



研究附件

Editorial cutoff: 25 October 2026 · Publication: 26 October 2026

## 数字繁荣悖论：共同依赖与共同冲击下的服务连续性测量框架

### The Digital Prosperity Paradox: A Service-Coverage Framework and an Executed Synthetic Dependency Experiment

MERIDIAN FUTURES LAB | M01 Scientific Companion | Working Paper 1.0 | 25 October 2026

作品类型：概念性工作论文，包含已执行且可复现的合成计算实验（Conceptual Working Paper with an Executed Synthetic Computational Experiment）。

状态：范围明确的原始证据评述、产生实际计算结果的合成试验性运行模型，以及拟议的数据与验证方案。本文不含沙特原始运行测量，也未经同行评审。

信息截止日期：2026 年 10 月 25 日。政策与检验范围：2026—2035 年。

#### 摘要

本文研究一个可能得到两种结果的问题：数字一体化会提高国家效率和危机中的持续运行能力，还是会因功能集中于共同依赖而放大某些冲击的影响？答案不能仅从互联网普及率或技术市场规模推导出来；这些指标测量的属性，与计算、通信、供应商和维护层同时承压时完成了多少必要服务并不相同。本文批判性梳理级联故障（Cascading Failure）、冗余相互依赖（Redundant Interdependencies）和韧性工程文献，并考察三类现实案例：2026 年海湾区域遭到打击并发生物理损坏，2024 年大范围软件故障恢复后的运行延误，以及 2023 年紧急呼叫未能接通的事件。

本文提出一个在确定时间窗口内、以服务为单位的有界有效需求覆盖率指标，并另行记录积压、恢复时间和成本。随后，我们执行一项合成实验：九组假设中每组运行 40,000 个窗口，比较三种抽象架构——一条共享路径、两条备用路径，以及带有限降级能力的两条路径。在一个假设条件下，48 小时内共同冲击概率为 20%，第二条路径与第一条路径相互独立，三种架构的需求覆盖率均值分别为 88.40%、92.44% 和 93.31%。若假设两条路径共享同一事件，同时保留额外能力负担，结果变为 88.37%、87.04% 和 88.81%。这些数字是在完全假设的数值下运行随附代码所得；它们不测量、也不预测沙特服务的表现。

概念层面的结论是，取舍方向取决于依赖类型、故障原因之间的实际协变关系、替代方案是否有效及其成本，以及用户需要服务的时间。本文提出一套验证方案：使用经授权恢复演练的聚合测量和比较设计，同时考虑机构质量、资金与服务复杂度差异。本文的贡献是一种明确识别“应测量什么、什么证据会改变决策”的工具，并非对任何具体基础设施出具安全报告。

关键词：数字国家韧性（Digital-State Resilience）；级联故障（Cascading Failure）；共同原因依赖（Common-Cause Dependency）；服务连续性（Service Continuity）；合成模拟（Synthetic Simulation）；可恢复性（Recoverability）；复合冲击（Compound Shocks）。

#### English abstract

This conceptual working paper examines a conditional proposition: digital integration may raise routine service efficiency while increasing exposure to failures shared across dependent functions; alternatively, integration may strengthen monitoring, redundancy and recovery. The paper distinguishes access, experience, cybersecurity market size, and operational service continuity. It critically reads foundational work on cascading failures alongside evidence that redundant interdependencies can improve robustness. Three real-world evidence clusters inform the mechanism without serving as measurements of Saudi performance: wartime physical damage to Amazon Web Services infrastructure in the Gulf in 2026, a software-update outage with post-restoration backlogs in 2024, and an Australian telecommunications outage affecting emergency calls in 2023.

We propose a bounded valid-demand-coverage measure and separately track backlog, recovery duration, cost and unequal exposure. An executed, fully synthetic Monte Carlo experiment compares a shared single path, two paths, and two paths with limited safe fallback. Nine illustrative parameter combinations each use 40,000 paired trial windows of 48 hours. Under one assumed common-shock probability of 0.20 and independent path failures, mean valid-demand coverage is 88.40%, 92.44%, and 93.31% respectively. When two paths are forced to share an outage event, the respective results are 88.37%, 87.04%, and 88.81%. These outcomes are **conditional outputs of an invented model, not empirical Saudi estimates or operational forecasts**. A validation protocol specifies authorized aggregate data, rival hypotheses, causal identification requirements, uncertainty and decision thresholds.

**Keywords:** digital public infrastructure; interdependent networks; common-cause failure; resilience; service-coverage measurement; stochastic simulation; Saudi Arabia.

## 1. 研究问题与推断难题

核心问题是：在计入依赖结构、替代方案、机构能力与成本后，扩大数字一体化会如何改变同步冲击期间各项服务能够正确、安全地持续满足的必要需求量？

由此引出五个子问题：

1. 在什么条件下，一体化会降低日常服务成本或改善质量？何时必须把这种结果与服务韧性分开？
2. 性能下降中有多少来自独立运行的组件，又有多少来自同一事件对共享组件的影响？
3. 备用路径何时是功能独立的替代方案，何时只是同受一个事件影响的重复配置？
4. 当完整处理或连接不可用时，能否安全地维持一部分有用服务？这会怎样影响积压与后续对账？
5. 如何比较替代方案的成本、预期损失与持续运行的社会价值，同时避免把人的基本权利当作普通商业交易定价？

