AI-GOVERNED POWER EFFICIENCY & REDUNDANCY

XR-VPP / XR-PMC Silicon Roadmap — FPGA to Programmable ASIC

- **產品系列**: Technical Whitepaper & Product Specification Proposal
- **文件編號.**: xr-vpp-silicon-001
- **版本**: v0.1 (draft)
- 日期: January, , 2026; Author: Dennis TY. Leo
- **階段**: Confidential — Partner Evaluation Only

智慧財產與法律聲明

文件名稱： XR-VPP 系列產品規格書（XR-VPP-SILICON-001）
版本： v0.1（草案）
文件等級： 機密 — 僅供合作夥伴評估（CONFIDENTIAL — Partner Evaluation Only）

保密 / 禁止揭露（Confidentiality / Non-Disclosure）

本文件包含 XR-VPP POS 電源平台之機密與專有資訊，僅供評估與 XR Series 建立潛在合作關係之目的使用。未經 XR Series 事前書面同意，嚴禁以任何形式對本文件或其內容（全部或部分）進行審閱以外之使用、複製、散布、公開、揭露或轉交第三方。

權利歸屬與著作權（Ownership & Copyright）

本文件全部內容（包括但不限於文字、圖表、方塊圖、規格參數、產品概念、命名規則、設計方法、交付流程、機構/外觀識別、治理邏輯與驗證方法）均屬 XR Series 之智慧財產，並受適用之著作權法、營業秘密法及相關法律保護。

無授權 / 無權利移轉（No License / No Transfer of Rights）

因本文件之揭露，並不構成任何明示或默示之專利、著作權、商標、營業秘密或其他智慧財產權之授權。
本文件任何內容均不得解釋為授與、讓與、移轉或承諾移轉任何 XR Series 之智慧財產權。

禁止逆向工程 / 衍生使用（Restriction on Reverse Engineering / Derivative Use）

收受方不得對本文件所揭示之任何資訊進行逆向工程、拆解、反編譯、反組譯、翻譯、複製、再現、模擬、重製或製作衍生作品，包括但不限於：

- 系統架構與功能方塊圖
- PoE 供電與資料通道之整合設計
- Ride-Through（RT）能量緩衝與控制策略
- 多來源輸入備援（Redundancy）之隔離、防回灌、優先級與 sharing-ready 拓撲

- 電源治理（governance）、事件證據化（evidence logging）、漂移偵測（drift detection）與序列/降載策略
- 機構平台、固定介面、散熱/ESD/EMI 參考平面策略
  除非 XR Series 以書面明確授權，否則一律禁止。

專利權利保留 / 概念受保護（Patent Rights Reserved / Concepts Under Protection）

XR Series 保留就本文件所述概念與設計進行專利申請及其他智慧財產保護之全部權利。受保護之概念包括但不限於：

面向 POS 的 PoE 部署架構：供電與資料通道整合，並結合 ride-through 能量緩衝與事件治理。

POS 原生電源平台之機構整合：含 VESA 介面鎖定之金屬平台（固定/走線/維護一致性）及其結構/配重/散熱/參考平面之工程化交付。

多來源輸入備援與 sharing-ready 電源路徑：PoE、DC Jack、USB-C、Battery rail-in 等多源輸入之隔離、防回灌、優先級選擇、（可選）主動分流與策略控制。

電源治理與診斷證據鏈：事件時間戳、ring buffer、摘要特徵、signature、信心分數、因果漂移偵測，以及序列/降載/回復策略之合規邊界內執行。

合規邊界下的交付與驗證方法：保護機制不被繞過之治理策略、測試/回放/追溯機制，以及可被審查之交付流程。

工業設計識別與機構 keying 策略：外觀與機構特徵之識別性、可復現性與防誤用策略。

商標與品牌（Trademarks & Branding）

「XR Series」、「XR-VPP」及本文件所引用之其他 XR 相關名稱、標誌或標記，可能為 XR Series 之商標或服務標章。未經 XR Series 事前書面同意，禁止使用、引用或以任何方式作為商業宣傳或標示。

第三方資訊（Third-Party Information）

本文件所引用之第三方標準、元件或參考資料（包括但不限於 IEEE 標準）僅用於互通性與技術評估目的。第三方商標與權利仍歸其各自權利人所有；本文件不構成任何第三方權利之授權。

免責聲明 / 無擔保（Disclaimer / No Warranty）

本文件係以「現狀（AS IS）」提供，僅供評估使用。XR Series 不提供任何明示或默示之擔保，包括但不限於適售性、特定目的適用性或不侵權保證。因使用本文件或依賴其內容所生之任何損害，XR Series 概不負責。

對外揭露限制（External Disclosure）

未經 XR Series 事前書面同意，收受方不得進行任何公開聲明、新聞稿、行銷宣稱或其他對外揭露，亦不得以任何形式引用 XR Series 或本文件所述概念、設計與內容。

聯絡方式： [Dennis Leo / dennis@dennisleo.com / HTTP://AICHIPCO.COM

REVISION HISTORY

版本	B 期	撰寫者	發行
V0.1	January 08, 2026	Dennis Leo	Draft

TABLE OF CONTENTS

AICHIP

1 EXECUTIVE SUMMARY

1.1 Industry Context: AI Density Drives Power as the Scaling Bottleneck

AI compute is entering a phase where performance growth is increasingly achieved by higher compute density and tighter power envelopes. In this trajectory, power consumption and its downstream effects—thermal headroom, stability margin, field reliability, and lifecycle degradation—become the primary constraints on system scaling (電力消耗成為產業發展瓶頸). The limiting factor is no longer only compute capability, but the ability to deliver, convert, distribute, and govern power efficiently across operating regimes.

1.2 Scope: "Throttling" as the Focus Area (節流)

Power constraints can be addressed through two macro paths: sourcing expansion ("open-source" / 開源) and consumption reduction ("throttling" / 節流). This document focuses exclusively on throttling: engineering mechanisms that reduce effective power loss and improve operational power quality without requiring upstream generation or grid expansion decisions.
Non-goals include energy generation strategy, grid capacity planning, or macro policy. The scope is board/system power governance, telemetry, evidence traceability, and a silicon roadmap that enables deployable control at scale.

PoE PD (IEEE 802.3) is treated as a **mandatory input interface** in the XR-VPP board context; PoE power-class derating profiles are used as one of the reference baselines for rail budgeting and RT sizing.

- **Key Claims / Engineering Claims)**
  XR-VPP silicon is specified as a **dual-domain integration**: (1) **Digital Governance** (telemetry, evidence logging, policy/profile versioning, rollback guardrails, host/EC boundary) and (2) **Board-level Power-Path Integration** (DC input diversity & convergence, isolation/reverse-block, priority/failover, transient shaping with RT engagement, and sharing-readiness). Without the second domain, the device reduces to a monitoring/governance component and cannot claim measurable peak-support envelope gains under transient windows.

- **Mandatory Interfaces)**
  PoE PD (IEEE 802.3) is treated as a **mandatory input interface** in the XR-VPP board context. The

baseline rail budget (P_base) used in RT sizing references a **PoE 802.3at 90W class system derating profile**, and is explicitly replaceable by product/rail-specific baseline budgets while keeping the same sizing chain.

本規格所定義之 XR-VPP silicon 為 **dual-domain integration**：其一為 **Digital Governance**（telemetry/evidence/policy-profile/versioning/rollback guardrails），其二為 **Board-level Power-Path Integration**（DC input diversity & convergence、isolation/reverse-block、priority/failover、RT engagement 與 sharing-readiness）。此雙域整合使平台可在既定電壓窗與時間窗內，將 transient peak-support envelope 由基準負載上推至可計算且可驗證的上緣（見 Table ES-RT-01）。

1.3 Throttling Framework: Redundancy + Efficiency Governance

Throttling is structured around two engineering levers:

1.3.1 Multi-Input Redundancy as a Sufficient Condition for Continuity

Multi-input power paths with controlled switching allow the system to maintain continuity when any source experiences brownout, quality degradation, or supply loss. Redundancy (冗餘) is treated as a sufficient condition for continuity when combined with deterministic guardrails: isolation/reverse-block, priority/failover, and controlled transient behavior during switching. The objective is to convert “power uncertainty” into a governed state machine with measurable outcomes.

- **Scope / Mandatory Interfaces)**
  PoE PD (IEEE 802.3) is treated as a **mandatory input interface** in the XR-VPP board context. The baseline rail budget (P_base) used in RT sizing references a **PoE 802.3at 90W class system derating profile**, and is explicitly replaceable by product/rail-specific baseline budgets while keeping the same sizing chain.

1.3.2 Efficiency as the Dominant Variable Under Light-Load and Transient

Conventional efficiency tuning often targets steady-state operating points. However, real systems spend substantial time in light-load conditions and are frequently stressed by transient events. These regimes dominate average loss, heat accumulation, and long-term reliability impact.
Steady-state efficiency primarily influences ON/OFF success, stability margins, and baseline thermal load; light-load and transient efficiency determines average energy waste and often correlates with latent failure

signatures (例如瞬間 transient 造成的壓力與失效徵兆). Therefore, the core technical problem becomes: how to increase average efficiency while preserving deterministic safety and stability.

1.3.3 Limitation of 80 PLUS and the “Efficiency Blind Spots”

80 PLUS certifications are widely used to communicate PSU efficiency, but the methodology is fundamentally steady-state and point-sampled. It evaluates conversion efficiency at a small set of fixed operating points (e.g., defined load percentages under controlled conditions) and therefore **does not represent how efficiency behaves in two dominant real-world regimes: light-load and transient.**（80 PLUS 的測試框架本質上是穩態、少數負載點的取樣，對真實運行的兩個關鍵區域覆蓋不足。）

The first blind spot is light-load efficiency. A large portion of deployed systems spend substantial time far below rated load due to duty cycles, idle windows, and power management states. In this regime, conventional control schemes may enter discontinuous or burst/skip-like modes, where losses are no longer proportional to load and the effective efficiency can degrade sharply. **This becomes a primary driver of average energy waste and long-term thermal accumulation.**（輕載區常是平均能耗與長時間熱累積的主因。）

The second blind spot is transient efficiency and stability during fast load steps and source switching. Transient events create short-duration but high-stress conditions—voltage droop/overshoot, control-loop saturation, protection threshold crossings, and rapid topology/mode transitions. These events are often where **efficiency governance “escapes” the steady-state assumptions** and where pre-fault signatures accumulate.（瞬態是效率與穩定性最容易脫離穩態假設、並累積失效徵兆的區域。）

Therefore, efficiency governance must be defined as a regime-aware control problem, not a single-number certification result. The engineering objective is to govern efficiency across (1) steady-state, (2) light-load, and (3) transient regimes with measurable telemetry and evidence-traceable actions. This is the core motivation for XR-PMC’s AI-governed power control and its FPGA-to-programmable-ASIC roadmap.（效率治理必須跨區間閉環、可量測、可追溯，而不是只用單一認證數字描述。）

Table 1–1 Steady-State Certification vs Regime-Aware Governance（穩態認證 vs 跨區間效率治理）

Item	80 PLUS / Point-Sampled Efficiency（認證式效率表達）	Regime-Aware Governance（跨區間治理：XR-PMC 目標）
Primary intent（目的）	Communicate steady-state conversion efficiency at fixed load points（以固定負載點描述穩態轉換效率）	Govern efficiency + stability + reliability across regimes（跨穩態/輕載/瞬態治理效率、穩定性、可靠度）

Coverage in load domain（負載域覆蓋）	A few steady-state points (e.g., 20/50/100%)（少數穩態點）	Continuous light-load → rated load, with defined mode boundaries（連續負載域，含模式邊界）
Light-load behavior（輕載行為）	Often not a primary focus; blind spot for real duty cycles（對真實 duty cycle 常是盲區）	Explicit targets for low-load modes (skip/burst/DCM, etc.) with measurable loss accounting（明確定義輕載模式目標與損耗核算）
Transient handling（瞬態處理）	Not represented by point sampling（不表達瞬態）	Explicit transient governance: load-step / source-switch / droop-overshoot control + evidence（納入負載步階/切換/壓降-過衝治理與證據鏈）
What “efficiency” means（效率定義）	Steady-state η at defined test points（定點 η）	Time-weighted and event-weighted efficiency + risk-weighted impact（時間加權/事件加權效率，並納入風險權重）
Telemetry requirements（遙測要求）	Minimal for certification（認證不要求系統級遙測閉環）	Mandatory telemetry schema: V/I/T, mode, state transitions, event stamps（必備遙測 schema）
Evidence & traceability（證據與可追溯）	Not part of the model（不屬於模型）	Evidence chain: snapshots, reason codes, integrity (hash/counter), rollback guardrails（證據鏈與完整性/防回滾）
Engineering validation（工程驗證）	Lab steady-state measurement at fixed points（實驗室定點量測）	Multi-regime validation: HIL/fault injection + field reproducibility packages（跨區間驗證：故障注入/HIL/可重現證據包）
Deployment implication（部署含義）	A label for PSU class comparison（產品等級標示）	A control stack and silicon roadmap (FPGA→Programmable ASIC) enabling system-scale governance（控制堆疊 + 矽路線：FPGA→可程式 ASIC）

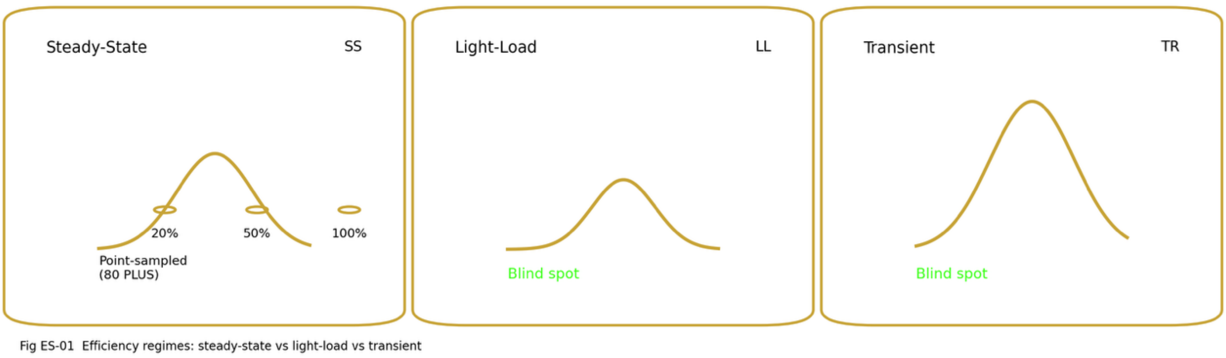


Figure 1–1 Efficiency Regimes: Steady-State vs Light-Load vs Transient

1.4 Ride-Through (RT) as the Board-Level Enabler for LL/TR Governance（RT：跨輕載/瞬態治理的板階使能）

RT（Ride-Through）在本文件在主機**板階（board-level）為實體能量緩衝模組**，由 XR-PMC 納入治理（governance）範圍，而非作為矽內（in-silicon）功率級整合項。基線配置為**電容串聯模組（series capacitor bank module），總電容量規劃 1.0–1.5 F**，部署於電源路徑上以吸收**切換瞬態（switchover）、負載步階（load-step transient）與短時跌落（short brownout window）**所造成的能量缺口。

整體定義 Global Insert (RT definition):
RT (Ride-Through / Hold-Up) in this document refers to an **external energy-buffer module** (e.g., supercap bank, bulk hold-up capacitance, UPS/battery at higher tiers). RT is **not integrated inside XR-PMC silicon**. XR-PMC provides RT **engagement semantics (Trigger/Hold/Exit)**, **guardrails**, **telemetry**, **evidence events**, and required **power-path control hooks** to coordinate with the external buffer.
（RT 指外部能量緩衝模組，不集成於 XR-PMC；XR-PMC 提供觸發語意、護欄、遙測、證據事件與控制鉤子。）

下表 Table 1-2 uantifies RT sizing using a 27V→24V window and 500ms boost; **P_base=71W** is a baseline rail budget referenced from a **PoE IEEE 802.3at (90W class) system derating profile**, and is replaceable by product/rail-specific baseline budgets while keeping the same sizing chain.
（ES-RT-01 以 27→24V 能量窗與 500ms 時域量化 RT sizing；P_base=71W 取自 PoE 802.3at（90W class）系統 derating profile 的基準負載，可替換為各產品/rail 的 baseline。）

Table 1–2 以 27→24V 能量窗與 500ms 時域量化 RT sizing；P_base=71W 取自 PoE 802.3at（90W class）系統 derating profile 的基準負載，可替換為各產品/rail 的 baseline。

- Demonstrate transient peak-support envelope from ~71W baseline to ~209W (1.0F) / ~278W (1.5F) @500ms under defined V-window, with evidence completeness.”
- This table specifies the **external RT module** interface contract (guardrails/telemetry/evidence) and its verifiable ranges; XR-PMC implements the semantics and hooks, while the energy buffer remains a separate module.

1.4.1 Why RT is mandatory for TR（為何 TR 必須有 RT）

在 TR（Transient）區域，系統的關鍵約束不是「穩態效率點」，而是**瞬態生存條件（survival constraints）**：電壓壓降/過衝、保護觸發次序、切換時間窗、以及對關鍵負載（critical rails）的維持能

Table ES-RT-01 RT module baseline sizing (27V→24V window, 500ms boost)

SuperCAP config (10S)	C_eq	V-window	E_cap (J)	E_use (J)	ΔP @500ms (W)	P_peak (W)	Positioning
10F cell ×10	1.0 F	27→24 V	76.5	68.9	138.0	209.0	Sweet spot / Base (180W@500ms margin)
15F cell ×10	1.5 F	27→24 V	114.8	103.3	206.6	277.6	Performance / Headroom (smaller droop / longer RT / aging margin)

Definitions / Assumptions

- $E_{cap} = \frac{1}{2} C_{eq}(V_{hi}^2 - V_{lo}^2)$, $V_{hi} = 27V$, $V_{lo} = 24V$
- $E_{use} = E_{cap} \cdot \eta$, $\eta = 0.90$ (path loss + ESR + guardband)
- $\Delta P \approx \frac{E_{use}}{0.5s}$, $P_{peak} \approx P_{base} + \Delta P$
- $P_{base} = 71W$ baseline rail budget (IEEE 802.3at 90W class, system derating profile)

Note: Replace P_base with product/rail-specific baseline budget while keeping the same sizing chain.

力。RT 提供可治理的 hold-up 能量，使 XR-PMC 能以可量測的護欄（guardrails）控制瞬態行為，避免以過度保守的穩態 margin（oversizing / aggressive throttling / early cut-off）來換取瞬態穩定。

1.4.2 How RT supports LL efficiency without becoming the LL “cause”（RT 如何支援輕載效率但不誤寫因果）

LL（Light-Load）效率的主因為**轉換器工作模式與控制策略**（例如 burst/skip、相位裁撤、死區與 gate timing、同步整流策略等）。RT 不是 LL 效率的唯一來源，但 RT 提供額外自由度：在輕載與短暫負載躍升/回落期間，允許系統維持更高效率的 operating mode，並以 RT 吸收短時能量擾動，降低 mode thrashing 與保護門檻過度抬高的代價。

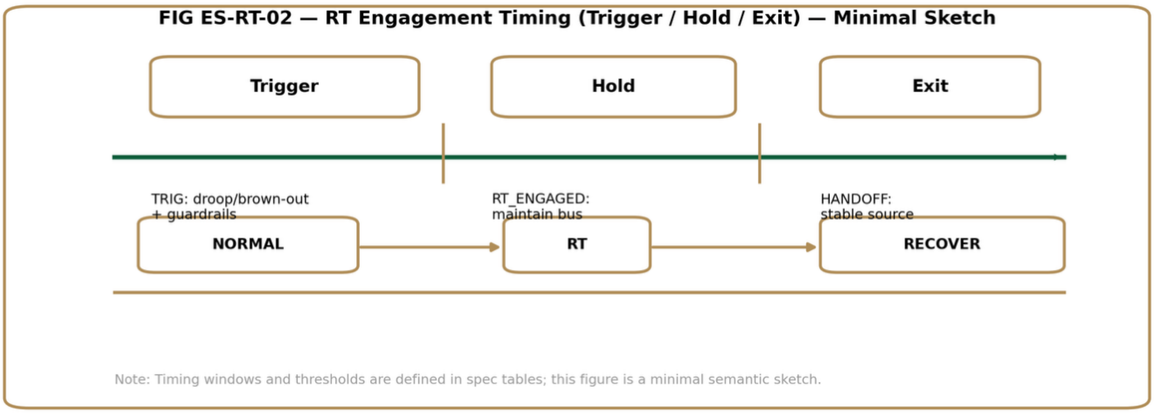


Figure 1–2

LL/TR governance assumes a board-level RT energy buffer (1.0–1.5 F series capacitor bank) under XR-PMC guardrails; TR constraints are treated as transient survival conditions rather than steady-state margining." （LL/TR 治理假設板級 RT（1.0–1.5F 串聯電容模組）受 XR-PMC 護欄控制；TR 約束以瞬態生存條件處理，而非以穩態加大 margin 取代。）

1.5 Why AI Is Required: Algorithm Guardrails + Machine Learning Optimization

Efficiency governance requires closed-loop reasoning across multi-dimensional signals (voltage/current/temperature/time-to-event/topology state). This cannot be addressed by static heuristics alone without over-conservatism. The required AI stack is explicitly split:

1.5.1 Algorithm (Deterministic Control & Guardrails)

Algorithms define safe operating envelopes and enforce hard constraints: protection sequencing, topology switching rules, timing guardrails, failover behavior, and rollback prevention. This layer is deterministic, auditable, and designed to remain stable across product lifecycles.

1.5.2 Machine Learning (Adaptive Efficiency & Pre-Fault Signatures)

Machine learning operates within algorithmic guardrails to improve average efficiency and detect pre-fault signatures. ML is used to select among a finite set of validated timing/topology options (有限 topology catalog) and to adapt thresholds based on observed evidence, without turning the system into an uncontrolled "self-modifying" device.

This document treats "programmability" as a mechanism for product differentiation across industries and deployments (不同產業 / 不同產品最佳化), not as a requirement for frequent updates. Updates are expected to be rare and evidence-triggered: when a previously unknown failure mode is discovered (historically NTF-like), the response is either (a) selecting a different pre-validated topology/timing profile, or (b) a silicon revision if a circuit-level change is required.

Table 1–3 AI Split Matrix: Algorithm vs ML (Scope / Inputs / Outputs / Guardrails)

Dimension	Algorithm (Deterministic Guardrails)	Machine Learning (Optimization & Signatures)
Primary purpose	Enforce safety, stability, and provable behaviors under all conditions（安全/穩定/可證明行為）	Improve average efficiency and detect pre-fault signatures within guardrails（提升平均效率/辨識失效徵兆）
Scope boundary	Hard constraints + state machines: protection sequencing, topology switching rules, timing guardrails, failover logic（保護序列/切換規則/時序護欄/故障切換）	Parameter selection + classification/regression within a finite validated option set（在有限候選集合內做參數/分類/回歸）
Operating regimes covered	Mandatory across all regimes (SS/LL/TR) as the safety envelope（全區間必備護欄）	Focus on LL/TR optimization and signature detection; SS used for baseline learning if needed（偏重輕載/瞬態最佳化與徵兆偵測）
Control authority	Direct actuation permission and veto rights; cannot be overridden by ML（具有否決權，ML 不可越權）	Suggest / select actions only when permitted by Algorithm; no direct override（僅在許可範圍內建議/選擇）
Typical inputs	Telemetry: V/I/T, rails status, source quality, fault flags; system state, mode, counters; integrity signals（遙測/狀態/故障旗標/完整性訊號）	Feature vectors derived from telemetry windows, event snapshots, historical evidence packages（由遙測窗與事件快照衍生特徵）
Feature formation	Rule-based features for thresholds and deterministic decisions（規則式特徵/門檻）	Learned features or engineered features validated by evidence; includes temporal features (ΔI/Δt, dwell time)（含時間特徵、變化率、停留時間）
Outputs	State transitions, enable/disable of modes, topology/timing option selection constraints, protection actions, failover commands（狀態轉移/模式使能/保護動作/切換指令）	Ranked candidate actions within allowed set; risk score / anomaly score; signature tags for evidence（候選排序/風險分數/異常分數/徵兆標籤）
Timing behavior	Deterministic latency bounds; worst-case safe response guaranteed（可證明的延遲上界）	Best-effort inference timing; bounded by service budget; can be disabled without losing safety（可退化/可停用，不影響安全）
Update philosophy	Rare changes; driven by spec evolution or silicon revision; strict regression gates（極少變更，需嚴格回歸驗證）	Updates are not “frequent by default”; used for cross-product differentiation and rare evidence-triggered patches（非頻繁更新定位；差異化＋證據觸發補丁）
Versioning unit	Policy core version, guardrail ruleset version, timing topology catalog version（護欄規則/拓樸目錄版本）	Model version, feature pack version, profile pack version (per industry/product)（模型/特徵包/Profile 包版本）
Rollback & compatibility	Mandatory: anti-rollback, compatibility matrix, safe defaults on mismatch（必備防回滾與相容矩陣）	Mandatory: model/profile rollback, bounded behavior under version mismatch（必備回滾；版本不匹配時需有界行為）

Evidence requirement	Every non-trivial action must be evidence-traceable (reason code + snapshot)（動作需可追溯：原因碼 + 快照）	Training/inference decisions must be auditable via evidence references; store signature context minimal set（決策需可稽核：保存最小上下文）
Failure mode handling	Guarantees safe fallback states; defines “no-regret” actions（保證安全退化路徑）	Flags unknown patterns; elevates to Algorithm-defined safe handling; generates candidate hypotheses（標記未知型態→交給護欄處置並產生假設）
Security & abuse resistance	Enforces service-mode gating, privilege separation, tamper detection, monotonic counters（權限分離/防竄改/單調計數）	Model/profile loading subject to same security chain; no hidden channels（同一安全鏈約束）
Verification & test	Formal checks where applicable; exhaustive state-machine tests; fault injection coverage（狀態機/故障注入/覆蓋率）	Offline validation + shadow-mode evaluation; acceptance gates tied to measurable deltas and no safety regression（離線驗證/影子模式；門檻以可量測提升且不影響安全）

Notes / Definitions（簡短補充）:

SS/LL/TR = Steady-State / Light-Load / Transient（穩態/輕載/瞬態）

“Finite validated option set” refers to a pre-qualified catalog of timing/topology profiles selectable at runtime（有限可選集合 = 事先驗證合格的拓樸/時序組合目錄）

1.6 Coverage: From System-Level Governance to Board-Level Control

The engineering approach is defined top-down (system → board → silicon) to ensure that power governance is consistent across nodes and can be aggregated into an operational dashboard with meaningful causality. Coverage is structured by application classes:

1.6.1 A1 — Mainboard AI-PMC (主機板 PMC)

Board-level power governance integrated near the system load, coordinating input options and local power policies.

1.6.2 A2-S — PSU Secondary-Side PMC (電源二次側)

Secondary-side governance for conversion efficiency, transient behavior, and evidence-driven diagnostics in the regulated output domain.

1.6.3 A2-P — PSU Primary-Side PMC (電源一次側，Optional Track)

Primary-side governance is treated as an optional, higher-impact track. If governance is limited to secondary-side only, primary-side efficiency and failure-mode control may remain as blind spots (“漏網之魚”), especially for losses and degradations upstream of regulation. The primary-side track therefore requires explicit entry criteria, safety boundaries, and verification gates.

1.6.4 A3 — Redundancy Backplane PMC (冗餘背板)

Backplane orchestration introduces active load sharing, failover, and hot-swap governance across multiple supplies. This domain must coordinate three control planes: mainboard PMC, backplane PMC, and PSU internal PMC (含 adapter 與 redundancy PSU).

1.6.5 A4 — Power Grid Node / Substation IPC Context (電網節點)

Upstream grid nodes and substation automation environments (SCADA/RTU/IED contexts) are included as an extension domain where governed telemetry and evidence chains can increase operational value.

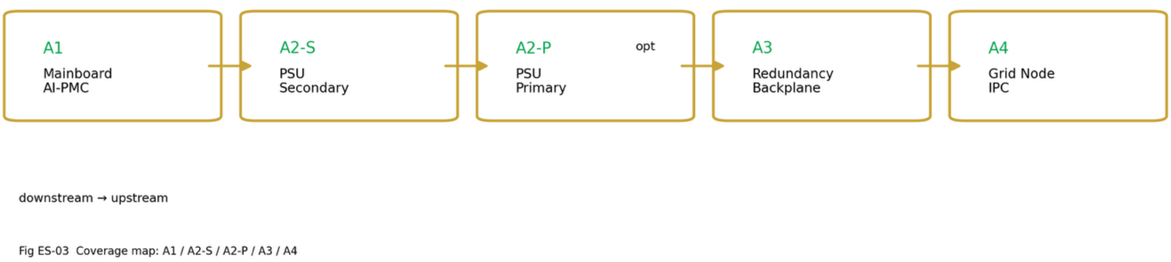


Figure 1–3 Coverage Map: A1 / A2-S / A2-P / A3 / A4

These nodes typically host industrial control computing functions and can act as aggregation points for power-quality and efficiency governance.

1.7 Silicon Roadmap: FPGA to Programmable ASIC

The silicon strategy is staged to minimize risk while preserving a coherent architecture:

1.7.1 Phase-1 FPGA: Wide-Coverage Validation (同步覆蓋、先驗證交集)

FPGA is used to validate the common-core contracts across application classes in parallel, focusing on the intersection between FPGA and ASIC: telemetry schema, evidence chain, governance state machines, service mode, and host integration boundaries. The goal is to freeze interface contracts and verification methods before committing to silicon.

1.7.2 Phase-2 Programmable ASIC: Roadmap-Partitioned Productization

Programmable ASIC implementation follows a product-first sequence:
(1) A1 mainboard AI-PMC → (2) A2-S secondary-side PMC → (3) A2-P primary-side optional track → (4) A3

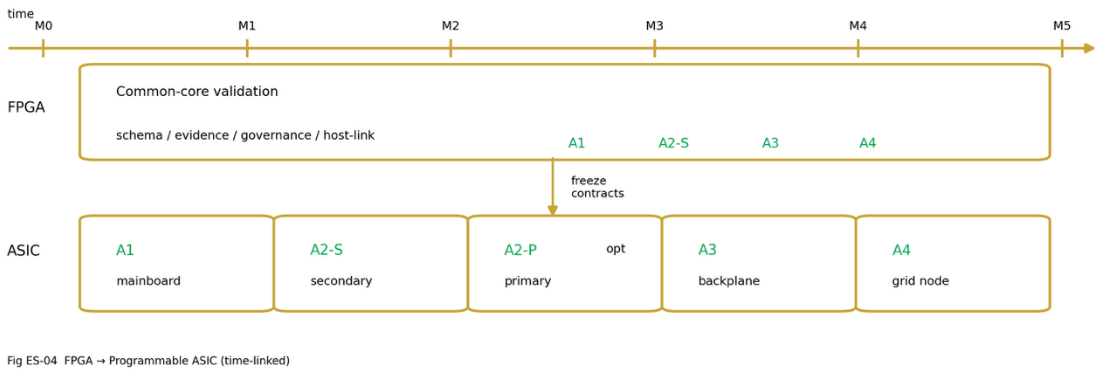


Figure 1–4 Roadmap Snapshot: FPGA→Programmable ASIC (Time-Linked)

redundancy backplane PMC → (5) A4 grid node extension.

Common-core modules are reused; differences are encapsulated as variant modules (相同點模組化、差異點配套化), enabling one coherent roadmap across multiple products.

1.8 Fixed Insert: Bus+Tap ASIC FBD (Final)

The Bus+Tap visual language (BARS + TAB) is a fixed reference artifact for the silicon-level functional partitioning and is inserted without modification.

【PLACEHOLDER-FIG-ES-06 | Bus+Tap ASIC FBD Final (BARS + TAB, Fixed Insert)】

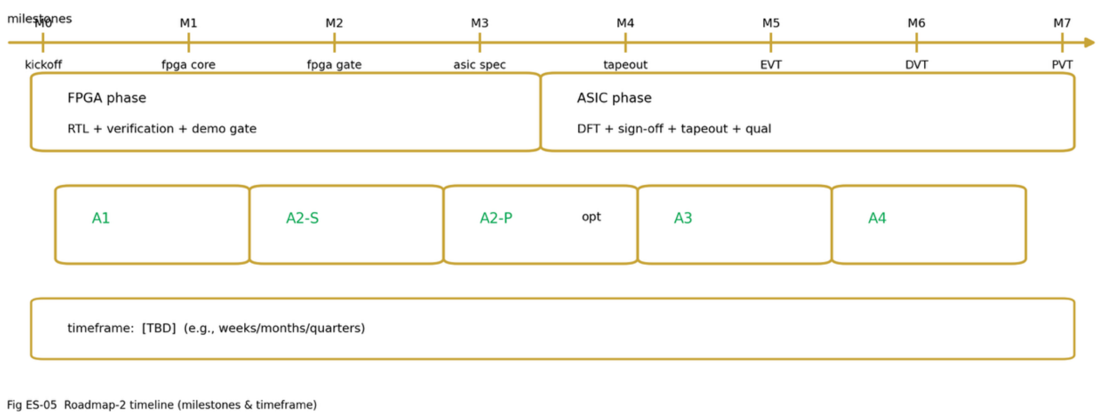


Figure 1–5 Roadmap-2 Timeline (Milestones & Timeframe)

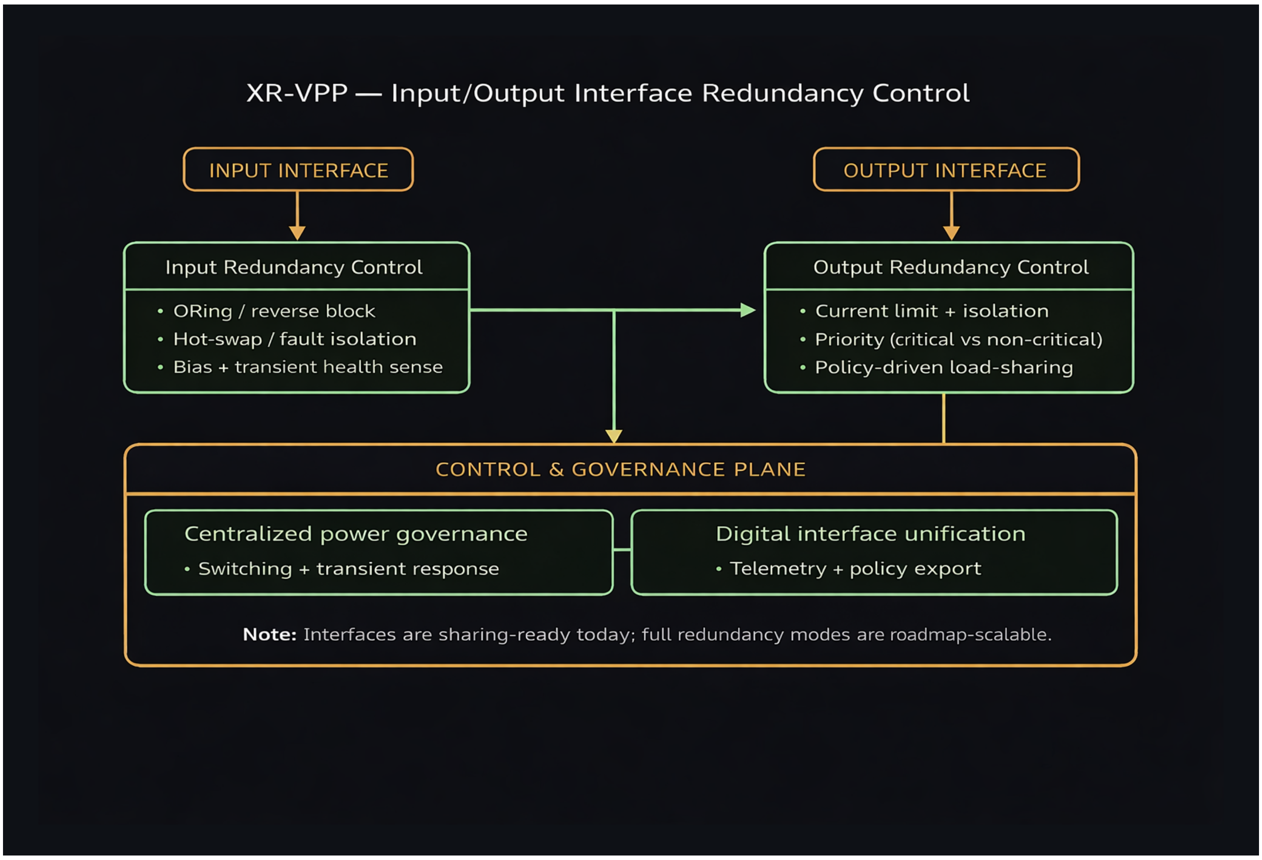


Figure 1–6 Functional Block Diagram

1.9 Key Claims (Engineering-Verifiable)

The following claims are explicitly framed as verifiable engineering outcomes, not marketing statements:

1.9.1 Efficiency Governance Must Address Light-Load and Transient

Average efficiency gains require governance beyond steady-state tuning; transient and light-load regimes must be managed with evidence-driven control.

