm{model}}]$，分歧特征值为 $\lambda_\perp^{(t)} = \sigma_0^2(1-\bar\rho_0)(1-\gamma)^{2t} + \frac{\sigma_\eta^2}{\gamma(2-\gamma)}(1-\rho_{\mathrm{model}})\,\gamma(2-\gamma)\,[1-(1-\gamma)^{2t}]$（$0^0 = 1$），且 $N_{\mathrm{eff}}(\Sigma^{(t)}) = 1 + (N-1)\lambda_\perp^{(t)}/\lambda_\parallel^{(t)}$。具体而言，（*1*）若 $\sigma_\eta^2 = 0$，超额有效样本量 $N_{\mathrm{eff}} - 1$ 将按几何速率收缩为 $(1-\gamma)^{2t}$；（*2*）若 $\sigma_\eta^2 > 0$ 且 $\rho_{\mathrm{model}} < 1$，$\lambda_\perp^{(t)}$ 将收敛至正下限，而 $\lambda_\parallel^{(t)} = \Theta(t)$，从而推动 $\bar\rho_t \to 1$ 和 $N_{\mathrm{eff}}(\Sigma^{(t)}) = 1 + \Theta(t^{-1}) \to 1$。

证明。将式 (11) 写作 $\varepsilon^{(t+1)} = W\varepsilon^{(t)} + \eta^{(t)}$，其中 $W = (1-\gamma)I_N + \frac{\gamma}{N}\mathbf{1}\mathbf{1}^\top = P_\parallel + (1-\gamma)P_\perp$，$P_\parallel = \frac{1}{N}\mathbf{1}\mathbf{1}^\top$，且 $P_\perp = I_N - P_\parallel$。根据正交性（$\mathrm{Cov}(\varepsilon^{(t)}, \eta^{(t)}) = 0$）和时间白噪声性（$\mathrm{Cov}(\eta^{(t)}, \eta^{(s)}) = 0$ for $t \neq s$），协方差通过 $\Sigma^{(t+1)} = W\Sigma^{(t)}W^\top + Q_\eta$ 传播。任意等相关矩阵 $M(\sigma^2,\rho) = \sigma^2[(1-\rho)I_N + \rho\mathbf{1}\mathbf{1}^\top]$ 均可在 $\{P_\parallel, P_\perp\}$ 上对角化，其特征值为 $\lambda_\parallel = \sigma^2[1+(N-1)\rho]$（重数为 1）和 $\lambda_\perp = \sigma^2(1-\rho)$（重数为 $N-1$）。由于 $WP_\parallel = P_\parallel$ 且 $WP_\perp = (1-\gamma)P_\perp$，对 t 使用归纳法可得

$$\lambda_\parallel^{(t)} = \sigma_0^2\big[1+(N-1)\bar\rho_0\big] + t\,\sigma_\eta^2\big[1+(N-1)\rho_{\mathrm{model}}\big],$$
$$\lambda_\perp^{(t)} = \sigma_0^2(1-\bar\rho_0)(1-\gamma)^{2t} + \tfrac{\sigma_\eta^2(1-\rho_{\mathrm{model}})}{\gamma(2-\gamma)}\big[1-(1-\gamma)^{2t}\big],$$

其中 $0^0 = 1$ 且 $N_{\mathrm{eff}}(\Sigma^{(t)}) = 1 + (N-1)\lambda_\perp^{(t)}/\lambda_\parallel^{(t)}$。两个渐近情形立即成立。 □

有界概率波波维丘约束。 对于几乎必然满足有界条件的概率信念 $Y_{(t)i} \in [0,1]$，波波维丘不等式给出 $\mathrm{Var}(Y_{(t)i} \mid S_\tau) \leq 1/4$，从而对所有 $t \geq 0$强制要求 $\lambda_\parallel^{(t)} = \frac{1}{N}\mathbf{1}^\top\Sigma_y^{(t)}\mathbf{1} \leq \mathrm{tr}(\Sigma_y^{(t)}) \leq N/4$。因此，加性持久化创新动态（$\sigma_\eta^2 > 0$）无法在无界时间范围内保持 $[0,1]$；将无界潜在分数 $z_i^{(t)} \in \mathbb{R}$ 与非线性概率读出 $y_i^{(t)} = \psi(z_i^{(t)})$ 分离后，可恢复精确一致性（`tests/test_theorems_and_counterexamples.py`）。