问题交织着三个目标：描述性目标测量已经发生的性能下降；因果目标估计某种架构选择相对于可行替代方案对服务表现的影响；决策目标判断哪种设计值得承担相应成本与约束。实现第一个目标并不等于证明后两个目标。一个更富裕、经验更丰富的国家可能因多种原因同时拥有更一体化的架构和更好的服务；平台数量与恢复之间的简单相关性因此并不足够。

### 竞争性假设

- H1——一体化收益：在资金、管理水平与需求类型相同时，一体化改善日常表现，并可能通过统一监测和集中专业能力改善恢复。
- H2——共同暴露：多项功能若共享一个关键运行条件，冲击该条件时，潜在性能下降的范围会扩大。
- H3——真正替代方案的作用：替代机制若足够独立且能安全启用，增加多重依赖可以减少服务损失。
- H4——形式性替代方案的边界：替代方案若与原方案共享同一个因果故障，备用能力的成本可能吞掉其收益。
- H5——积压属于绩效：技术连接恢复可能早于被延误的权利、业务和请求全部办结；修复时间因此可能不同于社会恢复时间。

H1 和 H3 使本论题能够在可测量的情形下得出一体化具有优势的结论。H2 和 H4 指出条件性损害的可能；H5 则防止我们只从系统界面衡量成功。我们不声称这些假设曾在任何外部机构预注册。

## 2. 本文在文献中的位置

2.1 从组件强度到复合网络强度

谢尔盖·布尔季列夫 (Sergey Buldyrev) 等人在 2010 年提出一个数学模型，说明特定类型网络之间的相互依赖如何反复传递节点损失，使影响超过最初的小规模冲击。这项研究有助于解释，为何单独检验每一层的稳健性并不足够。[S11](#) 但其网络假设十分具体；把数值结果直接移植到一个经济体或国家，会构成外部效度 (External Validity) 错误。

菲利浦·拉迪基 (Filippo Radicchi) 与吉内斯特拉·比安科尼 (Ginestra Bianconi) 2017 年的研究为这一观点提供了平衡。它采用另一种机制：在某些多层网络中，冗余相互依赖可以提高而非降低稳健性。[S12](#) 因此，研究必须明确组件之间的需要逻辑：所有组件都必须工作时是 AND，一个替代组件即可满足时是 OR，也可能是与服务质量和安全相关的更复杂规则。这不是措辞差异，而是会改变服务成功状态集合的差异。

从系统工程看，美国国家标准与技术研究院 (National Institute of Standards and Technology; NIST) SP 800-160 第 2 卷第 1 次修订版，为思考如何预判不利条件、承受冲击、恢复并在事后适应提供了参照。[S13](#) 该框架关注系统在全生命周期内执行功能的能力；本研究则尝试把其中若干方面转化为服务层面的量化指标。

2.2 复杂性 & 互联性的思想史

查尔斯·佩罗 (Charles Perrow) 在《常态事故》 (Normal Accidents) 中提出一个机构视角，区分难以预测的交互与不给干预留出时间的紧密耦合；这对考察高度交织的数字服务很有用。[S14](#) 赫伯特·A·西蒙 (Herbert A. Simon) 在《复杂性的架构》 (The Architecture of Complexity) 中奠定了思考近可分解性 (Near-Decomposability) 结构的基础，即让大型系统内部保有一定程度的功能独立性。[S15](#) 本文把两者作为解释工具，不将其历史案例转换成当代海湾情形的实证证据。

2.3 缺口在哪里？

理论论文显示了可能存在且方向相反的机制，事故报告则显示了具体的现实结果。这里的缺失环节，是将一体化程度、依赖类型与共同故障后完成的有效需求联系起来的测量数据。受益人满意度均值或数据中心数量无法填补这一缺口。因此，本文结合一项范围明确的评述、一个可复现实验和一套经授权现场验证方案。

本文没有对全部文献进行完整系统综述 (Systematic Review)。选文依据是能否奠定机制基础、是否包含竞争性视角，以及是否属于原始工程参考。我们不声称检索了每个数据库，也没有提取可用于荟萃分析 (Meta-analysis) 的实证实效应量。停止检索的标准是参考文献已足以阐明竞争性假设及其边界，而不是为了获得“系统综述”的称号。

3. 事件证据及其外推边界

| 原始事件                                                           | 有来源支持的观察                                                                                                           | 对本文有何帮助？                                                      | 不能证明什么？                              |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|--------------------------------------|
| 2026 年 3 月，亚马逊科技 (Amazon Web Services; AWS) 在海湾的设施受损；9 月发布恢复更新 | 阿拉伯联合酋长国 (United Arab Emirates) 两处设施遭受物理损坏，巴林 (Bahrain) 设施受附近袭击影响；9 月，一些仅托管在特定受损部分的资源仍无法访问。 <a href="#">S05S07</a> | 检验同步物理冲击下空间隔离与数据恢复的边界；也说明迁移业务的客户可能成功恢复运行。 <a href="#">S06</a> | 不能证明沙特设施受损、所有客户均丢失数据，或本地基础设施已经被证实薄弱。 |
| 2024 年 7 月 CrowdStrike 错误软件更新                                  | 公司承认缺陷；英国国家医疗服务体系 (NHS) 一家地方机构称，系统恢复后仍有工作积压。 <a href="#">S08S09</a>                                                | 说明必须区分技术恢复、积压清理与服务办结时间。                                       | 不能证明所有医疗机构的影响规模，或每项备用措施的因果结果。        |
| 2023 年 11 月澳大利亚 (Australia) Optus 中断                           | 监管机构认定 2,145 名用户无法接通紧急服务，369 次必要回访未能完成。 <a href="#">S10</a>                                                        | 说明服务质量和时效需要权重，尤其是价值取决于紧急接入时。                                  | 不能证明具体死亡或个人损失，也不能把概率推广到其他国家。         |

