Rincon Photonics

Preliminary Requirements and System Specification

Document Type: Pre-pipeline RFP / Functional Specification
Version: 0.6-2 (System/Subsystem Reorganization; M0-Ready)
Date: 2026-06-20
Prepared For: AI-Native Software Delivery Pipeline (HV M0-M7) - Epic/Feature Decomposition and Digital Twin Generation
Classification: Working Draft - Not for Distribution

Changes through v0.6-2

[v0.6-2] M0-readiness fixes (from pipeline review): moved the cross-cutting REQ-2/REQ-5/REQ-9 content OUT of the build spec into a separate internal Cross-Cutting Capabilities document so M1 cannot extract unplaced features; authored each subsystem's own fault detection inline in its F.3 (escalation/correlation to B4); narrowed A4's physics seam to modem-layer parameters (atmospheric channel belongs to A5); and stubbed B5's dependency on A7 enclosure-seal state (binary sealed/open at 1 Hz) pending the REQ-5 split.

[v0.6] Reorganized into a System -> Subsystem -> Epic hierarchy, losslessly: migrated epics retain their full features and activities; A1 Beam Steering authored in full; cross-cutting REQ-2/REQ-5/REQ-9 flagged split-pending; reference appendices A (Acceptance Traceability Index), B (Performance & DT-AT), C (Beam Steering Worked Decomposition & OQ-3), D (Verification & Evaluation Criteria).

[v0.5] Consolidated internal refinements since v0.4: (a) tightened the document to build requirements only - removed authoring/methodology statements and approach/value narrative, regrouping the interface and architecture constraints as REQ-12; (b) established the per-subsystem interface contract as the buildable unit, specifying the beam-steering HAL contract in full as subsystem A1 (signatures, data types, FSM, fault enum, performance bounds, seams); and (c) reframed REQ-11 and REQ-12 as the per-subsystem verification & evaluation criteria applied against each contract.

[v0.4] Added the physics-twin requirements (§6.4): per-seam parameter specs with backward-derived fidelity criteria, validation protocols, and provenance tiers.

Added REQ-11 (Engineering Validation & Test Software) and REQ-12 (Hardware/Software Co-Design & Interface Control), establishing the hardware-adjacent pipeline track alongside the operational-product epics (REQ-1-REQ-10).

Added a worked M3 decomposition for the Beam Steering subsystem (Gimbal/OPA) demonstrating the interface-contract vs. physics scope boundary (Appendix A).

Reconciled the term "digital twin" into two explicit layers - interface-contract twin (pipeline-generated) and physics twin (separate bench-calibrated workstream) - see §6.

Extended the §6.3 interface table with the parameter-ingestion contract carrying version + provenance/fidelity tier; introduced the two-seam-type dependency model.

Added acceptance tests DT-AT-13 through DT-AT-16 (HAL opacity enforcement, parameter provenance traceability, interface-contract twin conformance, cross-subsystem seam integration).

OQ-3 reclassified from BLOCKING to Resolved (pending parameters); added OQ-11 and OQ-12.

Contents

1. System Overview

1.1 What Is Rincon Photonics?

Rincon Photonics is a Tucson, Arizona optics startup building free-space optical communication (FSOC) terminals for satellite laser communications, founded in 2025. Its terminals transmit data as tightly collimated, invisible near-infrared laser beams between terminal pairs, achieving fiber-equivalent throughput without trenching, spectrum licensing, or right-of-way permitting. With bench hardware roughly twelve months out, Rincon is building a complete software twin of the terminal control stack — with physics held behind contracted seams and every parameter labeled with what it is worth — to give investors a full terminal pass and hand subsystem vendors interface contracts to build against.

The terminal roadmap spans several generations: an initial research terminal (2025-2026); the Rincon LT-1 (a dual-mirror mechanical tracking unit rated at 20 Gbps / 20 km / 99.9% availability); the Rincon LT-1P (carrier/space-grade, 20 Gbps, 99.999% availability with hitless RF/fibre switchover); and the Rincon SB-1 (25 Gbps / 10 km, solid-state silicon-photonic phased array with no moving parts). This specification treats the system generically across the terminal family unless a distinction is material to the requirement.

Target validation milestones (pre-hardware):

- Full terminal pass demonstrated in the software twin ahead of bench hardware.
- Interface contracts issued to subsystem vendors for parallel build.
- Physics parameters staged behind contracted seams with provenance/fidelity tiers (Rincon Photonics, 2026).

1.2 Problem Statement

Approximately 2.6 billion people lack reliable broadband. The primary barriers are not spectrum scarcity or radio interference, but cost and physical access: deploying fibre requires trenching rights, capital-intensive civil works, and years of permitting. RF/microwave backhaul is licensed, congested in dense urban areas, and bandwidth-limited. Satellite (e.g. LEO constellations) introduces latency and per-terminal cost at scale.

Rincon addresses the “last-mile and middle-mile gap” - specifically the scenario where a fibre point-of-presence exists within 20 km of an underserved population but civil infrastructure makes the final connection economically or logistically infeasible.

1.3 Operating Environment

Dimension	Constraints
Atmospheric	Fog is the primary adversary (scattering coefficient >50 dB/km in dense fog). Light rain acceptable; heavy precipitation degrades link. Haze, dust, particulates reduce margin. Thermal turbulence (scintillation) causes beam wander and intensity fluctuation.
Geographic	River crossings, urban rooftop-to-rooftop, campus inter-building, edge-of-network middle-mile. Line-of-sight (LOS) mandatory - no NLOS capability.
Infrastructure	Mounting on rooftops, poles, towers, or building facades. Power: 40 W typical, 60 W max per terminal; supports ±48 V DC or PoE++ (UPoE). IP65 enclosure. Operating temperature −20°C to +55°C ambient (+65°C with solar loading).
Regulatory	Operates in unlicensed 193 THz band (1535-1565 nm near-infrared). Eye-safe laser classification required. No spectrum license required in most jurisdictions.