1.9.2 Redundancy Requires Deterministic Guardrails to Be Operationally Meaningful

Multi-input redundancy becomes an engineering lever only when isolation, failover rules, and switching transients are governed by deterministic policies and validated measurements.

1.9.3 AI Requires a Two-Part Structure: Guardrails + Optimization

Algorithmic guardrails ensure safety and auditability; ML operates within a finite validated topology/timing catalog to improve efficiency and detect pre-fault signatures.

1.9.4 Evidence Chain Is a First-Class Deliverable

Telemetry, event schemas, snapshot structure, integrity checks, and rollback guardrails are core deliverables enabling reproducibility, field diagnostics, and lifecycle governance.

Table 1–4 Key Claims Summary (Claim / Verification Method / Deliverable)

Claim（主張）	**Verification Method（驗證方法）**	**Deliverable（交付物）**
Dual-domain integration：XR-VPP silicon 同時涵蓋 Digital Governance（telemetry/evidence/policy-profile/versioning/rollback guardrails）與 Board-level Power-Path Integration（DC input diversity	Spec traceability：將功能需求映射至 Architecture（Physical/Semantic/Governance/Settlement）與 FPGA/ASIC feature matrix；以 reference board 與 test plan 驗證每一項 control path 與 evidence schema 可落地。	1) Feature-to-Architecture Trace Matrix；2) FPGA demo bitstream + test report；3) ASIC requirement spec

& convergence、isolation/reverse-block、priority/failover、RT engagement、sharing-readiness）。		（含接口與資料結構版本規則）。
Transient peak-support envelope 可量化：在 27V→24V 能量窗與 500ms 時域下，RT（1.0–1.5F series capacitor bank）可提供 ΔP，使 P_peak 由 P_base 上推至 ~209W（1.0F）/ ~278W（1.5F） 上緣。	Bench measurement：programmable load step + brownout injector + scope/current probe；以固定 V-window/時間窗量測 droop/overshoot、RT 觸發/退出時間、ΔP 與 P_peak；與 sizing model 對照（η、ESR/路徑損耗保守量）。	1) Table ES-RT-01（PNG） sizing baseline；2) Lab report（waveforms + computed ΔP/P_peak）；3) RT event logs（reason code + snapshot）。
PoE PD 為 board-level mandatory input interface（IEEE 802.3）；rail budgeting 與 RT sizing 的 baseline 可引用 PoE class derating profile（例如 802.3at 90W class），並允許以產品/rail-specific baseline 替換而不改變 sizing chain。	Interface compliance + system budgeting review：PoE PD 供電階層與 derating 假設在文件中可追溯；在 reference platform 以 PoE source、load envelope 與 telemetry 對齊驗證。	1) PoE PD interface spec（適用範圍與假設）；2) Derating baseline note（可替換欄位）；3) Telemetry schema 對應 PoE power class/limits。
Evidence-first governance：所有 power-path critical events（switchover、isolation、RT engagement、fault isolation、policy transitions）皆輸出 versioned telemetry schema 與 evidence event（reason code + snapshot），並具備 rollback guardrails。	Conformance test：事件觸發覆蓋率（coverage）、payload 欄位完整性、schema version compatibility、rollback 行為（old profile / new profile）在 host/EC 端可重放（replay）與可審計（audit）。	1) JSON telemetry/event schema（含版本策略）；2) SDK/API + sample parser；3) Evidence log bundle（可重放資料集）。
FPGA→Programmable ASIC 可交付：FPGA 階段先驗證共用 IP 與治理/控制閉環；Programmable ASIC 階段以 profile/microcode/firmware 方式支援不同產業/產品差異化，變更以「明確 failure mode 驅動」為主而非頻繁更新。	Stage-gated demo：FPGA demo gate（功能閉環 + 可量測指標 + evidence）；ASIC readiness review（IP selection、DFT、sign-off checklist、tape-out package completeness）。	1) FPGA demo gate checklist + demo package；2) ASIC spec pack（interfaces, memories, DFT hooks, security）；3) Implementation & Foundry readiness checklist。

- Verification Method：以「可量測指標 + 測試條件 + 門檻」描述，不以口號描述。
- Deliverable：以「文件/規格/工具/測試包/日誌」形式具體交付，並可版本化（versioned）。
- RT is specified as an **external module**; XR-PMC defines only the **control/evidence contract** and verification gates, not the energy buffer itself.
  （RT 為外部模組；XR-PMC 定義控制/證據合約與驗證門檻，不定義能量元件本體。）

1.10 Adoption Models Snapshot (Retrofit vs Greenfield)

Adoption is defined at the specification level:

Retrofit: integrates digital governance on the existing board power control plane while preserving the legacy system controller boundary.

Greenfield: extends governance into the system controller architecture (including EC/PEC integration) with unified evidence and policy management across nodes.

定義前置（納入表格註解/表前說明）：本規格中 Retrofit 與 Greenfield 的區分**不以「是否需要改 layout」為準**。XR-VPP 涉及 input 增設、RT 能量緩衝與 failover power-path，板級實作多數情境下必然需要 layout rework。兩者的分界在於 **系統治理邊界（governance boundary）是否重構**：是否將 EC/PEC 納入治理核心與端到端 contract。

Table 1–5 Adoption Models: Retrofit vs Greenfield

Dimension	Retrofit（Board Retrofit）	Greenfield（System Greenfield）
Governance boundary（治理邊界）	**不重構**既有 Host/EC 架構；XR-PMC 作為板級外掛治理（overlay governance）。	**重構**系統治理邊界；XR-PMC 與 EC/PEC 形成統一治理迴路（system governance loop）。
Board change（板級變更）	需要：新增 XR-PMC、input diversity/convergence、isolation/reverse-block、RT cap bank、failover switches；保留原系統主 power architecture。	需要：同左，但可同步重塑 power architecture contract（rail partitioning、fault containment、service mode）。
Host/EC impact（系統端改動）	**最小化整合**：driver + telemetry/event ingestion；不要求 EC/OS 架構重寫。	**深度整合**：policy/profile/evidence schema 成為系統設計一部分；EC/PEC 需支援治理接口、服務模式與升級策略。
Evidence & telemetry（證據/遙測）	XR-PMC 產生 versioned events/schema；Host/EC 僅需接收、儲存、上報。	全系統一致的 schema 與 evidence chain；EC/PEC 參與事件關聯、策略分發與審計。
Power-path capabilities（電源路徑能力）	聚焦板級：input priority/failover、RT engagement、保護護欄；active sharing 以「準備度」為主。	可擴展到多節點：主機板 + 背板 + PSU（二次側→一次側）+ 上游節點的協同治理與 sharing 策略。

Verification scope（驗證範圍）	以板級閉環驗證為主：TR/RT、switchover、fault isolation、evidence completeness。	以端到端驗證為主：多節點協同、策略一致性、故障域隔離、升級/rollback 的全域一致性。
Time-to-adopt（導入時程）	較短：以 reference board + limited integration 快速導入量產變更。	較長：需同步更新系統設計規格、EC/PEC、驗證流程與量產測試策略。
Manufacturing/test impact（量產/測試影響）	增加板級測試項（RT/切換/事件記錄）與校準流程；系統測試變更較小。	需重整系統級測試與服務模式（service mode）與 field diagnostics 流程。
Deliverables（交付物差異）	XR-PMC BSP/SDK、telemetry/event schema、板級驗證報告、reference design guide。	在 Retrofit 交付物之外，追加：EC/PEC integration spec、system contract、fleet governance hooks、全域升級/rollback 策略。
Typical fit（適用情境）	既有平台需快速補強：新增 input/RT/failover，且不想重做系統治理架構。	新平台/新世代產品：把電源治理視為系統核心能力，並規劃多節點協同治理路線。

Adoption Decision Checklist (Boundary change / Validation scope / Manufacturing impact / Field service mode)

Specification Notes（規格層級備註）

- Retrofit 的核心是「板上數位控制整合」：以 XR-PMC 取代/整合部分數位管理器件，建立統一 telemetry + evidence + guardrails。
- Greenfield 的核心是「治理架構內建」：將 EC/PEC 也納入一致的 policy/evidence/telemetry 與權限模型，形成可運營的治理平面。

1.11 What This Document Delivers

This document provides: (1) a product overview and market landscape anchored in engineering applicability, (2) a system-to-board functional architecture with fixed silicon FBD references, (3) an IP BOM and supplier benchmarking framework with cost estimation fields and RFQ datasets, (4) FPGA and Programmable ASIC specifications aligned to the two-roadmap plan, and (5) a time-linked validation and program plan suitable for a product development proposal.

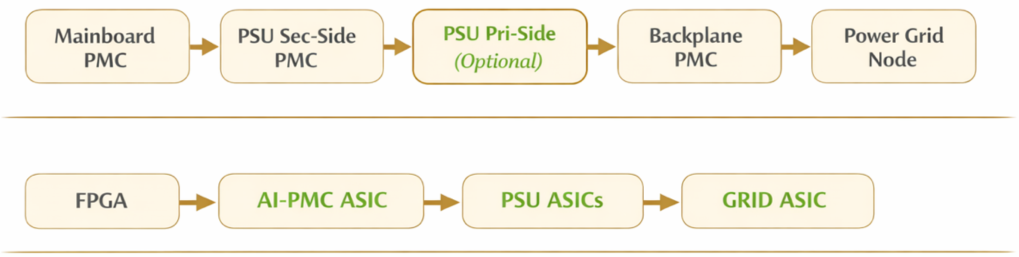


Figure 1–7 wo-Roadmap Snapshot (Power/Application + Silicon)

2 PRODUCT OVERVIEW

2.1 Product Definition and Positioning

XR-PMC（XR-VPP Silicon Line）為一顆面向電源路徑治理（power-path governance）的高整合數位控制晶片，定位於「板階（board-level）電源控制與治理」而非功率大元件整合。其核心價值在於：在不改動既有功率級（power stage：磁性元件、主功率開關、主要整流/變壓器等）的前提下，整合數位控制、遙測、事件與證據鏈（evidence chain）、以及可版本化的 policy/profile 管理，將冗餘切換與效率治理從「分散的點狀控制」提升為「可量測、可追溯、可回放、可部署」的治理能力。

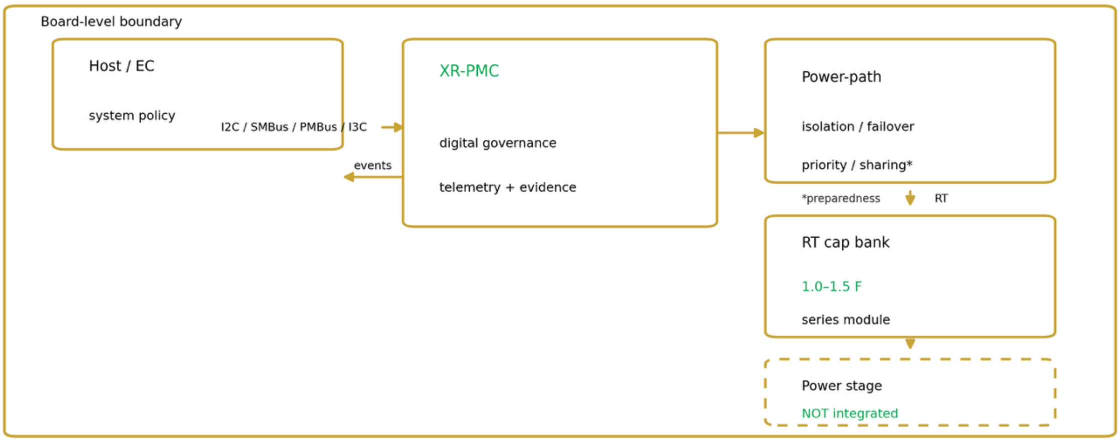


Fig PO-01 XR-PMC board-level role (incl. RT capacitor module)

Figure 2–1 XR-PMC Board-Level Role: Digital Governance vs Power Stage Boundary

2.2 Board-Level Role and Integration Boundary

2.2.1 Ride-Through (RT) Capacitor Module Under Governance

RT（Ride-Through）模組採用電容串聯（series）組態之板階儲能模組，容量規劃範圍為 **1.0–1.5 F**，用於電源缺口（brownout）、瞬間負載突變與切換瞬態期間的能量緩衝。RT 模組本體屬於「板階實體儲能元件」，不納入 XR-PMC 的功率大元件整合範疇；然而其 **充放電路徑、啟動/退出時序、保護護欄與事件證據** 必須納入 XR-PMC 的治理範圍，以確保：

切換瞬態期間的 droop/overshoot 被量測與受控；

RT 觸發條件、維持時間、退出條件具可追溯的原因碼與證據快照；

RT 相關失效風險（例如 ESR 漂移、漏電、充放電壓力與熱點）被納入 telemetry 與健康度監測；

在不同產品/產業 profile 下，RT 的啟動窗與時序拓樸可被選擇（selection）而非頻繁改寫（rewrite）。

Table 2–1 RT Capacitor Module Spec (Capacitance Range / ESR Targets / Charge-Discharge Guardrails / Telemetry / Evidence Events)

Category	Spec Item	Range / Baseline	Verification / Notes
Capacitance range（電容範圍）	Topology	Series bank (10S) supercap module	Balancing: passive baseline; active optional for high-reliability SKUs
	C_eq (effective)	**1.0–1.5 F**	1.0F = Base / 1.5F = Headroom（對應 ES-RT-01）
	Voltage window	**V_hi 26–28V / V_lo 23–25V**（default 27→24V）	Window is profile-controlled; must keep within rail safety limits
ESR targets（ESR 指標）	Module ESR @25°C	**8–25 mΩ**（module-level, at specified test freq）	4-wire + AC impedance @ 100–1000 Hz；以量產可測方法定義
	ESR vs temp drift	**≤+80% @ -20°C；≤+40% @ 60°C**（relative to 25°C)	用兩點/三點溫度測試建立 ESR-temperature curve
	Aging allowance	**Cap drop ≤20–35% @ EoL；ESR rise ≤50–120% @ EoL**	EoL: calendar + cycling；用「最差條件」覆蓋產品保固期
Charge/Discharge guardrails（充放電護欄）	Pre-charge / inrush control	Required; **I_inrush limited to 0.5–2.0 A**（system dependent）	Pre-charge timeout 0.3–2.0 s；不得造成 source brownout
	Charge current limit	**0.5–3.0 A**（cap bank charge path）	依 source 能力（PoE/adapter/PSU/backplane）調參
	Discharge current limit	**5–20 A**（短時）/ **2–10 A**（連續上限）	以熱點溫升與路徑電流額定決定；需防止保護誤觸發
	V_cap_min / V_cap_max	**V_cap_min 22–25V；V_cap_max 26–29V**	UV/OV 必須有 hysteresis（0.2–0.8V）避免振盪
	Engagement hold time	**200–800 ms**（default 500 ms）	Window 由 policy/profile 設定；需與切換時間窗一致
	Fail-safe	RT_ABORT within **1–10 ms** on RT fault	Fault: OVP/UVP/OTP/over-I/ESR anomaly; 需留下 evidence
Telemetry（遙測）	Required signals	**V_cap / V_rail / I_path / Temp_hotspot**（minimum）	I_cap、ESR proxy（可選）

	Sampling	**1–10 kS/s**（event window）; steady 10–200 S/s	event capture: pre 20–200 ms / post 200–800 ms
	Export buses	**I²C/SMBus mandatory**; PMBus/I3C optional	Interface map 綁定 BSP/SDK；schema must be versioned
Evidence events（證據事件）	Event IDs (fixed)	RT_TRIGGERED / RT_HOLD_ENTER / RT_HOLD_EXIT / RT_ABORT / RT_FAULT	必須包含 reason_code 與 snapshot
	reason_code	Enumerated, stable	Minimum set: dip/load-step/switchover/test/service/fault-class
	snapshot payload	Mandatory	thresholds + V/I/Temp traces + counters + timestamp (monotonic)
Interfaces（介面）	Control hooks	enable/disable, thresholds, window, hysteresis, limits	由 BSP/SDK 暴露；支援 rollback
	Service mode	force-RT / inhibit-RT / safe-discharge / self-test	製造與維修必備；不得影響 safety guardrails

Insert note：本表定義 RT 模組之「規格與可驗證欄位」，Sizing 量化依據與 1.0–1.5F 的選型理由見 **Table 1–2–2**；本表不重複 sizing 計算，僅定義工程可執行的 spec/targets/guardrails/telemetry/evidence。

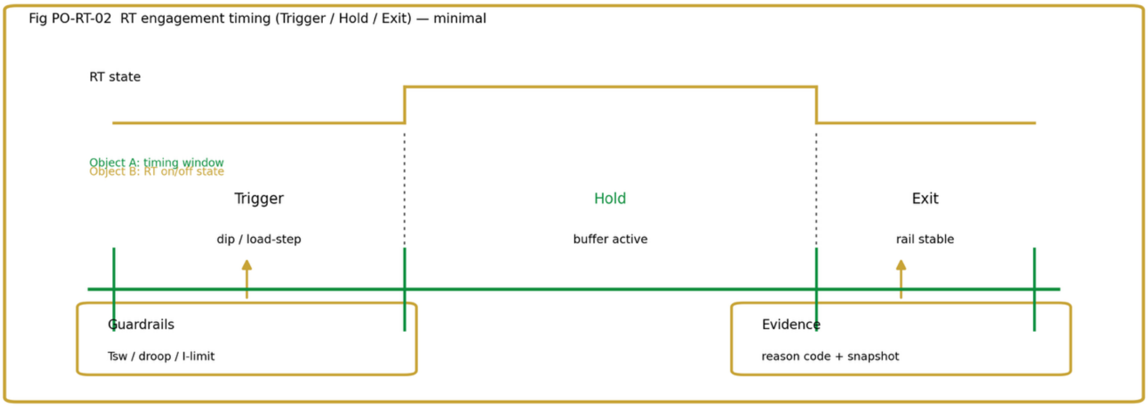


Figure 2–2 RT Engagement Timing (Trigger / Hold / Exit) — Minimal Timing Sketch

RT state represents **external buffer engagement**, not an on-die function.

2.2.2 What XR-PMC Integrates (Digital Domain)

XR-PMC 聚焦整合以下數位域功能模組：

- Multi-source input selection / redundancy control（多輸入冗餘與切換控制）
- Isolation / reverse-block / fault isolation guardrails（隔離/反灌阻斷/故障隔離護欄）
- Priority / failover policy enforcement（優先權與故障切換政策）
- Telemetry acquisition & normalization（遙測擷取與一致化）：I²C/SMBus/PMBus/I3C、ADC、GPIO/INT
- Evidence logging（證據記錄）：事件序列、快照、原因碼、完整性（hash/counter）、回放支援
- Policy / profile versioning and rollback guardrails（policy/profile 版本控管與防回滾）
- Host/EC link and service/debug modes（與 Host/EC 的連結、服務/除錯模式）

2.2.3 What XR-PMC Does NOT Integrate (Power Stage Non-Goals)

XR-PMC 不以整合功率大元件為目標，以下內容屬於明確 Non-Goals：

- 高功率磁性元件（inductors/transformers）、主功率 MOSFET/IGBT、主要整流與 PFC 主功率級
- PSU 內部 AC-DC 的主功率拓樸設計與其法規級安規責任
- 以「寫死 algorithm」的不可演進硬體控制邏輯（本產品為可程式化治理架構）

2.2.4 Host / EC / PEC Collaboration Boundary

XR-PMC 與 Host/EC（Embedded Controller）之間採用清晰邊界：

- XR-PMC：負責 power-path 的狀態機、護欄執行、遙測/證據鏈、受控的策略執行與回報
- Host/EC：負責系統層策略（例如 workload/power budget 協調）、平台級更新流程與運營策略
- Greenfield 模式下，可引入 PEC（Power Embedded Controller）概念，將部分治理與安全鏈收斂至平台控制層，但 XR-PMC 的護欄與證據鏈契約仍維持一致。

下表以 Authority（誰能決策/誰能下令）」與「Responsibility（誰必須提供/誰必須執行）」拆分 XR-PMC、Host CPU、EC（Embedded Controller）、PEC（Power/Policy Embedded Controller；Greenfield 情境）之邊界。Retrofit 主要對應 XR-PMC + Host/EC 的最小整合；Greenfield 會引入 PEC，形成 system governance loop。

Table 2–3 Boundary Matrix: XR-PMC vs Host/EC/PEC (Authority / Responsibilities / Interfaces)

Domain	**XR-PMC (ASIC/FPGA)**	**Host CPU (OS / App)**	**EC (Embedded Controller)**	**PEC (Power/Policy EC — Greenfield)**	**Interfaces / Artifacts**
Power-path	**Authority: Primary（**硬體	無直接控制；僅可讀狀態與策略版本	可參與 platform enable/sequence	**May coordinate**	GPIO/INT, ADC, power-path control

switching（輸入切換/匯流）	閉環；µs–ms）；執行 input priority/failover、reverse-block、hot-swap/fault isolation		（若既有）但不介入 fast loop	system-level sequencing；不進入 fast loop	pins；event: SWITCHOEVER_*
RT engagement（Ride-Through）	**Authority: Primary**（Trigger/Hold/Exit + guardrails）；輸出 evidence	僅設定 profile；可觸發 service mode（經 guardrails）	可觸發 service mode（制造/維修）	可下發 policy window（但不得繞過 guardrails）	Table PO-RT-01；Fig PO-RT-02；events: RT_*；telemetry traces
Current limiting / isolation（限流/隔離）	Authority: Primary（硬體保護優先）	無	可參與 enable/disable（平台安全）	可協同 fault domain policy	PMBus/SMBus regs；fault logs: OCP/OVP/UVP/OTP
Load sharing readiness（分享準備度）	提供 sharing hooks / measurement / policy knobs；可做 local control（視產品）	只做 fleet analytics / tuning	依平台而定（多為監控）	System-level coordination（多節點 sharing policy）	backplane/PSU interface spec；events: SHARE_*
Telemetry acquisition（遙測採集）	**Primary producer**：V/I/T/ESR proxy；sampling + event-window capture	consumer（dashboard/analytics）	consumer / forwarder	consumer / correlator	I^2C/SMBus mandatory；optional PMBus/I3C；schema versioning
Evidence logging（證據鏈）	**Primary producer**：reason_code + snapshot；monotonic counter	存檔/上傳/審計；fleet correlation	存檔/上傳（若無 OS）	**Correlator**（跨節點 evidence chain）	JSON event schema + version policy；hash/counter optional

Policy/profile mgmt（策略/配置）	enforce guardrails；apply profile; rollback-safe apply	Authority: Business/ops（選擇 profile pack、版本治理）	可作為 policy conduit（無 OS 平台）	Authority: Platform policy（Greenfield）	profile pack format；version/rollback rules；signing optional
Firmware / microcode update（韌體/微碼）	apply & attest; safe update; rollback	orchestrate update（fleet）	stage/trigger update（manufacturing/field）	orchestrate update（system governance）	secure boot optional；A/B slot；update manifest
Security boundary（安全邊界）	protect control registers; optional auth	userland / OS security	platform root-of-trust（若有）	platform root-of-trust	auth: challenge/response optional；key storage optional
Service mode（服務模式）	enforce safe service actions（force-RT / inhibit-RT / discharge）	UI/remote service tooling	manufacturing hooks / recovery	system service orchestration	service API + JTAG/UART access policy
Debug / DFT hooks（除錯/測試）	JTAG/DFT endpoints; production test registers	none	board bring-up support	system bring-up support	JTAG, boundary scan, DFT reports, test vectors
Compliance reporting（規範/一致性）	expose counters, limits, compliance telemetry	generate reports	assist	assist	standards map: PoE/PMBus/SMBus/I3C + test evidence

- Retrofit：PEC 欄位可視為 "N/A"；Host/EC 僅負責 profile 選擇、telemetry/event ingestion、與 service tooling。
- Greenfield：PEC 成為 policy/evidence correlation 的系統節點，但不得侵入 XR-PMC 的 fast protection loop（hard guardrails 仍由 XR-PMC 強制）。

2.3 Coverage Map — Application Tracks (Revised: RT as External Module)

2.3.1 A1 — Mainboard AI-PMC（主機板 PMC）

定位：IPC/POS 等系統主板的電源輸入治理與系統負載側之效率/可靠度治理；強調與 Host/EC 的最小侵入整合。

PoE / RT 適用範圍（Scope Note）：PoE PD（IEEE 802.3）在 A1 被定義為 **first-class input source**，與 adapter / battery / DC bus 同列，必須反映於 input diversity 介面定義與 rail budgeting baseline 假設。RT（Ride-Through / hold-up）在 A1 被定義為 **external energy-buffer module**（例如 supercap bank 或等效能量緩衝），**不被整合進 XR-PMC silicon**；XR-PMC 的責任在於 RT 的 **engagement semantics（Trigger/Hold/Exit）**、護欄（guardrails）、遙測（telemetry）與證據事件（evidence events），並提供與 power-path 的控制鉤子以保障切換連續性與 transient/light-load 條件下的穩定治理。RT sizing 與 timing 語意分別引用 **Table ES-RT-01** 與 **Fig PO-RT-02**。

2.3.2 A2-S — PSU Secondary-Side PMC（二次側）

定位：在 regulated DC domain 內進行效率治理、瞬態治理與可觀測性；支援 evidence-driven 的故障徵兆分析。

PoE / RT 適用範圍（Scope Note）：A2-S 位於受控 DC 域，PoE 不是此 stage 的必要介面需求，僅可作為上游供電類別（supply class）的參考基線。Ride-through/backup 在 A2-S 屬於 **secondary-side energy buffering / hold-up capacity**（外部或 PSU 內部的大電容、supercap、或等效緩衝設計），其目標是 load-step response、短時 brownout buffering 與事件窗（event-window）證據擷取。XR-PMC 在此 track 的角色為：對外部/內建緩衝元件提供 **control hooks + guardrails + evidence schema**，確保 transient 行為可被量測、可被審計、可與故障徵兆分析閉環對齊。

2.3.3 A2-P — PSU Primary-Side PMC（一次側，Optional Track）

定位：針對 AC-DC 前段與一次側損耗/失效盲區提供治理；必須以明確的進入條件與安規/隔離邊界規格化。

PoE / RT 適用範圍（Scope Note）：A2-P 的核心是一次側（regulation 前）之 loss/efficiency 與

failure blind spots；ride-through/backup 應以 **primary-side hold-up energy management**（外部 UPS、PFC/母線儲能、或等效 hold-up capacity 管理）方式表述，而非沿用板級 supercap sizing。所有一次側之 ride-through/hold-up 相關控制，必須先由 **entry conditions**、隔離邊界（isolation boundary）與 compliance-driven guardrails 定義其可行範圍；XR-PMC 的責任在於提供可驗證的遙測/證據鏈與保護邊界控制語意，避免因隔離/安規限制導致治理不可落地。

2.3.4 A3 — Redundancy Backplane PMC（冗餘背板）

定位：主動分流（active load sharing）、冗餘切換仲裁與多控制平面協作；要求明確權限模型（mainboard/backplane/PSU PMC）。

PoE / RT 適用範圍（Scope Note）：PoE 非 A3 的必要介面。Ride-through/backup 在 A3 必須保留，且其定位為 **system continuity insurance**：在 active load sharing 仲裁與 source switching transient 期間，透過背板端外部能量緩衝（shared buffer）、或與 PSU hold-up / mainboard buffer 協同，維持系統連續性並避免控制平面競態放大瞬態風險。此處的關鍵不在於緩衝元件形式，而在於 XR-PMC 提供的 **authority model + conflict rules + evidence alignment**：明確規格化 mainboard-PMC / backplane-PMC / PSU-PMC 的權限邊界、仲裁流程、以及跨平面事件/證據的一致性。

2.3.5 A4 — Power Grid Node IPC（電網節點 IPC）

定位：電網節點的效率治理與 failure mode 管理，並延伸至更上游的 power grid 可觀測、可審計與可控；典型部署落於工業電力監控與自動化節點。

PoE / RT 適用範圍（Scope Note）：A4 為 grid-node domain（SCADA/RTU/IED context），PoE 屬於 out-of-scope。Ride-through/backup 在 A4 為必備能力，但其形式以 **UPS/energy storage ride-through、保護協調、與事件窗遙測**為主，而非板級 supercap sizing。XR-PMC（或對應控制節點）在 A4 的共同性價值在於 semantic governance：將 continuity/ride-through 行為以統一的 telemetry、evidence events、policy guardrails 與 settlement/audit readiness 表達，使電網節點的 backup 行為可被量測、可被追溯、可被跨節點關聯分析。

Table 2–4 Coverage Summary Matrix (copy-paste)

Archetype	PoE	Ext RT / Hold-up / UPS	Sharing	Telemetry	Evidence	Authority
A1 (Mainboard AI-PMC)	M	M	M	M	M	OWN
A2-S (Secondary-side)	O	O	O	O	O	SUB

A2-P (Primary-side opt.)	—	O	C	O	O	EXT
A3 (Backplane)	—	O	C	O	O	ARB
A4 (Grid node IPC)	—	C	—	O	O	EXT

- Legend: **M**=Mandatory **O**=Optional **C**=Conditional **—**=Out-of-scope
- Authority: **OWN**=local loop owner（權責主體）
- **SUB**=subordinate（從屬） **ARB**=arbitration required（需仲裁）
- **EXT**=external/grid authority（外部/電網級）

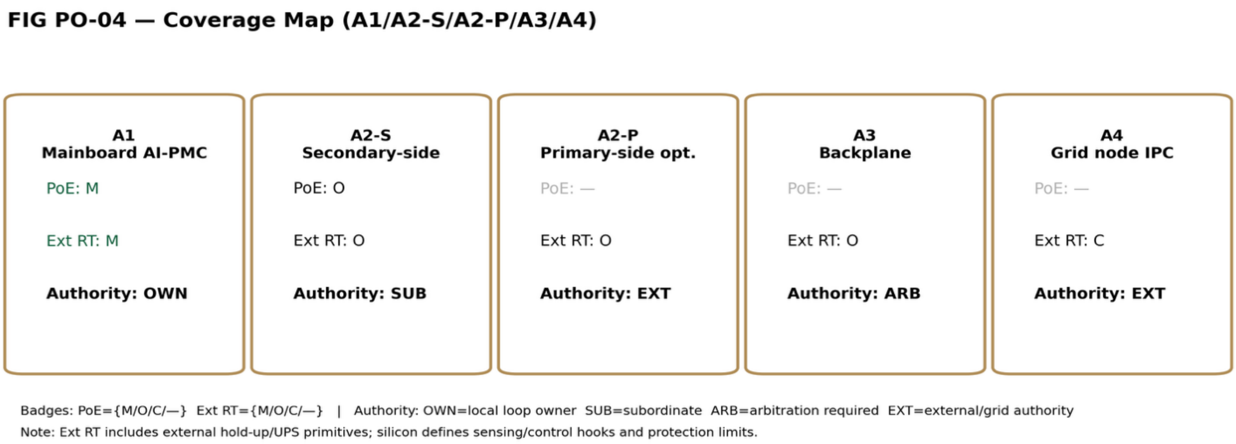


Figure 2–3 Coverage Map

2.4 Market Landscape (Fields, Not Claims)

本章節僅定義市場研究與競品分析在本文件中的欄位、方法與可查來源類型；定量數字均以「待查證」欄位呈現，不在此臆測填值。

2.4.1 Addressable Segments（可觸達細分市場）

- Mainboard (IPC/POS/Edge) power governance controllers（A1）
- PSU control and telemetry (adapter + redundancy PSU) controllers（A2-S/A2-P）
- Redundancy backplane / shelf power controllers（A3）
- Grid node automation IPC / power telemetry gateways（A4）

2.4.2 Competitive Landscape Categories（競品類型）

- Discrete power management controllers（分立式 PMC/Hot-swap/ORing/monitoring controllers）
- Digital power controllers with PMBus/telemetry（數位電源控制器）
- Power-path controllers + telemetry hubs（電源路徑控制 + 遙測集線）
- Platform EC/management ecosystems（平台管理生態：與 EC/BMC/管理軟體耦合）
- Industrial power automation controllers（工業電力自動化控制器：RTU/IED 相關）

Title: Competitive Comparison (Category / Functions / Interfaces / Evidence / Programmability / Target Node)

Table 2–5

Category	Interfaces	Evidence	Programmability	Target Node
PSU/PMIC local control	PMBus/SMBus/GPIO	—	O	A2-S/A2-P
PoE PD controller	IEEE 802.3af/at + I2C/SMBus	O	O	A1/A2-S
EC / PEC loop	GPIO/SMBus/ACPI hooks	O	M	A1/A3
BMC / OpenBMC	Redfish/IPMI + I2C/SMBus	M	M	A3
UPS / grid continuity	Power I/O + relays	O	O	A4
XR-PMC (FPGA→Prog. ASIC)	PoE/PMBus/SMBus + telemetry export	**M**	**M**	A1/A2-S/A2-P/A3/A4

FIG PO-05B — Competitive Landscape Boundary Map

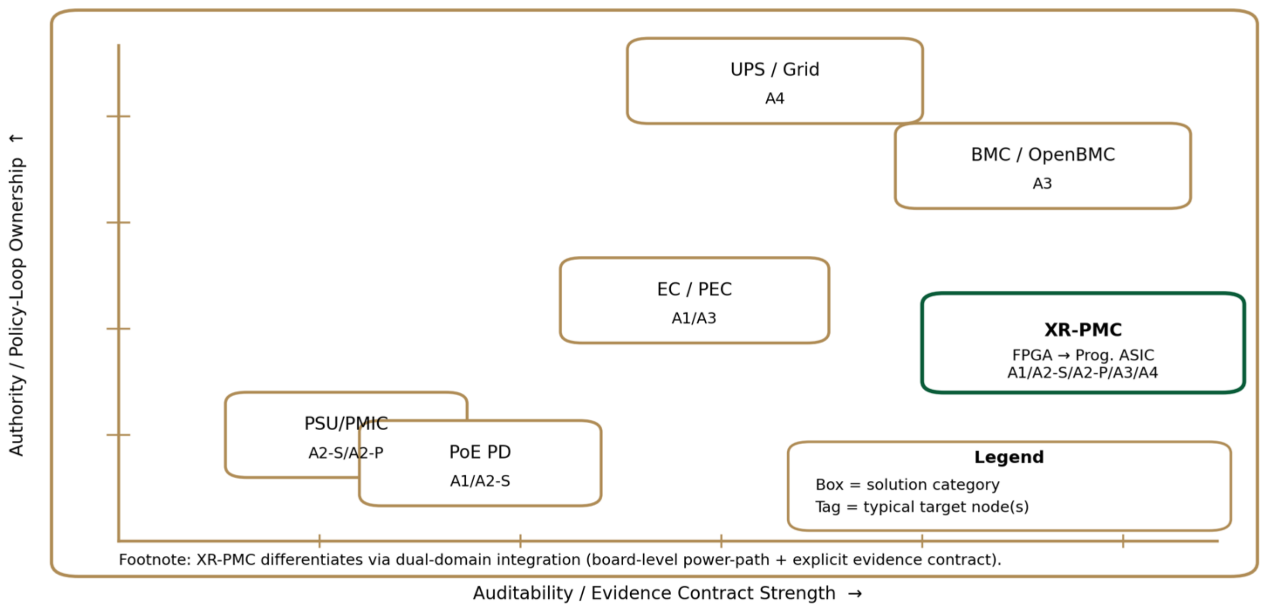


Figure 2–4

2.4.3 Quantitative Requirements Placement（定量需求放置位置與欄位定義）

This section defines the **quantitative fields** used as *engineering/program planning inputs* in later chapters (Key Features / Spec / BOM & Cost / Program Plan). Values below are **document-default bands** with **public anchors**. They are not treated as market-forecast commitments; they are the **baseline numbers** engineers shall use unless a project-specific commercial quote is explicitly substituted.