因果说明：路透社（Reuters）2026 年 3 月的报道提到，一家地区银行同期宣布其应用和服务发生故障，但并未把故障直接归因于 AWS 事件。[S05](#) 因此，本文不会仅凭时间上的同时发生，就断言影响从这些设施传导至某家点名银行。

沙特官方数据称，2025 年互联网普及率为 99.6%，该报告发布于 2026 年；2025 年对 50 个平台的评估显示，数字体验成熟度为 86.71%；2026 年 10 月发布的报告则称，2025 年网络安全市场规模为 163 亿沙特里亚尔。[S01S02S03](#) 本文不会把这些量拼装成一个持续性综合指标：它们的主题、单位、来源和分母都不同。它们用于证明活动的广度和待检验问题的重要性，而不证明检验结果。

## 4. 拟议指标：确定窗口内的有效服务量

设有服务  $j$ 、情景  $s$  和时期  $T > 0$ 。把  $D_{j,s}^*(t)$  定义为时点  $t$  一项基本服务的有合理依据的参考需求，把  $Q_{j,s}^{\text{valid}}(t)$  定义为同一期间内实际完成且满足安全、质量、可用性和时效条件的有效产出。则定义：

$$C_{j,s,T} = \frac{\int_0^T \min\{Q_{j,s}^{\text{valid}}(t), D_{j,s}^*(t)\} dt}{\int_0^T D_{j,s}^*(t) dt}.$$

该表达式可解释需要四个条件： $D^* \geq 0$ ， $Q^{\text{valid}} \geq 0$ ，分子与分母单位一致，且分母中的需求总量为正。假设立时， $\min$  使  $0 \leq C \leq 1$ 。若参考需求为零，应记录为不适用，而不是除以零或悄悄修改分母。

若需跨服务汇总，可提出  $R_{s,T} = \sum_j w_j C_{j,s,T}$ ，其中非负权重之和为一。但这需要对权重给出社会和机构层面的理由，单独报告每项服务，并审视需求在地区或受益人群体之间分布差异的影响。即使一项低权重、高风险服务失败，平均值仍可能很高。无法形成一组相容权重时，分别展示指标会更诚实。

### 为什么需要参考需求？

有时，记录到的需求下降，是因为用户根本无法提交请求，或系统停止接收业务。如果把中断期间记录到的需求当作唯一分母，受益人在系统外等待时，完成比例反而可能上升。因此，需要依据历史使用、季节、服务类型和危机期间人们行为建立合理基线，并估计结果对基线变化的敏感程度。

### 为什么这一指标不能单独使用？

因为它未必计入观察窗口后的延期工作、不可逆损害、对账错误、未观察到的业务质量或运行成本。我们建议同时记录：持续预定时长的最大缺口；达到所需服务阈值并稳定保持预定时长所需时间；积压规模及其清理方式；无法访问数据的状态；单独估算的经济成本；以及地区或服务之间的聚合差异。观察期结束前尚未恢复的情况应标注为右删失（Right-Censored），而不是写成“在最后一天恢复”。

## 5. 已执行的计算实验

### 5.1 实验目的与范围

实验狭义的科学任务，是检验覆盖率结果对替代架构和故障依赖的敏感程度。它不模拟真实网络，不估计海湾空袭或组件故障的频率，也不检验任何真实机构的响应计划。所有情况均为假设，输出是以这些假设为条件的模型结果。

我们建立五类没有机构名称的抽象服务，其需求权重为 ( $w = [0.28, 0.24, 0.20, 0.16, 0.12]$ )，总和为一。每项服务每小时有一个假设需求单位，持续 ( $T = 48$ ) 小时。危机期间，需求权重和强度保持不变；这一重要简化意味着，本研究不声称代表真实用户行为。每个窗口内，故障事件可能从该时段的某处开始；各项服务还各有独立的本地事件。同一组假设中，不同路径的比较使用只生成一次的共同事件，即配对比较（Paired Comparison），以降低设计差异的方差。

### 5.2 三种架构

**A——单一共享路径（Single Shared Path）**。服务依赖一个主要组件、没有共同冲击，以及本地组件正常。任何条件失败时，该小时的有效产出为零；否则为一个完整单位。

**B——两条可替代路径（Two Paths）**。在没有共同冲击且本地服务正常的前提下，两条主要路径中任意一条保持有效即可。我们把每个正常小时的常态能力设为 0.985 单位，即假设为运行这一设计付出 1.5%

的能力折损。这不是估算的财务成本，也不是分布式系统的普遍折扣，只是可在后续模型中改变的合成参数。

C——两条路径与有界降级运行（Two Paths with Bounded Fallback）。共享基础设施可用时与 B 相同；其不可用时，为部分服务类别增加受控的假设能力： $(f = [0.30, 0.25, 0.10, 0, 0])$ 。我们假设这些比例能够提供安全、有效的服务，但没有为任何真实服务证明这一点。后两类为零，是承认有些业务不应在降级模式下或缺少必要核验时执行。模型不计算对账错误或延期存储，而这些约束会影响现实可行性。