1.4 Key Technical Approach

Physical layer: Narrow collimated beam (~1550 nm wavelength) transmitted between two terminals. Beam divergence is minimised to maximise received power at distance.

Beam acquisition and tracking (LT-1): Two-mirror gimbal system with predictive algorithms and sensor fusion (inertial + optical) maintains sub-milliradian alignment. Lock-on after initial scan; continuous re-tracking during operation.

Beam acquisition and tracking (SB-1): Silicon-photonic optical phased array (OPA) with >1,000 miniature emitters on a fingertip-sized photonic module. Electronic beam steering - no moving parts. Enables faster acquisition, lower power, and higher reliability in vibration-prone environments.

Atmospheric adaptation: Real-time monitoring of received signal strength; automatic gain control and link margin management. Integration with RF or fibre backup on LT-1P for hitless switchover during link outages.

Link layer: Presents as a standard Ethernet interface to upstream networking equipment. Throughput: 20-25 Gbps full-duplex. Latency: sub-millisecond (physical layer); total end-to-end latency comparable to fibre over equivalent distances.

---

2. Stakeholders and System Roles

Role	Responsibilities	Pipeline Ownership
Network Operator	Deploys Rincon links as part of backhaul or access network topology. Configures routing, monitors SLAs, manages failover to RF/fibre.	Network Integration, Remote Management
Field Technician	Physically installs terminals, performs initial alignment and commissioning, replaces hardware. Does not write software.	Installation & Calibration, Physical Hardware Interface
Network Engineer	Designs link budgets, selects deployment sites, plans atmospheric margin, integrates with existing IP/MPLS routing.	Beam Tracking config, Link Adaptation parameters
Cloud/Platform Administrator	Manages the cloud fleet-management backend, user access, firmware updates, alerting, and API integrations.	Remote Management, Security & Access Control
ISP / Wholesale Customer	Purchases capacity on a Rincon link; receives an Ethernet hand-off; measures uptime against SLA.	Network Integration (SLA enforcement)
Enterprise Customer	End consumer of bandwidth. Requires high availability and consistent throughput.	Performance Acceptance Criteria
Regulatory Authority	Requires compliance with eye-safety standards (IEC 60825), export controls, and national telecoms regulations.	Security, Physical Safety
Rincon Platform Engineering	Develops and ships firmware, cloud management software, OPA/mirror control algorithms, and integration APIs.	All epics (system owner)
Test / Validation Engineer	**[v0.3]** Authors and runs the EVT/validation software; characterizes hardware on the bench; owns the verification suite against twin and hardware.	Verification & evaluation (per-epic F.3)

Role	Responsibilities	Pipeline Ownership
Physics / Simulation Engineer	**[v0.3]** Builds and calibrates the physics-twin modules (§6.1); supplies versioned, provenance-tagged performance parameters to the interface-contract twin.	Physics workstream (§6.1); parameter ingestion (per-epic F.5)

3. Architecture & Decomposition Model

This specification is organized for an AI-native, human-governed build pipeline. The hierarchy is **System -> Subsystem -> Epic -> Feature -> Activity.** Each epic is **self-contained**: it carries, inline, its own interface contract, behavior, verification & evaluation, constraints, and - for hardware-adjacent epics - physics seams, so the build can be decomposed locally without dereferencing cross-cutting sections.

Two systems: **System A - Optical Link Terminal** (hardware-adjacent epics; facets F.1-F.5) and **System B - Management & Operations** (software-service epics; facets F.1-F.4, no physics seams). The former cross-cutting verification & evaluation criteria and architecture constraints are applied inside each epic's F.3 and F.4.

NEW IN v0.6 v0.6 reorganizes the prior REQ-1-REQ-10 capability epics into self-contained subsystem epics, preserving their features and activities. Clean-mapping epics are migrated in full. Three **cross-cutting** capabilities (former REQ-2 atmospheric/adaptation, REQ-5 hardware interface, REQ-9 fault/self-healing) span multiple epics; their content is held in a **separate internal Cross-Cutting Capabilities document** (split pending), deliberately kept out of this build spec so the pipeline does not extract unplaced features from it. Per-subsystem fault *detection* (the REQ-9 detection layer) is authored locally in each epic's F.3; only cross-subsystem escalation/correlation is deferred to B4. A1 (Beam Steering) is authored in full as the facet template; the hardware interface contracts (F.1) and physics seams (F.5) for A4/A6/A7 remain to-author.

Prior-structure mapping

Prior	New home
REQ-1 Beam Acquisition & Tracking	A1 Beam Steering (full)
REQ-2 Atmospheric Compensation & Link Adaptation	CROSS-CUTTING -> A2/A3/A5; separate Cross-Cutting doc (split pending)
REQ-3 Link Layer & Error Correction	A4 Link / Modem (full)
REQ-4 Power & Thermal	A6 Power + A7 Thermal (full; clean split)
REQ-5 Physical Hardware Interface	CROSS-CUTTING -> A1/A7/B1; separate Cross-Cutting doc (split pending)
REQ-6 Network Integration	B1 Network Integration (full)
REQ-7 Remote Management	B2 Remote Management & Fleet Backend (full)
REQ-8 Field Installation & Calibration	B3 Field Installation & Commissioning (full)
REQ-9 Fault Detection & Self-Healing	CROSS-CUTTING -> each F.3 (detection) + B4 (escalation); separate Cross-Cutting doc (split pending)
REQ-10 Security & Access Control	B5 Security & Access Control (full)

4. System A - Optical Link Terminal

Hardware-adjacent subsystem epics (facets F.1-F.5). A1 is authored in full; A4/A6/A7 are migrated in full from prior requirements with F.1 (interface contract) and F.5 (physics seams) to-author; A2/A3/A5 depend on the cross-cutting REQ-2 split and are flagged.