Table 2–6 Quant Field Register (Defaults + Public Anchors

Field (欄位)	Default band used in this spec (本文件預設區間)	Unit	Public anchor (來源錨點)
Adoption / Attach rate (採用率/搭載率)	**A1:** 15–50% (planning band, capped by PoE ecosystem adoption)	%	PoE ports forecast “>50% of campus switch ports by 2027” (upper envelope for PoE-first-class segments).
ASP / price band (平均售價/價格帶)	**FPGA phase silicon target:** US$4–15; **ASIC phase silicon target:** US$2–12	US$/unit	Public distributor list price anchors for PoE PD IC and small FPGA; used as *reference points*, not volume quotes.
NRE per phase (一次性工程費)	**FPGA:** US$0.1–1.0M; **Programmable ASIC:** US$8–25M (mature-node envelope)	US$	IBS quotes widely repeated in SemiEngineering for 28nm “~US$40M average design cost”; this spec uses a smaller-program envelope (XR scope).
MRE / mask set (遮罩費)	**28nm-class:** US$1–3M (per tape-out)	US$	Mask-set scaling: “at 28nm it moves beyond $1M” (public discussion).
BOM delta savings (digital displaced)（數位料件替代節省）	**US$2–20 per unit** (range, design-dependent)	US$/unit	Distributor pricing examples: PoE PD IC and small FPGA list prices bound the “replaceable digital” order-of-magnitude.
Validation cost & lab infra (驗證成本/設備需求)	**US$35k–120k** (minimal-capable lab)	US$	Example public prices: scope (Newark), temp/humidity chamber catalog pricing, power analyzer MSRP.

Table 2–7 Segment Defaults (How PO-06A Bands Are Applied

Segment	TAM/SAM/SOM proxy (本章採用的 proxy)	Adoption / Attach (default)	ASP band (default)	NRE/MRE phase applicability	Confidence (用途信心)

A1 (Mainboard AI-PMC; PoE first-class)	PoE campus ecosystem adoption as ceiling proxy	**15–50%**	**US$2–12**	FPGA + ASIC + mask	Med
A2-S (Secondary-side)	Engineering-driven (no TAM claim in PO)	**10–35%**	**US$2–10**	FPGA + ASIC + mask	Med
A2-P (Primary-side optional; isolation/safety boundary)	Engineering-driven (no TAM claim in PO)	**5–20%**	**US$3–12**	ASIC + mask dominant	Low–Med
A3 (Backplane / arbitration)	Platform-driven (no TAM claim in PO)	**10–40%**	**US$3–12**	FPGA + ASIC + mask	Low–Med
A4 (Grid node IPC; UPS/coordination)	Infrastructure-driven (no TAM claim in PO)	**5–15%**	**US$2–8**	ASIC optional; validation heavier	Low

Source-Type Policy (What Sources Are Allowed)

- Permitted public anchors include:

standards bodies; (ii) vendor public datasheets/reference designs; (iii) distributor list pricing (as reference points, not contract quotes); (iv) reputable industry press repeating primary analyst statements; (v) EDA/license public price pages where available; (vi) foundry/packaging public capability notes; (vii) instrument vendor list/MSRP or reputable catalog pricing. This section's default bands are already populated using such anchors (see citations attached to the tables).

- Execution Rule (How Engineering Teams Use These Numbers)
  - Unless a project-specific commercial quote is provided, engineers shall:
  - use **PO-06A default bands** for sizing BOM deltas and program budget envelopes;
  - apply **PO-06B segment defaults** only for internal planning (not external market claims);
  - treat distributor pricing as **unit-price reference points** for *order-of-magnitude* displacement analysis, not as volume cost.

2.5 Engineering Spec Breakdown

This section defines the engineering specification breakdown for XR-VPP / XR-PMC, structured as auditable spec blocks that remain stable across the FPGA phase and the Programmable ASIC phase. Each block is expressed as: **Requirement → Threshold → Telemetry & Evidence Events（遙測與證據事件）→ Verification Method**. The goal is to prevent feature drift by forcing every capability to be measurable, reviewable, and replayable under a consistent evidence contract.

Formatting rule (fixed): All tables in 2.5.1–2.5.5 keep the same column names. Thresholds must be numeric ranges or enumerations (not narrative). Evidence must include **event name, minimal payload fields, severity, and ordering/timebase assumptions**. Rows may be appended, but column headers shall not be renamed.

2.5.1 Spec Block — Power Path & Source Selection (Multi-Input)

Table 2–8 Power Path — Requirements & Thresholds

Item	Requirement	Target / Threshold (Default Band)	Notes
Input sources	Enumerate supported sources per node class	A1: PoE+AC-DC+opt XBM; A2-S: AC-DC+opt PoE; A3: multi-PSU; A4: site-defined	Node-class dependent
Selection policy	Deterministic priority + hysteresis	Hysteresis 50–300 ms	Anti-chatter mandatory
Switchover	Bound transition and bus disturbance	Latency 0.2–3 ms; droop < 0.8 V; overshoot < 0.5 V	Rail budget may override
Brown-out detect	Threshold + debounce + ordering	Debounce 0.2–5 ms	Monotonic ordering required
Inrush control	Soft-start and inrush bound	Soft-start 1–50 ms	Source dependent
Protection	OCP/OVP/UVP/OTP thresholds	OCP 110–180%; OTP 85–125°C (planning band)	Latch/retry defined
State exposure	Explicit states	SELECTED/TRANSITION/DEGRADED/LOCKOUT	No ambiguous states
RT hook	RT may gate transitions	Interface-level gating only	See 2.5.2

Table 2–9 Power Path — Evidence & Verification

Item	Telemetry & Evidence Events (min payload)	Verification Method
Input sources	SRC_PRESENT{src,qual} SRC_CAP{src,maxW}	Source emulation + interface bring-up
Selection policy	SRC_SELECT{from,to,reason} SRC_DEGRADED{src,metric}	HIL switching sequences
Switchover	SWITCH_START{from,to} SWITCH_DONE{dt,vdroop,vov}	Scope + load step + current probe
Brown-out detect	BROWNOUT{src,v,dt}	Brownout injector + log replay
Inrush control	INRUSH_PEAK{src,Ip} SURGE_CLASS{src,cls}	Inrush bench + fault injection

Protection	PROT_TRIP{type,thr,meas} PROT_CLEAR{type}	Protection matrix test
State exposure	STATE{src,state}	Host query vs evidence consistency
RT hook	RT_GATE{allow,reason}	Scenario tests with RT engaged

2.5.2 Spec Block — External RT Buffer Module & Verification Gates

Table 2–10 External RT — Requirements & Thresholds

Item	Requirement	Target / Threshold (Default Band)	Notes
Module definition	RT is external buffer module	Capacitor series module; 1.0–1.5 F	Not on-die energy
Entry conditions	Deterministic triggers + debounce	Debounce 0.2–5 ms	Reason code required
Hold semantics	Sustain window definition	50–500 ms (planning band)	Node/rail dependent
Exit conditions	Stable-source handoff	Stability 20–300 ms	Cooldown optional
Guardrails	Protect module/rails	I/V/T guardrails + ESR anomaly proxy	ESR/aging external dominated
Telemetry minimum	Observability baseline	Vcap mandatory; T mandatory; Icap optional	SoE proxy optional
Validation gates	Pass/fail gates defined	A performance, B ordering, C stability, D containment	Gate IDs fixed

Table 2–11 External RT — Evidence & Verification

Item	Telemetry & Evidence Events (min payload)	Verification Method
Entry/exit	RT_ARM{reason} RT_ENTER{t} RT_EXIT{reason}	Brownout injector + recovery sequencing
Hold	RT_SUSTAIN{dt}	Time-window verification under load profile
Guardrails	RT_ABORT{code} RT_FAULT{code}	Fault injection + thermal/aging simulation
Telemetry	RT_TLM{Vcap,T,(Icap),(SoE)}	Telemetry completeness + range checks
Gate A	Evidence bundle + waveform capture	Bench test per fixed profile
Gate B	Monotonic ordering + timebase declaration	Log replay + gap detection

2.5.3 Spec Block — Telemetry Spine & Evidence Schema

Table 2–12 Evidence Schema — Requirements & Thresholds

Item	Requirement	Target / Threshold (Default Band)	Notes
Schema versioning	Versioned schema	Backward-read within N major versions	Contract across FPGA/ASIC
Integrity	Ordering + gap detect	Monotonic counter; reset semantics defined	Hash chain optional
Snapshot	Critical-event snapshot	Fixed minimal fields; bounded size	Avoid oversized payload
Timebase	Declare timebase and ordering	Single timebase or explicit mapping	Brownout window handled
Export	Export mechanism & bandwidth	Interface selectable; bandwidth budgeted	Node dependent

Table 2–13 Evidence Schema — Evidence & Verification

Item	Telemetry & Evidence Events (min payload)	Verification Method
Versioning	SCHEMA_VER{maj,min,patch}	Parser regression tests
Integrity	EVT_HDR{ts,cnt,(hash)}	Tamper + rollback tests
Snapshot	SNAP{rails,V/I/T,state}	Coverage audit
Timebase	TIMEBASE{id,rate}	Cross-domain correlation tests
Export	TLM_PUSH/PULL	Throughput + loss tests

2.5.4 Spec Block — Authority & Control Boundary

Table 2–14 Authority — Requirements & Thresholds

Item	Requirement	Target / Threshold (Default Band)	Notes
Roles	Explicit roles	Host / EC(PEC) / Service / Factory	Avoid ambiguity
Policy ownership	ACL matrix	Least privilege	Audit mandatory
Service gating	Dangerous ops gated	Strap or signed token	Prevent field misuse
Rollback	Safe fallback	Fail-closed if invalid	No brick condition

Table 2–15 Authority — Requirements & Evidence & Verification

Item	Telemetry & Evidence Events (min payload)	Verification Method
Roles	AUTH_ROLE{role}	Interface conformance
Policy writes	POLICY_WRITE{who,what}	Security/abuse-case tests
Service mode	SVC_ENTER/EXIT{why}	Service gating validation
Rollback	ROLLBACK{from,to}	Version mismatch negative tests

2.5.5 Spec Block — Programmability & Profile Contract (FPGA→ASIC)

Table 2–16 Profiles — Requirements & Thresholds

Item	Requirement	Target / Threshold (Default Band)	Notes
Profile unit	Unit of deployment	Profile pack w/ immutable ID	Differentiation mechanism
Update rule	Evidence-gated update	Rare updates; regression gated	Not frequent-by-default
Compatibility	Compatibility matrix	Explicit allowed pairs	Fail-closed
Auditability	Applied change traceable	Reason code + snapshot ref	Mandatory

Table 2–17 Profiles — Evidence & Verification

Item	Telemetry & Evidence Events (min payload)	Verification Method
Profile ID	PROFILE_ID{uid,ver}	Load + readback
Apply	PROFILE_APPLY{uid,reason}	Gate checklist execution
Reject	PROFILE_REJECT{code}	Negative tests
Audit	AUDIT{who,what,ref}	Log replay

2.6 Standards and Interface Anchor Points (Preview)

XR-VPP / XR-PMC interfaces and governance contracts shall anchor to established power-management and communication standards. This document shall explicitly mark **applicability scope (適用範圍)** for each standard by node class (A1–A4) and by interface area. Detailed compliance statements and normative references are specified in later chapters; this section provides the **standard anchors** that will be referenced throughout the specification.

PMBus / SMBus / I²C / I3C (telemetry and control buses；遙測與控制匯流排)

IEEE 802.3 PoE (only when A1/A3 nodes include PoE PD interfaces；僅限含 PoE PD 介面之節點)

Security & integrity (secure provisioning, anti-rollback, debug/service gating；安全與完整性)

DFT/DFM/qualification (ASIC sign-off and production qualification framework；量產驗證與簽核框架)

Table 2–18 Standards & Applicability Matrix (Standard / Applies to A1–A4 / Interface Area / Notes)

Standard / Framework	Applies to A1	Applies to A2-S	Applies to A2-P	Applies to A3	Applies to A4	Interface Area	Notes

PMBus	M	O	O	M	—	Telemetry & control	Required where PSU/VR telemetry is present
SMBus	M	M	O	M	O	Telemetry & control	Host/EC side-band transport
I²C	M	M	O	M	O	Telemetry & control	Board-level device interconnect
I3C	O	O	O	O	—	Telemetry & control	Optional upgrade path; not required for baseline
IEEE 802.3 (PoE PD)	C	—	—	C	—	Power input + negotiation	Conditional: only for nodes that implement PoE PD
Secure provisioning	M	M	M	M	O	Security & integrity	Key injection, identity, lifecycle states
Anti-rollback	M	M	M	M	O	Security & integrity	Firmware/profile rollback prevention
Debug/service gating	M	M	M	M	O	Security & integrity	Service-mode entry controls and audit
DFT/DFM framework	—	—	M	M	—	Manufacturing readiness	Becomes mandatory in ASIC phase sign-off
Qualification framework	—	—	M	M	—	Production validation	Reliability/qualification gates in ASIC phase

Legend: **M**=Mandatory, **O**=Optional, **C**=Conditional, **—**=Not applicable by default.

3 KEY FEATURES

3.1 Dual-Domain Integration: Digital Governance + Board-Level Power-Path Control

XR-VPP / XR-PMC is defined by **dual-domain integration**: (i) deterministic board-level power-path control (multi-input selection, protection, rail stability) and (ii) a **governance-grade evidence contract** that makes power decisions auditable and replayable. The feature boundary is not "more telemetry," but **telemetry + ordered evidence events + policy hooks** that allow a PEC/system loop to reason about causality and enforce guardrails across nodes A1–A4.

3.2 Multi-Input Power Path with Deterministic Selection and Anti-Chatter

XR-PMC supports deterministic selection across multiple power inputs (e.g., AC-DC, PoE PD where applicable, and optional buffer sources), using explicit **priority rules**, **hysteresis**, and **anti-chatter** constraints. Switching behavior is specified as bounded transition latency and bounded rail disturbance, with all transitions emitting evidence events including reason codes, measured deltas, and ordering guarantees.

3.3 External Continuity Primitives: RT / Hold-up / UPS as Governed Interfaces

XR-PMC treats continuity primitives as **external** (board/system) elements while enforcing a silicon-defined control surface: engagement policy hooks, guardrails, telemetry, and evidence events. This enables consistent continuity behavior across A1 (board-level RT), A2-S (secondary hold-up shaping), A2-P (primary-side energy management boundary), A3 (platform continuity arbitration), and A4 (grid-level continuity endpoints), without implying on-die energy storage.

3.4 Evidence-First Observability Contract (Telemetry + Ordered Events)

XR-PMC defines a minimum observability spine: a telemetry set plus an evidence-event contract that includes event IDs, minimal payload fields, severity, monotonic ordering, and explicit timebase semantics. The contract is designed for replay and audit, ensuring that key actions—source selection, protection trips, RT engagement, recovery sequencing, and policy updates—are observable as **machine-verifiable sequences**, not informal logs.

3.5 Policy Guardrails and Safety Containment

All safety-relevant actions are constrained by hard guardrails (OCP/OVP/UVP/OTP, inrush limits, thermal mitigation, and recovery sequencing). Guardrails are expressed as deterministic state machines with explicit entry/exit rules, bounded retry behavior, and evidence emission for every trip/clear path. Fault containment is mandatory: protection events must not induce oscillation in source selection or continuity engagement loops.

3.6 Authority Model and Arbitration Readiness (A1–A4)

XR-PMC exposes a control-plane boundary that makes **authority explicit**: who owns policy, who may override, and how arbitration is performed when multiple controllers exist (e.g., mainboard PMC vs backplane PMC vs PSU PMC). Service/debug access is governed via gating and audit evidence, enabling field operations without compromising safety or integrity.

3.7 Programmable Profiles with Versioned Compatibility and Anti-Rollback

XR-PMC behavior is expressed through programmable profiles (policy packs) with versioned compatibility rules and anti-rollback constraints. Updates are evidence-gated and auditable, with deterministic fallback behavior under mismatch. This allows deployment across verticals and node classes without spec drift, and preserves a stable software contract from FPGA phase to programmable ASIC phase.

3.8 Standards-Anchored Interfaces with Explicit Applicability

All interfaces and governance hooks anchor to established standards (PMBus/SMBus/I^2C/I3C; IEEE 802.3 PoE where applicable; security and integrity primitives; and ASIC qualification frameworks). Applicability is explicitly marked per node class to prevent accidental over-claiming and to keep implementation scope auditable.

Table 3–1 Key Features → Evidence Events Mapping (Feature / Evidence IDs / Minimal Payload)

Feature	Evidence ID (event name)	Minimal Payload Fields
Multi-Input Power Path	SRC_PRESENT	{src, qual}
Multi-Input Power Path	SRC_SELECT	{from, to, reason}
Multi-Input Power Path	SWITCH_DONE	{dt, vdroop, vov}
Protection / Guardrails	PROT_TRIP	{type, thr, meas}
Protection / Guardrails	PROT_CLEAR	{type}
External Continuity (RT/Hold-up/UPS)	RT_ARM	{reason}
External Continuity (RT/Hold-up/UPS)	RT_ENTER	{t}
External Continuity (RT/Hold-up/UPS)	RT_SUSTAIN	{dt}
External Continuity (RT/Hold-up/UPS)	RT_EXIT	{reason}
External Continuity (RT/Hold-up/UPS)	RT_ABORT	{code}
Telemetry Spine	SCHEMA_VER	{maj, min, patch}
Evidence Integrity	EVT_HDR	{ts, cnt, (hash)}
Authority / Control Boundary	AUTH_ROLE	{role}
Policy Governance	POLICY_WRITE	{who, what}
Service/Debug Gating	SVC_ENTER	{why}
Service/Debug Gating	SVC_EXIT	{why}
Programmable Profiles	PROFILE_ID	{uid, ver}
Programmable Profiles	PROFILE_APPLY	{uid, reason}
Programmable Profiles	PROFILE_REJECT	{code}
Audit Trail	AUDIT	{who, what, ref}

Table constraints (fixed): keep each payload ≤ 3 fields; avoid units here; detailed schema appears in later telemetry chapter.

FIG 3-1 — Key Features Overview (Feature Blocks → A1–A4 Applicability)

	ApplicabilityA1	A2-S	A2-P	A3	A4
Multi-Input Power Path	M	M	C	M	O
External Continuity Interface (RT / Hold-up / UPS)	M	O	M	O	C
Evidence Contract (Telemetry + Ordered Events)	M	M	M	M	M
Guardrails & Containment	M	M	M	M	M
Authority / Arbitration	M	O	O	M	O
Programmable Profiles	M	O	O	M	O
Standards Anchors	M	M	M	M	O

Note: Applicability is by node class; details are defined in later chapters.

Legend: M=Mandatory O=Optional C=Conditional —=Out-of-scope

Figure 3–1 Key Features Overview (Feature Blocks → A1–A4 Applicability)

4 DEVELOPMENT RESOURCES AND ENGINEERING ENVIRONMENT

4.1 Purpose and Phase Boundary (FPGA Platform → Productized ASIC)

This chapter defines the **development resource architecture** (開發資源架構): reusable IP inventory, phase deliverables, productization boundaries, and the engineering environment required to execute XR-VPP from **FPGA phase** to **Programmable ASIC phase**.

FPGA phase is a **superset platform** spanning node classes **A1–A4**, used to converge functional correctness, evidence contract, and validation gates under a unified implementation baseline.

ASIC phase is **productized** into distinct silicon SKUs (產品化切分) aligned to node classes: **A1 product**, **A2-S product**, **A2-P product**, **A3 product**, **A4 product**. Each product reuses a common governance/evidence backbone while selecting a cost/feature-appropriate IP set and packaging constraints.

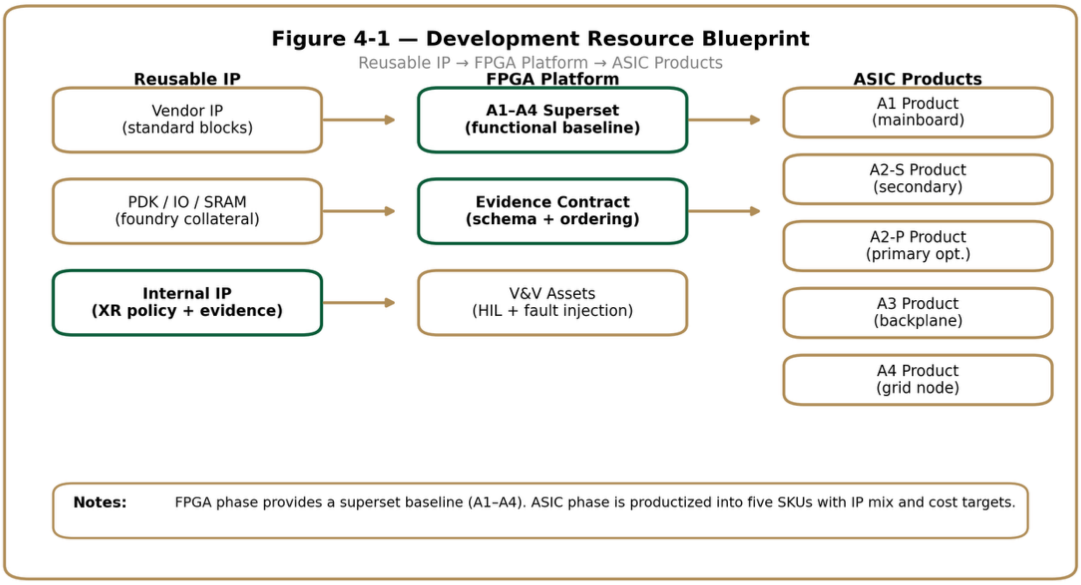


Figure 4–1 Development Resource Blueprint (Reusable IP → FPGA Platform → ASIC Products)

4.2 Reusable IP Inventory (What Is Reused vs Implemented)

XR-VPP development shall start from a **reusable IP-first** strategy. “Reusable IP” includes third-party licensed IP, vendor-provided reference IP, and internal reusable blocks. Engineering work shall focus on **integration, parameterization, verification, and evidence contract compliance**, rather than re-creating commodity blocks.

IP sourcing model (來源模型):

- **Vendor IP (商用 IP):** licensed cores for standard functions (e.g., memories, PLL, crypto, IO PHY).
- **Foundry/PDK-linked collateral (製程綁定資源):** IO libraries, standard cell libraries, SRAM compilers, ESD structures, signoff rule decks.
- **Internal IP (自有 IP):** XR-specific policy engine, evidence-event generator, and guardrail state machines.

Table 4–1 Reusable IP Inventory (Concise)

IP Block	Source Type	FPGA Use	ASIC Use	Integration Notes
Standard digital blocks (e.g., timers, watchdog, DMA)	Vendor IP	Yes	Yes	Prefer proven vendor cores; wrap with XR evidence hooks where applicable.
On-chip memory (SRAM compiler / ROM)	Foundry / PDK	N/A or FPGA RAM	Yes	PDK-tied; size by SKU; define MBIST coverage in ASIC phase.
Clocking (PLL / clock mux / reset gen)	Vendor + PDK	FPGA PLL primitives	Yes	Deterministic reset semantics; support audit of reset cause (evidence event).
IO libraries (GPIO/I^{2}C/I3C/PMBus pads)	Foundry / PDK	FPGA IO	Yes	IO ring selection is SKU-dependent; enforce electrical guardrails and ESD rules.
Security primitives (TRNG/PUF/crypto if used)	Vendor IP	Optional	Optional/Yes	If enabled, bind to secure provisioning & anti-rollback policy.
XR Policy Engine (state machines + guardrails)	Internal IP	Yes	Yes	Must remain semantics-identical across FPGA and ASIC products.
Evidence Event Generator (ordered events + IDs)	Internal IP	Yes	Yes	Enforces 20-core-event baseline + branch matrix; schema-versioned.

Telemetry Schema Pack (signals → fields)	Internal asset	Yes	Yes	Must declare rail inventory and timebase authority; versioned mapping.
Host/PSU log normalizers (A1/A4)	Internal asset	Yes	Yes	A1/A4 only; normalizes host logs + PMBus logs into EvidenceBundle format.

- Note: add SKU-specific IP deltas in Table 4-3 (product matrix)

4.3 FPGA Platform Baseline (A1–A4 Coverage as One Implementation Envelope)

The FPGA baseline is a **single implementation envelope** covering A1–A4 to lock down:

- deterministic state machines for source selection and protection,
- evidence contract (telemetry + ordered events) and replay semantics,
- authority boundary behaviors (Host / EC(PEC) / service mode), and
- validation gates and bench assets.

FPGA implementation shall be treated as the **golden functional reference** for ASIC products. Any ASIC product-specific scope reduction must be expressed as:

- a removed interface surface, or
- a profile default that disables a feature,
  without changing the semantics of remaining interfaces and evidence events.

Table 4–2 FPGA Baseline Coverage (Superset A1–A4)

Baseline Item	Scope	Evidence Requirement	Validation Asset
Power-path state machine (source select / transition)	A1–A4	Ordered state transitions + reason codes	HIL sequencing + fault injection
Protection & containment (OCP/OVP/UVP/OTP)	A1–A4	Trip/clear events + thresholds snapshot	Fault injection + limit sweep
Evidence contract (telemetry + ordered events)	A1–A4	Schema-ver + monotonic ordering + gaps	Schema tests + replay tests
Authority boundary hooks (Host / EC(PEC) / service)	A1–A4	Actor attribution + gated actions events	Mode switching tests

Continuity interface hooks (External RT / hold-up / UPS)	A1–A4 (as applicable)	Engage/hold/exit events + guardrails	Brownout profile tests
A1/A4 multi-source ingest (Host + PMBus + XR-PMC)	A1 & A4	Normalized origin tagging + time mapping	Cross-stream alignment tests

4.4 ASIC Productization (A1, A2-S, A2-P, A3, A4) and IP Mix

ASIC is developed as **five products**, each selecting an IP mix appropriate to its node boundary and cost target:

- **A1 product (Mainboard AI-PMC):** PoE-first-class input may be applicable; board-level continuity interface (external RT buffer) is governed; evidence bandwidth and authority hooks are typically stronger.
- **A2-S product (Secondary-side):** focuses on secondary hold-up/transient shaping semantics; may omit PoE PD interface; keeps evidence spine and guardrails.
- **A2-P product (Primary-side optional):** emphasizes isolation/safety boundary constraints; focuses on hold-up energy management and protection coordination; interface set is safety-driven.
- **A3 product (Backplane):** focuses on arbitration readiness and multi-controller authority model; may coordinate with PSU-side telemetry; emphasizes deterministic containment.
- **A4 product (Grid node IPC):** PoE out-of-scope; focuses on endpoint observability, policy guardrails, and integration with grid-level continuity primitives.
- **IP mix implication (IP 用量差異):** productization determines which interfaces are mandatory, which are conditional, and which are out-of-scope; this directly impacts licensed IP count (royalty structure), IO ring selection, memory sizing, and verification scope.

Table 4–3 ASIC Product Matrix (Five SKUs, Concise)

Product (SKU)	Node Class	Mandatory Interfaces	Optional Interfaces	Key IP Mix Notes
A1 Product	A1	XR-PMC bus (PMBus/SMBus/I^{2}C/I3C), Evidence spine, Authority hooks	PoE PD (if used), Host/PSU log ingest	Strongest governance + evidence bandwidth; supports multi-source L1 ingest.
A2-S Product	A2-S	Evidence spine, Guardrails, Secondary-side telemetry/control	—	No PoE requirement; continuity expressed as secondary hold-up/transient shaping.

A2-P Product	A2-P	Evidence spine, Guardrails, Primary-side boundary signals	Isolation/safety-related telemetry	Continuity as hold-up energy management under safety boundary constraints.
A3 Product	A3	Evidence spine, Guardrails, Arbitration-ready authority model	PSU telemetry coordination	Backplane scope; authority model must be explicit (mainboard/backplane/PSU PMC).
A4 Product	A4	Evidence spine, Endpoint telemetry/events, Authority hooks	Host/PSU log ingest	PoE out-of-scope; integrates with grid-level continuity primitives via evidence & policy.

4.5 28nm-Class ASIC EDA Flow Anchor Points (Tool Classes and Deliverables)

For a 28nm-class programmable ASIC, the development environment shall be defined as a **foundry-compatible reference flow** (製程相容流程) with explicit deliverables at each stage. Tool selection is constrained by:

- foundry/PDK availability and signoff requirements,
- internal team familiarity, and
- ecosystem availability of required licensed IP and verification collateral.

4.5.1 EDA selection rule (選型規則):

Choose a coherent stack (single-vendor-dominant or proven mixed flow) that is compatible with the target foundry signoff decks and the selected IP provider deliverables. The specification mandates **deliverables and checks**, not a single mandatory brand.

Table 4–4 28nm ASIC EDA Flow Anchors (Concise)

Stage	Tool Class	Mandatory Checks	Output Artifacts
1) Spec-to-RTL Setup	Requirements & version control	Interface freeze; schema/version alignment; lint rules baseline	RTL baseline tag; interface spec snapshot; change log
2) RTL Development	RTL editor + synthesis-ready coding	Lint (style + semantic); CDC/RDC pre-check; reset/clock policy compliance	Clean RTL; lint report; CDC/RDC prelim report

3) Functional Verification	Simulation + assertion + coverage	UVM/unit tests; assertions; coverage targets; replay of evidence timelines	Regression report; coverage report; failing-seed archive
4) Logic Synthesis	Synthesis engine	Constraints consistency; timing intent sanity; power intent (if used)	Gate-level netlist; SDC; synthesis QoR report
5) DFT Insertion	DFT/ATPG tooling	Scan coverage; MBIST coverage; JTAG/service gating compliance	DFT-inserted netlist; coverage reports; test protocol
6) Formal / Equivalence	Formal / LEC	RTL↔netlist equivalence (LEC); safety properties (as applicable)	LEC report; formal proof summary
7) Floorplan & Power Plan	Physical design (P&R)	Power grid sanity; IO ring checks; congestion risk review	Floorplan DB; power plan summary; early congestion report
8) Place & Route	Physical implementation (P&R)	Setup/hold closure; clock tree checks; DRC pre-clean	Routed DB; timing reports; CTS summary
9) Signoff Timing	Static timing analysis	Full-corner STA; OCV/AOCV/derates; async checks	Signoff STA reports; constraint signoff pack
10) Signoff Power / IR	Power analysis + IR/EM	Vector-based (if available); IR drop/EM limits; thermal assumptions declared	Power report; IR/EM reports; assumptions record
11) Physical Verification	DRC/LVS/antenna	DRC clean; LVS clean; antenna checks; density rules	DRC/LVS reports; clean signoff summary
12) Package / IO Validation	Package/IO planning tools	Pinout review; ESD strategy; SI risk screen (as applicable)	Package pin map; IO checklist; review log
13) Tape-out Package	Release management	Reproducibility; artifact integrity; signoff checklist complete	GDSII/OASIS; signoff reports bundle; manifest (hashes)

4.6 Circuitry Design Resources Beyond IP (What Must Be Engineered)

Beyond licensed IP, the ASIC program must engineer product-specific circuitry (自研電路) that preserves the FPGA baseline semantics while meeting PPA constraints:

- **Clock/reset strategy** (clocking/reset domains；時鐘/重置域) with deterministic recovery semantics under brownout windows.
- **Mixed-signal boundary** where required (sensing front-end integration; ADC selection strategy).

- **Protection and containment circuitry** that enforces guardrails in silicon-consumable form (state machines, comparators, limit paths).
- **DFT and production readiness** (scan/MBIST/JTAG gating；量產可測性) aligned to signoff.