注 B.1（相关性坍缩与单智能体误差）。仅相关性坍缩并不会使错误率恢复到单个智能体的水平：如果 $N = 5$ 独立智能体（$\bar\rho_0 = 0$）抽取 $y_i^{(0)} \sim$伯努利分布(0。30)，应用无噪声凸平均（$\gamma = 1$，$\sigma_\eta^2 = 0$），并以 0。5 为阈值，其投票将变得完全相关（$\bar\rho_1 = 1$），但一致性错误共识等于第0轮多数尾部概率 $\sum_{j=3}^{5}\binom{5}{j}0.3^j0.7^{5-j} = 0.16308 < 0.30$。对称平均通过将 5-of-5 门控折叠为第0轮 3-of-5 门控，破坏了投票多样性；而实证辩论在 $\bar\rho_0 \gg 0$ 或非对称谄媚性 [7, 8, 21]下进一步恶化。

参考文献

[1] J. He 和 D. Yu，《KedgeFlow：企业级 AI 智能体的可编程控制平面》，arXiv:2610.14810，2026年10月。[2] Y. Du、S. Li、A. Torralba、J. B. Tenenbaum 和 I. Mordatch，《通过多智能体辩论提升语言模型的事实性与推理能力》，载于 ICML 会议论文集，2024年。[3] H. K. Choi、X. Zhu 和 Y. Li，《辩论还是投票：在多智能体大语言模型中，哪种方式能产生更好的决策？》，载于神经信息处理系统大会论文集，2025年（arXiv:2508.17536）。[4] X. Zhu、C. Zhang、Y. Chi、T. Stafford、N. Collier 和 A. Vlachos，《揭秘多智能体辩论：置信度与多样性的作用》，arXiv:2601.19921，2026年1月。[5] L. Lamport、R. Shostak 和 M. Pease，《拜占庭将军问题》，《ACM程序设计语言与系统汇刊》，第4卷第3期，第382–401页，1982年。[6] J. He 和 D. Yu，《诚实法定人数问题：面向智能体基础设施的认知拜占庭容错》，arXiv:2607.16109，2026年7月。[7] Y. Li、A. Naito 和 H. Shirado，《分布式信息下多智能体大语言模型集体推理中的系统性失效（HiddenBench）》，载于 ICML 会议论文集，2026年（arXiv:2505.11556）。[8] B. Yao、C. Shang、W. Du、J. He、R. Lian、Y. Zhang、H. Su、S. Swamy 和 Y. Qi，《和事佬还是麻烦制造者：谄媚性如何影响多智能体辩论》，arXiv:2509.23055，2025年9月。[9] J. de Kleer，《一种基于假设的真值维护系统》，《人工智能》，第28卷，162，1986年 2，第127no. pp. –。[10] J. de Kleer 和 B. C. Williams，《诊断多个故障》，《人工智能》，第32卷第1期，第97–130页，1987年。[11] R. Reiter，《从第一性原理出发的诊断理论》，《人工智能》，第32卷第1期，第57–95页，1987年。[12] T. J. Green、G. Karvounarakis 和 V. Tannen，《来源半环》，载于 ACM PODS 会议论文集，2007年，第31–40页。[13] A. W. Appel 和 E. W. Felten，《携带证明的认证》，载于 ACM CCS 会议论文集，1999年，第52–62页。[14] G. C. Necula，《携带证明的代码》，载于 ACM POPL 会议论文集，1997年，第106–119页。[15] S. Sheng、D. Parker 和 L. Feng，《通过安全屏蔽实现安全 POMDP 在线规划》，载于 IEEE ICRA 会议论文集，2024年，第126–132页。[16] P. J. Ramadge 和 W. M. Wonham，《一类离散事件过程的监督控制》，《SIAM控制与优化期刊》，第25卷第1期，第206–230页，1987年。[17] M. P. Herlihy 和 J. M. Wing，《线性一致性：并发对象的一种正确性条件》，《ACM程序设计语言与系统汇刊》，第12卷，492，1990年 3，第463no. pp. –。[18] C. Gray 和 D. Cheriton，《租约：一种高效的容错机制，用于分布式文件缓存一致性》，载于 ACM SOSP 会议论文集，1989年，第202–210页。[19] H. Berenson、P. Bernstein、J. Gray、J. Melton、E. O'Neil 和 P. O'Neil，《对 ANSI SQL 隔离级别的批评》，载于 ACM SIGMOD 会议论文集，1995年，第1–10页。[20] J.-P. Aubin，《可存活性理论》。马萨诸塞州波士顿：Birkhäuser，1991年。[21] A. Wynn、H. Satija 和 G. Hadfield，《交谈并不总是廉价的：理解多智能体辩论中的失效模式》，arXiv:2509.05396，2025年。[22] Y. Li、Y. Tao、K. Zhang、T. Wang、G. Gu 和 Y. Zhou，《多样化证据，更佳预测：信息不对称下的多智能体协商（InfoDelphi）》，arXiv:2607.01661，2026年7月。[23] N. Kadyrbek 和 M. Mansurova，《携证智能体动作实现语言模型工具使用的可验证许可》，《科学报告》，第16卷，文章编号74900，2026年，doi:10.1038/s41598-026-74900-x。[24] Z. Wang，《携证智能体动作：异构智能体系统的模型无关运行时治理》，arXiv:2606.04104，2026年6月。