A1 - Beam Steering [AUTHORED IN FULL]

Scope: Establish and maintain a locked optical link by steering the beam (two-mirror gimbal or silicon-photonic OPA) from power-on through continuous tracking; expose orientation for commissioning. Migrates former REQ-1; reflects the IMU/orientation portion of REQ-5 (full REQ-5 in the separate Cross-Cutting Capabilities document, split pending).

Features

- **REQ-1.1** The system shall perform an autonomous wide-angle scan to locate the opposing terminal within a configurable angular search space upon activation.
- **REQ-1.2** The system shall transition from scan mode to fine-tracking mode and establish a locked optical link within the beam acquisition time budget.
- **REQ-1.3** The system shall maintain beam alignment to sub-milliradian precision under continuous operation, including thermal expansion of mounting structures.
- **REQ-1.4** The system shall re-acquire a dropped link automatically without operator intervention, within the target re-lock time budget.
- **REQ-1.5** The system shall detect and compensate for vibration inputs (wind, traffic, HVAC) using predictive feed-forward and sensor feedback.
- **REQ-1.6** The system shall log all acquisition events, lock durations, and re-acquisition attempts with timestamps for post-hoc analysis.

F-A1.1 Interface contract

Method (signature)	Description
`set_mode(mode: Mode, seq: u32) -> Ack`	Request an operating-mode transition (see FSM).
`set_beam_angle(az_mrad: f32, el_mrad: f32, seq: u32) -> Ack`	Absolute pointing setpoint; rejected RANGE_EXCEEDED if outside envelope.
`get_beam_state() -> BeamState`	Angle estimate, mode, abstracted actuator state, RSS, timestamp; pollable >= 1 kHz.
`get_capabilities() -> Capabilities`	Per-variant descriptor; the only place variant differences surface.
`get_orientation() -> Orientation`	Az/el/tilt from IMU at 10 Hz (commissioning + alignment assist).
`subscribe_faults(cb: fn(FaultEvent)) -> SubId`	Asynchronous fault events from the unified taxonomy.
Type	**Definition / values**
BeamAngle	`{ az_mrad: f32, el_mrad: f32 }` az +/-87.3, el +/-52.4 mrad (OQ-1); res <= 0.05 mrad
Mode	`enum { IDLE, SCAN, ACQUIRE, FINE_TRACK, HOLD, FAULT, SAFE }`

Method (signature)	Description
ActuatorState	`enum { NOMINAL, DEGRADED, FAULT }` (abstracted; never raw per-element health)
BeamState	`{ angle, mode, actuator_state, rss_dbm: f32, ts_utc: i64, seq_ack: u32 }`
Capabilities	`{ variant: {GIMBAL|OPA}, az/el_range_mrad, resolution_mrad, max_slew_mrad_s, settle_ms, supported_faults: FaultCode[] }`
FaultCode	`enum { COMMAND_INVALID, FEEDBACK_LOST, RANGE_EXCEEDED, ACTUATOR_DEGRADED, APERTURE_DEGRADED, OVER_TEMP }`

Operating-mode FSM:

From	Event	To	Guard / note
IDLE	activate	SCAN	after calibration state loaded
SCAN	signal_detected	ACQUIRE	RSS > acquisition threshold
SCAN	scan_timeout	FAULT	emits FEEDBACK_LOST (peer-not-found)
ACQUIRE	converged	FINE_TRACK	pointing error < 0.5 mrad
ACQUIRE	converge_timeout	SCAN	> 5 s without lock
FINE_TRACK	link_loss	SCAN	RSS below floor > 100 ms; warm restart
FINE_TRACK	hold_requested	HOLD	operator / maintenance
HOLD	resume	FINE_TRACK	-
(any)	unrecoverable_fault	FAULT	hardware fault; escalates to A5/B4
(any)	safe_requested	SAFE	eye-safety interlock
FAULT / SAFE	reset	IDLE	operator-cleared

F-A1.2 Behavior

- **SA-1.1.1 (Normal):** On power-on, read stored site calibration and initialise the steering mechanism (mirror or OPA) to the last-known peer bearing.
- **SA-1.1.2 (Normal):** Execute a spiral or raster scan across the configured angular search space, sampling received optical power at each dwell position.
- **SA-1.1.3 (Normal):** On received power above the acquisition threshold, halt the scan, refine pointing via hill-climbing, and transition to fine-tracking.
- **SA-1.1.4 (Failure):** If no signal after a full scan, log 'peer not found', back off, and repeat up to a retry limit before a critical fault.
- **SA-1.1.5 (Performance):** Full scan-to-lock latency <= 20 s under clear-air from cold start with coarse alignment pre-set.
- **SA-1.2.1 (Normal):** On initial detection, engage closed-loop fine-tracking, driving pointing error below 0.5 mrad before declaring lock.
- **SA-1.2.2 (Normal):** Transmit a lock-confirmed event with timestamp, peer identity, and RSS at lock.