用代数表示这一逻辑：令  $C_t$  为使主要系统失效的共同冲击事件， $P_t$  为第一条路径失效， $B_t$  为备用路径失效， $L_{j,t}$  为服务  $j$  的本地组件有效性。各故障事件在中断小时取值一，其余时间为零； $L$  则相反。为简化表达，我们使用逻辑掩码相乘。抽象有效产出为：

$$Q_{j,t}^A = L_{j,t}(1 - C_t)(1 - P_t),$$

$$Q_{j,t}^B = 0.985L_{j,t}(1 - C_t)(1 - P_tB_t),$$

$$Q_{j,t}^C = L_{j,t}[0.985U_t + f_j(1 - U_t)], \quad U_t = (1 - C_t)(1 - P_tB_t).$$

这一表达区分了单路径服务条件必须同时成立，与两条路径之间的相互替代；也把假设的“服务有效”结果与单纯的网络连接分开。

### 5.3 冲击事件与随机性

| 参数            | 使用的合成数值           | 解释与边界                                           |
|---------------|-------------------|-------------------------------------------------|
| 窗口长度          | 48 小时             | 标准化比较时段，不等于真实恢复时间。                              |
| 实验次数          | 九组中每组 40,000 个窗口  | 共生成 360,000 个窗口；每种设计在组内比较，产生 27 组设计输出。          |
| 窗口内主要故障概率     | 0.38              | 实验假设，不代表云服务或机构的故障频率。                            |
| 每项服务发生本地故障的概率 | 0.10              | 各类别的本地事件独立抽取。                                   |
| 共同冲击概率        | 0、0.20、0.50       | 三种敏感性条件，不是对未来 48 小时的预测。                         |
| 两条路径共享故障事件的程度 | 0、0.50、1.00       | 混合独立事件与相同事件；这些数字不是皮尔逊相关系数（Pearson Correlation）。 |
| 第一条路径事件时长     | 4 或 12 小时         | 每次实际事件中随机选择。                                    |
| 共同冲击时长        | 6 或 18 小时         | 同时作用于两条路径的主要基础设施。                               |
| 本地服务事件时长      | 2 或 6 小时          | 即使共享路径仍可用，也会影响一项服务。                             |
| B 与 C 的常态能力   | 98.5%             | 假设的合成能力代价，不包括金钱、能源或维护。                          |
| 部分服务的降级能力     | 30%、25%、10%、0%、0% | 这些数值以服务安全为条件；在真实服务测试前无法保证。                      |

每个事件窗口从可容纳该组件最长设定时长的起始小时中抽取，因此较短事件可能偏向较早开始。这是公开说明的情景属性，不是对真实故障时间分布的描述。“故障共享”水平为 1 时，备用路径复制主路径的同一中断窗口；水平为零时，备用路径按相同边际值独立抽取事件；中间水平则按代码规定的混合规则，在复制与独立之间选择。

我们使用 NumPy 随机数生成器，原始种子为 20261025，各组的派生种子均有记录。生成输出的代码位于 `analysis/reproduce.py`，完整结果表写入 `data/simulation_results.csv`，假设文件写入 `data/assumptions.json`。代码已实际运行并生成随附表格与图。按记录的环境和软件版本重复运行，可得到相同数字。

### 5.4 输出与统计量

对每个实验窗口，我们计算加权需求覆盖率的时间均值，再取 40,000 个窗口的平均值。另计算未达到 90% 覆盖率的窗口比例，以及加权总量低于 50% 的实验小时比例。这两个阈值只是模型内的展示检验，未经机构认可，也没有按真实服务安全阈值校准。

除均值外，我们报告蒙特卡洛标准误（Monte Carlo Standard Error），即窗口输出的标准差除以窗口数量的平方根。它描述模拟规模造成的数值估计波动，不测量我们对真实概率的无知、权重选择错误或模型外推能力。因此，计算图中的误差条不能称为“沙特韧性的置信区间”。