Table 4–5 Circuitry Ownership Map (Concise)

Function	Implemented as IP vs Custom	Verification Asset	Signoff Gate
Clock / reset strategy (時鐘/重置域)	Mixed: IP PLL + custom reset sequencing	Reset/clock-domain sims; CDC/RDC; brownout recovery tests	CDC/RDC clean; STA async checks
IO + bus controllers (PMBus/SMBus/I²C/I3C)	Prefer IP / proven controller; custom wrappers	Bus functional models; protocol compliance tests	LEC (wrapper); STA for IO paths
Rail sensing aggregation (V/I/T collection)	Custom integration (sensor-dependent)	HIL sensing replay; range/offset tests	Functional regression; signoff timing
Source selection / gating control (ORing/FET)	Custom control + board interface	Fault injection (droop/inrush); sequencing tests	Formal for safety properties (if used)
Protection comparators & limit paths (OCP/OVP/UVP/OTP)	Custom (policy-defined)	Threshold sweep; trip/clear sequence tests	STA + IR/EM for limit paths
Evidence event generator (ordered events)	Internal IP (core)	Ordering tests; gap handling; schema validation	Regression pass; schema compliance gate
Telemetry schema pack (signal→field mapping)	Internal asset (core)	Schema tests; backward-read tests	Versioning gate; compatibility checklist
Authority / arbitration hooks (Host/EC/service)	Custom (system policy)	Mode switching tests; service gating tests	Security review; regression pass
Profile store / update interface	Custom + optional secure IP	Update/rollback tests; manifest validation	Anti-rollback gate; integrity checks
Security primitives (crypto/TRNG/PUF)	Prefer IP	Known-answer tests; provisioning simulation	Security signoff; LEC where applicable
DFT (scan/MBIST/JTAG gating)	Tool-assisted + custom gating	ATPG vectors; MBIST tests; coverage reports	Coverage targets met; DRC/LVS clean
Power intent + power gating (if used)	Mixed (UPF + custom)	Low-power sims; state retention tests	Low-power signoff; STA multi-mode

4.7 AI Development Resource Stack (4-Layer Code Structure as a Reusable Asset)

AI is treated as a **development resource stack** (AI 開發資源) rather than an ad-hoc feature. Most engineering teams are unfamiliar with ML/AI operational constraints; therefore the specification defines a reusable **four-layer code structure** (四層程式架構) that remains stable across FPGA and ASIC products.

- **Layer 1 — Data & Evidence Ingest (資料與證據匯入):** parses telemetry/events, enforces schema versioning, reconstructs ordered timelines.
- **Layer 2 — Feature & Regime Model (特徵與區間模型):** derives regime states (efficiency regimes, droop signatures, thermal hotspots) and normalizes per node class.
- **Layer 3 — Reasoning & Policy Suggestion (推論與策略建議):** produces bounded suggestions (not direct actuation) with explicit confidence and guardrail compatibility.
- **Layer 4 — Governance Integration (治理整合):** produces signed/traceable policy proposals, links to evidence references, and supports audit replay.

The AI stack must emit outputs that are **policy-compatible artifacts** (e.g., recommended profile deltas, reason codes, and evidence references), not opaque "model decisions."

Table 4–6 AI Stack Modules (Concise)

Layer	Inputs	Outputs	Guardrails	Evidence Reference
L1 — Ingest & Normalize (資料/證據匯入)	XR-PMC telemetry/events (all nodes); + Host logs & PSU PMBus logs (A1/A4)	EvidenceBundle (ordered events + gaps + timebase authority + snapshots)	Schema validation; explicit gap marking; origin tagging; no implicit clock merge	EvidenceBundle segments (event ranges, gap windows, origin records)
L2 — Features & Regimes (特徵/區間)	EvidenceBundle	FeatureFrame (regimes + normalized features + bounds)	Deterministic transforms; regime definitions versioned; no hidden state	Regime entry/exit linked to event ranges + snapshots
L3 — Reasoning (推論)	FeatureFrame (+ optional rules/models)	PolicySuggestion + DiagnosisDraft	Bounded outputs only; must pass guardrail compatibility check; confidence required	Each suggestion/report section cites evidence IDs and ranges

L4 — Governance Output (治理輸出)	EvidenceBundle + FeatureFrame + L3 outputs	PolicyProposal (JSON, component-facing) + Diagnosis Report (text, human-facing)	Autonomy mode (Advisory/Delegated/Locked) enforced; audit metadata mandatory	PolicyProposal contains evidence_refs; diagnosis text includes evidence pointers

4.7.1 AI Stack Deliverable Definition (Layer Architecture + Runnable Skeleton)

This deliverable provides a **contract-first, runnable skeleton** of the 4-layer AI stack so engineers can adopt it without ambiguity. The skeleton is not a production model; it is a **reference implementation** that proves: (i) schema compliance, (ii) ordered evidence reconstruction under system-clock authority, and (iii) generation of both **Policy Proposal** and **Diagnosis Report** with evidence references.

4.7.1.1 Reference Repository Layout (What Engineers Get)

Engineers receive a single reference repository with a fixed layout. Each folder maps to a layer responsibility and is testable in isolation. The repository includes schemas, sample recordings, and a smoke-run test that must pass in CI.

```
ai_stack/
  README.md
  pyproject.toml (or equivalent lockfile)
  schemas/
    telemetry.schema.json
    events.schema.json
    evidence_bundle.schema.json
    policy_proposal.schema.json
```

```
xr-vpp-silicon-001
    diagnosis_report.schema.json
  src/
    common/
      types.py
      timebase.py
      errors.py
    l1_ingest/
      parser.py
      schema_validate.py
      ordering.py
      normalize_host_logs.py          # A1/A4 only
      normalize_pmbus_logs.py          # A1/A4 only
    l2_features/
      feature_extract.py
      regimes.py
    l3_reasoning/
      suggest.py
      guardrail_check.py
    l4_governance/
      proposal.py
      diagnosis.py
      audit_ref.py
```

```
      signer_stub.py
  tests/
    test_schema.py
    test_ordering.py
    test_smoke_run.py
  samples/
    sample_events.jsonl
    sample_telemetry.jsonl
    sample_host_logs.jsonl          # A1/A4 only
    sample_pmbus_logs.jsonl         # A1/A4 only
    expected_policy_proposal.json
    expected_diagnosis_report.txt
```

Folder intent (engineer-facing):

- schemas/: the normative contracts. Do not change meaning; only version.
- src/common/: shared types/timebase/errors—single source of truth across layers.
- src/l1_ingest/: converts raw sources into an ordered EvidenceBundle (system-clock anchored).
- src/l2_features/: derives regimes and normalized features from EvidenceBundle.
- src/l3_reasoning/: produces bounded suggestions + guardrail compatibility checks.
- src/l4_governance/: emits two deliverables: component JSON + human-readable text, both evidence-linked.
- samples/ + tests/: smoke-run must reproduce expected artifacts.

4.7.1.2 Layer Contracts (fixed IO) Contract Types (Shared Across Layers)

The skeleton locks the inter-layer contract using fixed data types. All layers import these from src/common/types.py only (no local re-definition).

- **L1 Output:** EvidenceBundle

xr-vpp-silicon-001

Contains: ordered events + minimal snapshots + declared timebase + gap markers

- **L2 Output:** FeatureFrame

Contains: regimes + normalized features + confidence bounds

- **L3 Output:** PolicySuggestion

Contains: bounded recommendations **compatible with guardrails**, with confidence + reasons

- **L4 Output:** PolicyProposal

Contains: proposed profile delta / parameter change + **evidence references** + audit metadata

---

```
# src/common/types.py

"""

Purpose:

- Define the immutable data contracts used across L1–L4.

- Engineers must not redefine these structures per layer.

- Contract changes are versioned via schema_ver / proposal_ver and corresponding JSON schemas.

"""

from dataclasses import dataclass

from typing import Any, Dict, List, Optional, Literal


@dataclass

class SchemaVer:

    maj: int

    min: int
```

```
    patch: int


@dataclass
class EvidenceEvent:
    """
    Minimal event unit. 'ts' is anchored to the integrated system clock.
    'cnt' is a monotonic counter for ordering within the originating stream.
    """
    evt: str
    ts: int
    cnt: int
    payload: Dict[str, Any]
    severity: Optional[Literal["INFO", "WARN", "ERR"]] = None
    origin: Optional[str] = None    # XR_PMC / HOST / PMBUS (A1/A4 may include HOST/PMBUS)


@dataclass
class EvidenceBundle:
    """
    L1 output:
    - Ordered events with explicit gaps (loss windows) and declared timebase authority.
    - Snapshots are minimal, but rail inventory is not artificially reduced.
    """
```

```
    schema_ver: SchemaVer
    timebase: Dict[str, Any]          # system-clock authority + optional mapping records
    events: List[EvidenceEvent]
    gaps: List[Dict[str, Any]]        # explicit loss windows (start/end + reason)
    snapshots: List[Dict[str, Any]] # minimal snapshots (rail fields + selection states)


@dataclass
class FeatureFrame:
    """L2 output: regimes + normalized features + bounds/confidence."""
    schema_ver: SchemaVer
    regimes: Dict[str, Any]
    features: Dict[str, Any]
    bounds: Dict[str, Any]


@dataclass
class PolicyProposal:
    """
    L4 component-facing output (JSON):
    - Proposed profile deltas with bounded ranges.
    - Evidence references are mandatory.
    """
    proposal_ver: SchemaVer
```

```
    target: Dict[str, Any]            # node_class / sku / profile_id
    deltas: List[Dict[str, Any]]
    reason_codes: List[str]
    evidence_refs: List[Dict[str, Any]]
    guardrail_compatibility: Dict[str, Any]
    audit: Dict[str, Any]
```

4.7.1.3 Timebase / Ordering Utilities (System-Clock Anchored)

Engineers use src/common/timebase.py to normalize multiple clocks into system-clock authority. For A1/A4, this is where HOST/PMBus streams are mapped into the same timeline contract.

Minimal Sample Code Skeleton (runnable, contract-first)

```
# src/common/timebase.py
"""
Purpose:
- Declare timebase authority: integrated system clock.
- Provide optional mapping records for multiple clocks (e.g., PMC tick → system clock).
- All L1 normalizers must emit timebase records through these helpers.
"""


from typing import Dict, Any


def make_timebase(system_clock_id: str, rate_hz: int) -> Dict[str, Any]:
```

```
    return {"authority": "SYSTEM", "clock_id": system_clock_id, "rate_hz": rate_hz, "mappings": []}


def add_mapping(tb: Dict[str, Any], origin: str, mapping: Dict[str, Any]) -> None:
    # mapping example: {"origin_clock": "PMC_TICK", "to_system": {"offset":..., "scale":...}, "confidence":...}
    tb["mappings"].append({"origin": origin, **mapping})
```

4.7.1.4 L4 Governance Outputs (Policy Proposal + Diagnosis Report)

src/l4_governance/ generates both mandatory outputs:

component JSON proposal (for firmware/tooling)

human text diagnosis report (for review/debug/audit)

Below is the minimal reference implementation: it builds a bounded proposal and a diagnosis summary, both linked to evidence ranges.

```
# src/l4_governance/proposal.py
"""
Purpose:
- Convert (EvidenceBundle + FeatureFrame + L3 suggestions) into a component-facing PolicyProposal.
- Enforce: bounded deltas + mandatory evidence_refs + guardrail_compatibility.
"""


from common.types import EvidenceBundle, FeatureFrame, PolicyProposal, SchemaVer
```

```
def propose_policy(evb: EvidenceBundle, ff: FeatureFrame) -> PolicyProposal:
    deltas = []
    reason_codes = []
    evidence_refs = []

    # Example bounded change: hysteresis tuning under frequent droop regime
    if ff.regimes.get("droop_regime") == "FREQUENT":
        deltas.append({"param": "SRC_HYST_MS", "set_to": 150, "bounds": [50, 300]})
        reason_codes.append("RC_DROOP_FREQ")
        evidence_refs.append({"evt": "BROWNOUT", "range": "cnt[1200..1280]"})

    return PolicyProposal(
        proposal_ver=SchemaVer(0, 1, 0),
        target={"node_class": ff.features.get("node_class"), "profile_id": ff.features.get("profile_id")},
        deltas=deltas,
        reason_codes=reason_codes,
        evidence_refs=evidence_refs,
        guardrail_compatibility={"status": "CHECKED", "notes": "bounded by spec defaults"},
        audit={"generator": "ai_stack_skeleton", "schema_ver":
f"{evb.schema_ver.maj}.{evb.schema_ver.min}.{evb.schema_ver.patch}"},
    )
```

```
# src/l4_governance/diagnosis.py
```

```
xr-vpp-silicon-001

"""

Purpose:

- Generate the human-facing Diagnosis Report (text) with explicit evidence references.

- Must not contradict the component-facing PolicyProposal; both share the same reason codes and evidence refs.

"""

from common.types import EvidenceBundle, FeatureFrame

def make_diagnosis_report(evb: EvidenceBundle, ff: FeatureFrame) -> str:

    lines = [ ]

    lines.append("XR-PMC Diagnosis Report")

    lines.append(f"Schema: {evb.schema_ver.maj}.{evb.schema_ver.min}.{evb.schema_ver.patch}")

    lines.append(f"Node class: {ff.features.get('node_class')}")

    lines.append("")

    lines.append("Regime summary:")

    for k, v in ff.regimes.items():

        lines.append(f" - {k}: {v}")

    lines.append("")

    lines.append("Evidence references:")

    lines.append(" - Example: BROWNOUT cnt[1200..1280] (see evidence bundle ordering)")

    return "\n".join(lines)
```

4.7.1.5 Smoke-Run Acceptance (Engineers Know "Done")

The repository is considered usable only if a smoke run passes:

- schema validation for all artifacts
- ordering reconstruction under system-clock authority
- output generation:
- policy_proposal.json (component JSON)
- diagnosis_report.txt (human text)
- both outputs contain evidence references and version fields

Table 4–7 AI Stack Smoke-Run Gate (Concise)

Input Samples	Expected Artifacts	Pass Criteria
sample_events.jsonl + sample_telemetry.jsonl (all nodes)	policy_proposal.json + diagnosis_report.txt	Schemas validate; ordering is monotonic (with explicit gaps); outputs include schema_ver / proposal_ver; evidence references present.
+ sample_host_logs.jsonl (A1/A4 only)	Same as above	Host log normalization preserves origin tags; timebase authority declared; cross-stream alignment emits mapping record if needed.
+ sample_pmbus_logs.jsonl (A1/A4 only)	Same as above	PMBus log normalization preserves rail identifiers; timing aligns to system clock via mapping; no silent drops.
Injected gap window (simulated loss)	Same as above	Gap window is explicitly represented in EvidenceBundle; downstream layers do not crash; diagnosis report calls out data loss.
Counter reset / reboot marker	Same as above	Reset is captured as evidence event; ordering resumes with declared discontinuity; proposal generation remains bounded and auditable.

4.7.2 AI Stack Resource Specification (Normative)

This section defines the **4-layer AI stack** as a reusable engineering resource (可重用工程資源) with fixed input/output contracts, evidence linkage rules, and implementation modes. The objective is to eliminate integration ambiguity for teams unfamiliar with AI/ML by specifying **data sources, timebase authority, core event taxonomy, snapshot scope, outputs, and artifact formats**.

4.7.2.1 L1 Data Ingest Scope (Sources by Node Class)

L1 shall ingest evidence streams according to node class applicability:

A1 and A4: L1 ingests **XR-PMC telemetry/events** plus **Host logs** and **PSU PMBus logs**.

A2-S / A2-P / A3: L1 ingests **XR-PMC telemetry/events only**.

xr-vpp-silicon-001

All non-XR sources (Host logs / PMBus logs) shall be normalized into the same evidence timeline format and must declare their origin and mapping method.

Table 4–8 L1 Data Sources (Concise)

Node Class	Source Type	Transport	Normalization Notes
A1	XR-PMC telemetry/events	PMBus/SMBus/I²C/I3C (as implemented)	Normalize into EvidenceBundle; tag origin=XR_PMC; enforce schema + ordering.
A1	Host logs	Host-side log channel (OS/service log export)	Convert to EvidenceEvent with origin=HOST; map timestamps to system clock; preserve actor/mode markers.
A1	PSU PMBus logs	PMBus telemetry/log readout	Convert to EvidenceEvent with origin=PMBUS; normalize rail IDs; align to system clock; never silently drop gaps.
A2-S	XR-PMC telemetry/events	PMBus/SMBus/I²C/I3C (as implemented)	XR-only ingest; EvidenceBundle ordering + gap marking required.
A2-P	XR-PMC telemetry/events	PMBus/SMBus/I²C/I3C (as implemented)	XR-only ingest; emphasize isolation/safety boundary fields where present.
A3	XR-PMC telemetry/events	PMBus/SMBus/I²C/I3C (as implemented)	XR-only ingest; arbitration/authority markers captured as events.
A4	XR-PMC telemetry/events	PMBus/SMBus/I²C/I3C (as implemented)	Normalize into EvidenceBundle; tag origin=XR_PMC; enforce schema + ordering.
A4	Host logs	Host-side log channel (OS/service log export)	Convert to EvidenceEvent with origin=HOST; map timestamps to system clock; preserve service-mode gating markers.
A4	PSU PMBus logs	PMBus telemetry/log readout (if present)	Convert to EvidenceEvent with origin=PMBUS; normalize rail IDs; align to system clock; explicit gap windows required.

4.7.2.2 Timebase Authority and Ordering Rules (System-Clock Anchored)

Timebase shall be anchored to the **integrated system clock** (整合系統時鐘) of the deployment environment. L1 shall therefore:

- declare the **time authority** (system clock ID),
- preserve a **monotonic ordering counter** per evidence stream, and
- provide explicit mapping when multiple clocks exist (if any).

Where multiple clocks are present (e.g., PMC internal tick vs host wall time), L1 shall emit a **time mapping record** rather than forcing implicit alignment.

Table 4–9 Timebase & Ordering Contract (Concise)

Field	Meaning	Required	Notes
timebase.authority	Declares time authority	Yes	Must be SYSTEM (integrated system clock).
timebase.clock_id	Identifier of system clock	Yes	Set by integration environment; stable per deployment.
timebase.rate_hz	Tick rate of timebase	Yes	Required for converting ticks to real time; document assumptions.
timebase.mappings[]	Mapping records for non-system clocks	Conditional	Required when XR-PMC tick or HOST timestamps are not native system-clock.
event.ts	Timestamp in system timebase	Yes	Always expressed in system-clock units after mapping.
event.cnt	Monotonic counter within origin stream	Yes	Used to reconstruct ordering even under timestamp jitter.
event.origin	Evidence source	Yes	XR_PMC / HOST / PMBUS.
ordering.policy	Ordering rule used	Yes	Example: “primary order by ts; tie-break by origin priority; then cnt”.
gaps[]	Explicit loss windows	Conditional	Mandatory if any discontinuity occurs (capture loss, reboot, transport drop).
reset_markers[] (or equivalent)	Declared counter/time discontinuities	Conditional	Mandatory if origin counter resets or reboot markers occur.
integrity.flags[]	Contract-level integrity flags	Yes	Examples: SCHEMA_OK, MAPPING_OK, GAPS_PRESENT, RESET_PRESENT.

4.7.2.3 Core Evidence Events: “20 Event IDs” with Category Branch Matrix

The evidence contract shall define **20 core event IDs** as the minimum baseline. Each core event may have **category branches** (分支) per node class, interface presence, or protection mode. The baseline shall therefore be specified as a **matrix**: 20 core IDs × category variants × A1–A4 applicability.

Core-event definition requirements:

- Each core ID shall have a fixed **event name**, fixed **severity class**, and a bounded **minimal payload**.
- Branch variants may extend payload, but shall not redefine the meaning of the core ID.
- Applicability shall be explicit (M/O/C/—) per node class.

Table 4–10 Core Evidence Event Matrix (20 Core IDs, Concise)

Category	Core Event ID	Variants (branch examples)	Applies A1–A4	Minimal Payload (required fields)
Power-Path (電源路徑)	EV-01 SRC_SELECT	by source type (PoE/ACDC/Batt/Ext)	A1:M A2-S:M A2-P:C A3:M A4:O	src_id, from_state, to_state, reason_code
Power-Path	EV-02 SRC_TRANSITION_START	by transition class (fast/soft-start)	A1:M A2-S:M A2-P:C A3:M A4:O	src_id, target_state, ramp_profile_id
Power-Path	EV-03 SRC_TRANSITION_DONE	by success/fallback	A1:M A2-S:M A2-P:C A3:M A4:O	src_id, result, fallback_src_id?
Power-Path	EV-04 POWER_GOOD_ASSERT	by rail group / domain	A1:M A2-S:M A2-P:M A3:M A4:M	rail_group, pg_state, latency_ms
Power-Path	EV-05 POWER_GOOD_DEASSERT	by droop/UV condition	A1:M A2-S:M A2-P:M A3:M A4:M	rail_group, pg_state, uv_flag, min_v
Protection (保護)	EV-06 OCP_TRIP	by rail / channel	A1:M A2-S:M A2-P:M A3:M A4:M	rail_id, i_peak, i_limit, trip_mode
Protection	EV-07 OVP_TRIP	by rail	A1:M A2-S:M A2-P:M A3:M A4:M	rail_id, v_peak, v_limit, trip_mode

Protection	EV-08 UVP_TRIP	by rail / brownout class	A1:M A2-S:M A2-P:M A3:M A4:M	rail_id, v_min, v_limit, duration_ms
Protection	EV-09 OTP_TRIP	by sensor / hotspot	A1:M A2-S:M A2-P:M A3:M A4:M	sensor_id, t_peak, t_limit, zone
Protection	EV-10 INGRESS_INRUSH_LIMIT	by input path	A1:O A2-S:O A2-P:M A3:O A4:—	src_id, i_inrush, limit_profile_id
Continuity External (外部續航)	EV-11 CONT_ARM	RT/hold-up/UPS (external)	A1:M A2-S:O A2-P:M A3:O A4:C	cont_mode, guardrail_set_id, arm_reason
Continuity External	EV-12 CONT_ENGAGE	trigger class (droop/command)	A1:M A2-S:O A2-P:M A3:O A4:C	cont_mode, trigger_id, v_entry, rail_group
Continuity External	EV-13 CONT_SUSTAIN	periodic marker / interval	A1:M A2-S:O A2-P:M A3:O A4:C	cont_mode, t_elapsed_ms, v_bus, i_bus
Continuity External	EV-14 CONT_EXIT	normal/abort/timeout	A1:M A2-S:O A2-P:M A3:O A4:C	cont_mode, exit_reason, v_exit, duration_ms
Authority/Mode (權限/模式)	EV-15 AUTH_MODE_CHANGE	host/ec/service transitions	A1:M A2-S:O A2-P:O	actor, mode_from, mode_to, auth_token_id?

			A3:M A4:M	
Authority/Mode	EV-16 POLICY_APPLY	profile delta applied	A1:M A2-S:O A2-P:O A3:M A4:M	actor, profile_id, delta_id, result
Telemetry Integrity (遙測完整性)	EV-17 SCHEMA_VERSION	schema change boundary	A1:M A2-S:M A2-P:M A3:M A4:M	schema_ver, compat_rule, producer_id
Telemetry Integrity	EV-18 DATA_GAP	loss window detected	A1:M A2-S:M A2-P:M A3:M A4:M	origin, gap_start_ts, gap_end_ts, reason
Telemetry Integrity	EV-19 RESET_MARKER	reboot / counter reset	A1:M A2-S:M A2-P:M A3:M A4:M	origin, reset_reason, cnt_before, cnt_after
Host/PSU Integration (整合)	EV-20 EXT_LOG_ANCHOR	host/PMBus anchor point	A1:M A2-S:— A2-P:— A3:— A4:M	origin, ext_seq_id, map_confidence, link_id

Notes (normative):

Every event includes the common header: ts (system-clock), cnt (per-origin monotonic), origin (XR_PMC/HOST/PMBUS).

4.7.2.3.1 Snapshot Scope: "All Rails" as Mandatory Baseline

Snapshot scope shall follow standard power-management practice: **all integrated power rails** are required for computing power, efficiency, timing adjustments, and causality analysis. Therefore, the minimum snapshot shall not be reduced to a small subset unless a node-specific rail inventory explicitly declares exclusions.

Snapshot definition rules:

- Snapshot shall include rail-level **V/I/T** (where sensors exist), selected source state, and continuity buffer interface fields (where applicable).
- Rail inventory and sensor availability shall be node-class and product dependent, but the schema shall remain stable.

Table 4–11 Snapshot Minimum Fields (Concise)

Domain	Field	Required	Notes
Meta	ts	Yes	Timestamp in **system clock** timebase.
Meta	schema_ver	Yes	Snapshot schema version; aligns with EvidenceBundle schema.
Meta	node_class / sku_id	Yes	Declares node class (A1–A4) and product/SKU identifier (ASIC phase).
Meta	profile_id	Yes	Active profile identifier; enables audit/replay.
Input Sources	src_present[]	Yes	Enumerates detected sources (e.g., PoE/ACDC/Batt/Ext); no implicit assumptions.
Input Sources	src_selected	Yes	Current selected source ID.
Input Sources	src_state[]	Yes	Per-source state (READY/ACTIVE/FAULT/DERATE).
Power Rails	rail_v[]	Yes*	Per-rail voltage; rail list is declared by Table 4–8B. (*Required if sensor exists.)
Power Rails	rail_i[]	Yes*	Per-rail current; (*Required if sensor exists.)
Power Rails	rail_t[]	Conditional	Rail/zone temperature; required where thermal sensors exist.
Power Rails	rail_p[]	Conditional	Per-rail power if computed; if absent, define computation method elsewhere.
Aggregates	p_in_total	Conditional	Total input power (if measurable/computable).
Aggregates	p_out_total	Conditional	Total output/rail power (if measurable/computable).
Aggregates	efficiency	Conditional	Efficiency estimate; must declare computation assumptions.
Protection	prot_flags	Yes	Bitset or structured flags (OCP/OVP/UVP/OTP active/latched).
Protection	limit_state[]	Conditional	Current limit thresholds per domain/rail where applicable.
Authority	authority_state	Yes	Host/EC/service mode; actor authority declared.

Authority	service_gating	Conditional	Debug/service gating state (enabled/locked/temporary).
Continuity (External)	cont_mode	Conditional	RT/hold-up/UPS mode label when external continuity interface exists.
Continuity (External)	cont_state	Conditional	ARMED/ENGAGED/SUSTAIN/EXIT; aligns to events EV-11~EV-14.
Continuity (External)	cont_guardrail_set_id	Conditional	Guardrail profile applied for external buffer engagement.
Continuity (External)	cont_vcap	Conditional	External buffer measurement (e.g., Vcap) if instrumented.
Telemetry Integrity	gap_marker	Conditional	Snapshot may reference an active loss window; do not hide data loss.

Table 4–12 Rail Inventory Declaration (Concise)

Product	**Rail List (IDs)**	**Sensor Availability**	**Exclusions**
A1 Product	RAIL_01…RAIL_N (mainboard-defined)	V/I: per-rail where instrumented; T: zone + hotspots	None by default; exclusions must be explicitly declared and justified.
A2-S Product	RAIL_01…RAIL_N (secondary-defined)	V/I: secondary rails; T: secondary zones	Primary-side rails not present are excluded by definition (declare as not applicable).
A2-P Product	RAIL_01…RAIL_N (primary boundary-defined)	V/I: boundary rails; T: safety zones	Secondary distribution rails excluded by boundary definition (declare).
A3 Product	RAIL_01…RAIL_N (backplane-defined)	V/I: shared domains where instrumented; T: backplane zones	End-device rails excluded; only backplane-managed domains included.
A4 Product	RAIL_01…RAIL_N (grid node-defined)	V/I: endpoint rails where instrumented; T: enclosure zones	PoE rails out-of-scope; UPS/grid-level rails handled externally (declare).

Notes (normative):

Rail IDs are **declared** (not inferred). Each product/SKU must ship a rail inventory declaration compatible with the snapshot schema.

"Sensor Availability" indicates which snapshot fields are required; if a sensor does not exist, the field must be omitted or explicitly marked as unavailable per schema rules (no silent zeros).

4.7.2.4 Regime Analysis: All Abnormal Regimes Must Be Detectable

L2 shall support analysis across **all abnormal regimes** relevant to power-path integrity and continuity behavior. Regimes are defined as named states with entry/exit conditions and evidence linkage (not informal labels). At minimum, the regime set shall cover:

- droop/brownout regimes,
- thermal hotspot/overtemperature regimes,
- ESR/aging proxy regimes for external buffers (where continuity interfaces exist),
- source-chatter / oscillation regimes,
- protection-trip clustering regimes,
- telemetry integrity/anomaly regimes (gaps, resets, drift).

Table 4–13 Regime Catalog (Concise)

Regime	Entry Criteria (examples)	Exit Criteria (examples)	Evidence References
Droop / Brownout Frequent	≥ N droop events within window W; PG_DEASSERT + UVP_TRIP clustering	No droop for window W; rails stable above threshold	EV-05, EV-08; snapshot rail_v[] minima
Droop / Brownout Severe	Single droop below critical threshold; multiple rail groups affected	Recovery to stable PG_ASSERT state for all required groups	EV-05, EV-04, EV-08
Source Chatter / Oscillation	Repeated SRC_SELECT toggles within short interval; transition abort patterns	Source remains stable for window W; no rapid toggles	EV-01, EV-02, EV-03; snapshot src_selected
Inrush Stress / Limiting	Inrush limit engaged repeatedly during ingress; abnormal ramp time	Inrush within expected envelope; no repeated limiting	EV-10; snapshot src_state[] + ramp profile
OCP Trip Cluster	≥ N OCP trips on same rail/channel within W	No OCP trips for W; rail load stabilizes	EV-06; snapshot rail_i[] vs limits
OVP / UVP Instability	Alternating OVP/UVP trips or repeated UVP with partial recovery	Stable rail voltage margins maintained	EV-07, EV-08; snapshot rail_v[]
Thermal Hotspot Escalation	Hotspot sensor crosses warn/crit thresholds; repeated OTP near-trip	Temperature returns below warn threshold with hysteresis margin	EV-09; snapshot rail_t[] / zone temps

Telemetry Integrity — Data Gaps	Any DATA_GAP beyond allowed duration; missing required snapshots	Gap closes and integrity flag clears; data continuity restored	EV-18; EvidenceBundle gaps[]
Telemetry Integrity — Counter Reset	RESET_MARKER or non-monotonic counter detected	Ordering re-established with declared discontinuity	EV-19; ordering policy record
External Continuity Engage Frequent	CONT_ENGAGE triggered ≥ N times within W	No engagement for W; stable without external buffer	EV-12; snapshot cont_state
External Continuity Sustain Overrun	Sustain duration exceeds profile guardrail; repeated sustain markers	Exit occurs within allowed duration; guardrail compliance restored	EV-13, EV-14; snapshot cont_guardrail_set_id
External Buffer ESR/Aging Proxy	Increasing droop depth during continuity; Vcap sag slope exceeds baseline	Proxy metrics return within baseline envelope	EV-13/EV-14 + snapshot cont_vcap + droop metrics
Authority Thrash / Mode Instability	Frequent AUTH_MODE_CHANGE; repeated service gating toggles	Mode stable for W; gating stable	EV-15; snapshot authority_state
Policy Apply Failure / Rollback	POLICY_APPLY fails or triggers rollback marker	Successful apply with audit completeness	EV-16; audit fields + result
Cross-Stream Alignment Low Confidence (A1/A4)	Host/PMBus mapping confidence below threshold; inconsistent anchors	Mapping confidence restored; anchors consistent	EV-20; timebase mappings[]

Notes (normative):

Regimes are **named states with explicit criteria**; implementations may refine thresholds, but must preserve regime semantics and evidence linkage.

Entry/exit criteria must reference **core evidence events (EV-01…EV-20)** and/or snapshot fields declared in Table 4–8A.

4.7.2.5 L3 Outputs: Both Policy Proposal and Diagnosis Report Are Mandatory

- L3 shall produce two output families:
- **Policy Proposal** (策略提案): bounded, guardrail-compatible recommendations intended for profile updates or runtime policy adjustments.

- **Diagnosis Report** (診斷報告): human-readable analysis that references evidence ranges and explains causal chains and constraints.
- L3 shall never emit opaque outputs without evidence references. Every recommendation shall cite the evidence bundle segments that triggered it and shall declare compatibility against guardrails.

Table 4–14 L3 Output Contract (Concise)

Output Type	Required Fields	Evidence Linkage	Guardrail Check
PolicySuggestion (策略建議)	target(node_class, profile_id); suggestions[] (param, set_to, bounds); confidence; reason_codes[]	Each suggestion includes evidence_refs[] (core event IDs + ranges + snapshot pointers)	Mandatory: guardrail_compatibility computed before emitting; suggestions must be bounded.
DiagnosisDraft (診斷草稿)	summary; regime_list; key_findings[]; assumptions[]	Each finding cites evidence_refs[]; must call out DATA_GAP and RESET_MARKER when present	Mandatory: diagnosis must declare whether any conclusion is limited by missing data or mode constraints.
GuardrailReport (護欄檢查報告)	guardrail_set_id; checks[] (rule_id, pass/fail, margin); blocked_actions[]	Each failed check links to the evidence that triggered the boundary	Mandatory gate: if failures exist, suggestions must be clipped or moved to “blocked_actions”.
Confidence & Bounds Report (信心/界限)	bounds[] per key suggestion; uncertainty_sources[]	Links uncertainty to evidence quality (gaps, mapping confidence, sensor availability)	Mandatory: if uncertainty exceeds threshold, proposals must be “Advisory-only” by mode policy.

4.7.2.6 L4 Artifacts and Interfaces: JSON for Components, Text for Human Interface

L4 shall publish artifacts in two formats:

Component-facing artifact: JSON (元件使用 JSON) conforming to a versioned schema, consumable by firmware/host/PEC tooling and CI gates.

Human-facing artifact: text (human interface 使用 text), suitable for board bring-up, validation reviews, and partner audits.

Both formats shall share the same underlying identifiers (schema version, proposal version, evidence reference IDs) to ensure traceability across machine and human workflows.

Table 4–15 Artifact Formats (Concise)

Artifact	Format	Consumer	Versioning	Notes

EvidenceBundle	JSON (schema)	L2/L3/L4 pipeline; validation tools	schema_ver	Must include timebase authority + events ordering + gaps[]; origin tagging required.
FeatureFrame	JSON (schema)	L3/L4; analytics tools	schema_ver	Regimes + features + bounds; deterministic transforms preferred.
PolicyProposal	JSON (schema)	Firmware/PEC tooling; CI gates; profile packager	proposal_ver + schema_ver	Component-facing artifact; includes deltas[], evidence_refs[], guardrail_compatibility, audit.
Diagnosis Report	Text (plain / Markdown-like)	Engineers / reviewers / partners	report_ver (or proposal_ver reference)	Human-facing; must reference evidence ranges and call out gaps/resets.
Guardrail Set	JSON (schema)	L3/L4; runtime policy checker	guardrail_ver	Declares hard limits, margins, blocked actions; used for delegated autonomy.
Profile Pack	JSON (schema)	Runtime policy engine	profile_ver	Parameter set + defaults; compatible with guardrail set; supports rollback constraints.
Audit Manifest	JSON	Release / compliance / partner review	manifest_ver	Hash list of artifacts + build metadata; ties to secure provisioning.

4.7.2.7 Guardrails Ownership and Autonomy Mode: Selectable by Deployment

AI authority shall be **selectable** (可選) by deployment context. The specification defines three operating modes:

Mode A — Advisory (Human-in-the-loop): AI produces proposals and reports; execution requires explicit approval.

Mode B — Delegated (Bounded Autonomy): AI may apply a constrained subset of changes within pre-approved guardrails and authority rules; all actions require audit evidence.

Mode C — Locked-down (No Actuation): AI performs analysis only; no runtime policy change is permitted.

Autonomy mode shall be an explicit configuration with authority ownership declared, service/debug gating enforced, and auditability mandatory.