- **SA-1.2.3 (Failure):** If fine-tracking fails to converge within 5 s of detection, fall back to scan mode and log a convergence failure.
- **SA-1.2.4 (Performance):** Detection-to-declared-lock <= 3 s under clear-air.
- **SA-1.3.1 (Normal):** Run a continuous feedback loop sampling pointing error at >= 1 kHz, issuing corrections to the steering actuator.
- **SA-1.3.2 (Normal):** Apply a thermal drift correction model, adjusting the setpoint as a slow bias (default 60 s interval).
- **SA-1.3.3 (Normal):** Monitor RMS pointing error; warn if sustained error exceeds 0.8 mrad (mounting instability).
- **SA-1.3.4 (Performance):** Steady-state pointing error <= 0.5 mrad RMS under normal conditions.
- **SA-1.4.1 (Normal):** On link loss (RSS below noise floor > 100 ms), enter warm-restart scan centred on last-known good bearing.
- **SA-1.4.2 (Normal):** Warm-restart uses a reduced window (±1° default) to cut re-acquisition latency vs. cold start.
- **SA-1.4.3 (Failure):** If warm-restart fails within 5 s, expand to the full cold-start scan.
- **SA-1.4.4 (Performance):** Warm-restart re-acquisition <= 5 s from link-loss detection in clear air.
- **SA-1.4.5 (Integration):** Publish link-loss and re-acquisition events to the management backend in real time for SLA accounting.
- **SA-1.5.1 (Normal):** Fuse IMU accelerometer data with optical pointing error to distinguish structural vibration from true beam wander.
- **SA-1.5.2 (Normal):** A feed-forward vibration model predicts displacement from IMU input and issues pre-emptive corrections.
- **SA-1.5.3 (Normal):** Adapt the vibration model in real time to building-specific resonance frequencies observed on site.
- **SA-1.5.4 (Failure):** If IMU data is unavailable/corrupt, fall back to optical-only feedback and log 'IMU degraded'.
- **SA-1.6.1 (Normal):** Write every acquisition, lock, drop, and re-acquisition event to the local log (timestamp, duration, RSS, cause).
- **SA-1.6.2 (Normal):** Compute aggregated acquisition statistics hourly (mean lock time, drop rate, mean re-acq time) and report them.
- **SA-1.6.3 (Integration):** Export raw event logs via REST API in JSON and CSV.
- **SA-1.7.1 (Normal, from REQ-5):** Report az/el/tilt from the IMU at 10 Hz via the commissioning API; broadcast a pointing-quality score for alignment assist; gate on IMU plausibility (±16 g, ±2000 °/s).

F-A1.3 Verification & evaluation

- Conformance: verify implemented HAL against F-A1.1.
- Interface-contract twin: reproduce FSM/timing/error modes, parameterized by F-A1.5; stamp each run with parameter-set version + fidelity tier.
- HIL harness: steering-interface simulator binding stack to twin or hardware identically; inject feedback-loss / range-exceedance.
- Acceptance (inline): cold-start scan-to-lock <= 20 s [DT-AT-01]; warm re-acq <= 5 s [DT-AT-02]; fine-track convergence <= 3 s; steady pointing <= 0.5 mrad RMS under wind/HVAC PSD [DT-AT-10]; loop >= 1 kHz; HAL opacity [DT-AT-13].
- Fault detection (this subsystem owns these): `feedback_lost` emitted when actuator/feedback telemetry is stale, implausible, or missing > 100 ms (FSM -> FAULT/SAFE); `range_exceeded` emitted and the command rejected when a setpoint is outside the configured envelope; `actuator_degraded` emitted when gimbal pointing-error variance exceeds the F-A1.5

threshold; `aperture_degraded(level)` emitted from the F-A1.5 OPA aperture-loss map; `over_temp` consumed from A7. Each surfaced via the unified taxonomy with the correct FaultCode. Acceptance: each injected fault condition produces the correct FaultCode within one control cycle. Cross-subsystem correlation, classification, and switchover decisions are B4's (system-level).

F-A1.4 Constraints

- HAL opacity: tracking consumes only BeamState + FaultCode; raw per-element/actuator health never exposed (DT-AT-13).
- Parameter ingestion: every F-A1.5 parameter carries `physics_parameter_set_version` + fidelity tier.
- Seam integration (end-to-end): steering <-> Tx-power (`beam_safe_state` eye-safety interlock); steering <-> commissioning app.

F-A1.5 Physics seams

Field	Type	Source
max_slew_mrad_s	f32	physics: slew rate
settle_ms	f32	physics: settling
resolution_mrad	f32	physics: resolution
resonance_hz	f32[]	physics: resonance/bandwidth
actuator_degradation_curve	lookup<f32,f32>	physics: gimbal degradation
aperture_loss_map	lookup<level,far_field>	physics: OPA aperture loss
eye_safety_envelope	fn(geometry)->max_dbm	physics: eye-safety

Sets stamped `physics_parameter_set_version: u32` + `fidelity_tier enum { datasheet_estimate | literature_model | bench_measured | validated }`. Curve/map fields delivered as sampled lookup tables over the ingestion contract; physics workstream owns derivation.

A2 - Optical Transmit

Scope: Laser source, modulator, transmit-power control, eye-safety power envelope.

SPLIT PENDING Primary behavior derives from former REQ-2.4 (adaptive Tx power), which is cross-cutting. Full REQ-2 content in the separate Cross-Cutting Capabilities document (split pending). F-A2.1 interface contract and F-A2.5 physics seams (laser power/divergence/far-field) to-author once the split is agreed.

A3 - Optical Receive

Scope: Aperture, detector, AGC, RSS / link-margin sensing.

SPLIT PENDING Primary behavior derives from former REQ-2.1 (RSS monitoring) and REQ-2.2 (AGC), which are cross-cutting. Full REQ-2 content in the separate Cross-Cutting Capabilities document (split pending). F-A3.1 contract and F-A3.5 seams (detector sensitivity, noise floor) to-author once the split is agreed.

A5 - Link Adaptation & Switchover

Scope: Atmospheric-degradation classification, link-margin-driven adaptation, hitless switchover to/from backup.

> **SPLIT PENDING** Primary behavior derives from former REQ-2.3-2.6 (classification, switchover, restoration) plus REQ-9.4 (fault-triggered switchover) - both cross-cutting. Full REQ-2 and REQ-9 content in the separate Cross-Cutting Capabilities document (split pending). The atmospheric channel is the highest physics-fidelity risk (OQ-12); F-A5.5 seam to-author.