## 6. 已执行结果及其解读

### 6.1 冲击和依赖改变时的覆盖率

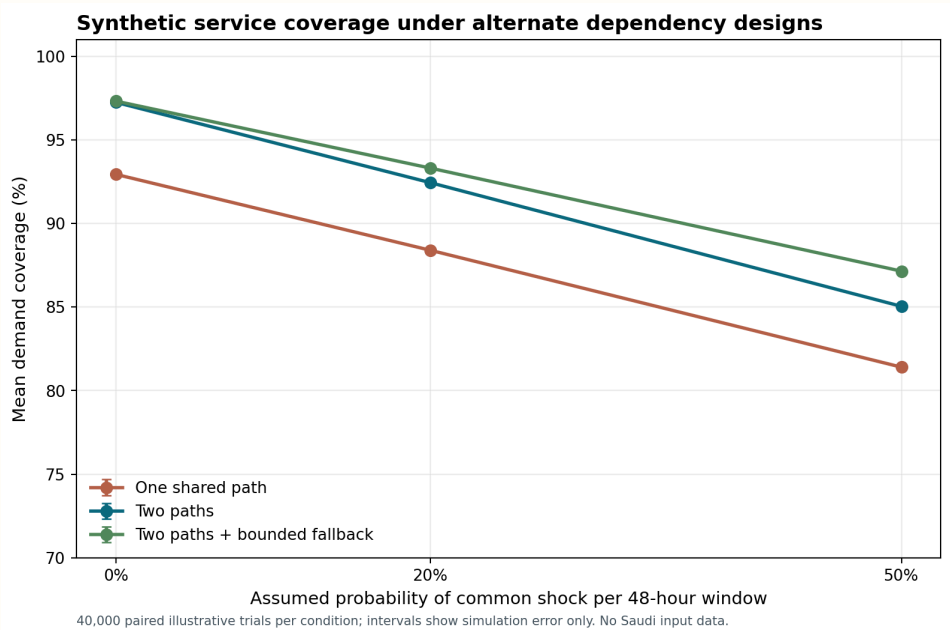
| 每个窗口的共同冲击概率 | 两条路径故障混合程度 | A：一条路径 | B：两条路径 | C：两条路径+有限持续运行 |
|-------------|------------|--------|--------|---------------|
| 0%          | 0.0        | 92.93% | 97.24% | 97.31%        |
| 0%          | 0.5        | 92.88% | 94.32% | 94.88%        |
| 0%          | 1.0        | 92.96% | 91.56% | 92.58%        |
| 20%         | 0.0        | 88.40% | 92.44% | 93.31%        |
| 20%         | 0.5        | 88.24% | 89.61% | 90.95%        |
| 20%         | 1.0        | 88.37% | 87.04% | 88.81%        |
| 50%         | 0.0        | 81.40% | 85.04% | 87.14%        |
| 50%         | 0.5        | 81.44% | 82.67% | 85.17%        |
| 50%         | 1.0        | 81.40% | 80.18% | 83.09%        |

表 3——合成模型的实际结果。每个单元格为 40,000 个窗口的平均值，不是对任何行业或国家的测量。A 的部分行之间零点几个百分点的细小差异，来自不同条件组的独立随机抽样。

第一项条件性结论是，故障原因是否独立，比路径数量本身影响更大。假设共同冲击概率为 20%，两条路径不共享个别故障事件时，B 比 A 高约 4.04 个百分点。强制两条路径共享同一个故障事件时，A 与 B 的排序反转，A 高约 1.33 个百分点；在本模型中，原因是 B 承担了假设的能力负担，却没有获得实际独立性的补偿。这不是“备用方案有害”的现实定律，而是参数选择与故障规则的结果。

第二项条件性结论是，降级模式在所有展示情形中都增加了覆盖率，因为它加入了另两种架构没有的正向假设：路径中断时仍有有效服务能力。这个结论写在数学结构之中。要把它转化为建议，必须证明该能力真实、安全，能够被用户和监管机构接受，而且成本与后续对账义务不会使它比有序延期更差。

第三，单靠增加路径数量无法消除同时使两条路径失效的共同冲击。假设共同冲击概率为 50% 时，即使两条路径的个别事件相互独立，B 的覆盖率仍低于 86%。缺口大小取决于假设的冲击时长；改变时长会改变结果，这是本版尚未执行的后续敏感性检验。



共同冲击变化时合成模拟的平均需求覆盖率

研究论文图 1——两条路径不共享个别故障事件情景下的合成平均比例。来源：仅来自本研究代码的运行结果。

## 6.2 尾部指标：未达到 90% 的窗口

共同冲击概率为 20%、两条路径相互独立时，平均覆盖率低于 90% 的窗口比例，A 约为 37.7%，B 为 21.5%，C 为 21.2%。强制两条路径共享同一故障事件时，三者分别变为 37.7%、41.0% 和 37.8%。这个问题不同于平均覆盖率：均值可能接近，糟糕时段的数量却可能明显不同。但它仍是以所选 90% 阈值为条件的合成计算。

这里没有测量观察期结束时丢失的业务，或之后对其进行的补偿。实验未接收未完成需求积压、真实个案优先级，或家庭与地区间损害分布等变量，因此不代表这些因素。不能因为标题写着“模拟研究”，就把它扩张成对全部经济与社会生活的模拟。

## 6.3 结论在什么条件下会翻转？

- 如果 B 在常态下损失的能力成本上升，独立性的预期收益超过成本的临界点就会改变。本文尚未检验广泛的成本范围。
- 如果替代方案的故障模式比我们假设的更相关，冗余的收益会下降；若实际采用独立的技术和供应商，收益可能提高。
- 如果降级模式无法核验受益人身份或数据完整性，其有效份额可能降为零；即便技术上可运行，也可能不可接受。
- 如果故障期间需求上升，或资源恢复后仍有积压，需求覆盖率及后续运行结果可能以当前模型无法捕捉的方式变化。
- 如果一体化帮助更快发现故障或迁移服务，实际故障时长会缩短；即使存在共同依赖，其韧性也可能提高。模型没有直接估计这项机构优势。

# 7. 如何在沙特真实服务中检验假设？

应用研究必须从一个克制的起点出发：我们没有获准使用的运行记录，无法测量战争或恢复演练期间特定沙特服务的连续性。公开数字绩效指标也没有提供有效需求、中断、积压和替代方案的详细时间序列。所以下文是一套拟议方案，不是对已经收集的数据或已经执行的实验的描述。

## 7.1 分析单位与样本

最合适的初始单位是确定时间窗口和确定故障中的一项必要服务。可在不泄露敏感设施特征的前提下，比较聚合地点或机构组。服务根据时效、安全和可用性条件选择，并须获准访问聚合数据。确定最终服务数量或观察时长之前，应评估记录是否充足、分类方式是否公平；不能仅因某个样本量看起来“科学”就将其编造出来。