Table 4–16 Autonomy Modes (Concise)

Mode	Allowed Actions	Preconditions	Evidence & Audit Requirements

Mode A — Advisory (Human-in-the-loop)	Generate PolicyProposal + Diagnosis only; no runtime application	Guardrails defined; authority model present	Proposal must include evidence_refs[], guardrail_compatibility, and audit manifest entry.
Mode B — Delegated (Bounded Autonomy)	Apply a bounded subset of policy deltas automatically within guardrails; generate diagnosis	Guardrails + approved action list; service/debug gating enforced; rollback available	Every applied delta emits POLICY_APPLY event; audit manifest + integrity check required; blocked actions must be recorded.
Mode C — Locked-down (No Actuation)	Analysis-only; no proposal application (may still emit proposal as “non-actionable”)	High-risk environments or incomplete validation	Diagnosis must call out limitations; all suggestions marked non-executable; evidence gaps/resets must be highlighted.

5 FPGA PHASE SPECIFICATION

The FPGA phase provides the **A1–A4 superset baseline** as an executable reference implementation. Its primary objective is to de-risk architecture semantics, evidence contracts, and validation flows before productizing into **ASIC SKUs (A1 / A2-S / A2-P / A3 / A4)**. The FPGA deliverable is therefore judged by **contract fidelity, replayability, and validation coverage**, not by cost or final form-factor optimization.

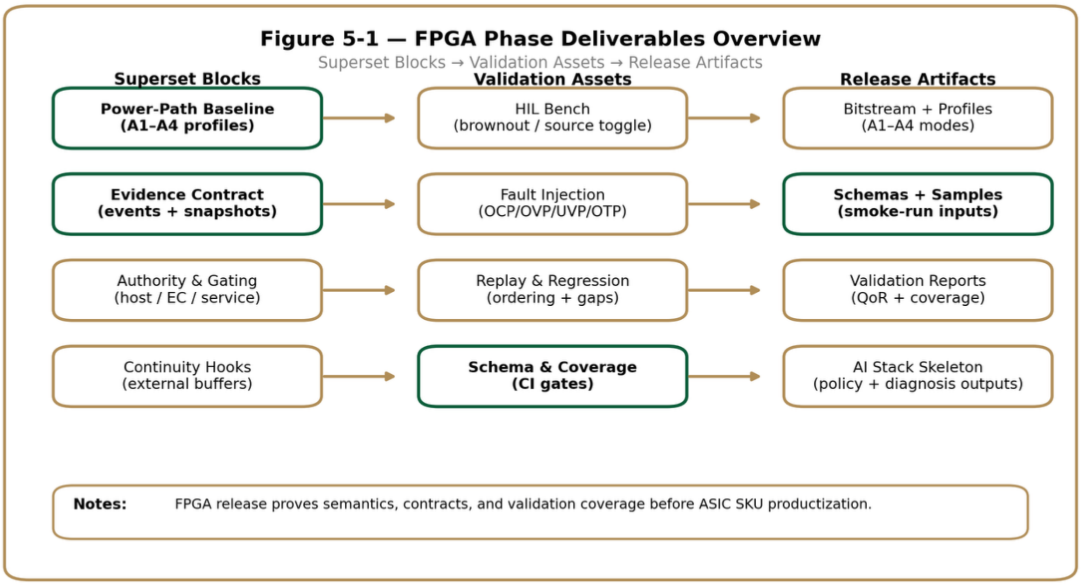


Figure 5–1 FPGA Phase Deliverables Overview (Superset Blocks → Validation Assets → Release Artifacts)

5.1 Scope and Non-Goals

The FPGA phase shall implement the following as **mandatory scope**:

- Power-path control baseline sufficient to express A1–A4 node behaviors (source selection, transitions, protection, containment).
- Evidence contract baseline: ordered events (EV-01…EV-20), gaps/resets, schema versioning, and snapshot minimum fields.
- Authority and mode semantics sufficient for governance boundary definition (Host / EC(PEC) / service gating).
- Continuity interface hooks for external buffers where applicable (RT / hold-up / UPS) with engagement timing evidence.

Non-goals (explicit):

- Tapeout-optimized power/performance/area (PPA) targets.
- Final product partitioning or SKU-level BOM minimization.
- On-die energy storage claims or integration of RT energy elements.

5.2 FPGA Platform Targets (A1–A4 Superset)

The FPGA platform shall be constructed as a superset baseline that can be configured into A1–A4 operating profiles through parameterization and interface enablement.

A1/A4 profiles shall additionally enable multi-source evidence ingest alignment (Host logs / PSU PMBus logs) at L1.

A2-S / A2-P / A3 profiles shall remain XR-PMC evidence-only at L1.

Table 5–1 FPGA Profiles (Concise)

Profile	Node Class	Enabled Interfaces	Evidence Sources	Notes
P-A1	A1	XR-PMC bus (PMBus/SMBus/I^{2}C/I3C); authority hooks; continuity hooks (external buffer); optional PoE PD interface (if present)	XR-PMC events/telemetry + Host logs + PSU PMBus logs	A1 is the richest integration profile; requires cross-stream time mapping into system clock.
P-A2S	A2-S	XR-PMC bus; secondary-side control/telemetry; continuity hooks (if used as hold-up shaping)	XR-PMC events/telemetry only	No PoE requirement; evidence-only ingest.
P-A2P	A2-P	XR-PMC bus; primary boundary signals; continuity hooks for hold-up energy mgmt under safety boundary	XR-PMC events/telemetry only	Explicitly constrained by isolation/safety boundary; avoid claims of board-level RT module.
P-A3	A3	XR-PMC bus; arbitration/authority markers; backplane telemetry/control	XR-PMC events/telemetry only	Authority model must be explicit (mainboard/backplane/PSU PMC).
P-A4	A4	XR-PMC bus; authority hooks; continuity hooks (grid continuity interface, if applicable)	XR-PMC events/telemetry + Host logs + PSU	PoE out-of-scope; supports multi-source evidence ingest similar to A1.

			PMBus logs (if present)	

5.3 Evidence Contract Compliance (Normative)

The FPGA implementation shall be compliant with the following evidence requirements:

- Implement all **20 core Evidence Event IDs** with applicable branch variants per node class.
- Enforce system-clock anchored timestamps with monotonic per-origin counters, explicit gaps, and reset markers.
- Emit snapshots compliant with the minimum field set and a declared rail inventory for the active profile.
- FPGA compliance shall be verified via schema validation and replay tests using recorded samples and injected faults.

Table 5–2 Evidence Compliance Gates (Concise)

Check	Method	Pass Criteria	Artifacts
Schema validity	JSON/schema validation on EvidenceBundle + Snapshot	100% records validate; schema_ver declared; required fields present per node profile	Validation report; schema version manifest
Timebase authority	Verify timebase.authority and mapping records	authority=SYSTEM; mappings exist when non-system clocks present; no silent clock merge	Timebase mapping report; mapping confidence log
Ordering correctness	Replay ordering by (ts, origin priority, cnt) with gap handling	Monotonic ordering holds; ties resolved deterministically; no negative jumps; explicit discontinuities only	Ordering audit log; replay checksum
Core event coverage (EV-01…EV-20)	Coverage scan over event stream	All applicable core IDs present per profile; variants allowed but do not alter meaning	Event coverage report; per-ID sample excerpts
Payload minimality	Validate minimal payload fields per event ID	Minimal payload always present; optional fields	Payload compliance report

		permitted; no "all-zero" placeholders	
Gap declaration	Inject loss windows + monitor runtime detection	Any loss emits DATA_GAP (EV-18) + gaps[]; downstream layers remain stable	Gap-injection test report; EvidenceBundle excerpts
Reset marker correctness	Inject reboot/counter reset	RESET_MARKER (EV-19) emitted; discontinuity declared; ordering resumes cleanly	Reset test report; before/after excerpts
Snapshot completeness	Snapshot validator against Table 4–8A	Required snapshot fields present; rail list declared; absent sensors are declared (no silent zeros)	Snapshot compliance report; rail inventory declaration
Authority attribution	Mode switching + gated actions tests	AUTH_MODE_CHANGE (EV-15) and POLICY_APPLY (EV-16) include actor/mode; gating states auditable	Mode/gating regression logs
Cross-stream alignment (A1/A4)	Host/PMBus anchoring tests	Host+PMBus events normalized; mapping to system clock recorded; low-confidence emits explicit flag/event	Alignment report; EV-20 samples
Evidence references in outputs	Run AI stack smoke-run	PolicyProposal + diagnosis include evidence_refs[]; gaps/resets are cited where relevant	policy_proposal.json; diagnosis_report.txt; manifest

5.4 Power-Path Control Baseline (Functional)

The FPGA baseline shall implement:

- Deterministic source selection and transition sequencing (EV-01~EV-03).
- Power-good assertion/deassertion semantics (EV-04~EV-05).
- Protection trip/clear semantics (EV-06~EV-10) with audit-friendly payloads.
- Containment behavior that preserves safety and prevents uncontrolled oscillation.

Where node profiles exclude certain input sources (e.g., PoE out-of-scope), the FPGA profile shall explicitly disable related logic and associated event variants to prevent ambiguous behavior.

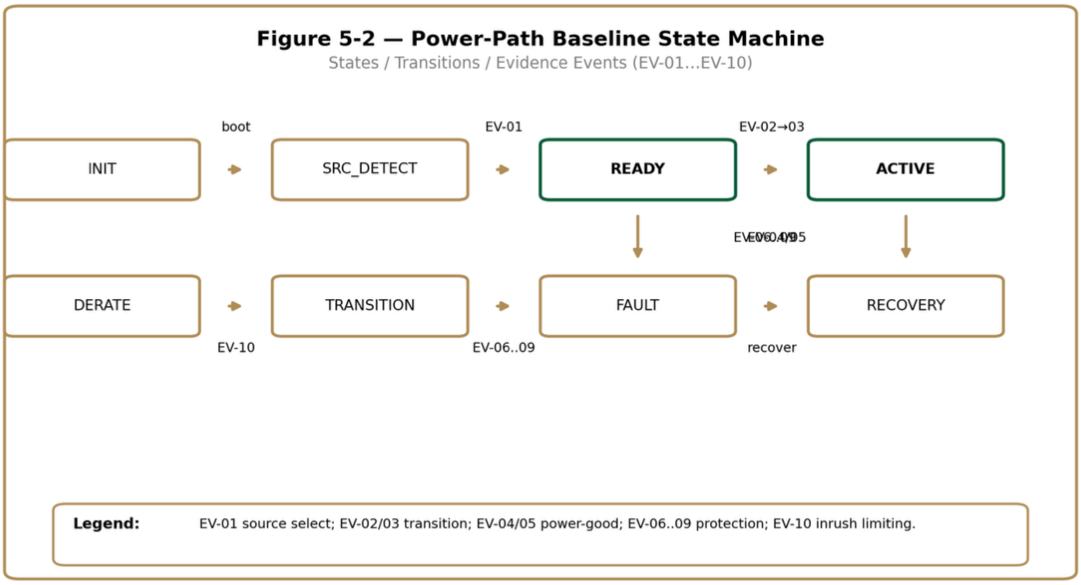


Figure 5–2 Power-Path Baseline State Machine

5.5 Continuity Interface Hooks (External Buffer)

Continuity behavior in FPGA phase shall be expressed via external continuity interface hooks and evidence events, and is validated by timing windows and guardrails.

Architecture template line (RT external): Physical Layer includes interfaces to external hold-up/ride-through energy buffers; silicon defines sensing/control hooks and protection limits, not the energy storage element itself.

Continuity evidence must include arm/engage/sustain/exit semantics (EV-11~EV-14) and must be replayable under injected brownout profiles.

Table 5–3 Continuity Hooks (Concise)

Signal	Meaning	Evidence Event	Guardrail
CONT_PRESENT	External continuity buffer/module detected and qualified	EV-11 CONT_ARM (qualify result included)	Must be present=TRUE and integrity=OK before any engage is allowed

CONT_ARM	Policy arms continuity function for the current power regime	EV-11 CONT_ARM	Arm only in allowed modes; rate-limit arming; require authority token / service gating
CONT_ENGAGE	Engage external buffer (ride-through/hold-up assist)	EV-12 CONT_ENGAGE	Engage only when trigger window satisfied; block if Vcap<Vcap_min or integrity low
CONT_SUSTAIN	External buffer is sustaining load (hold phase)	EV-13 CONT_SUSTAIN	Enforce T_max sustain; enforce thermal / ESR-proxy constraints; emit DATA_GAP if telemetry missing
CONT_EXIT	Disengage external buffer and return to nominal path	EV-14 CONT_EXIT	Require recovery criteria; enforce cooldown; prevent chatter via hysteresis and minimum off-time
VCAP_SENSE (opt.)	Capacitor/buffer voltage telemetry (if instrumented)	Referenced by EV-12/13 payload	Use as Vcap_min / dV/dt sanity; flag aging/anomaly when drift exceeds bounds
IBUF_SENSE (opt.)	Buffer current telemetry (if instrumented)	Referenced by EV-13 payload	Clamp to Ibuf_max; detect abnormal spikes; latch safe exit on violation
CONT_INHIBIT	Hard inhibit line to prevent engage (safety / debug / policy)	Included in EV-11/12 context	Any asserted inhibit forces “analysis-only”; proposals must record blocked action with evidence

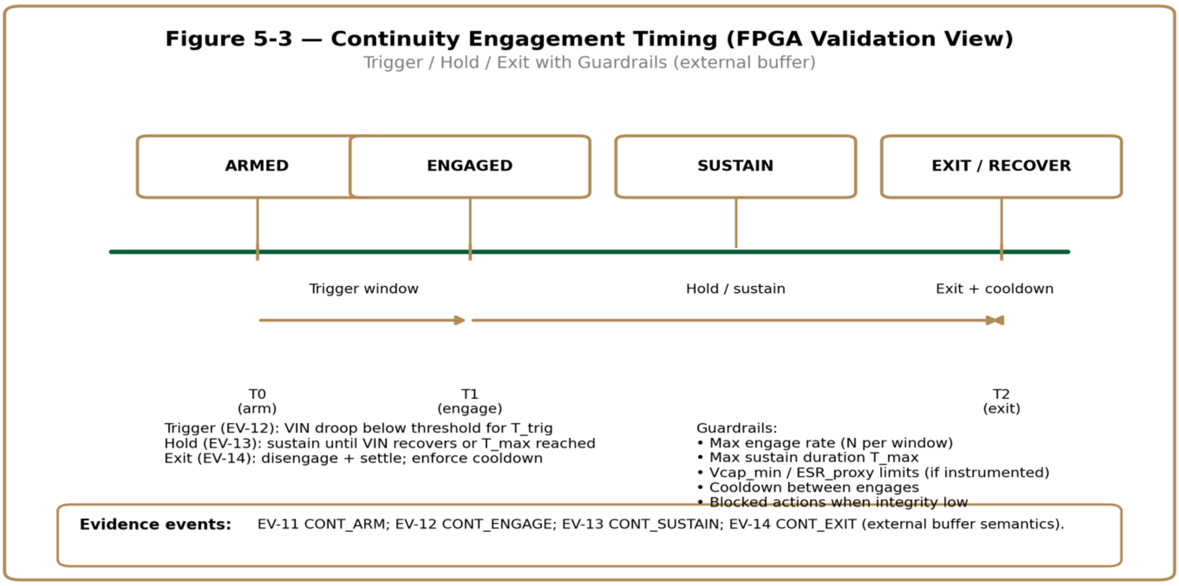


Figure 5–3 Continuity Engagement Timing (Trigger / Hold / Exit) — FPGA Validation View

5.6 Validation Plan and Lab Assets (FPGA)

The FPGA phase shall be validated using an evidence-driven methodology:

- Hardware-in-the-loop (HIL) execution with programmable droop profiles and input source toggling.
- Fault injection coverage for OCP/OVP/UVP/OTP thresholds and timing margins.
- Replay and regression tests for ordering, gaps, resets, and cross-stream alignment (A1/A4).
- Audit completeness checks: every policy-relevant action produces evidence references and manifests.

Table 5–4 FPGA Validation Assets (Concise)

Asset	Purpose	Coverage	Output Artifacts
HIL Power Bench	Deterministic droop / brownout / source-toggle injection	Trigger/hold/exit timing; transition sequencing; anti-chatter	Run logs; EV streams; timing plots; pass/fail summary
Programmable Load + Step Profiles	Validate transient response windows under controlled load	Engage thresholds; sustain limits; recovery margins	Step-response captures; EV-12/13/14 samples; guardrail compliance report
Fault Injection Harness	Force OCP/OVP/UVP/OTP and latch/clear behavior	EV-06..09 correctness; containment; recovery safety	Fault matrix report; per-fault evidence excerpts; replay checksums
Multi-Source Evidence Ingest (A1/A4)	Validate host/PSU logs alignment into system clock	Timebase mapping; ordering; confidence flags	Alignment report; mapping tables; EV-20 samples
Evidence Schema Validator	Enforce schema + minimal payload contracts	EV-01...EV-20 presence; payload required fields; gaps/resets	Validation report; schema manifest; rejection cases
Replay & Regression Runner	Deterministic replay of recorded runs	Ordering determinism; gap handling; output stability	Replay checksum; diff report; regression dashboard
Mode/Gating Test Suite	Verify authority model + service/debug gating	EV-15/16 audit; blocked actions; autonomy mode constraints	Mode transition logs; policy-apply logs; audit manifest
Coverage Scanner	Quantify event/regime/rail coverage by profile	Per-profile applicability; missing events/variants	Coverage matrix; heatmap (optional); release gate summary
Golden Sample Packs	Provide canonical input samples for smoke-runs	Minimal & stress samples; reset/gap scenarios	samples/; expected artifacts set; pass criteria sheet
Release Manifest Builder	Tie artifacts to integrity/provisioning	Hashing; version binding; reproducibility	manifest.json; hashes; build metadata; provenance notes

5.7 FPGA Release Artifacts (What is Shipped)

The FPGA phase release shall include:

- Bitstream/package + configuration profiles for A1–A4 modes.
- Evidence schemas and sample recordings for smoke-run gates.
- Validation reports and coverage summaries sufficient to justify ASIC productization decisions.
- A reference AI stack skeleton that can run end-to-end on the recorded evidence streams.

Table 5–5 FPGA Release Package (Concise)

Item	Format	Owner	Notes
FPGA Bitstream	.bit / .bin	FPGA	Signed build; traceable build metadata; profile-compatible
Profile Packs	JSON (machine) + text (human)	Silicon/Platform	Per-profile enablement (A1–A4); versioned; rollback-safe
Evidence Schema Bundle	JSON Schema + ID registry	Governance	Event IDs (EV-01…EV-20), payload minima, ordering contract
Sample Evidence Packs	.jsonl / .csv / .pcap (as applicable)	Validation	Includes gap/reset cases; A1/A4 multi-source samples included
Validation Reports	PDF/MD	Validation	Gate summary + exception list; references to run IDs and manifests
Replay/Regression Tooling	scripts + configs	Validation/Tools	Deterministic replay; checksum diffs; CI-friendly
HIL/Fault Injection Recipes	configs + wiring notes	Validation	Bench recipes to reproduce claims; links to required equipment
AI Stack Skeleton	source tree + minimal runners	AI/Platform	End-to-end smoke-run; outputs policy+diagnosis; uses samples/
BSP/SDK Stubs (FPGA)	headers + examples	Platform	Interface contract only; binds to evidence schema and profiles
Release Manifest	manifest.json + hashes	Release Eng	Artifact hash tree; provenance; version binding across items

6 PROGRAMMABLE ASIC PHASE SPECIFICATION

The programmable ASIC phase productizes the XR-VPP superset baseline into **five ASIC products** (A1 / A2-S / A2-P / A3 / A4), preserving the same governance/evidence backbone while selecting a cost/feature-appropriate IP set and packaging. The ASIC phase is evaluated by **contract equivalence** (evidence + ordering + authority), **guardrail determinism**, and **qualification readiness** (DFT/DFM/signoff), rather than feature expansion

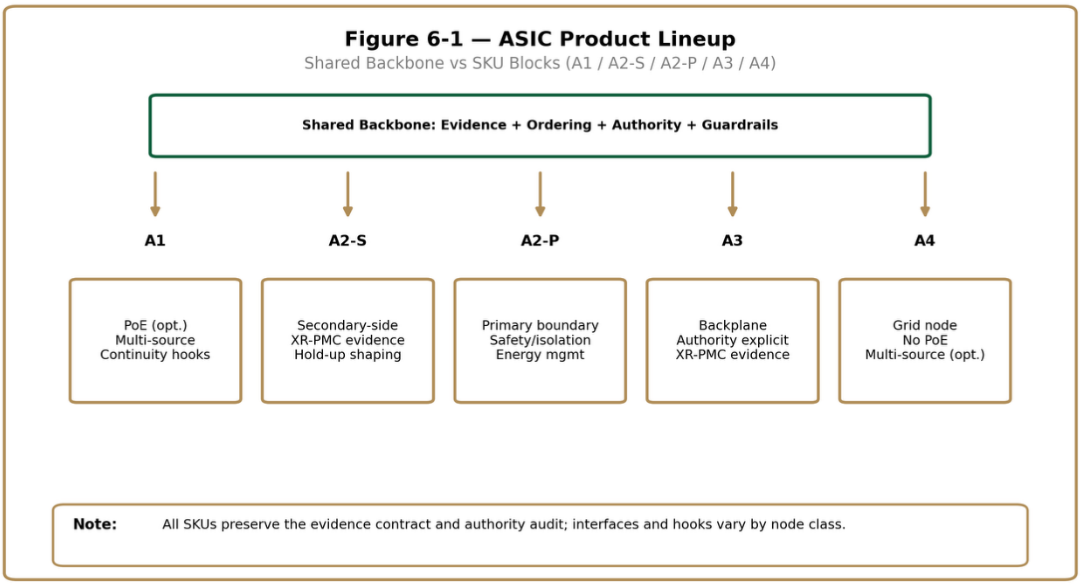


Figure 6–1 ASIC Product Lineup (A1/A2-S/A2-P/A3/A4) — Shared Backbone vs SKU Blocks

6.1 Productization Rules (FPGA → ASIC)

The following rules are normative for ASIC productization:

- Evidence contract equivalence: EV-01…EV-20 semantics are preserved; any SKU-specific omission must be explicit and justified by scope (interface not present).
- Ordering equivalence: timebase fields, gap/reset markers, and deterministic tie-break rules remain unchanged.
- Authority equivalence: auditability of mode, actor, and gating remains mandatory even when interfaces are reduced.
- Continuity semantics equivalence: external buffer engagement is expressed through hooks + events; ASIC does not imply on-die energy storage.

Table 6–1 ASIC Productization Rules (Concise)

Rule	Rationale	Enforcement Gate	Artifacts
Evidence Contract Equivalence	Preserve cross-phase comparability (FPGA→ASIC)	EV schema validation; required IDs present or explicitly N/A by SKU	Evidence schema bundle; EV registry; compliance report
Ordering Contract Equivalence	Deterministic replay and auditability	Timebase fields + gap/reset markers validated; replay checksum stable	Ordering spec; replay logs; checksum diff report
Authority & Audit Mandatory	Prevent ambiguous control in multi-PMC systems	Mode/actor recorded on every action; blocked actions logged	Audit manifest; autonomy mode logs; gating test results
Explicit Interface Exclusions	Avoid "silent scope creep" per SKU	Interface disable bits + negative tests for disallowed ports	SKU profile; exclusion test suite; HIL configs
Continuity is External-buffer Semantics	Avoid invalid "on-die RT" interpretation	Continuity hooks/events present; no claims of on-die energy storage	Continuity hook spec; EV-11..14 samples; guardrail report
Guardrail Determinism	Ensure predictable containment under stress	Max-rate, hysteresis, cooldown, `T_max` enforced under injection	Guardrail config; fault-storm test logs; pass/fail summary
Sensor Absence is Declared	Prevent fake zeros / hidden blind spots	Rail inventory declaration + sensor availability required	Rail list manifest; snapshot schema; validation output
Qualification Readiness	ASIC must meet DFT/DFM/signoff + production tests	DFT insertion, test modes, signoff checks, qual matrix complete	Signoff checklist; DFT report; qual matrix; release manifest
Artifact Version Binding	Prevent drift across firmware/profile/schema	Versioned packs with hashes; anti-rollback where applicable	`manifest.json`; hashes; provisioning notes
Regression Parity vs FPGA	Ensure ASIC does not regress baseline behaviors	Golden sample replay parity; key scenarios pass	Golden samples; regression dashboard; parity report

6.2 ASIC SKU Definitions (A1 / A2-S / A2-P / A3 / A4)

Each ASIC SKU shall be defined by:

- Node class applicability (A1–A4).
- Enabled interfaces (PoE/PMBus/I3C/etc.) and exclusions.
- Evidence sources (XR-PMC only vs multi-source ingest).
- Authority model constraints and autonomy mode availability.
- Continuity hook availability and guardrail defaults.

Table 6–2 ASIC SKU Summary (Concise)

SKU	Node	Interfaces	Evidence Sources	Authority	Notes
A1	Mainboard (A1)	PoE PD *(if enabled)*; PMBus/SMBus/ I^{2}C/I3C; host link *(system-defined)*	XR-PMC telemetry/events + **host logs** + **PSU PMBus logs** (multi-source)	Host-anchored authority; XR-PMC enforces guardrails; audit mandatory	PoE treated as first-class input option; continuity hooks for external buffer required where RT/hold-up is claimed
A2-S	Secondary-side (A2-S)	PMBus/SMBus/ I^{2}C/I3C (scope-limited); local rails sensors	XR-PMC telemetry/events only	Local authority with explicit gating; audit mandatory	PoE not required; continuity described as secondary shaping/hold-up assistance rather than board-level RT primitive
A2-P	Primary-side optional (A2-P)	Isolation/safety boundary interfaces *(as defined by platform)*; limited bus exposure	XR-PMC telemetry/events only (boundary-safe)	Safety-first authority; autonomy constrained by compliance gates	Not a “board-level RT module” claim; spec focuses on hold-up energy management + safety/isolation constraints
A3	Backplane (A3)	Backplane management bus; optional PMBus/SMBus/ I^{3}C; inter-controller link	XR-PMC telemetry/events; optional upstream summaries	**Arbitrated authority** (mainboard/backplane/ PSU PMC) with explicit ownership map	RT/continuity must be qualified as “continuity and insurance” and bound to the authority model (no ambiguous engage ownership)

A4	Grid node IPC (A4)	Industrial mgmt bus *(platform-defined)*; PMBus/SMBus/ I^2C/I3C optional	XR-PMC telemetry/events + **host logs** + **PSU PMBus logs** (when present)	System authority (site controller / host) with strict audit	PoE out-of-scope; continuity expressed via grid primitives (UPS/ride-through/protection coordination) + evidence alignment to system clock

6.3 Evidence, Telemetry, and Event Costs (ASIC Constraints)

ASIC implementations must preserve evidence completeness while meeting bandwidth and silicon constraints:

- Mandatory event set EV-01…EV-20 with minimal payload; optional fields are gated by SKU.
- Snapshots must include the minimum field set and a declared rail inventory; absent sensors must be declared (no silent zeros).
- Event-rate guardrails must prevent log floods under chatter/fault storms while preserving auditability.

Table 6–3 ASIC Evidence Budget (Concise)

SKU	Max Event Rate	Snapshot Period	Storage/Transport Notes
A1	≤ 200 events/s (burst), ≤ 50 events/s (sustained)	200–500 ms (adaptive)	Multi-source ingest may dominate bandwidth; require rate-limit + priority classes; transport via platform host link + optional mgmt bus
A2-S	≤ 120 events/s (burst), ≤ 30 events/s (sustained)	500–1000 ms	XR-PMC-only evidence; prioritize continuity + protection events; store rolling window locally when uplink absent
A2-P	≤ 80 events/s (burst), ≤ 20 events/s (sustained)	1000–2000 ms	Boundary-safe payloads only; strict minimal fields; prefer aggregated snapshots; transport under safety/isolation constraints
A3	≤ 150 events/s (burst), ≤ 40 events/s (sustained)	300–800 ms	Must include authority/arbitration metadata; transport to both upstream (mainboard) and local (backplane) logs as applicable
A4	≤ 200 events/s (burst), ≤ 50 events/s (sustained)	200–800 ms (adaptive)	When host/PSU logs present, evidence alignment adds metadata; require gap/reset markers and confidence flags for multi-source merges

Notes (normative):

- "Burst" budgets apply under fault storms; sustained budgets must remain within storage/transport thermal limits.
- Event-rate guardrails shall preserve auditability: when rate-limited, emit a **rate-limit summary** record rather than silently dropping.

6.4 Physical Interface and Integration Notes

ASIC interface selection is SKU-dependent:

- A1 may include PoE PD interface support and multi-source evidence integration.
- A2-S / A2-P prioritize boundary correctness (secondary shaping vs primary safety/isolation constraints).
- A3 must explicitly encode authority/arbitration model across mainboard/backplane/PSU controllers.
- A4 excludes PoE; focuses on grid continuity primitives integration and multi-source evidence ingest where present.

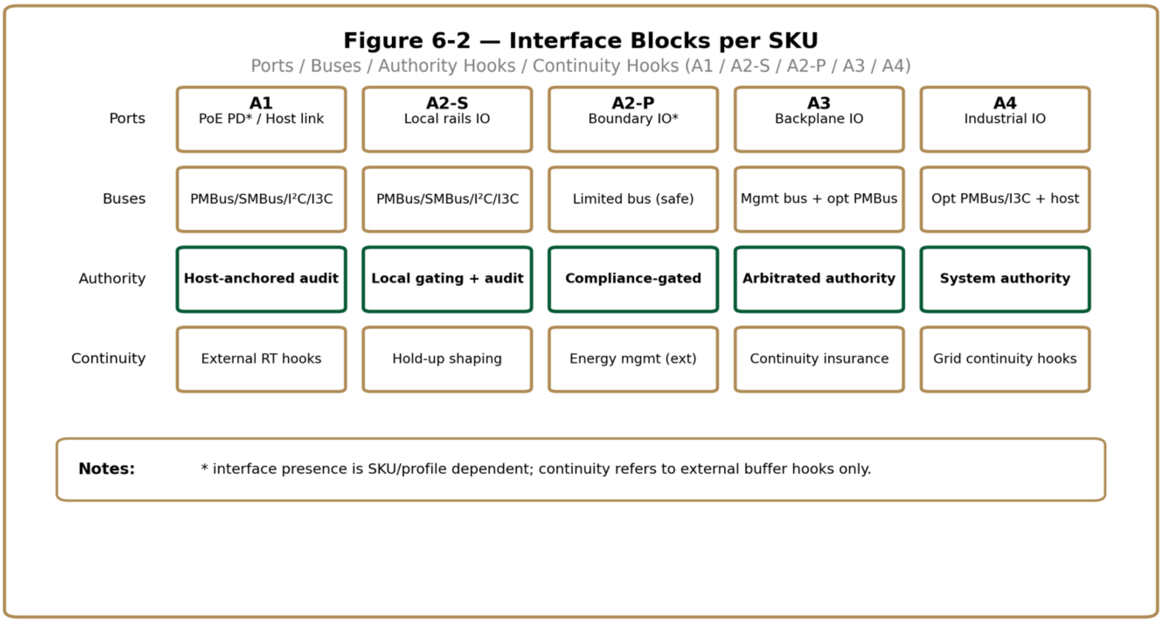


Figure 6–2 Interface Blocks per SKU (Ports / Buses / Authority Hooks / Continuity Hooks)

6.5 Continuity (External Buffer) — ASIC Requirements

ASIC continuity requirements remain strictly **external-buffer** oriented.

Architecture template line (RT external): Physical Layer includes interfaces to external hold-up/ride-through energy buffers; silicon defines sensing/control hooks and protection limits, not the energy storage element itself.

ASIC SKUs that expose continuity hooks must:

- Implement deterministic engage/exit timing, anti-chatter, cooldown, and T_max sustain limits.
- Emit EV-11...EV-14 events with minimal payload and guardrail context.
- Provide instrumentation hooks for Vcap / ESR proxy / thermal proxy where available, and degrade gracefully when absent.

Table 6–4 Continuity Hooks by SKU (Concise)

SKU	Hooks	Evidence	Default Guardrails
A1	CONT_PRESENT, CONT_ARM, CONT_ENGAGE, CONT_SUSTAIN, CONT_EXIT; optional VCAP_SENSE, IBUF_SENSE, CONT_INHIBIT	EV-11 CONT_ARM, EV-12 CONT_ENGAGE, EV-13 CONT_SUSTAIN, EV-14 CONT_EXIT	Trigger debounce (T_trig); T_max sustain; cooldown; anti-chatter hysteresis; Vcap_min / ESR-proxy (if available); rate-limit engages per window; block on integrity low
A2-S	CONT_PRESENT, CONT_ARM, CONT_ENGAGE, CONT_EXIT; optional VCAP_SENSE	EV-11..14 (subset allowed; no multi-source dependency)	Conservative T_max; engage only in secondary-side shaping regimes; tighter cooldown; require present=TRUE; block on sensor absence if policy requires
A2-P	CONT_PRESENT, CONT_INHIBIT (mandatory); optional CONT_ARM, CONT_ENGAGE under compliance gate	EV-11 (presence/gating), EV-12 (if engage allowed)	Compliance-gated engage; hard inhibit dominates; minimal payload only; engage allowed only in pre-qualified regimes; strict rate-limit; forced safe-exit on uncertainty
A3	CONT_PRESENT, CONT_ARM, CONT_ENGAGE, CONT_SUSTAIN, CONT_EXIT; optional VCAP_SENSE / IBUF_SENSE	EV-11..14 + authority context (owner/controller ID)	Ownership/arbitration required before engage; T_max + cooldown enforced per-owner; anti-chatter across controllers; block engage on authority conflict or missing arbitration token
A4	CONT_PRESENT, CONT_ARM, CONT_ENGAGE, CONT_SUSTAIN, CONT_EXIT; optional grid hooks (UPS status in)	EV-11..14 + optional grid continuity references	Trigger windows aligned to system clock; conservative cooldown; sustain bounded by site policy; block engage when grid integrity is low; emit gap/reset markers for multi-source merges

Normative note (RT external): Continuity hooks and evidence events describe engagement of an **external** hold-up/ride-through buffer; they do not imply on-die energy storage.

6.6 DFT/DFM/Qualification Anchors (ASIC)

ASIC deliverables shall include qualification-ready provisions:

- DFT: scan insertion, BIST where applicable, test mode gating that preserves service security.
- DFM: signoff rules, derating profiles, and packaging constraints.
- Qualification: validation matrix referencing FPGA evidence baselines, HIL recipes, and regression suites.