A4 - Link / Modem [migrated from REQ-3]

Scope: Data-plane functions from the optical detector to the Ethernet hand-off: FEC, framing, full-duplex, link statistics, QoS.

Features

- **REQ-3.1** The system shall present a standard IEEE 802.3 Ethernet interface (10GbE or 25GbE).
- **REQ-3.2** The system shall implement FEC sufficient to meet the target BER at the link margin floor.
- **REQ-3.3** The system shall support full-duplex operation with simultaneous transmit and receive.
- **REQ-3.4** The system shall enforce maximum frame size (MTU) and transparently pass IEEE 802.1Q VLAN tags.
- **REQ-3.5** The system shall report per-second link statistics (throughput, error rate, frame loss, FEC events).
- **REQ-3.6** The system shall pass QoS/DSCP markings through unmodified.

F-A4.1 Interface contract

- [to author] IEEE 802.3 Ethernet/MAC interface; statistics counter set; FEC configuration; carrier-detect signal.

F-A4.2 Behavior

- **SA-3.1.1 (Normal):** On link lock, assert Ethernet carrier detect on the data port, bringing the logical link up.
- **SA-3.1.2 (Normal):** Negotiate or configure interface speed (10GbE or 25GbE) by terminal model and operator config.
- **SA-3.1.3 (Failure):** On optical link loss, de-assert carrier detect within 100 ms, triggering upstream failover.
- **SA-3.2.1 (Normal):** FEC encoder wraps outbound optical data in error-correcting codes (Reed-Solomon or LDPC).
- **SA-3.2.2 (Normal):** FEC decoder corrects bit errors and passes clean frames to the Ethernet interface.
- **SA-3.2.3 (Normal):** Track and report FEC correction rate as a leading indicator of margin degradation.
- **SA-3.2.4 (Failure):** On an uncorrectable block, drop the frame, increment frame-loss counter, log a FEC overrun.
- **SA-3.3.1 (Normal):** Operate simultaneous Tx/Rx optical paths with no time-division multiplexing.
- **SA-3.3.2 (Normal):** Monitor per-direction throughput and error rates independently.

- **SA-3.4.1 (Normal):** Pass Ethernet frames up to the configured MTU (default 1500; up to 9000 jumbo).
- **SA-3.4.2 (Normal):** Preserve IEEE 802.1Q VLAN tags unmodified; do not inspect or strip.
- **SA-3.4.3 (Failure):** Drop oversized frames and count them; no fragmentation.
- **SA-3.5.1 (Normal):** Maintain per-second counters: Tx/Rx bytes & frames, FEC corrections, FEC overruns, dropped frames, link-down events.
- **SA-3.5.2 (Integration):** Expose counters via SNMP MIB, NETCONF, and REST API; reset on reboot / operator command.
- **SA-3.6.1 (Normal):** Pass IP DSCP markings unmodified.
- **SA-3.6.2 (Normal):** Report aggregate traffic distribution across DSCP classes (optional telemetry).

F-A4.3 Verification & evaluation

- **Acceptance:** post-FEC BER <= 1e-12 at minimum link margin (30 dB/km, 1 km) [DT-AT-05]; frame-forwarding latency <= 500 us; one-way physical-layer latency <= 1 ms; carrier-detect de-assert <= 100 ms; FEC overrun frame loss < 0.001%.
- **Conformance / twin / HIL:** interface-contract twin + HIL harness for the Ethernet/modem boundary.
- **Fault detection (this subsystem):** FEC overrun emitted when an uncorrectable block exceeds correction capacity (frame dropped, counter incremented); link-down emitted on carrier loss. Acceptance: each produces the correct fault within one reporting interval. Cross-subsystem correlation is B4's.

F-A4.4 Constraints

- HAL opacity; IEEE 802.3-compliant interfaces, no proprietary framing; QoS markings unmodified.

F-A4.5 Physics seams

- **[to author] modem-layer physics only:** FEC codec characteristics and detector SNR floor. (The atmospheric-channel-vs-link-margin dependency belongs to A5 Link Adaptation, not A4, and resolves when A5 is authored.)

A6 - Power [migrated from REQ-4]

Scope: Power-input conditioning, power-budget enforcement, graceful power-down sequencing.

Features

- **REQ-4.1** The system shall accept ±38-58 V DC (±48 V nominal) and PoE++ (IEEE 802.3bt Type 4) interchangeably.
- **REQ-4.2** The system shall operate within a typical 40 W envelope and shall not exceed 60 W under any condition.
- **REQ-4.4** The system shall implement graceful power-down sequencing to prevent data corruption and optical-component damage on power loss.

F-A6.1 Interface contract

- [to author] power state / telemetry API (rail voltages, draw, source type, shutdown command).

F-A6.2 Behavior

- **SA-4.1.1 (Normal):** At power-on, detect input source type (DC or PoE++) and configure conditioning accordingly.

- **SA-4.1.2 (Normal):** Validate input voltage in range (±38-58 V DC) before enabling downstream; else halt + 'power input fault'.
- **SA-4.1.3 (Failure):** On loss of primary power, initiate graceful shutdown within 200 ms, flushing logs + persisting calibration.
- **SA-4.2.1 (Normal):** Monitor total power draw at 10 Hz; maintain a rolling 1 s average.
- **SA-4.2.2 (Normal):** Near the 60 W ceiling, reduce non-critical subsystems in preference order before throttling optical output.
- **SA-4.4.1 (Normal):** On shutdown, sequence: disable optical Tx -> flush log buffer -> persist calibration -> power down in reverse-boot order.
- **SA-4.4.2 (Normal):** Complete shutdown within 500 ms; disable optical Tx within 50 ms (eye-safety).
- **SA-4.4.3 (Failure):** On storage-write failure, log to a separate fault register and complete shutdown; validate calibration next boot.