[25] M. Abadi 和 L. Lamport，《精化映射的存在性》，理论计算机科学，第82卷第2期，第253–284页，1991年。[26] G. M. Provan，《多上下文真值维护系统的计算复杂性》，载于第九届欧洲人工智能会议（*ECAI*）论文集，1990年，第522–527页。[27] Y. Cui、H. Fu、H. Zhang、L. Wang 和 C. Zuo，《Free-MAD：无共识的多智能体辩论》，*arXiv:2509.11035*，2025年。[28] D. Melcer、C. Amato 和 S. Tripakis，《一般部分可观测多智能体环境中安全强化学习的屏蔽分解》，强化学习期刊（*RLC*），2024年。[29] W. Scarbro 和 R. Mangal，《面向不完美感知智能体的区间 POMDP 屏蔽》，*arXiv:2604.20728*，2026年4月。[30] M. Sampath、R. Sengupta、S. Lafortune、K. Sinnamohideen 和 D. Teneketzis，《离散事件系统的可诊断性》，*IEEE*自动化控制汇刊，第40卷第9期，第1555–1575页，1995年。[31] A. A. Feldbaum，《二元控制理论 I》，自动化与远程控制，第21卷第9期，第874–880页，1960年。[32] E. Debenedetti 等，《通过设计击败提示注入（CaMeL）》，*arXiv:2503.18813*，2025年。[33] D. Prinster、C. Fannjiang、J. W. Park、K. Cho、A. Liu、S. Saria 和 S. Stanton，《保形策略控制》，载于*ICML* 会议论文集，2026年（arXiv:2603.02196）。[34] C. Ciliberto、A. Rudi 和 E. Tassi，《携证明合约：人工智能智能体无法违背的承诺》，*arXiv:2610.28484*，2026年10月。[35] P. E. O'Neil，《托管事务方法》，*ACM*数据库系统汇刊，第11卷第4期，第405–430页，1986年。[36] D. Barbará 和 H. Garcia-Molina，《界定协议：在分布式数据库系统中维护线性算术约束的技术》，载于*EDBT* 会议论文集，LNCS 第580卷，1992年，第373–388页。[37] M. Burrows，《松耦合分布式系统的 Chubby 锁服务》，载于*USENIX OSDI* 会议论文集，2006年，第335–350页。