Table 6–5 ASIC Qualification Gates (Concise)

Gate	Mandatory Checks	Evidence	Output Artifacts
G0 Spec Freeze	SKU scope, exclusions, and contracts frozen	Approved SKU summary; interface applicability matrix	Frozen spec revision; change-log
G1 Evidence Contract	EV registry + payload minima complete; N/A rules explicit	Schema validation runs; sample EV packs	Schema bundle; compliance report
G2 Ordering & Replay	Timebase + gap/reset rules enforced; deterministic replay	Replay checksums; multi-source alignment tests (A1/A4)	Replay report; checksum manifest
G3 Guardrail Determinism	Rate-limit, hysteresis, cooldown, T_max verified	Fault-storm benches; guardrail logs	Guardrail report; injected-run IDs
G4 Continuity Semantics	External-buffer hooks/events correct; no on-die RT claims	EV-11..14 samples; timing plots; inhibit tests	Continuity validation report
G5 Interface Correctness	Negative tests for excluded ports; protocol conformance for enabled	Bus compliance tests; PoE profile tests (A1 if enabled)	Interface conformance report
G6 DFT Readiness	Scan insertion; test modes; BIST where applicable; secure test gating	DFT reports; test coverage numbers	DFT package; ATPG summaries
G7 DFM & Signoff	STA, IR/EM, LVS/DRC, CDC/RDC, power intent	Tool signoff logs; waivers list	Signoff checklist; waiver log
G8 Qualification Matrix	Temperature/voltage corners; aging; ESD/latch-up; burn-in plan	Lab results; corner-run evidence	Qualification matrix; lab report set
G9 Production Test Plan	Manufacturing tests defined; limits; binning; traceability	ATE vectors; limits tables	Production test spec; vector release
G10 Release Integrity	Secure provisioning; anti-rollback; manifest binding	Provisioning trials; rollback attempt logs	Release manifest; security checklist

Table 6–6 Packaging & Cost Anchors (Template, concise)

SKU	Package	IO Budget	Notes
A1	【TBD】	【TBD】	PoE/host link may dominate pins; prioritize mgmt bus + continuity hooks; package must support thermals for always-on telemetry
A2-S	【TBD】	【TBD】	Secondary-side integration; minimal external IO; emphasize cost-optimized package
A2-P	【TBD】	【TBD】	Safety/isolation boundary constraints may dictate package; keep bus exposure minimal
A3	【TBD】	【TBD】	Backplane arbitration needs dedicated signals/IDs; consider redundancy in mgmt connectivity
A4	【TBD】	【TBD】	Grid node often needs robust industrial IO; ensure telemetry path and secure provisioning pins

Notes (normative):

Packaging choice and IO budget are gated by the **interface applicability** of each SKU; any added IO must map to an explicit interface contract.

Cost anchors here are placeholders for the later BOM/Program Plan sections; this table fixes **which fields must be declared per SKU** (package + IO + rationale) before tape-out decisions.

6.7 Release Artifacts (ASIC Phase)

The ASIC phase release package shall provide:

- Signed firmware/profile packs and schema bundles aligned to FPGA baselines.
- Reference drivers/BSP stubs and validation recipes.
- Evidence samples demonstrating equivalence and regressions vs FPGA.
- Manufacturing-oriented manifests and compliance documentation.

Table 6–7 ASIC Release Package (Concise)

Item	Format	Owner	Notes
Silicon Datasheet (per SKU)	PDF	Silicon	Includes interface applicability, guardrails, evidence contract summary
Register Map & Programming Guide	PDF/MD + .h	Silicon/Platform	Versioned; ties fields to evidence IDs and profiles
Firmware/ROM (if applicable)	binary + source tag	Silicon	Signed; traceable build metadata; anti-rollback policy stated

Profile Packs	JSON (machine) + text (human)	Platform/Governance	Versioned profile defaults; per-SKU enablement; rollback-safe
Evidence Schema Bundle	JSON Schema + EV registry	Governance	EV-01…EV-20; payload minima; ordering contract; N/A rules
BSP/SDK Package	headers + libs + examples	Platform	BSP template line applies for continuity APIs (external buffer semantics)
Validation Recipe Set	configs + wiring notes	Validation	HIL benches, fault injection, PoE derating tests (A1 if enabled)
Golden Sample Evidence Packs	`.jsonl` / `.pcap` / `.csv`	Validation	Includes multi-source samples for A1/A4; gap/reset cases included
Replay/Regression Runner	scripts + configs	Tools/Validation	Deterministic replay; checksum diff; CI integration
Qualification Package	checklist + reports	Silicon/QA	DFT/DFM/signoff outputs; qualification matrix; waivers list
Production Test Package	vectors + limits	Manufacturing Test	ATE vectors; limits tables; binning; traceability mapping
Security Provisioning Kit	docs + scripts	Security/Platform	Secure provisioning, key handling, debug/service gating policy
Release Manifest	`manifest.json` + hashes	Release Eng	Hash tree binds schema/profile/fw/datasheet; provenance and build IDs

7 BSP / SDK / TELEMETRY SCHEMA (BOARD-LEVEL DELIVERABLES)

This chapter defines the board-level deliverables required to integrate XR-VPP silicon into A1–A4 nodes with **deterministic control**, **evidence-grade observability**, and **auditable authority**. The BSP/SDK package is not only a driver layer; it is the enforcement point for (i) interface applicability, (ii) ordering and timebase normalization, and (iii) evidence emission contracts that remain stable across FPGA and ASIC phases.

BSP template line (RT external): APIs expose RT engagement policy, guardrails, and evidence events for an external buffer module; they do not imply on-die energy storage.

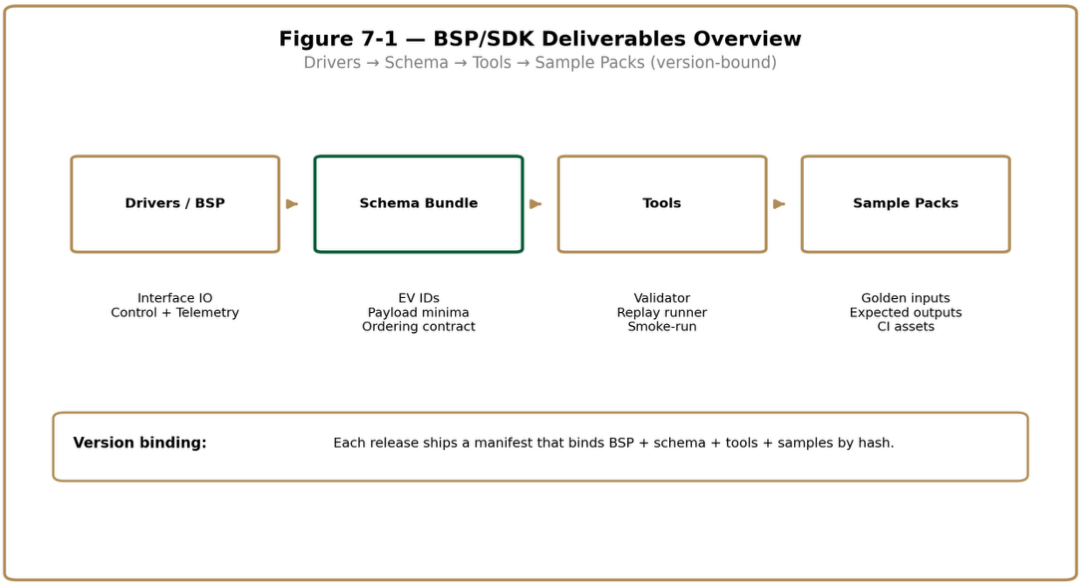


Figure 7–1 BSP/SDK Deliverables Overview (Drivers → Schema → Tools → Sample Packs)

7.1 Deliverable Set and Version Binding

The BSP/SDK release shall be version-bound to the silicon profile packs and evidence schema bundle. A release is valid only when all artifacts share the same version lineage and manifest hashes.

Required items:

- Driver/BSP binaries and headers for enabled interfaces (per SKU/node class).
- Evidence schema bundle (EV registry + payload minima + ordering contract).
- Telemetry normalization rules (unit conventions, rail naming, confidence flags).
- Sample packs and smoke-run scripts that reproduce core claims.

Table 7–1 BSP/SDK Release Items (Concise)

Item	Version Binding	Consumer	Notes
BSP Drivers (per enabled interface)	Bound to silicon SKU + profile version	Platform FW / OS / Host	Includes negative tests for excluded interfaces
BSP Headers / HAL	Bound to register map rev	Platform FW / Integrators	Stable API surface; separates control/telemetry/evidence
Evidence Schema Bundle	Bound to EV registry version	Governance / Tools / BSP	EV IDs + minimal payload + ordering contract
EV Registry (ID list)	Bound to schema bundle	Governance / Validation	EV-01…EV-20 + variant rules; N/A conditions explicit
Ordering & Timebase Spec	Bound to schema bundle	BSP / Tools	Time fields, gap/reset markers, tie-break rules
Telemetry Normalization Rules	Bound to schema bundle	BSP / Analytics	Units, rail naming, confidence flags; no silent zeros
Profile Packs (machine + human)	Bound to manifest	Operations / Governance	JSON for components; text summary for review
Schema Validator Tool	Bound to schema bundle	Validation / CI	Rejects non-conformant payloads; emits reasons
Replay Runner	Bound to ordering spec	Validation / CI	Deterministic replay; checksum diff outputs
Smoke-Run Scripts	Bound to samples + expected artifacts	Validation / CI	Executes ingest→normalize→validate→emit artifacts
Golden Sample Packs	Bound to expected artifacts	Validation / Integrators	Includes A1/A4 multi-source samples; gap/reset cases
Expected Artifact Set	Bound to smoke-run gate	CI / Review	Canonical outputs for pass/fail comparisons
Release Manifest	Root of binding	All	Hash tree binds BSP+schema+tools+samples; provenance + build IDs

7.2 API Surface: Control, Telemetry, Evidence

The BSP/SDK shall expose a minimal, stable API surface with strict separation:

- **Control APIs**: configure profiles, apply policies (subject to authority), set guardrails.
- **Telemetry APIs**: query snapshots and read raw sensor channels with declared validity.
- **Evidence APIs**: emit or relay EV-01...EV-20 records, including blocked actions and audit context.

All APIs must preserve:

- Node-class applicability (A1–A4).
- Authority model constraints (who may call what, when).
- Evidence linkage (every control action has an evidence record).

Table 7–2 API Surface Map (Concise)

API Group	Calls (examples)	Authority Requirement	Evidence Emission
Profile Management	profile_list(), profile_get(), profile_stage(), profile_commit()	Commit requires authorized actor + mode gating	EV-15 MODE_CHANGE (if mode affected), EV-18 POLICY_APPLY (commit), EV-19 BLOCKED_ACTION (if denied)
Guardrails	guardrails_get(), guardrails_set(), guardrails_lock()	Set/lock requires authority token; lock may be irreversible per mode	EV-18 POLICY_APPLY (new limits), EV-19 (if attempted while locked)
Power-Path Control	source_select(), source_lock(), rail_enable(), rail_disable()	Requires ownership + safe preconditions; blocked under inhibit/fault	EV-05 SOURCE_SWITCH, EV-19 (blocked), include actor/mode
Continuity (External Buffer)	cont_arm(), cont_engage(), cont_exit(), cont_status()	Engage/exit only when authorized and guardrails satisfied	EV-11 CONT_ARM, EV-12 CONT_ENGAGE, EV-14 CONT_EXIT, EV-19 (blocked)
Telemetry Snapshot	snapshot_read(), rail_read(v/i/t), health_read()	Read allowed in all modes (unless security policy restricts)	EV-20 SNAPSHOT (periodic/triggered), EV-17 DATA_GAP (if partial)
Evidence Stream	ev_subscribe(), ev_read(), ev_ack()	Read access may be role-gated	No new EV by reading; audit access logs optional

Timebase & Ordering	timebase_get(), time_map_attach(), ordering_status()	Attach mapping requires privileged actor (A1/A4)	EV-16 AUDIT_CTX (mapping change), EV-19 (blocked)
Diagnostics / Regimes	regime_get(), diag_report_get()	Report retrieval role-gated	EV-21 DIAG_REPORT *(if defined)* or attach as artifact referenced by EV-18
Artifact I/O	artifact_export(), artifact_import(), artifact_verify()	Import requires authority + anti-rollback compliance	EV-18 (import/apply), EV-19 (rejected), include hash/version
Service / Debug Gating	svc_mode_enter(), svc_mode_exit(), debug_gate_set()	Strict secure provisioning rules; physical presence optional	EV-15 (mode change), EV-16 (audit context), EV-19 (blocked)

Notes:

- Calls are examples; each SKU exposes only applicable groups (interface exclusions must be enforced).
- Continuity APIs are defined for **external buffer modules** (RT external semantics), not on-die energy storage.

7.3 Timebase and Ordering Normalization

The BSP is responsible for mapping silicon-side counters and any multi-source logs into the system timebase and enforcing ordering rules:

- For A1 and A4, BSP shall support alignment of XR-PMC events/telemetry with host logs and PSU PMBus logs where present.
- Ordering rules must be deterministic, including tie-break behavior, gap/reset flags, and confidence tagging.

Table 7–3 Timebase & Ordering Contract (Concise)

Field	Meaning	Required	Notes
ts_sys	System timebase timestamp	Yes (A1/A4), Optional (others)	Uses integrated system clock; when absent, ts_pmc is primary
ts_pmc	XR-PMC internal counter timestamp	Yes	Monotonic; resets must be signaled via reset_seq increment
time_map_id	Identifier of the active time mapping	Yes (A1/A4)	Changes must emit audit context record

seq	Per-source monotonically increasing sequence	Yes	Tie-break within same timestamp; resets require reset_seq
src_id	Evidence source identifier	Yes	At minimum: XR_PMC, optionally HOST, PSU_PMBUS
reset_seq	Reset generation counter	Yes	Increment on reboot or counter reset; prevents false ordering
gap_flag	Indicates missing interval / dropped segment	Yes	When true, downstream must treat subsequent inference as lower confidence
conf	Confidence level of alignment/merge	Yes (A1/A4), Optional (others)	Enumerated (e.g., HIGH/MED/LOW) derived from alignment method
hash_ref	Hash pointer to raw log chunk (optional)	Optional	Used when raw logs are stored separately; preserves traceability
actor_id	Actor/role initiating control action	Yes (for control-related EVs)	Mandatory for auditability; “unknown” not allowed for control actions
mode_id	Autonomy/service mode at emission	Yes	Mode changes require explicit evidence

Table 7–4 Multi-Source Merge Rules (Concise)

Source Pair	Alignment Method	Conflict Policy	Evidence Flags
XR_PMC ↔ HOST	ts_sys primary; fallback correlation using time_map_id + windowed matching	Prefer HOST time for global ordering; preserve both timestamps when mismatch exceeds threshold	conf, gap_flag, time_drift_flag (if defined), audit record on mapping change
XR_PMC ↔ PSU_PMBUS	Windowed correlation on ts_sys (if present) else on ts_pmc + polling phase	If PSU sample cadence differs, interpolate only for visualization; never invent values for evidence	conf, psu_sample_skew_flag (if defined), gap_flag
HOST ↔ PSU_PMBUS	ts_sys join by nearest-neighbor within tolerance	If both report rail values, treat PSU as “source-of-truth” for PSU-side rails; host values kept as context	conf, conflict_flag (if defined), gap_flag
XR_PMC ↔ XR_PMC (multi-controller)	Explicit controller IDs + arbitration token ordering	If authority conflict, **block action** and	authority_conflict_flag, blocked_action_flag, conf

		record as evidence; do not merge as if single stream	
Any ⇔ Any (when gap_flag=TRUE)	Resume with reset_seq/seq continuity checks	Downstream inference must downgrade regime claims; require explicit "gap-aware" reasoning	gap_flag, conf=LOW, inference_limited_flag (if defined)

Normative note: Multi-source merge is permitted only where the **source pair and method are declared** in the BSP/SDK release; undeclared merges are non-compliant.

7.4 Telemetry Schema: Snapshots and Rail Inventory

Telemetry exposure is defined as two coupled contracts:

- **Snapshot minimum set**: the smallest set of fields guaranteed to exist (or be declared absent) for governance decisions.
- **Rail inventory declaration**: a manifest declaring which rails exist, which sensors exist, and which exclusions apply.

Silent omissions are not permitted. Sensor absence must be explicit, with reason codes and confidence flags.

Table 7–5 Snapshot Minimum Fields (Concise)

Domain	Field	Required	Notes
Identity	src_id	Yes	XR_PMC (and controller ID if multi-PMC)
Identity	sku_id	Yes	A1/A2-S/A2-P/A3/A4
Timebase	ts_pmc	Yes	Monotonic; coupled with seq + reset_seq
Timebase	ts_sys	Yes (A1/A4), Optional (others)	System clock when integrated
Ordering	seq, reset_seq	Yes	Deterministic replay
Ordering	gap_flag	Yes	Evidence-grade gap declaration
Power State	selected_source	Yes	Enumerated per platform (e.g., PoE/DC/PSU)

Power State	path_state	Yes	Nominal / transition / inhibited / fault-contained
Power Summary	p_in, p_out	Yes (if measurable)	If not measurable, must be declared “unavailable,” not zero
Power Summary	efficiency	Optional	Derived; never required if inputs absent
Rails	rail_count	Yes	Must match rail inventory declaration
Rails	rail_v[]	Yes (if sensor exists)	Per-rail voltage with validity flags
Rails	rail_i[]	Yes (if sensor exists)	Per-rail current with validity flags
Rails	rail_t[]	Optional	Per-rail or hotspot temperature where present
Continuity	cont_state	Optional	Armed / engaged / inhibited / unavailable
Continuity	vcap	Optional	Only if instrumented; otherwise declare absent
Health	fault_latch	Yes	Protection summary (UV/OV/OCP/OTP etc.)
Health	derating_state	Optional	PoE derating regime or thermal derating where applicable
Authority	mode_id	Yes	Autonomy/service mode
Authority	actor_id	Yes (for control snapshots)	Actor initiating latest applied change
Quality	conf	Yes (A1/A4), Optional (others)	Alignment confidence for multi-source contexts

Table 7–6 Rail Inventory Declaration (Concise)

Product	**Rail List**	**Sensor Availability**	**Exclusions**
A1	Enumerated rails for mainboard integration (platform-defined list)	V/I required for all governance rails; T optional; declare per-rail validity	Any rail without sensor must be explicitly marked “no-sensor” with rationale
A2-S	Secondary-side rail subset (platform-defined)	V required; I optional by cost; T optional	Rails outside secondary shaping scope excluded by definition
A2-P	Primary boundary rails (boundary-safe list)	Limited sensing permitted; strict validity flags	No exposure of prohibited domains across isolation/safety boundary
A3	Backplane rails + controller domains	V/I as available; arbitration signals declared	Shared rails must declare ownership (which controller senses/acts)
A4	Grid node rail set (platform-defined)	V/I required where continuity claims exist; T optional	PoE-related rails excluded; UPS/grid primitives represented separately

Normative note: The rail inventory declaration is a manifest tied to each SKU/profile release; it is the authoritative source for what a “missing field” means (absent rail vs absent sensor).

7.5 Evidence Records: Minimal Payload and IDs

Evidence records must be schema-valid, versioned, and compact. The BSP shall guarantee that each emitted record includes:

Event ID and version.

Timebase fields + ordering markers (gap/reset).

Actor/mode/authority context.

Minimal payload fields required by the EV registry.

Where rate-limits apply, the BSP shall emit summary records rather than silently dropping evidence.

Table 7–7 Evidence Event Mapping (Concise)

Feature	Evidence IDs	Minimal Payload
Boot & Identity	EV-01 BOOT, EV-02 SRC_DETECT, EV-03 READY	ts_pmc, seq, reset_seq, src_id, sku_id, selected_source, mode_id
Source Selection / Switching	EV-05 SOURCE_SWITCH	from_source, to_source, reason_code, actor_id, mode_id, guardrail_check
Protection / Containment	EV-06 PROTECT_ENTER, EV-07 PROTECT_EXIT	fault_type, rail_id(s), threshold, latch_state, path_state
Derating	EV-08 DERATE_ENTER, EV-09 DERATE_EXIT	cause (thermal/poe/etc), limit_value, duration
Inrush / Power-Good	EV-10 INRUSH_LIMIT	rail_id, limit, duration, outcome
Continuity (External Buffer)	EV-11 CONT_ARM, EV-12 CONT_ENGAGE, EV-13 CONT_SUSTAIN, EV-14 CONT_EXIT	cont_state, trigger, duration, vcap (if avail), guardrail_hit (if any), inhibit_reason (if blocked)
Mode / Autonomy	EV-15 MODE_CHANGE	from_mode, to_mode, actor_id, preconditions_ok
Audit Context / Authority	EV-16 AUDIT_CTX	actor_id, authority_token_id (or none), controller_id, time_map_id (if changed)
Data Gaps / Resets	EV-17 DATA_GAP	gap_flag, gap_len, reset_seq, affected_sources
Policy Apply / Profile Commit	EV-18 POLICY_APPLY	profile_id, version, diff_hash, guardrails_hash, actor_id, mode_id
Blocked Action	EV-19 BLOCKED_ACTION	attempted_call, reason, actor_id, mode_id, precondition_failed

Snapshot Record	EV-20 SNAPSHOT	rail_summary fields + validity flags, selected_source, path_state, conf (if A1/A4)

Table 7–8 Rate-Limit Policy (Concise)

Class	Threshold	Action	Evidence Summary Payload
Protection Storm	≥ 200 EV/s burst OR ≥ 50 EV/s sustained	Keep **all** protection enter/exit; rate-limit repeats by coalescing	class=PROTECT, window_ms, dropped_count, kept_ids, top_fault_types
Continuity Chatter	≥ N engages per window *(default N=3 / 10s)*	Enforce cooldown; block engages beyond limit	class=CONT, window_ms, blocked_count, last_guardrail_hit, next_allowed_ts
Telemetry Snapshots	Snapshot period < 100 ms sustained	Clamp to min period; downsample	class=SNAPSHOT, requested_ms, applied_ms, downsample_ratio
Source Switch Loops	≥ 5 switches / 30s	Lockout to stable source; require manual override per mode	class=SRC_SWITCH, switch_count, lockout_ms, selected_source
Audit Context Spam	Repeated identical audit ctx within 1s	Deduplicate; keep first + final	class=AUDIT, dedup_count, last_ctx_hash
Multi-source Merge Conflicts	Conflict rate ≥ 10% in window	Mark confidence LOW; emit merge-warning	class=MERGE, conflict_count, conf=LOW, dominant_conflict_type

Rule (normative): Rate-limits must never silently discard compliance-relevant events; when coalescing occurs, emit a summary record with counts and window metadata.

7.6 Policy Artifacts and Versioning

Policy artifacts shall be stored and transported in two parallel forms:

Machine artifact: JSON schema-bound packs for components and automated validation.

Human artifact: text-form summaries for review, audit, and board-level governance narratives.

Artifacts must support semantic versioning, hash binding, and anti-rollback policies where applicable.

Table 7–9 Artifact Formats (Concise)

Artifact	Format	Consumer	Versioning	Notes
Profile Pack (machine)	JSON	Components / BSP / CI	SemVer + hash	Canonical configuration for silicon and board-level modules
Profile Summary (human)	Text (MD/TXT)	Engineers / Review	Matches JSON version	Readable diff; references evidence IDs and guardrails
Evidence Schema Bundle	JSON Schema + EV registry	BSP / Tools	SemVer + hash	Payload minima + ordering contract bundled
Release Manifest	manifest.json + hashes	All	Hash tree	Binds BSP+schema+tools+samples+profiles; provenance and build IDs
Diagnostic Report	Text + referenced evidence excerpts	Engineering / Ops	SemVer + run ID	Must link to evidence events (IDs + timestamps + hashes)
Policy Proposal	JSON + human text	Governance / Review	SemVer + hash	Proposal only unless mode allows apply; includes guardrail checks
Audit Trail Extract	JSONL / CSV	Compliance / Review	Run ID + schema ver	Extract of EV stream for audits; preserves ordering fields
Validation Summary	PDF/MD	Validation / Mgmt	Release tag	Gate outcomes + exceptions; points to run IDs and manifests
Golden Sample Pack	JSONL/PCAP/CSV	CI / Validation	Dataset version	Input samples paired with expected artifact hashes
Time Mapping Config	JSON	BSP / Tools	SemVer + mapping ID	Declares time_map_id and alignment parameters (A1/A4)

7.7 Smoke-Run Gate (SDK + Schema + Samples)

Each BSP/SDK release shall include a smoke-run gate that executes end-to-end on representative samples:

Ingest sample packs → normalize → validate schema → run minimal governance loop → produce artifacts.

Pass criteria require schema validity, deterministic ordering, and correct audit trails.

Table 7–10 BSP Smoke-Run Gate (Concise)

Input Samples	Expected Artifacts	Pass Criteria
SMP-01 Normal boot → source detect → ready	ART-01 EV stream (EV-01..03) + manifest.json	Schema-valid; ordering fields present; no gap/reset unless true
SMP-02 Source switch (PoE↔DC/PSU) ***(A1 if enabled)***	ART-02 EV-05 SOURCE_SWITCH + snapshot diff	Switch emits EV with actor/mode; guardrail checks recorded; deterministic replay checksum stable
SMP-03 Fault storm injection (UV/OCP/OTP mix)	ART-03 fault EV set + rate-limit summary EV	No silent drops; rate-limit summaries emitted; containment state transitions correct
SMP-04 Continuity engage cycle ***(external buffer emulation)***	ART-04 EV-11..14 + timing plot	Engage/exit events present; T_max respected; inhibit path produces EV-19 blocked action
SMP-05 Multi-source alignment pack (XR_PMC + HOST) ***(A1/A4)***	ART-05 merged audit extract + time_map_id record	ts_sys alignment within tolerance; conflicts flagged; confidence tags populated
SMP-06 PSU PMBus log merge (XR_PMC + PSU_PMBUS) ***(A1/A4 when present)***	ART-06 merge report + skew flags	Sample skew flagged; no invented values; gap handling correct
SMP-07 Rail inventory manifest (missing sensors case)	ART-07 rail declaration + snapshot with validity flags	Missing sensors declared, not zeroed; snapshot conforms to manifest
SMP-08 Profile apply + anti-rollback attempt	ART-08 policy apply record + reject record	Valid apply emits EV-18; rollback attempt rejected with EV-19; manifest hash matches
SMP-09 Service/debug gating attempt (unauthorized)	ART-09 blocked action record	Unauthorized operations blocked; audit context complete; no state corruption
SMP-10 Replay parity run (same input twice)	ART-10 checksum + diff report	Replay deterministic: identical checksum; allowed nondeterminism set is empty

Normative note (RT external): Continuity smoke-run uses an **external buffer emulation** to validate hooks/events/guardrails; it does not imply on-die energy storage.

8 STANDARDS, COMPLIANCE, AND REFERENCE ANCHORS

This chapter enumerates the standards and compliance anchor points that constrain XR-VPP interfaces, governance contracts, and production readiness. Standards are referenced with explicit **applicability** (A1–A4 and FPGA/ASIC phase) to prevent ambiguous scope. Detailed conformance procedures and test plans are defined in later validation and qualification chapters; this section defines what must be **anchored** and how it is **invoked** by the specification.

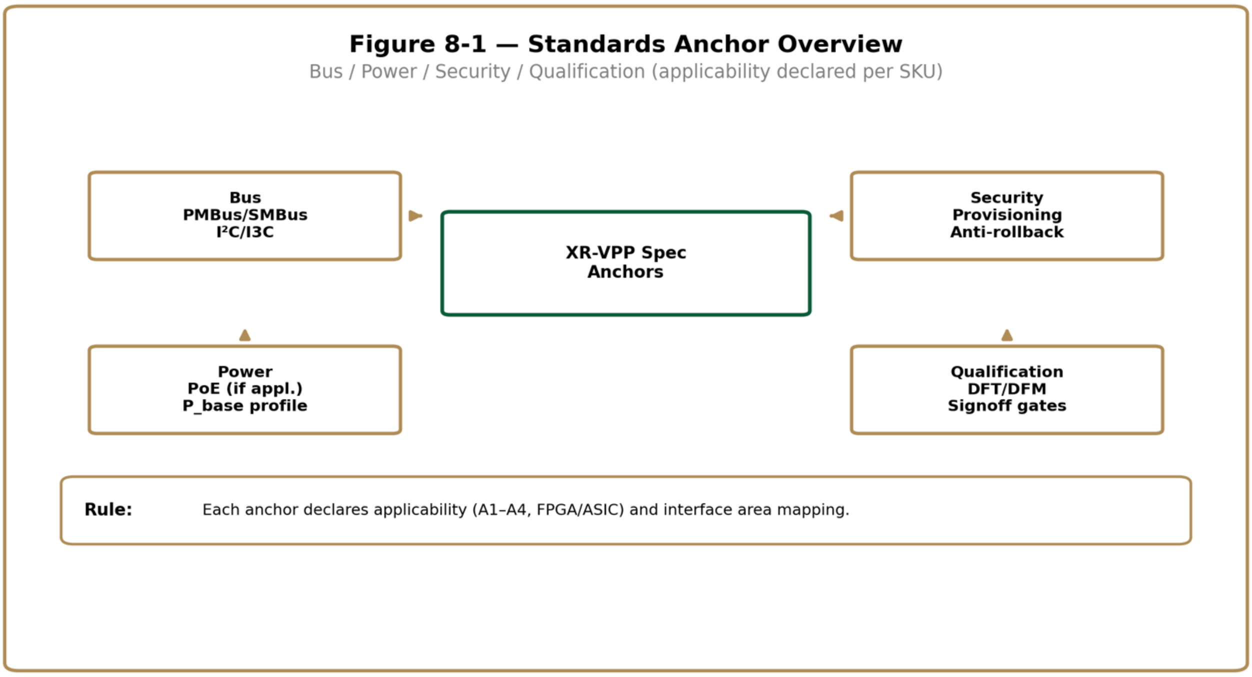


Figure 8–1 Standards Anchor Overview (Bus / Power / Security / Qualification)

8.1 Telemetry and Control Buses

XR-VPP telemetry/control contracts shall attach to established management buses. The specification shall state which bus is mandatory vs optional by node class, and how bus selection affects evidence completeness.

PMBus / SMBus (電源管理匯流排): telemetry readout, limit configuration, fault/status access.

I²C / I3C (通用控制匯流排): transport for schema-bound telemetry/evidence where PMBus is not used or is insufficient.

Applicability constraints shall be declared per SKU (A1/A2-S/A2-P/A3/A4), including interface exclusions and negative tests.

Table 8–1 Bus Applicability Matrix (Concise)

Bus	Applies to A1–A4	Interface Area	Notes
PMBus	A1, A3*, A4*	Power telemetry/control	Used when interacting with PSU/PD/controller domains; optional where no PSU-side PMBus is exposed
SMBus	A1, A2-S, A3, A4*	Power + platform mgmt	Often the practical transport for board mgmt; treated as subset/compat layer of I²C
I²C	A1, A2-S, A2-P*, A3, A4	Control + evidence transport	Default control bus for XR-PMC peripheral links; A2-P subject to safety boundary constraints
I3C	A1*, A3*, A4*	High-rate telemetry + multi-drop	Optional upgrade path; used where higher bandwidth / in-band interrupts are needed
Host Link (logical)	A1, A4	Authority + log alignment	Not a physical “bus standard” entry; denotes host-side timebase/log merge integration obligations

Legend: * = Optional / platform-dependent; must be explicitly declared in each SKU profile and enforced via negative tests when excluded.

8.2 PoE Reference Anchor (When Applicable)

Where the node class includes PoE PD, the spec shall anchor a baseline PoE capability and a replaceable derating profile used as the reference P_base (基準功率輪廓). PoE is treated as an interface option bound to SKU/profile applicability rather than a universal requirement.

IEEE 802.3 PoE (e.g., 802.3at reference anchor) applies to A1 and optionally A3 when PoE PD exists.

PoE derating profiles must be explicitly declared and versioned.

Table 8–2 PoE Anchor Points (Concise)

Anchor	Applies	Parameter	Notes
IEEE 802.3 PoE Family	A1; A3*	Standard reference	Applicability requires PoE PD interface presence; otherwise N/A by SKU/profile

PD Power Class Baseline	A1	P_base reference	Baseline uses 802.3at 90W-class derating profile as a replaceable reference curve
Derating Profile Pack	A1; A3*	P(t, T, V) limits	Versioned profile artifact; must be hash-bound in release manifest
Detection / Classification Events	A1	EV IDs	Evidence must record detect/class outcomes and any constrained enable behavior
Inrush / Startup Guardrails	A1	I_inrush_max, T_inrush_max	Enforced at BSP+silicon; violations emit protection/blocked evidence
Power Budget Telemetry	A1; A3*	p_in, p_out, eff	eff derived; never required if inputs absent; validity flags mandatory
Interface Exclusion Rule	A2-S, A2-P, A4	N/A declaration	PoE is out-of-scope unless explicitly enabled; exclusion must be negative-tested
Replaceability Clause	A1; A3*	P_base swap	PoE anchor is a reference point; projects may replace the profile pack while preserving evidence contract semantics

Legend: * = Optional / platform-dependent; PoE anchors must be declared “not applicable” for SKUs without PoE PD.

8.3 Security, Integrity, and Provisioning

XR-VPP silicon and board-level deliverables shall enforce integrity and auditability through a security anchor set:

- Secure provisioning (安全佈署): device identity, key injection, manufacturing provisioning flow.
- Anti-rollback (防回滾): profiles, firmware/ROM artifacts, and schema bundles must be version-bound and rollback-protected where required.
- Debug/service gating (除錯/維修閘控): service access must be role- and mode-gated with evidence records for entry/exit and blocked attempts.

Table 8–3 Security Anchors (Concise)

Anchor	Mechanism	Evidence	Notes
Device Identity	Unique ID + provisioning record	EV-16 AUDIT_CTX	Identity must bind to manifest lineage; used for traceability
Secure Provisioning	Key injection + provisioning scripts	EV-16 + provisioning log hash	Provisioning flow is part of release package; operator actions auditable
Anti-Rollback	Version policy + reject older artifacts	EV-19 BLOCKED_ACTION	Applies to profiles, firmware/ROM, schema bundle; reject must be logged

Manifest Binding	Hash tree across release artifacts	EV-16 (manifest hash reference)	Manifest is the root of trust for what "this release" means
Debug / Service Gating	Role/mode gating + optional physical presence	EV-15 MODE_CHANGE, EV-19	Enter/exit service modes must be evidenced; blocked attempts must be logged
Secure Updates (OTA/field)	Signed artifacts + verification	EV-18 POLICY_APPLY + verify result	Verification failures produce blocked evidence and no state change
Access Control (API)	Authority token / capability check	EV-19	Every denied control call must be evidenced with reason
Data Integrity (Evidence)	Append-only log + ordering fields	EV-17 DATA_GAP	Gaps/resets must be explicit; no silent truncation
Confidentiality Boundaries	Payload minimization + redaction	EV schema constraints	Especially relevant for A2-P safety/isolation domains

8.4 Qualification and Production Readiness Framework

ASIC productization requires a qualification framework that references standard signoff/production readiness gates rather than ad-hoc checklists:

- DFT/DFM (可測試/可製造): scan strategy, production test coverage, manufacturing limits.
- Signoff anchors: STA, IR/EM, LVS/DRC, CDC/RDC, power intent checks.
- Qualification matrix: temperature/voltage corners, aging, ESD/latch-up, and burn-in strategy (as applicable).
- **Normative rule:** Security anchors are not "documentation only"; each anchor must map to an enforceable gate and an evidence record for allow/deny outcomes.