F-A6.3 Verification & evaluation

- **Acceptance:** steady-state draw <= 40 W; peak <= 60 W [DT-AT-09]; graceful shutdown < 500 ms; optical Tx disabled < 50 ms on trigger.
- Conformance / twin / HIL for the power-interface boundary.
- **Fault detection (this subsystem):** power_supply_fault emitted on rail out-of-range / PSU fault; power-input fault on out-of-range input voltage. Acceptance: each injected condition produces the correct fault. Cross-subsystem correlation is B4's.

F-A6.4 Constraints

- HAL opacity; accept ±38-58 V DC (±48 V nominal) and PoE++ (IEEE 802.3bt Type 4) interchangeably.

F-A6.5 Physics seams

- [to author] power-dissipation model -> physics workstream.

A7 - Thermal [migrated from REQ-4; + REQ-5 seal pending]

Scope: Thermal regulation, thermal telemetry, optical-power throttling. Will also host enclosure-seal monitoring (REQ-5) once the split is agreed.

Features

- **REQ-4.3** The system shall regulate internal operating temperature within component-safe bounds across -20°C to +55°C (+65°C with solar load).
- **REQ-4.5** The system shall report internal temperature, power draw, and power-supply status via the management interface.
- **REQ-4.6** The system shall throttle optical transmit power before thermal shutdown if component temperature limits are approached.

F-A7.1 Interface contract

- [to author] thermal state / telemetry API (per-sensor temps, margins, cooling actuator state); enclosure-seal status (pending REQ-5 split).

F-A7.2 Behavior

- **SA-4.3.1 (Normal):** Read temperature sensors across critical components (laser, detector, processor, PSU) at 1 Hz.
- **SA-4.3.2 (Normal):** PID controller modulates active cooling (fan, thermoelectric) to keep components in rated bounds.

- **SA-4.3.3 (Normal):** A thermal model predicts component temps from ambient + draw, enabling proactive cooling.
- **SA-4.3.4 (Failure):** If any component exceeds 90% of rated max, raise a thermal warning and begin optical throttling.
- **SA-4.5.1 (Normal):** Report per-sensor temps, aggregate draw, rail voltages, cooling-actuator state every 10 s.
- **SA-4.5.2 (Integration):** Thermal/power telemetry via SNMP MIB + REST API for DCIM integration.
- **SA-4.6.1 (Normal):** On thermal warning, reduce optical Tx power in 1 dB steps at 10 s intervals until below threshold.
- **SA-4.6.2 (Normal):** Log each throttle step (component, temp, new setpoint).
- **SA-4.6.3 (Failure):** If throttling reaches minimum and temp keeps rising, emergency optical shutdown + critical thermal fault.

F-A7.3 Verification & evaluation

- **Acceptance:** component temps within bounds over -20..+55 C (+65 C solar); throttling engages before shutdown.
- Conformance / twin / HIL for the thermal-interface boundary.
- **Fault detection (this subsystem):** thermal_limit / over_temp emitted when a component exceeds 90% of rated max; emergency optical shutdown on continued rise. Enclosure-seal self-test depends on the A7 seal scope (pending REQ-5 split; stub seal as binary sealed/open at 1 Hz). Acceptance: each injected condition produces the correct fault. Cross-subsystem correlation is B4's.

F-A7.4 Constraints

- HAL opacity; parameter ingestion; operating envelope -20..+55 C (+65 C solar).

F-A7.5 Physics seams

- **[to author] thermal-envelope model:** dissipation, ambient+solar rise, throttle thresholds -> physics workstream.

---

5. System B - Management & Operations

Software-service epics (facets F.1-F.4, no physics seams). B1/B2/B3/B5 migrated in full; B4 depends on the cross-cutting REQ-9 split and is flagged.

B1 - Network Integration [migrated from REQ-6; + REQ-5 ports pending]

Scope: Integration of the Rincon link into an operator's IP/Ethernet network. Will also host physical port-state enumeration (REQ-5) once the split is agreed.

Features

- **REQ-6.1** The system shall operate transparently as a Layer 2 bridge, passing all Ethernet frames without modification.
- **REQ-6.2** The system shall support configuration as a point-to-point link in an IP/MPLS backhaul topology.
- **REQ-6.3** The system shall support link aggregation (IEEE 802.3ad LACP) for bonding with parallel RF or fibre paths.
- **REQ-6.4** The system shall expose link state via carrier detect / SNMP trap for upstream failover.

- **REQ-6.5** The system shall support management-VLAN isolation separating management-plane from data-plane traffic.
- **REQ-6.6** The system shall interoperate via SNMP v2c/v3 and/or NETCONF/YANG.

F-B1.1 Interface contract

- [to author] network config API; SNMP MIB (IF-MIB + Rincon FSO MIB); NETCONF/YANG model; port-state enumeration (pending REQ-5 split).