数字依赖可按五类进行描述性分类，同时不披露弱点细节：计算供应商、通信、身份与授权、对账或集成组件、人力或运行能力。目标是判断功能是否依赖单一供应商类别、单一恢复机制或单一组织关键点，而不公开运行路径、地址或可用于定位攻击的细节。分类还应结合服务性能下降时长数据，而不是只有硬件清单。

## 7.2 最低变量矩阵

| 拟议变量    | 必须事先批准的操作定义             | 保护效度的方法                   |
|---------|-------------------------|---------------------------|
| 服务类型    | 具有确定敏感级别和容许延误的功能类别      | 不把紧急服务与可延期且不会造成同等损害的服务混合。 |
| 参考需求量   | 由历史数据或含不确定性的模型合理支持的预期需求 | 报告需求时段、季节，以及请求未能进入系统的情况。  |
| 有效产出    | 按固定成功定义，安全、正确、及时完成的请求   | 审计完成数据样本，区分接收与办结。         |
| 共同依赖    | 聚合层面的依赖与供应商类别           | 防止发布可推断其可被攻击性的节点或机构。      |
| 替代方案独立性 | 经授权实际切换演练的结果和服务迁移时间     | 核验副本、密钥和流程是否工作，而非仅确认其存在。  |
| 积压      | 未在规定时间内完成，或需要后续对账的请求    | 记录请求时长、错误和退回，而非只记数量。      |
| 成本      | 持续能力的全生命周期成本和测试事件支出     | 区分固定成本、事件成本与未实现损失。        |
| 机构背景    | 资源、用户性质、管理成熟度与服务复杂度     | 归因于一体化之前，先把这些因素纳入差异解释。    |

初步研究可在服务层面计算  $C_{j,s,T}$ ，并附上积压请求数量的时间序列与某项明确替代演练的结果。报告应说明数据来自实验、内部测试还是观察到的真实事件；不能仅因一个综合表格容纳得下，就把不同类型压成同一平均值。

### 7.3 定义因果取舍

假设拟议决策是从运行架构 A 转向架构 B。真正的因果问题，是服务在两种架构下处于可比条件时的结果差异。我们无法同时观察同一项服务在同一次冲击中采用两种架构的潜在结果，因此需要推断设计。

若防御性演练得到授权且安全，可以在统一需求规则与明确测量下比较架构或恢复情景，同时防止测试团队的经验累积，让最后测试的设计仅因团队多接受了一轮训练而显得更好。若组间和时间差异能够理解，分阶段采用设计或重复比较可能有帮助；但应检查既有趋势、同期事件，以及影响在机构或供应商之间的传递。

一种薄弱方案，是用同一份问卷收集“一体化”和“韧性”评分，再从高度相关推断因果关系。预算更高、专家团队更强的机构，可能在两项评分上都更高。这些属于混杂变量（Confounders），应予描述，其中一些还可能难以通过统计方法控制。有时，因果识别（Causal Identification）的条件并不存在；此时，受控的描述性比较更符合事实。

### 7.4 能够改变本文结论的标准

若多次独立演练显示，在控制供应商选项、资金与管理成熟度后，一体化服务在不同冲击下均提高有效需求覆盖率，并降低恢复时间与积压，那么本文对共同暴露的论题在该服务类别中就会减弱。若同步功能下降能够归因于有记录的共同依赖，且实验显示独立替代方案能减少损失而不引入重大新错误，该论题则会增强。无论方向如何，都应解释成本、收益与边界，并检验影响能否延伸到其他服务类别。

## 8. 从指标走向经济与社会决策

机构负责人可能持续为一项多数日子都用不上的备用能力付费。若只看普通一天的平均表现，这笔钱看起来像浪费。但当中断代价不只是修复计算机，而是等待药物、无法证明某项业务、工厂生产延误，或紧急呼叫无法送达的风险时，它可能成为理性选择。没有伦理与方法依据，不能把这些损害合并为一个货币数字；同样不能因为它们难以定价，就从预算中抹去。

一种概念性的经济比较可以写成：

$$\text{Total expected lifecycle burden} = \text{routine operating cost} + \text{resilience investment} + \mathbb{E}[\text{permitted disruption loss}] + \text{transition a}$$

这不是对沙特经济的数值估计，也不暗示所有人类利益都可以定价。每一项都需要定义和来源，并须避免同一损失在供应商和交易方之间转移时被重复计算。决策会随冲击强度和时长、保险赔偿、监管合规

及可用外部替代方案而变化。它可能支持为一项服务采用适度持续方案，为另一项作大额投资，并为第三项安排有序延期。

从计算经济学（Computational Economics）角度，应把常态运行节省，与共同依赖可能增加的性能下降强度、速度和成本相比较。如果服务能在损害窗口结束前切换路径或恢复业务，独立性价值就会提高。如果备用中心的持续支出挤占了更有用的资源，却未带来可测量的改善，增加复杂性可能并无正当理由。确定这一关系的数字需要真实数据。

问题还有分配层面：大多数人享有较高平均服务率，不保证无法使用替代渠道的人也能接入，也不保证预算不足以购买第二个云副本的小企业能接入。因此，评估持续运行结果时，本文建议区分平均值、严重缺口和接入公平。任何权重或阈值选择都应连同其变化造成的影响一并公布，避免单一指标遮蔽受损群体。