Table 8–4 Qualification Anchor Points (Concise)

Area	Mandatory Checks	Output Artifacts
DFT	Scan strategy, test modes, coverage targets, secure test gating	DFT report, ATPG summary, test-mode spec
DFM	Manufacturability rules, layout constraints, yield-risk review	DFM checklist, waiver log, risk notes
Signoff: STA	Timing closure across corners; CDC/RDC review	STA reports, CDC/RDC reports, waiver log
Signoff: IR/EM	Power integrity and electromigration checks	IR/EM reports, limits tables
Signoff: LVS/DRC	Netlist/layout consistency and design rule compliance	LVS clean report, DRC clean report
Power Intent	Power domains, isolation/retention rules, safe-state behavior	Power intent report, domain map

ESD / Latch-up	Device-level robustness targets and test plan	ESD/latch-up plan, lab results (when executed)
Corner Validation	Voltage/temperature corners; functional stability	Corner test matrix, result logs
Aging / Drift	Stress/aging assumptions and detection hooks	Aging plan, evidence-driven drift detection rules
Package / Thermal	Package thermal assumptions; derating strategy	Thermal notes, package selection rationale
Production Test	Limits, binning, traceability, sample plan	Production test spec, vector package, bin table
Release Integrity	Version binding, anti-rollback, manifest verification	Release manifest, verification report

Note: This table fixes the **anchor structure**; per-SKU applicability and detailed procedures are defined in the qualification and program plan chapters.

8.5 Applicability Declaration Rule (Normative)

Every standards reference in this document shall be accompanied by:

Node class applicability (A1–A4) and phase applicability (FPGA / ASIC).

Interface area mapping (bus/power/security/qualification).

Notes stating whether the standard is used for **transport**, **conformance**, or **reference anchoring** only.

This rule prevents “implicit compliance claims” and ensures engineers can execute conformance without ambiguity.

Table 8–5 Standards & Applicability Matrix (Concise)

Standard	Applies to A1–A4	Interface Area	Notes
PMBus	A1, A3*, A4*	Power mgmt bus	Telemetry/control for PSU/PD domains where present
SMBus	A1, A2-S, A3, A4*	Mgmt bus	Common platform transport; treated as I^2C-compatible layer
I^2C	A1, A2-S, A2-P*, A3, A4	Control bus	Default control + telemetry transport under applicability rules
I3C	A1*, A3*, A4*	High-rate telemetry	Optional upgrade; declared per SKU/profile
IEEE 802.3 (PoE)	A1, A3*	Power input	Applies only when PoE PD exists; anchored via P_base derating profile

Secure Provisioning (anchor)	A1–A4	Security	Provisioning + identity + manifest binding; enforced via release gates
Anti-rollback (anchor)	A1–A4	Security	Applies to profiles/firmware/schema; deny is evidence-recorded
Debug/Service Gating (anchor)	A1–A4	Security	Mode/role gating with evidence; blocked attempts recorded
DFT / DFM (framework)	A1–A4 (ASIC)	Qualification	Manufacturing readiness; outputs required for tape-out signoff
STA / IR/EM / LVS/DRC / CDC (framework)	A1–A4 (ASIC)	Signoff	Standard signoff gates; waivers tracked and justified

Legend: * = Optional / platform-dependent; applicability must be explicitly declared and negative-tested when excluded.

9 EDA, VERIFICATION INFRASTRUCTURE, AND PROGRAM EXECUTION

This chapter defines the execution infrastructure required to deliver XR-VPP from FPGA to programmable ASIC with predictable quality gates. It focuses on the engineering "how to execute" layer: EDA flow anchors, verification assets, lab/HIL infrastructure, and the minimum program artifacts required to prevent drift across SKUs and phases.

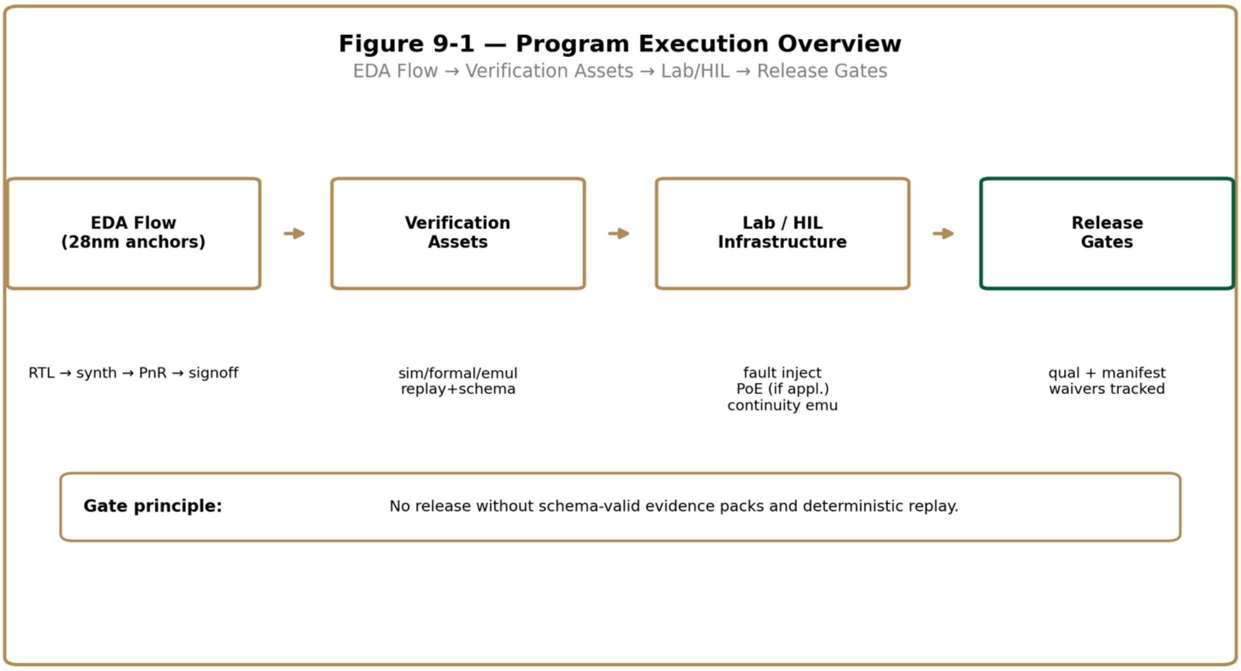


Figure 9–1 Program Execution Overview (EDA Flow → Verification Assets → Lab/HIL → Release Gates)

9.1 EDA Flow Anchors for 28nm ASIC

The ASIC flow shall be anchored by explicit stage outputs and mandatory checks. The intent is not to prescribe a single vendor toolchain in this chapter, but to lock the **classes of tools** and **signoff artifacts** required for 28nm implementation.

Table 9–1 28nm ASIC EDA Flow Anchors (Concise)

Stage	Tool Class	Mandatory Checks	Output Artifacts

RTL Freeze	RTL mgmt / lint	Lint clean; CDC precheck; spec trace tags	RTL tag, lint report, CDC pre-report
Synthesis	Logic synthesis	Timing intent; area/power budget; scan intent	Gate-level netlist, synth report, constraints snapshot
DFT Insertion	DFT/ATPG	Scan insertion; test modes; coverage targets; secure test gating	DFT netlist, DFT report, ATPG plan summary
Formal / Equivalence	Formal tools	RTL↔netlist equivalence; key invariants (where defined)	EQ report, invariant proof/waiver log
Floorplan	PnR floorplanning	IO placement vs SKU IO budget; power grid plan; congestion risk	Floorplan db, IO plan, power grid notes
Place & Route	Digital PnR	Setup/hold closure plan; congestion/DRC avoidance; clock tree plan	Routed db, CTS report, PnR summary
Clock Tree (CTS)	CTS	Skew/jitter targets; clock gating checks	CTS db, skew report, gating report
STA Signoff	STA	Multi-corner multi-mode (MCMM); derates; SI (if used)	STA signoff reports, constraint package
Power Integrity	IR/EM	Static/dynamic IR; EM limits; hotspot review	IR drop report, EM report, hotspot notes
Physical Verification	LVS/DRC	DRC clean; LVS clean; ERC as required	DRC report, LVS report, waiver log
CDC/RDC Signoff	CDC/RDC	CDC clean (or waived with rationale); reset safety	CDC/RDC signoff reports
Power Intent Signoff	UPF/CPF tools	Isolation/retention rules; safe state; sequencing assumptions	Power intent report, domain map
Gate-Level Sim	GLS	Reset/boot paths; scan mode sanity; X-prop policy	GLS logs, coverage notes
Package / IO Review	Package planning	Pinout vs buses; ESD considerations; test access pins	Pinout table, package notes
Tape-out Readiness	Release mgmt	Checklist complete; waivers signed; manifests bound	Tape-out checklist, waiver approvals, release manifest
Post-Silicon Bring-up Plan	Validation planning	ATE plan; lab/HIL plan; smoke-run recipes	Bring-up plan, test vectors package refs

9.2 Verification Asset Taxonomy

Verification assets are treated as first-class deliverables, not “project byproducts.” The asset taxonomy shall cover:

- Functional simulation and assertion checks.
- Formal checks for safety-critical invariants (where applicable).
- Emulation/FPGA prototypes for superset behavior.
- HIL/lab validation for power-path and continuity behavior.
- Evidence schema validation + deterministic replay as compliance checks.

Table 9–2 Verification Assets (Concise)

Asset	Purpose	Coverage	Output Artifacts
Lint + Style Rules	Prevent structural RTL defects	All RTL blocks	Lint reports; rule waivers
CDC/RDC Suite	Detect clock/reset domain violations	Cross-domain paths	CDC/RDC reports; signed waiver log
UVM/Directed Sim	Functional verification of control/telemetry paths	Interface contracts; state machines	Sim logs; functional coverage
Assertion Library	Enforce invariants (guardrails, safety)	Key regimes and transitions	Assertion results; failure traces
Formal (select invariants)	Prove safety-critical properties	Lockouts, inhibit dominance	Proof results; counterexample traces
Equivalence Check	Ensure RTL↔netlist correctness	All synthesized logic	EQ reports
Emulation / FPGA Prototype	High-speed scenario validation	Superset behaviors (A1–A4)	Bitstreams; scenario logs
Power-Path HIL Bench	Validate source switching + faults	A1/A3 backbones	Bench recipes; measurement logs
Continuity Emulation Bench	Validate external buffer hooks/events	Engage/hold/exit; guardrails	Timing plots; EV-11..14 packs
PoE Derating Bench	Validate P_base profile (if applicable)	A1 (and A3* if enabled)	Profile validation report; EV packs
Fault Injection Suite	Stress protection and rate-limit behavior	UV/OV/OCP/OTP storms	Injection configs; EV summaries
Schema Validator	Enforce evidence payload minima	EV-01…EV-20	Validator logs; reject reasons
Replay Runner	Deterministic regression	Evidence packs → artifacts	Checksums; diff reports
Golden Sample Packs	Canonical inputs for CI	Core scenarios; gaps/resets	Dataset version; expected hashes
Smoke-Run Scripts	End-to-end gate	Ingest→normalize→validate→emit	Pass/fail report; manifest binding
Qualification Precheck	Readiness prior to lab qual	Corners + robustness plan	Precheck checklist; gaps list

9.3 Evidence-Driven Validation Loop (Replay as a Gate)

Evidence-grade logs are used as both the product contract and the validation substrate:

- Each major scenario produces evidence packs and expected artifacts.
- Replay determinism is used as a regression gate (checksum + diff).
- Gaps/resets/confidence tagging are verified as compliance items, not “nice-to-have telemetry.”

Table 9–3 Evidence Compliance Gates (Concise)

Check	Method	Pass Criteria	Artifacts
Schema Validity	Run schema validator on EV stream	100% schema-valid; rejects produce explicit reasons	Validator logs; schema bundle version
Ordering Completeness	Verify ts_pmc/seq/reset_seq/gap_flag presence	Required fields present per event class	Ordering audit report
Deterministic Replay	Replay same pack twice	Identical checksums; empty allowed-nondeterminism list	Replay checksum + diff report
Gap/Reset Explicitness	Inject drop/reset cases	gap_flag/reset_seq emitted; confidence downgraded	EV-17 packs; replay report
Authority Attribution	Audit control-related events	Control actions always include actor_id/mode_id	Authority audit extract
Blocked Action Coverage	Attempt disallowed calls	EV-19 emitted with reason; no silent failures	Negative-test EV packs
Rate-Limit Compliance	Stress event rates beyond thresholds	No silent drops; summaries emitted with counts/window	Rate-limit summary EV packs
Continuity Semantics (external)	Engage/hold/exit scenarios via emulation	EV-11..14 complete; T_max and cooldown enforced	Timing plot; continuity EV packs
Interface Applicability	Attempt excluded interface paths	Proper denial + EV evidence; no unintended responses	Interface exclusion report

Profile/Manifest Binding	Apply profile and verify hashes	Manifest binds artifacts; mismatches rejected with evidence	Manifest + verify logs
Multi-source Merge (A1/A4)	Merge XR_PMC+HOST(+PSU) packs	Alignment within tolerance; conflicts flagged; conf set	Merge report; audit extract

9.4 Lab / HIL Infrastructure Requirements

Lab/HIL must support injection and measurement for:

- Source switching and path state transitions.
- Fault storm injection (UV/OV/OCP/OTP) and containment behavior.
- External-buffer continuity emulation (trigger/hold/exit) with guardrail observability.
- PoE derating baseline validation where PoE PD is applicable.
- Multi-source log capture (XR-PMC + host + PSU PMBus) for A1/A4 scenarios.

Table 9–4 Lab & HIL Infrastructure (Concise)

Capability	Instrumentation	Required for SKUs	Notes
Source Switching Bench	Programmable sources + load; switch matrix	A1, A3	Validates SOURCE_SWITCH evidence and path-state transitions
Fault Injection (UV/OV/OCP/OTP)	Fault injector; programmable load; thermal stimulus	A1, A2-S, A3, A4	Must support burst + sustained storm patterns for rate-limit gates
Continuity Emulation (External Buffer)	External buffer emulator or cap module + controlled droop	A1, A2-S*, A3, A4	Validates EV-11..14 timing; enforces cooldown/T_max guardrails
PoE PD Validation	PoE PSE emulator; classification monitor	A1; A3*	Validates P_base derating profile and startup/inrush constraints
PMBus/SMBus Capture	Bus analyzer/sniffer	A1, A3*, A4*	Enables merge with PSU-side telemetry where present
I^{2}C/I3C Capture	Bus analyzer	A1, A2-S, A2-P*, A3, A4	Confirms transport correctness and negative tests
Thermal Characterization	IR camera; thermocouples; chamber (optional)	A1, A3, A4	Supports thermal hotspot regimes and derating validation

Power Measurement	High-bandwidth probes; power analyzer	A1, A3, A4	Supports p_in/p_out/eff where measurable; otherwise declares unavailable
Host Log Capture	Host agent + time sync	A1, A4	Required for multi-source merge and ordering confidence validation
CI Replay Node	Compute node for replay/validator	All	Enforces deterministic replay and schema validity in regression
Manufacturing Test Prep	Basic ATE interface; boundary scan tools	ASIC SKUs	Prepares vectors/limits; ties to production test package

Legend: * = Optional / platform-dependent (only if interface is enabled by SKU/profile).

9.5 Program Plan Artifacts and Change Control

To avoid scope drift and “SKU divergence,” the program shall maintain a minimal control set:

- SKU definition pack (interfaces, exclusions, authority model).
- IP ownership map (reuse vs custom) and licensing assumptions.
- Release manifest binding BSP/schema/tools/samples/profiles.
- Qualification matrix and waiver log discipline.

Table 9–5 Program Control Artifacts (Concise)

Artifact	Owner	Update Rule	Gate Impact
SKU Definition Pack	Product + Silicon	Change requires spec revision + review signoff	Affects interface applicability, authority model, evidence scope
Interface Applicability Matrix	Silicon	Must be updated with every SKU change	Drives negative tests; blocks undeclared interfaces
IP Ownership Map	Silicon	Update on IP source/licensing changes	Impacts schedule, NRE, and signoff assumptions
Evidence Contract Bundle	Governance + Platform	EV registry/schema changes require backward-compat note	Breaks replay if changed; must bump version
Ordering/Timebase Contract	Platform	Changes require golden pack regeneration	Affects deterministic replay; CI gate
Profile Packs (defaults)	Governance	Versioned; anti-rollback enforced	Impacts guardrails and autonomy behaviors
Lab Recipe Set	Validation	Updated with bench changes; must stay reproducible	Affects qualification and evidence gate repeatability

Golden Sample Packs	Validation	Update only with schema/version bump	CI baseline; checksum-bound
Waiver Log	Silicon + QA	Waivers require rationale + approver	Signoff/tapeout readiness gate
Release Manifest	Release Eng	Regenerated per release; immutable after tag	Root binding of all deliverables
Qualification Matrix	QA	Update with SKU/package changes	Blocks tapeout/production if incomplete
Program Risk Register	Program Mgmt	Weekly update or per major change	Drives mitigation actions and gate criteria

9.6 Phase-to-Phase Traceability (FPGA → ASIC)

Traceability is defined as contract continuity plus explicit deltas:

Evidence contract equivalence is preserved; deltas must be declared and justified.

FPGA superset coverage is the reference baseline for ASIC SKU subsets.

Each ASIC SKU inherits verification assets and adds SKU-specific signoff and qualification outputs.

Table 9–6 Traceability Matrix (Concise)

Contract	FPGA Baseline	ASIC Enforcement	Notes
Evidence IDs (EV-01…EV-20)	Superset implemented across A1–A4	Subset per SKU; IDs preserved; N/A declared	No renumbering; variants allowed but must be declared
Payload Minima	Validator-enforced payload set	Same schema bundle, per-SKU applicability rules	ASIC may add fields; must not drop required fields
Ordering/Timebase	ts_pmc/seq/reset_seq/gap_flag enforced	Same; plus tighter determinism requirements	A1/A4 require ts_sys mapping where integrated

Authority Model	Mode + actor attribution on control actions	Same; stronger secure gating	Deny/blocked actions must emit evidence
Interface Applicability	FPGA supports widest interface envelope	ASIC locks interface per SKU	Negative tests must prove exclusions
Power-Path State Machine	Baseline state transitions validated	Same semantics; optimized implementation	Timing deltas must be documented as constraints, not behavior changes
Continuity Hooks (external)	Hooks/events validated via emulation	Same hooks/events/guardrails	Silicon defines hooks/limits; external buffer performance remains external
Rate-Limit Policy	Baseline thresholds validated	Per SKU tuned, policy preserved	No silent drop; summary evidence required
Replay Determinism	CI replay required for baseline	CI replay mandatory for all SKUs	Expected artifact hashes per release tag
Qualification Gates	Not applicable (FPGA) or limited	Full ASIC signoff + qual matrix	Waivers tracked; tie to release manifest
Release Binding	Manifest binds BSP/schema/samples	Manifest binds silicon+bsp+profiles	Anti-rollback applies to field artifacts

10 BOM, COST, AND COMMERCIAL ANCHORS (ENGINEERING VIEW)

This chapter defines the cost anchors that engineering teams must use when making architecture, IP, and SKU decisions. It is intentionally engineering-facing: it binds cost items to **ownership choices**, **verification scope**, and **release artifacts**, rather than market narratives. Cost fields are expressed as **bands** and **anchor references** and must be attached to traceable source types (公開來源/供應商型錄/分銷報價區間/EDA 公開授權資訊等).

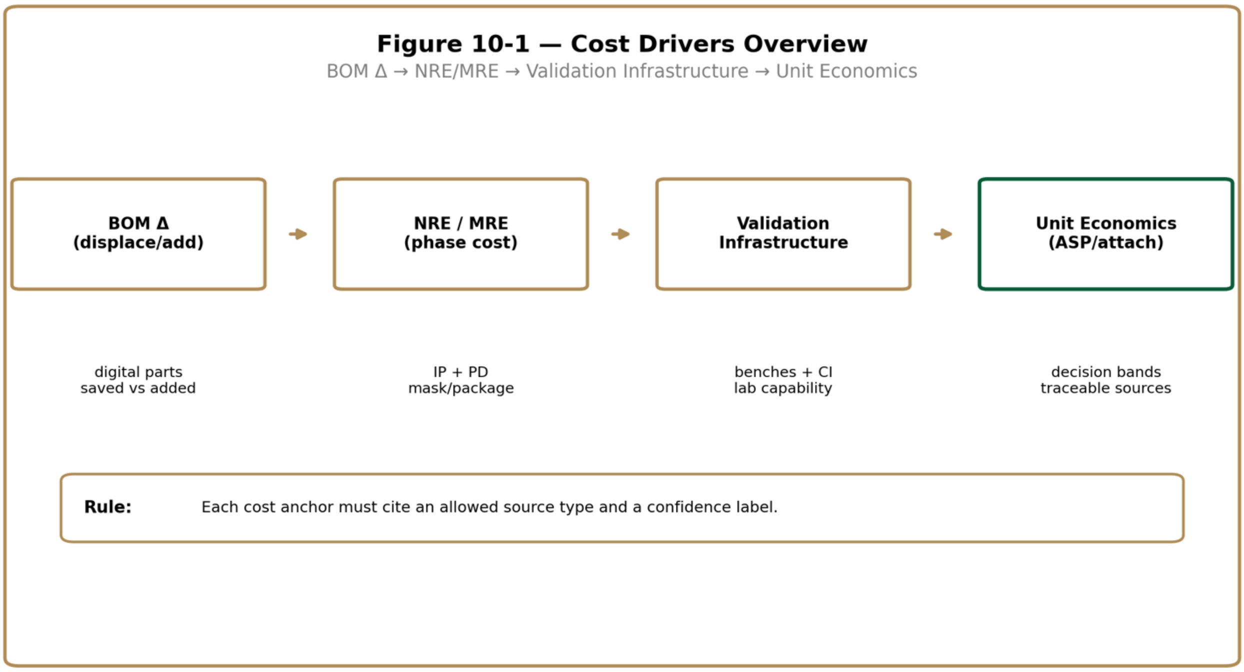


Figure 10–1 Cost Drivers Overview (BOM Δ → NRE/MRE → Validation Infra → Unit Economics)

10.1 BOM Delta Categories (Digital Displacement vs Adders)

BOM impact is defined as delta to a node's baseline implementation. The delta shall be categorized as:

Digital displacement savings (數位料件替代節省): displaced MCUs, supervisors, glue logic, level shifters, discrete telemetry components, etc.

Digital adders: XR-PMC silicon, required passives, clocks, security elements (if external), connectors (if added), etc.

Verification adders: test headers, debug access (gated), instrumentation allowances required by qualification.

Table 10–1 BOM Delta Categories (Concise)

Category	Typical Parts	Applies to A1–A4	Notes
Displaced MCU / Supervisor	small MCU, reset supervisor, watchdog	A1, A2-S, A3	Only count as "displaced" if XR-PMC assumes the same governance boundary + evidence duties
Displaced Glue Logic	GPIO expanders, muxes, simple CPLD	A1, A2-S, A3	FPGA phase often replaces many; ASIC phase displaces per SKU subset
Displaced Telemetry Front-Ends	ADC helpers, discrete monitors	A1, A2-S, A3, A4*	Only where sensors can be consolidated without reducing required observability
Displaced Level Shifters	I/O level translators	A1, A2-S, A3	Depends on IO voltage plan and package choice
Add: XR-PMC Silicon	FPGA module / ASIC die	A1–A4	Primary adder; cost modeled per phase and per SKU
Add: Clocks / References	crystal/oscillator, clock buffers	A1–A4	May be shared with platform; must be declared in BOM ownership
Add: Security Element (optional)	secure element, OTP aid	A1–A4*	Optional where provisioning requires external root component
Add: Passives (support)	decoupling, pull-ups, filters	A1–A4	Treated as minor adders; still tracked for completeness
Add: Test/Debug Access (gated)	test pads, header options	ASIC SKUs	Required for manufacturing test; service exposure must remain gated
Add: Storage/Transport Enablement	small flash, log transport parts	A1, A4*	Only if platform lacks a host path and needs local buffering
Neutral: Board RT Module	external cap module (1.0–1.5F)	A1, A3, A4	**Not** silicon BOM; tracked as platform primitive; XR-PMC governs hooks/events/guardrails
Neutral: UPS / Grid Primitives	UPS interface, protection coordination	A4	External to silicon; represented as continuity primitives in system scope

Legend: * = Platform-dependent; must be explicitly declared per SKU/profile.

10.2 NRE/MRE and IP Licensing Anchors

Program cost is decomposed into:

NRE (一次性工程費): RTL/verification, integration, physical design, signoff, packaging enablement.

MRE / mask (遮罩費): dependent on node, layers, and foundry packaging options.

IP licensing: interface IPs, security IP, memory macros, analog companions (if any), and verification collateral.

Cost anchors must be tied to one of the allowed source types and expressed as bands with confidence labels.

Table 10–2 NRE/MRE Bands by Phase（一次性工程費/遮罩費區間）— 28nm anchor

Phase	Cost Band (USD)	Key Drivers	Source Anchors
FPGA Phase — Platform & Proof (FPGA 平台/驗證)	**NRE:** 0.3M–1.5M	Platform RTL integration; board bring-up; evidence schema + logging; HIL hooks; profile tooling	FPGA has **no foundry mask NRE** (contrast statement).
ASIC Phase — Design-to-GDS (ASIC 設計至版圖)	**NRE:** 4M–15M	RTL hardening; verification closure; DFT; physical design; signoff; EDA license utilization; 3rd-party IP integration	EDA license spend is often a dominant cost line item vs infra (directional).
Tape-out & Masks (投片/光罩)	MRE (per tape-out): 1.0M–2.0M	Mask set; foundry tape-out services; packaging NPI kick-off; test program initial	28nm mask set cost reference ~**$1.2M** (order-of-magnitude).
Re-spin Exposure (重投/重罩風險)	MRE (per re-spin): 1.2M–3.0M	Additional mask set + schedule; incremental verification & lab rerun; ECO back-end	Mask set cost anchor enables bounding per re-spin exposure.
Validation Infra Scale-out (驗證設備/實驗室擴建)	**NRE:** 0.5M–5M	Power-path emulation; programmable loads; fault injection; PoE fixtures; thermal; log capture/storage	Total 28nm program costs vary widely; high-end SoC references can exceed this class (used only as ceiling).

Table 10–3 IP Cost Ownership Map（IP 成本歸屬）

IP Class	Typical Source Type	Pricing Model (typical)	Notes
Foundry Collateral (PDK / std-cell / IO)	Foundry-provided	Included/packaged with foundry engagement; NDA-based	Mandatory baseline for 28nm; drives signoff closure.
Memory (SRAM/ROM/OTP)	Foundry / 3rd-party	Often bundled or separately licensed; integration NRE	OTP/eFUSE + anti-rollback ties into security anchors.

Digital Interfaces (I^2C/SMBus/PMBus, SPI, UART)	Internal / 3rd-party	Internal dev cost or per-project license	Prefer internal where feasible to reduce royalties & audit risk.
High-speed / SerDes (if any)	3rd-party / foundry ecosystem	Upfront license + possible per-unit royalty	Only if SKU requires; otherwise keep out-of-scope to protect cost.
Security IP (secure boot, crypto, key mgmt)	3rd-party / internal	Upfront + maintenance; sometimes royalty	Provisioning & debug/service gating are compliance-critical.
CPU Core (optional)	3rd-party (e.g., Arm)	Upfront license + per-unit royalty (typical model)	Public reporting cites Arm upfront fees **~$1M–$10M** + royalties (range varies by deal).
Analog Sensing (ADC/Temp/V/I monitors)	Mixed	Often custom + small licensed macros	Power telemetry accuracy impacts evidence quality and guardrails.
XR Internal IP (policy engine / evidence contract / ordering)	Internal	Engineering NRE only	Must remain invariant across FPGA baseline → ASIC SKUs for traceability.
EDA Tooling (synthesis/PD/STA/DFT/verification)	EDA vendors	Subscription/ELA; utilization-driven	License spend can outweigh compute infra spend; manage via utilization discipline.

10.3 Validation Cost and Lab Infrastructure Allocation

Validation cost is treated as a structured budget linked to required capabilities:

- Power-path benches (source switching, fault injection).
- Continuity external buffer emulation benches.

- PoE PD validation (where applicable).
- Multi-source capture and deterministic replay CI.
- Costs shall be allocated per SKU class, since ASIC productization splits A1/A2-S/A2-P/A3/A4 into distinct products with distinct lab coverage.

Table 10–4 Validation Infrastructure Cost Anchors (Capability / SKU Need / Cost Band / Notes)

Capability	SKU Need	Cost Band (USD)	Notes
High-power programmable DC electronic load **(programmable load / 可程式電子負載)**	A1, A3 (mandatory); A2-S (recommended); A4 (platform-dependent)	**$9k–$20k / unit**	Anchor examples: 3kW class ~$9.3k ; 10kW class ~€15k (order-of-magnitude)
High-power programmable DC source **(programmable supply / 可程式電源供應器)**	A1, A3 (mandatory); A2-S/A4 (recommended)	**$3k–$10k / unit**	5kW programmable supply examples in the low-to-mid k€ range
DC power analyzer / data-logger **(power analyzer / 功率分析+記錄)**	A1, A3 (mandatory); others (recommended)	**$10k–$20k / mainframe**	Example listing for Keysight N6705C mainframe ~$12k
Environmental / thermal chamber **(環境箱/溫循)**	A1, A3 (recommended); A4 (recommended when grid/UPS coordination tested)	**$8k–$75k**	New chamber pricing range (size/range dependent)
Bus protocol analyzer **for I^2C/SMBus/PMBus (匯流排分析儀)**	A1–A4 (mandatory for bring-up + evidence)	**$0.4k–$1.5k / unit**	Example: Total Phase Beagle I2C/SPI analyzer ~$450
PoE validation tool **(PoE 測試/負載/抓取)**	A1 (mandatory when PoE PD applies); A3 (optional)	**$5k–$20k**	Field/kit-class PoE test tools can be ~$18.7k MSRP (Use conformance rigs separately if required by customer contracts.)
Fault injection & switch-over fixture **(故障注入/切換治具)**	A1, A3 (mandatory); A2-S (recommended)	**$2k–$15k**	Typically custom fixture + relays + safety interlocks; cost depends on current level and automation scope.
Continuity external-buffer emulator **(外部 RT/hold-up 模擬器)**	A1, A3 (mandatory for continuity claims); A4 (platform-dependent)	**$5k–$25k**	Implemented as programmable load/source + ESR emulation network; use for worst-case ESR/aging sweeps (ties to evidence gates).
Capture & replay CI storage/transport **(擷取/回放 CI 基礎設施)**	A1–A4 (mandatory for evidence auditability)	**$3k–$30k**	Depends on event rate and retention; include timebase

			alignment artifacts and deterministic replay pipelines.

10.4 ASP / Price Bands and Attach Rate Anchors

Commercial anchors are represented in engineering as **price bands** and **attach-rate assumptions** (採用率/搭載率) that drive SKU and packaging decisions. Values must be traceable to acceptable source types and must be versioned in the program control artifacts so that engineering decisions remain auditable.

10.5 Cost-Decision Linkage (Normative)

The following design decisions must cite the relevant cost anchors:

- Interface inclusion/exclusion decisions (affects IP and verification).
- Evidence budget targets (affects storage/transport and CI).
- Package/IO choices (affects unit cost and qualification).
- External buffer continuity scope (affects lab capability allocation, not silicon energy storage).

Table 10–5 Commercial Anchors (SKU / ASP Band / Attach Rate Band / Source Type / Confidence)

SKU	ASP Band (USD, silicon)	Attach Rate Band (%, of addressable nodes)	Source Type	Confidence
A1 (Mainboard AI-PMC)	**6–15**	**15–45**	Distributor reference pricing to bound silicon value (PoE PD controller class + FPGA upper bound) + PoE endpoint adoption proxies	Medium
A2-S (Secondary-side)	**3–9**	**10–30**	Distributor reference pricing (control/telemetry IC class) + PoE/endpoint adoption proxies (secondary varies by platform)	Low–Medium
A2-P (Primary-side optional)	**2–7**	**5–20**	Distributor reference pricing (power/monitor class) + platform retrofit/greenfield gating assumption	Low

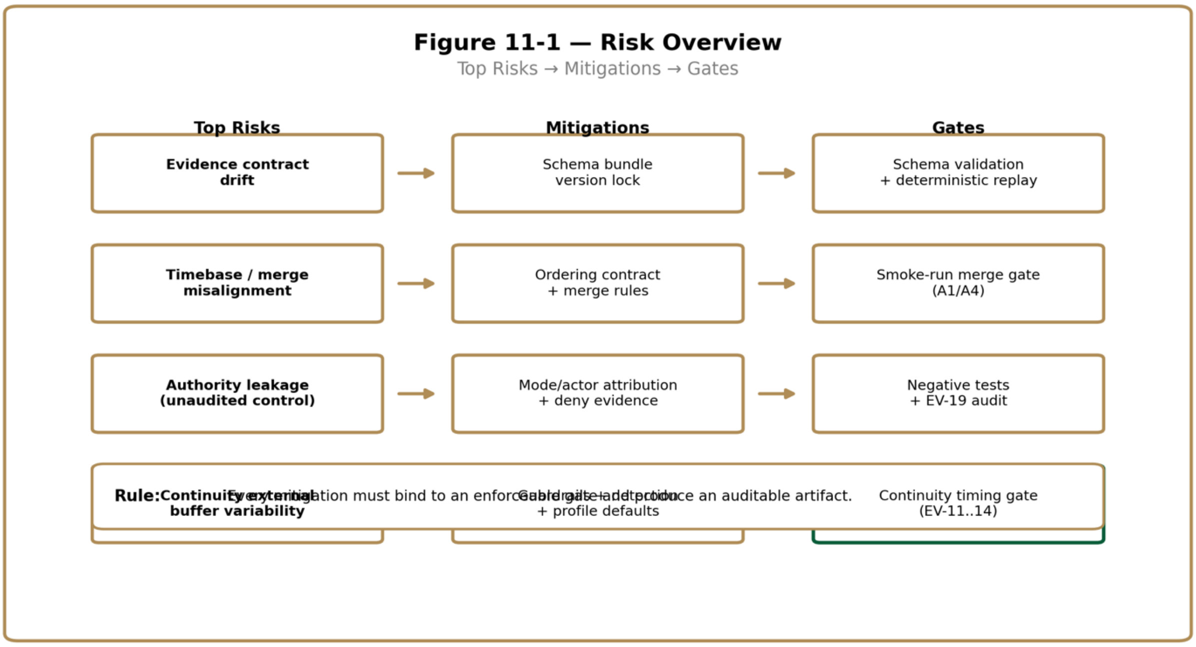
A3 (Backplane PMC)	**4–12**	**10–35**	Distributor reference pricing (multi-port/aggregator value band) + PoE endpoint adoption proxies (when PoE present)	Medium
A4 (Grid node IPC)	**5–14**	**5–25**	Distributor reference pricing (governance + multi-source merge value band) + non-PoE continuity governance adoption proxy	Low–Medium

Anchor notes (how the bands are bounded; not placeholders):

- **Lower bound anchor (single-function PoE PD controller class):** TI TPS2373 distributor pricing shows a few USD/unit band at volume breaks, used as a floor reference for PoE-related interface silicon.
- **Upper bound anchor (FPGA silicon used for prototype/superset):** Lattice CertusPro-NX distributor pricing shows ~€70–€90+ (or similar) depending on device/package/quantity, used as a practical ceiling for "FPGA phase" silicon cost expectation.
- **Attach-rate plausibility proxy (PoE endpoint mix + growth):** market research summaries indicate PoE endpoint concentration in surveillance/network devices and sustained PoE market growth, supporting non-trivial adoption where PoE/centralized power is a primary integration driver.