F-B1.2 Behavior

- **SA-6.1.1 (Normal):** Forward all Ethernet frames between data port and optical path, unmodified (transparent L2 bridge).
- **SA-6.1.2 (Normal):** No MAC learning / ARP inspection / stateful L2 - a transparent wire replacement.
- **SA-6.1.3 (Performance):** Frame-forwarding latency <= 500 us.
- **SA-6.2.1 (Normal):** Configure as a point-to-point Ethernet segment without reboot.
- **SA-6.2.2 (Integration):** Support NETCONF/YANG config push from external controllers (Cisco NSO, Juniper Contrail).
- **SA-6.2.3 (Usability):** Simplified link-config wizard for operators without MPLS expertise.
- **SA-6.3.1 (Normal):** Participate in IEEE 802.3ad LACP, advertising the optical link as aggregatable.
- **SA-6.3.2 (Normal):** On optical loss, signal LACP partner to remove this link within 100 ms.
- **SA-6.3.3 (Failure):** On LACP negotiation timeout, log failure and fall back to standalone.
- **SA-6.4.1 (Normal):** Assert carrier detect / SNMP linkUp on lock.
- **SA-6.4.2 (Normal):** De-assert carrier detect / SNMP linkDown within 100 ms of optical loss.
- **SA-6.4.3 (Integration):** Publish link-state changes to REST API + webhooks.
- **SA-6.5.1 (Normal):** Apply operator-assigned management VLAN to management-plane traffic.
- **SA-6.5.2 (Normal):** Forward customer data-plane traffic without VLAN modification.
- **SA-6.5.3 (Access):** Deny management-plane access on non-management VLANs/interfaces.
- **SA-6.6.1 (Integration):** Expose SNMP MIB (IF-MIB RFC 2863 + Rincon FSO MIB) via v2c/v3.
- **SA-6.6.2 (Integration):** Support NETCONF (RFC 6241) with published YANG model.
- **SA-6.6.3 (Access):** SNMP v3 requires auth; community-string v2c may be disabled by policy.

F-B1.3 Verification & evaluation

- **Acceptance:** carrier-detect / linkDown trap <= 100 ms; LACP member removal <= 100 ms.
- Conformance / interface-contract twin for the network boundary.
- **Fault detection (this subsystem):** port/link fault emitted on port-down or no data-port link-up within 60 s of boot. Acceptance: each injected condition produces the correct fault. Cross-subsystem correlation is B4's.

F-B1.4 Constraints

- Open protocols SNMP v2c/v3 + NETCONF/YANG, no proprietary NMS; management-VLAN isolation; RBAC on management access.

B2 - Remote Management & Fleet Backend [migrated from REQ-7]

Scope: Cloud-based and on-device configuration, monitoring, updating, and operation at fleet scale.

Features

- **REQ-7.1** The system shall provide a cloud-based fleet management interface accessible via web browser and REST API.

- **REQ-7.2** The system shall support OTA firmware updates with rollback on a failed update.
- **REQ-7.3** The system shall stream real-time telemetry to the management backend at >= 1 s granularity.
- **REQ-7.4** The system shall support threshold-based alerting (email, webhook, SNMP trap).
- **REQ-7.5** The system shall maintain a local event log (>= 30-day rolling window) accessible without cloud connectivity.
- **REQ-7.6** The system shall support multi-tenant management segregating visibility and control by customer organisation.

F-B2.1 Interface contract

- [to author] versioned REST API (OpenAPI); telemetry payload schema; OTA package + signature format.

F-B2.2 Behavior

- **SA-7.1.1 (Normal):** Aggregate telemetry from all terminals; per-terminal/per-link health on map + list views.
- **SA-7.1.2 (Normal):** Expose all management functions via a versioned REST API (OpenAPI).
- **SA-7.1.3 (Access):** All API calls require a valid bearer token (OAuth 2.0; default 8 h expiry).
- **SA-7.1.4 (Usability):** Fleet map loads with status indicators within 3 s for up to 1,000 terminals.
- **SA-7.2.1 (Access):** Firmware-update commands only from authenticated administrator sessions.
- **SA-7.2.2 (Normal):** Verify firmware signature against a trust anchor; reject on failure.
- **SA-7.2.3 (Normal):** Stage new firmware to a secondary partition without interrupting the link.
- **SA-7.2.4 (Normal):** Apply at a maintenance window/operator trigger; reboot; restore link within budget.
- **SA-7.2.5 (Failure):** On failed post-update self-test, boot the previous partition; log firmware-update-failed.
- **SA-7.2.6 (Usability):** Show per-terminal version/update status/history; bulk-update scheduling.
- **SA-7.3.1 (Normal):** Stream telemetry (availability, throughput, BER, RSS, margin, temp, power, fault count) at >= 1 s.
- **SA-7.3.2 (Normal):** Timestamp telemetry at the terminal with NTP-synced UTC.
- **SA-7.3.3 (Failure):** Buffer telemetry locally if backend unreachable; replay on reconnect.
- **SA-7.4.1-7.4.4 (Normal/Failure):** Threshold alert rules; dispatch to email/webhook/SNMP; suppression windows; retry with backoff.
- **SA-7.5.1-7.5.4 (Normal/Access/Integration):** Local rolling event log (>= 30 days), readable offline with operator auth; export JSON/syslog.
- **SA-7.6.1-7.6.4 (Normal/Access/Integration):** Multi-tenant isolation; super-admin; admin-only tenant assignment; per-tenant API keys.

F-B2.3 Verification & evaluation

- **Acceptance:** telemetry delivery latency <= 5 s (99th pct) [DT-AT-08]; telemetry granularity 1 s; fleet map <= 3 s @ 1,000 terminals; OTA rollback on failed self-test [DT-AT-07].
- Conformance / interface-contract twin for the management-API boundary.

F-B2.4 Constraints

- OAuth 2.0 bearer tokens; TLS 1.2+; multi-tenant isolation; containerised / Kubernetes-deployable, no single-cloud lock-in.

B3 - Field Installation & Commissioning [migrated from REQ-8]

Scope: Processes and system-assisted functions to install, align, and commission a Rincon link pair.

Features

- **REQ-8.1** The system shall complete full terminal installation within a 4-hour budget per link with a two-person crew.
- **REQ-8.2** The system shall guide coarse alignment via a mobile/tablet app with real-time signal-strength feedback.
- **REQ-8.3** The system shall perform autonomous fine-tracking lock-on from a coarsely aligned position.
- **REQ-8.4** The system shall execute and log a commissioning self-test as a prerequisite to declaring the link operational.
- **REQ-8.5** The system shall support site-survey mode (GPS + terrain) to validate link feasibility before deployment.
- **REQ-8.6** The system shall persist site-specific calibration across power cycles and firmware updates.