## 9. 到 2035 年的条件性情景

这些情景不是附有估计概率的预测，而是用来界定决策，以及应随之变化的指标。

1. 一体化可靠性改善路径：机构沿用户旅程测量服务，测试向独立替代方案切换，并管理积压。可观察检验：低性能时段缩短，成本成比例，需求覆盖更有效。
2. 依赖集中路径：用户、业务和设备数量增长，但实际切换仍依赖少数相似机制。可观察检验：不同演练中切换反复失败，或数据仍仅存于广泛冲击时难以跨越的边界内。
3. 机构学习与专业产业路径：功能监测、恢复和降级运行能力形成可测试、可向多家机构销售的产品。可观察检验：真实销售和独立客户处有记录的表现，且收益可以重新测量。

更新这些情景必须以有记录的数据变化或新测试为依据。关于潜在军事威胁的新闻报道可以改变值得检验的情景，却不足以记录事件已经发生，也不能为其发生日期赋予精确概率。建立预测校准（Forecast Calibration）需要在结果出现前发布的预测记录和明确判定规则，超出本文现阶段成果范围。

## 10. 研究局限与合理性评估

信息局限：政府公开页面提供普及率、成熟度和市场指标，但没有提供分析沙特服务在复合冲击中表现所需的组成数据。本文没有这些数据，并不证明机构自身也没有。云设施事件有原始和专业来源记录，但我们没有客户记录，无法推断损失频率、分布或对沙特功能的影响。

事故来源局限：服务供应商声明是其公开内容的第一手来源，其中一些结论仍可能需要独立核检；另一家机构同期发生故障，也不足以单独证明故障已经传导过去。监管机构关于 Optus 的认定，不能把未接通情况转化成未经证明的个人健康主张。英国医疗服务证据也仅涉及特定服务与地点。

实验局限：类别、权重、概率、中断时长、架构和降级能力全部是合成的。实验没有实际配置财务资源或法律考虑，没有拥堵模型或跨服务需求转移，没有社会损害分布，也没有每次事件后的机构学习。每个组件在 48 小时内只有一个中断窗口的假设，也未必适用于长期危机或连续攻击。“故障共享”是实验中的概率混合，不是供应商间普遍相关性的估计。

绩效指标局限：正常运行小时数不自动等于权利持续得到保障。若参考需求无效，或不计延误影响和接入分布，需求覆盖率本身也不够。若不同服务对“正确完成”或未进入门户的工作采用不同计算方式，跨服务比较就会误导。

文献局限：本评述具有选择性，以机制为范围。两篇网络论文假设不同；表面上的结果矛盾，实质上提供了系统运行条件的信息。我们没有全面检索所有已发表论文，也没有按系统综述报告规则开展分类评述。

已实际验证的内容：模拟程序已经运行，生成了可读的数值、假设文件和图。服务权重之和及基本合成能力边界已经检查。这只是有限的计算验证，不意味着模型对外部现实有效，也不意味着未来会与其样本相同。

## 11. 拟议的下一阶段研究计划

本文可以通过四个相互关联的步骤发展为独立实证研究，前提是在看到结果前，就数据访问与定义达成一致：

第一步：服务定义方案。确定一组可测量、对时效要求各不相同的必要功能，定义完成质量与可接受延误。建立隐私保护与个别设施结构遮蔽路径；在确认性分析之前，方案应规定排除不足数据和处理缺失值的规则。

第二步：聚合依赖图与经过测试的替代方案。研究者区分供应商、软件、区域、身份和修复方式的共享。不得发布暴露关键设施的运行图；必要时只用行业级表格、匿名或合成数据。应测量切换时间与完成质量，而不是计算采购文件中写了多少个替代方案。

第三步：采用可证伪假设的比较。经授权演练应包含单组件故障、多个独立组件故障，以及影响共同依赖的假设事件，并采用事先商定的严重程度梯度。研究识别对时效最敏感的功能，追踪丢失、延误或通过替代方式完成的需求。积压与恢复的计算规则应提前登记。

第四步：经济分析与独立复现。计算全生命周期成本；比较备用和减少依赖的方案与实际服务连续性。用另一组服务或后续演练检验可迁移性。只有积累出可用于样本外比较和置信校准的一系列结果后，才能建立未来的量化预测，而不能依据一次实验。

如果研究发现，一体化在常态与冲击期间都提高需求覆盖率，这将是值得发布的战略性结果。如果发现某项共同依赖造成广泛缺口，应在保护基础设施安全的前提下，连同边界一起公布解释。拟议替代方案也须接受独立测试，防止一则震撼事件变成购买未知效用设备的现成理由。

## 12. 可复现输出与数据可用性

本工作包完成的资产包括：

- `analysis/reproduce.py`：生成合成事件、计算指标和制作图表的完整源代码。
- `data/assumptions.json`：情景变量、权重、约束、种子和解释边界。
- `data/simulation_results.csv`：9组假设、3种架构选择产生的27行结果。
- `figures/figure_01_dependency_map.svg` 和 `.png`：抽象关系示意，不代表具体设施。
- `figures/figure_02_coverage_sensitivity.svg` 和 `.png`：一组条件下的分类均值与模拟误差。
- `analysis/requirements.txt`：运行示例所需的软件库列表。

数据文件不含任何沙特记录、用户数据或设施地图。模拟数字的唯一来源，是文中说明的合成情景生成器；按 `analysis/README.md` 运行程序即可复现。现实来源则是公开参考资料，再次使用时应访问其带日期版本，并记录任何后续更正。