11 RISK REGISTER AND MITIGATION PLAN

This chapter defines the risk register (風險登錄) and mitigation discipline used to deliver XR-VPP from



FPGA superset to programmable ASIC SKUs without contract drift. Risks are framed as **engineering execution risks** tied to enforceable gates, measurable artifacts, and evidence-driven detection, rather than narrative concerns.

Figure 11–1 Risk Overview (Top Risks → Mitigations → Gates)

Table 11–1 Risk Register (Compact Index: ID / Risk / L / I / D / Owner)

ID	Risk (short)	L	I	D	Owner
R-01	Evidence contract drift	3	5	2	Platform
R-02	Timebase/ordering incoherence	3	5	3	Platform
R-03	Authority leakage (unaudited control)	2	5	2	Silicon
R-04	Rate-limit failure (storm handling)	3	4	3	Platform
R-05	Interface exclusion regression (SKU split)	3	4	3	Silicon
R-06	FPGA→ASIC traceability gap	2	4	3	Program
R-07	IP sourcing/licensing volatility	3	4	4	Silicon
R-08	Qualification scope creep	3	4	3	QA
R-09	Package/IO budget surprise	2	4	3	Silicon
R-10	Lab/HIL non-reproducibility	3	4	3	Validation

R-11	Continuity/RT external buffer variability	4	4	3	Validation
R-12	PoE baseline mismatch (P_base)	2	3	3	Validation
R-13	Security anchor under-implementation	2	5	2	Platform
R-14	EDA/signoff waiver debt	3	5	4	Silicon

Table 11–2 Risk Register (Controls: ID / Mitigation / Gate / Artifacts)

ID	Mitigation (short)	Gate	Artifacts
R-01	Schema bundle version-lock + manifest binding	Schema validation + deterministic replay	Schema bundle; validator logs; manifest
R-02	Ordering contract + merge rules + confidence tagging	Smoke-run merge gate (A1/A4)	Merge report; audit extract; golden packs
R-03	Capability checks + deny evidence + service gating	Negative tests + EV-19 audit	Deny logs; EV packs; waiver log
R-04	Rate-limit policy + summary emissions + backpressure	Rate-limit compliance gate	Stress packs; summary EV packs
R-05	Applicability matrix enforcement + feature flags	Interface applicability gate	SKU pack; exclusion tests; reports
R-06	Traceability matrix + explicit deltas per release	Release readiness gate	Traceability matrix; delta notes; manifest
R-07	IP ownership map + early license lock + fallback	Tape-out readiness gate	IP map; licensing status; decision log
R-08	SKU-bound qual matrix + waiver discipline	Qualification readiness gate	Qual matrix; waiver log; signoff set
R-09	Early IO budget lock + pinout reviews + constraints	Floorplan/IO review gate	IO plan; pin table; review records
R-10	Versioned lab recipes + automation + environment pinning	Lab reproducibility gate	Recipe set; run logs; env notes
R-11	Guardrails + detection + profile defaults (external RT framing)	Continuity timing gate (EV-11..14)	Timing plots; EV packs; default profiles
R-12	Replaceable derating profile + bench validation	PoE validation gate	Derating profile; bench report; EV packs
R-13	Secure provisioning + anti-rollback + debug gating	Security compliance gate	Provision logs; block evidence; manifest
R-14	Weekly waiver review + closure owners + blockers	Tape-out readiness gate	Waiver log; signoff reports; approvals

11.1 Risk Scoring and Ownership Rules

Risks shall be scored using a simple, execution-oriented rubric:

- **Likelihood (L):** probability of occurrence within the phase window.
- **Impact (I):** effect on schedule, cost, contract compliance, or field stability.
- **Detectability (D):** ability to detect early via evidence packs and validation assets.

Risk ownership is mandatory (Silicon / Platform / Validation / Program). Any mitigation must bind to a **gate** (驗證門檻) and output a tangible artifact (report/log/waiver/manifest).

Table 11–3 Risk Register (Compact, A4-friendly)

ID	Risk (short)	L/I/D	Owner	Mitigation (short)	Gate	Artifacts
R-01	Evidence contract drift	3/5/2	Platform	Schema lock + manifest bind	Schema+replay	Schema; validator; manifest
R-02	Timebase/merge incoherence	3/5/3	Platform	Ordering contract + merge rules	Merge smoke-run	Merge rpt; golden packs
R-03	Authority leakage	2/5/2	Silicon	Capability checks + deny evidence	Neg tests + EV-19	Deny logs; EV packs
R-04	Rate-limit failure	3/4/3	Platform	Rate-limit + summary emissions	Rate-limit gate	Stress packs; summaries
R-05	SKU exclusion regression	3/4/3	Silicon	Applicability enforcement	Applicability gate	SKU pack; exclusion rpt
R-06	FPGA→ASIC trace gap	2/4/3	Program	Trace matrix + deltas	Release readiness	Trace matrix; manifest
R-07	IP/licensing volatility	3/4/4	Silicon	IP map + early lock	Tape-out readiness	IP map; decision log
R-08	Qualification creep	3/4/3	QA	SKU-bound qual matrix	Qual readiness	Qual matrix; waivers
R-09	Package/IO surprise	2/4/3	Silicon	IO budget lock + reviews	IO review gate	IO plan; pin table

R-10	Lab non-reproducible	3/4/3	Validation	Versioned recipes + automation	Lab reproducibility	Recipes; run logs
R-11	**RT external variability**	4/4/3	Validation	Guardrails+detection+defaults	Continuity EV-11..14	Timing; EV; profiles
R-12	PoE baseline mismatch	2/3/3	Validation	Replaceable P_base + bench	PoE validation	Profile; bench rpt
R-13	Security under-impl	2/5/2	Platform	Provision+anti-rollback+gating	Security compliance	Provision logs; manifest
R-14	Signoff waiver debt	3/5/4	Silicon	Weekly waiver closure discipline	Tape-out readiness	Waiver log; signoff rpt

11.2 Core Technical Risks (Cross-Phase)

The following technical risks are considered cross-phase and must be continuously tracked from FPGA baseline through ASIC SKU productization:

Evidence contract drift: schema/version divergence between platform, BSP, and silicon leading to non-replayable regression.

Ordering/timebase incoherence: multi-source merge misalignment (A1/A4) producing ambiguous causality.

Authority model leakage: control actions executed without attributable mode/actor or without deny evidence.

Rate-limit instability: event storms causing silent loss or uncontrolled payload growth.

Mitigations must be expressed as “contract-first gates,” including schema validation, deterministic replay, negative tests for exclusions, and manifest binding as release blockers.

Table 11–4 Contract Stability Risks (Concise)

Risk	Trigger	Mitigation	Gate
Evidence schema drift	EV payload fields added/removed without version bump	Schema bundle version-lock + backward-compat note	Schema validation gate

Evidence ID drift	EV IDs renumbered or semantics changed	EV registry immutable; only variants allowed with declaration	Traceability gate
Ordering contract drift	Missing seq/reset_seq/gap_flag in some sources	Enforce ordering fields per source; reject non-compliant packs	Deterministic replay gate
Timebase mapping ambiguity	ts_sys mapping undefined (A1/A4)	Define mapping contract + tolerances; embed confidence	Merge smoke-run gate
Authority contract drift	Control actions emitted without actor_id/mode_id	Capability checks + attribution required + deny evidence	EV-19 audit gate
Interface applicability drift	SKU excludes reintroduced via shared code	Compile-time feature flags + applicability matrix enforcement	Applicability negative-test gate
Rate-limit policy drift	Storm behavior changes silently	Versioned rate-limit policy + required summary evidence	Rate-limit compliance gate
Profile/manifest unbound	Profiles applied without manifest binding	Manifest binding + anti-rollback enforcement	Release readiness gate
Lab recipe non-determinism	Bench scripts change without versioning	Versioned recipe set + environment pinning	Lab reproducibility gate
Waiver accumulation	Waivers accepted without closure plan	Weekly waiver review + blockers for critical waivers	Tape-out readiness gate

11.3 Continuity / RT Risk (External Buffer Dominance)

Risk template line (mandatory, RT external framing): **RT performance risk is dominated by external buffer ESR/aging/thermal; mitigation is via guardrails, evidence-driven detection, and profile defaults.**（RT 風險主要來自外部模組 ESR/老化/熱，靠護欄+證據事件+profile 預設管控。）

Continuity-related risks shall therefore be tracked as a coupled system risk (silicon hooks + external module behavior), and mitigations must include: (1) guardrail enforcement, (2) evidence events for engagement/hold/exit, (3) detection of ESR/aging signatures through regime analysis, and (4) profile defaults that bound unsafe operation under uncertain buffer conditions.

Table 11–5 Continuity / RT External Risk Items (Concise)

Risk	External Cause	Silicon Hook	Evidence	Default Guardrails	Gate
Under-hold (short ride-through)	Buffer **ESR rise** / capacitance loss (aging)	Vcap sense + engagement control	EV-11 engage; EV-12 hold; EV-14 exit	T_max bound; min Vcap threshold; cooldown	Continuity timing (EV-11..14)
Overstress / thermal runaway	Buffer heating; poor airflow; high ripple	Thermal inputs + inhibit	EV-15 thermal regime; EV-16 inhibit	Temp-based derating; hard inhibit	Thermal regime gate
Chatter / oscillation	ESR variability; marginal thresholds	Hysteresis + debounce	EV-13 exit reason; EV-18 rate-limit	Min dwell; hysteresis window	Rate-limit + replay gate
False engage (unnecessary)	Noise on Vcap sense; transient spikes	Filtering + qualify trigger	EV-11 trigger fields; confidence	Trigger qualification; noise filter	Noise-injection bench gate
Late exit (unsafe)	Slow recovery of source; bad recovery estimate	Exit policy + source-ready check	EV-14 exit; EV-17 gap flag if needed	Exit requires stable source for N cycles	Replay determinism gate
Evidence loss during storm	Burst events exceed transport	Rate-limit + summary	EV-18 summary; EV-17 gap flags	Hard rate caps; summary payload	Rate-limit compliance gate
Module mismatch / wrong part	Wrong buffer spec or assembly variance	Part-ID binding (if available)	EV-20 config snapshot	Profile defaults assume worst-case ESR; require declare buffer class	Smoke-run config gate
Protection miscoordination	External protection/UPS interaction (A4)	Authority hooks + inhibit	EV-16 inhibit; EV-19 deny	Authority dominance; safe-state fallback	Authority/negative-test gate

RT external framing (required): RT performance risk is dominated by external buffer ESR/aging/thermal; mitigation is via guardrails, evidence-driven detection, and profile defaults.

11.4 ASIC Productization Risks (SKU Split Effects)

ASIC phase risks concentrate on SKU split and its secondary consequences:

Interface fragmentation: SKU-level exclusions accidentally reintroduced by shared backbone logic.

IP sourcing and licensing: different IP sources per product causing schedule and cost volatility.

Qualification scope creep: inconsistent qualification matrices across SKUs leading to delayed release.

Package/IO budget surprise: late changes in pinout or IO voltage plan triggering rework.

Mitigations must bind to SKU definition packs, IP ownership maps, and qualification matrices that are version-locked and manifest-bound at release.

Table 11–6 ASIC Productization Risks (Concise)

Risk	SKU Impact	Mitigation	Gate	Artifacts
Shared backbone reintroduces excluded interfaces	All SKUs	Applicability matrix + compile-time feature flags	Interface applicability gate	SKU pack; exclusion test report
IO budget overrun / pinout churn	A1/A3 highest risk	Early IO budget lock; pinout reviews; constraint binding	Floorplan/IO review gate	IO plan; pin table; review record
IP source mismatch (cost/schedule)	SKU-dependent	IP ownership map + licensing lock + fallback	Tape-out readiness gate	IP map; licensing status; decision log
Qualification matrix divergence	All SKUs	SKU-bound qual matrix; common gate checklist	Qualification readiness gate	Qual matrix; signoff checklist
Evidence budget insufficient (rate/storage)	A1/A4 highest	Evidence budget table per SKU; rate-limit defaults	Evidence compliance gate	Budget sheet; stress packs; summaries
Packaging choice misfit	A2-S/A2-P sensitive	Packaging & IO budget anchors; early package review	Package review gate	Package notes; pin map
DFT coverage shortfall	All SKUs	DFT plan early; ATPG targets; design-for-test reviews	DFT gate	DFT report; ATPG coverage
Security gating incomplete	All SKUs	Provisioning + anti-rollback + debug/service gating	Security compliance gate	Provision logs; deny evidence; manifest
Post-silicon bring-up gaps	All SKUs	Bring-up plan + golden packs + smoke-run recipes	Bring-up readiness gate	Bring-up plan; recipe set; packs

11.5 Program Execution Risks and Gate Discipline

Program risks shall be expressed as violations of gate discipline:

Missing or non-reproducible lab recipes.

Unbounded waiver accumulation without closure plan.

Incomplete smoke-run inputs (no canonical packs) or non-deterministic outputs.

Mitigations require: a weekly waiver review, mandatory smoke-run gates for BSP/schema/profile alignment, and a “no release without evidence packs + deterministic replay” rule enforced by CI.

Table 11–7 Program Execution Risks (Concise)

Risk	Owner	Mitigation	Gate	Artifacts
Gate discipline erosion (rules bypassed under schedule pressure)	Program	Gate checklist is release-blocking; no “verbal pass”	Release readiness gate	Gate checklist; approvals
Non-reproducible lab runs	Validation	Versioned recipes + environment pinning + automation	Lab reproducibility gate	Recipe set; run logs; env notes
Golden pack drift	Validation	Packs are immutable per schema/version; regenerate only with version bump	Deterministic replay gate	Golden pack tag; checksums
Waiver debt accumulates	Silicon + QA	Weekly waiver review; closure owners; blocker list	Tape-out readiness gate	Waiver log; closure plan
Toolchain mismatch across teams	Platform	Containerized tool versions; recorded build hashes	Smoke-run gate	Build manifests; hashes
Evidence transport overload	Platform	Rate-limit + summaries; backpressure rules	Rate-limit compliance gate	Stress packs; summary EV
Merge rules not enforced	Platform	Merge validator required; conflict policy mandatory	Merge smoke-run gate	Merge reports; conflict flags
Security exceptions become default	Platform	Secure provisioning + anti-rollback enforced; debug gating audited	Security compliance gate	Provision logs; EV-19 blocks
SKU scope creep	Product	Change-control via SKU definition pack	SKU change gate	SKU pack diffs; decision log
Release artifacts incomplete	Release Eng	Manifest binding required; missing items fail CI	Release readiness gate	Release manifest; CI logs

12 APPENDICES (DELIVERABLES, TEMPLATES, AND REFERENCE PACKS)

This chapter consolidates the normative templates, registries, and sample packs required to execute the program without ambiguity. Appendix items are considered **release artifacts**: each must be versioned, manifest-bound, and referenced by the gates defined in Chapters 9–11.

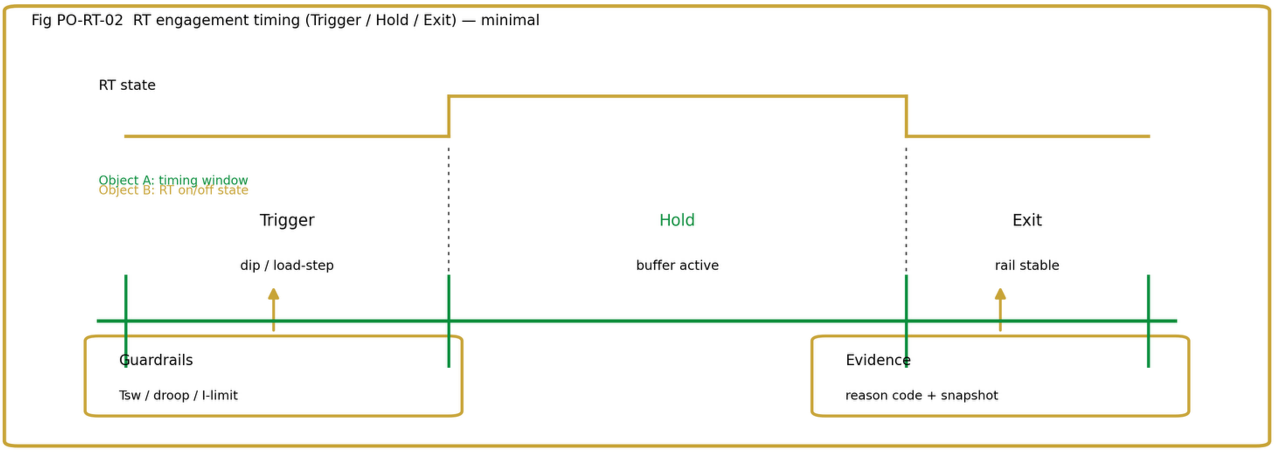


Figure 12–1 Appendix Map (Registries → Schemas → Sample Packs → Checklists)

12.1 Evidence Registry (EV Core Set) and Naming Rules

The evidence registry defines the stable core set of evidence events (核心事件) and their naming rules. Evidence IDs must remain stable across FPGA baseline and ASIC SKUs; any SKU-specific exclusions must be expressed as “not applicable” by applicability matrices rather than renumbering or semantic changes.

Table 12–1 Evidence Registry Index (EV Core Set)

EV ID	Name	Category	Applies (A1–A4)	Notes
EV-01	Power Source Selected	Authority	A1, A3, A4	Selected input source + reason code
EV-02	Source Health Snapshot	Telemetry	A1, A3, A4	Summary health for active/standby sources
EV-03	Rail Telemetry Snapshot	Telemetry	A1–A4	Minimal rail set (see Snapshot min fields)
EV-04	Protection Action Taken	Protection	A1–A4	OCP/OVP/UVP/OTP actions + actor
EV-05	Fault Detected	Fault	A1–A4	Fault class + affected domain
EV-06	Fault Cleared	Fault	A1–A4	Clear condition + dwell time

EV-07	Rate-Limit Activated	Transport	A1–A4	Rate-limit class + threshold crossed
EV-08	Rate-Limit Summary Emitted	Transport	A1–A4	Summary counters + drop flags
EV-09	Policy Proposal Emitted	AI/L3	A1–A4	Proposed policy delta + confidence
EV-10	Diagnosis Report Emitted	AI/L3	A1–A4	Report pointer + linkage to evidence
EV-11	Continuity Engage	Continuity	A1, A3, A4*	Engage trigger + Vcap + actor/mode
EV-12	Continuity Hold Status	Continuity	A1, A3, A4*	Hold duration + Vcap/rail minima
EV-13	Continuity Exit Request	Continuity	A1, A3, A4*	Exit reason + preconditions
EV-14	Continuity Exit Confirmed	Continuity	A1, A3, A4*	Exit completion + post-conditions
EV-15	Regime Entered	Regime	A1–A4	Regime ID (droop/thermal/ESR/...)
EV-16	Regime Inhibit Applied	Regime	A1–A4	Inhibit policy + bounded action
EV-17	Ordering Gap Flag	Ordering	A1, A4	Gap/reset indicators for replay
EV-18	Multi-Source Merge Flag	Ordering	A1, A4	Conflict/alignment flags + method
EV-19	Authority Deny Evidence	Authority	A1–A4	Denied action + reason + actor
EV-20	Config Snapshot (Profile/Build)	Governance	A1–A4	Profile hash + schema/version binding

Legend: A4* = continuity semantics may map to UPS/grid primitives; still emits continuity-class events when enabled by profile and authority model.

12.2 Schema Bundle and Backward Compatibility Notes

The schema bundle (schema + validator + examples) is the normative contract between silicon, BSP/SDK, and tooling. Any schema change must include a backward compatibility note and a migration rule, and

Table 12–2 Schema Bundle Contents (Concise)

Item	Format	Version Rule	Notes
Evidence event schema (EV core)	JSON Schema	SemVer; **minor** for additive fields; **major** for breaking	Normative contract for EV-01..EV-20
Ordering & timebase contract	Markdown + JSON Schema	SemVer; change requires smoke-run refresh	Defines ts/seq/reset_seq/gap_flag expectations
Registry index (EV IDs)	Markdown/CSV	Immutable IDs; add via append-only	No renumbering; variants declared separately
Validator (CLI)	Python package / binary	Tied to schema version	Produces pass/fail + reports used by gates
Canonical sample packs	ZIP (JSONL/CSV/logs)	Tied to schema+ordering version	Used for deterministic replay + CI

Golden outputs	JSON/CSV	Must match sample packs	Expected artifacts for smoke-run and replay
Profile schema	JSON Schema	SemVer; major on meaning changes	Machine-consumed policy artifact template
Human-readable render template	Text/MD	Track with profile schema version	Generated from same canonical source as JSON
Manifest template	YAML/JSON	Versioned	Lists hashes of all bundle artifacts
Changelog & migration notes	Markdown	Required each release	Explicit delta + compatibility statement

Table 12–3 Backward Compatibility Rules (Concise)

Change Type	Allowed	Requires Version Bump	Notes
Add optional field to EV payload	Yes	Minor	Must not change existing field meaning
Add new EV ID (append-only)	Yes	Minor	EV registry updated; no renumbering
Add new regime ID (catalog append)	Yes	Minor	Requires updated validator test vectors
Add new autonomy mode value	Yes	Minor	Must declare preconditions and audit needs
Rename field (schema)	No (direct)	Major	Use alias/dual-field migration window
Remove field	No	Major	Requires migration note + replay refresh
Change field meaning/units	No	Major	Must provide mapping rule and examples
Tighten validation constraints	Yes (if non-breaking)	Minor/Major (case-by-case)	If it invalidates prior compliant data → Major
Change ordering/timebase semantics	Limited	Major	Requires canonical pack refresh + merge smoke-run
Change merge conflict policy	Limited	Major	Requires updated flags and replay baseline
Change default guardrails	Yes	Minor	Must log as “default change” and bind to profile version
Change artifact format (JSON↔protobuf)	Limited	Major	Must support dual-read window if fielded
Add new source type (host logs/PSU logs)	Yes	Minor	Requires normalization spec + sample packs

12.3 Ordering and Timebase Reference Packs

This appendix provides canonical reference packs that demonstrate ordering fields, reset handling, and multi-source merge alignment for A1/A4. These packs are used in smoke-run gates and in CI deterministic replay.

Table 12–4 Canonical Packs (Concise)

Pack ID	Sources	Purpose	Expected Outputs	Notes
PACK-01	XR-PMC events/telemetry	Baseline schema compliance	Validator PASS; EV index coverage report	Core “hello world” pack
PACK-02	XR-PMC + host logs	A1/A4 multi-source merge	Merge report; EV-18 flags; replay PASS	Includes alignment confidence tags
PACK-03	XR-PMC + PSU PMBus logs	A1/A4 power-source correlation	Correlation summary; ordering PASS	PSU logs normalized into common fields
PACK-04	Ordering reset / gap	Replay determinism under resets	EV-17 gap flags; deterministic replay	Contains reset_seq transitions
PACK-05	Event storm / rate-limit	Transport resilience	EV-07/08 summaries; drop accounting	Must demonstrate bounded payload growth
PACK-06	Authority deny scenarios	Safety & gating	EV-19 deny evidence; negative test PASS	Covers unauthorized control attempts
PACK-07	Continuity engage/hold/exit	Continuity timing contract	EV-11..14 sequence; timing report	External buffer behavior represented via fields
PACK-08	Thermal regime entry/exit	Regime catalog behavior	EV-15/16; inhibit actions logged	Includes thermal hotspot signature
PACK-09	ESR anomaly signature	External buffer degradation	EV-15 regime=ESR; guardrail clamp	Supports aging/ESR detection logic
PACK-10	Policy proposal + diagnosis	L3 output contract	EV-09/10; artifact linkage validated	Ensures evidence linkage fields are present

12.4 Profile Pack Templates and Manifest Binding

Profile packs define policy defaults and guardrails. All profile packs must be manifest-bound and anti-rollback protected in field updates. Human-facing text summaries (for review) must be generated from the same canonical source as machine-consumed artifacts.

Table 12–5 Profile Pack Template (Concise)

Field	Meaning	Required	Notes
profile_id	Profile identifier	Yes	Immutable ID; human-readable alias allowed
profile_version	Profile semantic version	Yes	Tied to guardrails + defaults
sku	Target SKU / node class	Yes	A1/A2-S/A2-P/A3/A4 mapping
enabled_interfaces	Enabled ports/buses	Yes	Must respect applicability matrix
authority_mode	Autonomy/authority mode	Yes	Must log actor/mode in control paths
rate_limit_policy	Rate-limit thresholds/actions	Yes	Emits EV-07/08 when active
ordering_contract_ref	Ordering/timebase contract ref	Yes	Version-pinned reference
guardrails	Hard limits & clamps	Yes	Safety-first; AI may propose but not override by default
continuity_policy	Continuity/RT external engagement rules	Optional	External buffer hooks only; emits EV-11..14
regime_catalog_ref	Regime catalog reference	Yes	Version-pinned; supports EV-15/16
evidence_budget	Event/snapshot budget	Yes	Per SKU constraints; transport/storage notes
artifact_formats	Output formats selection	Yes	JSON for machine, text for human summaries
defaults_hash	Hash of default set	Yes	Ensures deterministic baseline
notes	Human-readable rationale	Optional	For review; not used by enforcement

Table 12–6 Manifest Binding Rules (Concise)

Artifact	Hash Rule	Consumer	Notes
Schema bundle	SHA-256 over bundle file set	Validator/CI	Bundle is atomic; partial updates forbidden
Evidence registry	SHA-256 over registry index	BSP/tools	EV IDs append-only; hash pins semantics

Ordering contract	SHA-256 over contract doc + schema	Merge tool/CI	Required for A1/A4 smoke-run
Canonical packs	SHA-256 per pack + index	CI/replay	Packs immutable per release
Golden outputs	SHA-256 per output set	CI/replay	Must match canonical packs deterministically
Profile pack (JSON)	SHA-256 over canonical JSON	Device/BSP	Machine-consumed artifact
Profile summary (text)	Derived from same canonical source	Human review	Must include source hash pointer
Firmware/bitstream	SHA-256 over binary	Device	Bound to profile + schema compatibility
Tool binaries	SHA-256 over build artifacts	Dev/CI	Recorded build hash and version
Release manifest	SHA-256 over manifest file	All	Manifest is the root-of-trust for release package

12.5 Lab Recipe Templates and Reproducibility Checklist

Lab recipes define repeatable validation procedures. A reproducibility checklist is required for every bench and every automation script used by qualification gates.

Table 12–7 Lab Recipe Template (Concise)

Recipe	Inputs	Steps	Outputs	Notes
LAB-01 Baseline bring-up	DUT + profile + schema bundle	Flash → enable telemetry → run PACK-01	Validator PASS; baseline logs	First-run sanity
LAB-02 Multi-source merge	DUT + host + PSU log tap	Collect aligned streams → run PACK-02/03	Merge report; EV-18 flags	A1/A4 focus
LAB-03 Ordering reset/gap	DUT + reset script	Inject resets/gaps → run PACK-04	EV-17 gap flags; replay PASS	Deterministic replay
LAB-04 Storm / rate-limit	DUT + load generator	Burst events → enforce policy	EV-07/08; bounded payload	Stress + compliance
LAB-05 Authority deny	DUT + unauthorized actor	Attempt forbidden actions	EV-19 deny evidence	Negative tests mandatory
LAB-06 Continuity timing	DUT + external buffer emulator	Trigger → hold → exit sweeps	EV-11..14 + timing report	External RT hooks only

LAB-07 Thermal regime	DUT + chamber / heater	Raise temp → observe regime	EV-15/16 + inhibit actions	Hotspot signatures
LAB-08 ESR anomaly sweep	DUT + ESR emulation network	Sweep ESR/aging proxy	Regime enter + guardrail clamps	External buffer risk
LAB-09 PoE derating (if applies)	PoE source + PD path	Apply derating profile	Bench report + EV packs	P_base replaceable
LAB-10 Release smoke-run	Full release pack	Run all canonical packs	CI pass + signed manifest	Release-blocking

Table 12–8 Reproducibility Checklist (Concise)

Item	Required	Evidence	Notes
DUT identifiers (HW rev, SKU, serial)	Yes	DUT manifest entry	Immutable per run
Firmware/bitstream hash	Yes	Hash in run log	Must match release manifest
Profile pack hash	Yes	Hash pointer in logs	Binds policy & guardrails
Schema bundle version + hash	Yes	Validator header	Contract pinning
Toolchain versions (validator/merge tools)	Yes	Build hashes	Prefer container/pinned env
Timebase source declared	Yes	ts_sys mapping note	A1/A4 mandatory
Lab setup photo/diagram (minimal)	Optional	Attachment ref	Only for ambiguous wiring
Instrumentation model + calibration status	Yes	Cal date / cert ref	Power analyzer/chamber/load
Test script version	Yes	Git commit / tag	No untracked edits
Raw logs retained	Yes	Storage path + checksum	Enables deterministic replay
Golden pack used (pack IDs)	Yes	Pack list in report	Must match Table 12–4
Pass/fail criteria recorded	Yes	Gate report	No “verbal pass”
Waivers recorded with owner + closure	If any	Waiver log entry	Weekly review required

12.6 Program Checklists (FPGA, ASIC, BSP/SDK Release)

This appendix contains the release checklists used to enforce gate discipline. Checklists must be signed off and attached to the release manifest.

【PLACEHOLDER｜Table 12–9 FPGA Release Checklist (Check / Pass Criteria / Artifacts / Notes)】
【PLACEHOLDER｜Table 12–10 ASIC Release Checklist (Check / Pass Criteria / Artifacts / Notes)】
【PLACEHOLDER｜Table 12–11 BSP/SDK Release Checklist (Check / Pass Criteria / Artifacts / Notes)】

Table 12–9 — FPGA Release Checklist (Concise)

Table 12–9 FPGA Release Checklist (Concise)

Check	Pass Criteria	Artifacts	Notes
Schema bundle pinned	Manifest lists schema+validator hashes	Release manifest	No floating versions
Canonical packs replay	All PACK-01..10 replay PASS	Replay report	Deterministic required
Evidence coverage	EV core coverage ≥ target threshold	Coverage report	SKU/applicability aware
Ordering compliance	ts/seq/reset_seq/gap_flag valid where required	Ordering report	A1/A4 mandatory
Merge smoke-run (if applicable)	PACK-02/03 merge PASS + conflict policy applied	Merge report	A1/A4 focus
Rate-limit compliance	Storm test emits EV-07/08; bounded payload	Stress report	No silent drops
Authority gating	Negative tests emit EV-19; no unauthorized control	Deny logs	Release-blocking
Continuity timing (external)	EV-11..14 sequences valid; guardrails applied	Timing plots; EV packs	External buffer hooks only
Regime catalog behavior	EV-15/16 emitted with correct entry/exit	Regime report	Includes thermal & ESR cases
Traceability baseline	FPGA baseline manifest created and signed	Baseline manifest	Used for ASIC comparison

Table 12–10 ASIC Release Checklist (Concise)

Check	Pass Criteria	Artifacts	Notes
SKU definition pack locked	Interfaces/authority/evidence budgets declared	SKU pack	Productization rule enforced
IP ownership complete	All IP licensed/cleared; fallback decided	IP map; decision log	No “TBD IP” at release
Signoff complete	Mandatory signoff reports PASS (as defined)	Signoff set	Waivers tracked explicitly
Qualification matrix PASS	SKU-bound qual matrix complete	Qual matrix; reports	Consistent across SKUs
Evidence budget enforced	Event rates within declared maxima	Budget compliance report	Rate-limit policy validated
Security anchors PASS	Provision+anti-rollback+debug gating validated	Security report; logs	EV-19 coverage required
Continuity hooks validated	EV-11..14 timing + guardrails PASS	Timing report; profiles	External buffer framing
FPGA baseline traceability	Deltas declared; no silent behavior drift	Trace matrix; delta notes	Release-blocking

Bring-up smoke-run PASS	Canonical packs run on silicon	Bring-up report	PACK subset allowed per SKU
Release manifest complete	All artifacts hashed and packaged	Release manifest	Root-of-trust

Table 12–11 BSP/SDK Release Checklist (Concise)

Check	Pass Criteria	Artifacts	Notes
Schema compatibility	SDK validates against pinned schema bundle	SDK CI logs	Matches release manifest
API surface complete	API groups documented; authority rules enforced	API docs; tests	Deny evidence on violations
Telemetry ingestion	All required sources parse/normalize	Parser tests	Host/PSU logs for A1/A4
Timebase contract	ts_sys mapping + ordering fields produced	Ordering report	Replay must be deterministic
Merge rules implemented	Conflict policy applied; EV-18 flags correct	Merge test report	Smoke-run required
Evidence emission	EV core mapping correct; minimal payload	EV mapping report	No ID drift
Rate-limit behavior	EV-07/08 emitted; summaries correct	Stress report	Bounded payload
Continuity API (external)	RT policy/guardrails/events exposed (no on-die storage)	API tests; docs	External buffer semantics
Sample packs shipped	Canonical packs + expected outputs included	Pack index	Used by users/CI
Manifest binding	SDK release binds to manifest hashes	Release manifest	No partial installs

12.7 Document Control and Versioning

All tables, figures, schema bundles, sample packs, and checklists are version-controlled. Revisions must indicate the change scope, impacted gates, and compatibility status.

Table 12–12 Document Control (Concise)

Item	Version	Change Summary	Impacted Gates
Main spec document	v1.0	Baseline spec release (FPGA→ASIC)	Release readiness
Evidence registry (EV index)	v1.0	EV-01..EV-20 core set defined	Coverage, replay, audit
Schema bundle	v1.0	EV schema + validator + examples pinned	Schema validation, replay
Ordering/timebase contract	v1.0	ts/seq/reset_seq/gap_flag rules pinned	Ordering, merge smoke-run
Merge rules	v1.0	Alignment/conflict policy + EV-18 flags	Merge smoke-run

Canonical packs set	v1.0	PACK-01..10 established	Replay, smoke-run
Golden outputs	v1.0	Expected outputs for canonical packs	Replay
Profile pack template	v1.0	Profile fields + guardrails structure pinned	Release readiness
Rate-limit policy template	v1.0	Threshold/actions + summary payload pinned	Rate-limit compliance
Continuity/RT policy template	v1.0	External buffer hooks + EV-11..14 timing	Continuity timing
FPGA baseline manifest	v1.0	Baseline hashes for FPGA superset release	Traceability
ASIC SKU definition pack	v1.0	SKU split + applicability + budgets	Applicability, readiness
Qualification matrix	v1.0	SKU-bound qual scope + checks	Qualification readiness
Lab recipe set	v1.0	LAB-01..10 recipes versioned	Lab reproducibility
Release checklists	v1.0	FPGA/ASIC/BSP checklist baselines	Release readiness
Waiver log template	v1.0	Waiver tracking + closure discipline	Tape-out readiness