## 13. 科学结论与开放问题

已发表证据充分说明，数字国家值得检验共同依赖；与之相对的理论证据则说明，如果一体化创造出独立替代方案，它也可能成为提高稳健性的途径。有记录的事故表明，服务、数据与积压可能遵循不同的恢复时间。我们执行的模拟只在模型内部证明：从独立替代方案转为共享故障原因的替代方案时，比较结果会改变；有效的降级运行可以挽回一部分需求，却不能解决所有故障。

可检验的实践结论：数字国家若想知道自身在压力下进步到何种程度，应以聚合方式测量仍能安全满足的必要需求量、恢复到明确水平的速度，以及实现这些选择的成本，同时公开现有数字无法证明的内容。留给下一项研究的开放问题是：在成本、权利、场所和资源约束下，哪一种运行独立性最适合保护不同类型的服务？

---

## 参考文献与归引规则

以下来源均带有出版者日期，其链接用于核查主张。部分动态政府页面的内容通过搜索索引或相连的官方版本得到核验，相关情况已记录在 `source_register.csv`。证明报告已经发布，不等于证明对其数字的每一种解释都成立。

1. [S01](https://www.cst.gov.sa/en/knowledge-center/reports/saudi-internet-25) Communications, Space and Technology Commission (CST), *Saudi Internet 2025*, 2026.  
<https://www.cst.gov.sa/en/knowledge-center/reports/saudi-internet-25>

2. [S02](#) Digital Government Authority (DGA), *The Digital Experience Maturity Index for 2025 Rises to 86.71%*, August 2025. <https://dga.gov.sa/en/news/rise-in-the-digital-experience-maturity-index-2025>
3. [S03](#) National Cybersecurity Authority (NCA), *Key Economic Indicators in the Cybersecurity Sector 2026*, 14 October 2026, figures for 2025. <https://nca.gov.sa/en/news/report-on-key-economic-indicators-in-the-cybersecurity-sector-in-the-kingdom-2026/>
4. [S04](#) Amazon Web Services, *AWS Health Dashboard: Service Health and Historical Incident Updates*, March – October 2026; consult event history as revised. <https://health.aws.amazon.com/health/status>
5. [S05](#) Reuters, *Amazon cloud unit's data centers in UAE, Bahrain damaged in drone strikes*, published 2 March 2026, updated 3 March 2026. <https://www.reuters.com/world/middle-east/amazon-cloud-unit-flags-issues-bahrain-uae-data-centers-amid-iran-strikes-2026-03-02/>
6. [S06](#) Amazon Staff, *AWS Bahrain Region disrupted by ongoing conflict*, 24 March 2026. <https://www.aboutamazon.com/news/aws-bahrain-region-middle-east-conflict>
7. [S07](#) Reuters, *Amazon's AWS is unable to restore access to Bahrain, one UAE cloud data zone after war damage*, 15 September 2026. <https://www.reuters.com/world/middle-east/amazons-aws-is-unable-restore-access-bahrain-one-uae-cloud-data-zone-after-war-2026-09-15/>
8. [S08](#) CrowdStrike, *To Our Customers and Partners*, 19 July 2024. <https://www.crowdstrike.com/en-us/blog/to-our-customers-and-partners/>
9. [S09](#) NHS Shropshire, Telford and Wrekin, *Update on IT outage – EMIS up and running but some delays expected*, 22 July 2024. <https://www.shropshiretelfordandwrekin.nhs.uk/news/update-on-it-outage-emis-up-and-running-but-some-delays-expected/>
10. [S10](#) Australian Communications and Media Authority (ACMA), *Optus pays \$12 million penalty for Triple Zero outage*, 8 November 2024, referring to the 8 November 2023 outage. <https://www.acma.gov.au/articles/2024-11/optus-pays-12-million-penalty-triple-zero-outage>
11. [S11](#) Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., and Havlin, S., *Catastrophic Cascade of Failures in Interdependent Networks*, *Nature* 464 (2010), 1025 – 1028. DOI: 10.1038/nature08932. <https://www.nature.com/articles/nature08932>
12. [S12](#) Radicchi, F., and Bianconi, G., *Redundant Interdependencies Boost the Robustness of Multiplex Networks*, *Physical Review X* 7 (2017), 011013. DOI: 10.1103/PhysRevX.7.011013. <https://journals.aps.org/prx/abstract/10.1103/PhysRevX.7.011013>
13. [S13](#) National Institute of Standards and Technology (NIST), *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, SP 800-160 Vol. 2 Rev. 1, December 2021. DOI: 10.6028/NIST.SP.800-160v2r1. <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>
14. [S14](#) Perrow, C., *Normal Accidents: Living with High-Risk Technologies*, updated edition, Princeton University Press, 1999. <https://www.jstor.org/stable/j.ctt7srgf>
15. [S15](#) Simon, H. A., *The Architecture of Complexity*, *Proceedings of the American Philosophical Society*, 106 (1962), 467 – 482; bibliographic and scholarly discussion at Santa Fe Institute Press. <https://www.sfi.press.org/21-simon-1962>
16. [S16](#) Reuters, *Iran has detailed plans to hit Gulf undersea cables if war resumes, officials say*, 23 October 2026; statements are conditional and unverified as future actions. <https://www.reuters.com/world/middle-east/iran-has-detailed-plans-hit-gulf-undersea-cables-if-war-resumes-officials-say-2026-10-23/>