F-B3.1 Interface contract

- [to author] commissioning app <-> terminal local API; self-test result record schema; site-survey input/output.

F-B3.2 Behavior

- **SA-8.1.1-8.1.3 (Usability/Normal/Integration):** Step-by-step install workflow with per-step time; timestamp phases; upload elapsed-time record.
- **SA-8.2.1-8.2.3 (Normal/Usability/Failure):** App reads alignment-assist score over Wi-Fi/Ethernet; overlay on camera/compass; connectivity troubleshooting if unreachable.
- **SA-8.3.1-8.3.3 (Normal/Failure):** Auto-engage fine-tracking at lock threshold; show 'locking'/'link locked' with RSS+margin; prompt re-check after two failures.
- **SA-8.4.1-8.4.4 (Normal/Failure):** Commissioning self-test (Tx power, RSS, pre-FEC BER, data-port link-up, mgmt reachable, NTP, seal); record pass/fail per check; not operational until all pass; present corrective action on failure.
- **SA-8.5.1-8.5.3 (Normal/Integration):** Site survey from GPS + terrain (distance, attenuation, Fresnel, predicted margin); go/no-go; store as pre-deployment record.
- **SA-8.6.1-8.6.4 (Normal/Failure):** Persist calibration with CRC; verify on boot; fall back to default bearing + recalibration prompt on corruption; survive OTA.

F-B3.3 Verification & evaluation

- **Acceptance:** installation <= 4 h (two-person crew); commissioning self-test thresholds - Tx ±1 dB, RSS >= -40 dBm, pre-FEC BER < 1e-9, data-port link-up, mgmt reachable, NTP sync, seal nominal [DT-AT-11].
- Conformance / interface-contract twin for the commissioning boundary.

F-B3.4 Constraints

- Password complexity policy; default-credential change enforced at commissioning.

B4 - Fault Detection & Self-Healing (system-level)

Scope: Cross-subsystem fault correlation, classification, escalation, switchover decisions, structured fault reporting, no-field-visit recovery.

SPLIT PENDING Former REQ-9 is cross-cutting: per-subsystem detection belongs in each epic's F.3, while B4 owns escalation/correlation. Per-subsystem detection is now authored in each epic's F.3; only the system-level escalation/correlation remains deferred - full REQ-9 reference content is in the separate Cross-Cutting Capabilities document (split pending). The <= 2 s classification-latency bound is B4's classified-output latency (not per-subsystem detection).

B5 - Security & Access Control [migrated from REQ-10]

Scope: Authentication, encryption, and access management for both management and data planes.

Features

- **REQ-10.1** The system shall require authenticated access for all management-plane operations; default credentials invalid post-commissioning.
- **REQ-10.2** The system shall encrypt all management-plane communications using TLS 1.2 or higher.
- **REQ-10.3** The system shall implement RBAC with at minimum read-only, operator, and administrator roles.
- **REQ-10.4** The system shall log all authenticated management-plane access (timestamp, identity, source IP, action).
- **REQ-10.5** The system shall support certificate-based mutual authentication between terminal and backend.
- **REQ-10.6** The optical data path shall be inherently interception-resistant; optional data-plane encryption supported if required.
- **REQ-10.7** The system shall enforce tamper-evidence and generate a tamper event on unauthorised enclosure opening.

F-B5.1 Interface contract

- [to author] auth API; RBAC role model (read-only/operator/administrator); audit-log schema (CEF); certificate provisioning.

F-B5.2 Behavior

- **SA-10.1.1 (Normal):** At commissioning self-test, verify default factory credentials have been changed; fail if not.
- **SA-10.1.2 (Normal):** Enforce password complexity (>= 12 chars, mixed case, digit, special) when setting initial credentials.
- **SA-10.1.3 (Failure):** Deny + security-event any attempt to re-enable default credentials post-commissioning.
- **SA-10.2.1 (Normal):** All management-plane connections over TLS 1.2+; TLS 1.0/1.1 disabled at the server.
- **SA-10.2.2 (Normal):** Provision TLS certs from Rincon PKI or customer CA; alert 30 days before expiry.
- **SA-10.2.3 (Failure):** Refuse + log on TLS cert error; never fall back to plaintext.
- **SA-10.3.1 (Normal):** Enforce three roles - read-only, operator, administrator.
- **SA-10.3.2 (Access):** Roles stored in backend, enforced at the API layer; terminals enforce locally for local interface.
- **SA-10.3.3 (Failure):** Operations beyond a role's permission return HTTP 403 + 'unauthorised access attempt'.
- **SA-10.4.1 (Normal):** Log every authenticated API call (timestamp, user, source IP, method, endpoint, status, payload hash).

- **SA-10.4.2 (Normal):** Audit logs separate from operational logs; read-only to operator/read-only; export admin/super-admin only.
- **SA-10.4.3 (Integration):** Export audit logs in CEF for SIEM.
- **SA-10.5.1 (Normal):** Provision a unique client cert per terminal (CN encodes serial).
- **SA-10.5.2 (Normal):** Validate terminal cert on every connection; refuse revoked/unrecognised.
- **SA-10.5.3 (Failure):** Quarantine expired/revoked terminals (reject telemetry, block config pushes, alert).
- **SA-10.6.1 (Normal):** Log beam-geometry parameters at commissioning for interception-risk assessment.
- **SA-10.6.2 (Normal):** Pass operator-enabled MACsec/IPsec frames transparently.
- **SA-10.7.1-10.7.4 (Normal/Access/Failure):** Tamper detection from enclosure seal (consumes A7 seal state); audit-logged, admin-ack to clear; authorised-access token window; tamper-sensor-fault warning.

F-B5.3 Verification & evaluation

- **Acceptance:** TLS 1.2 minimum; RBAC across all epics - no privilege escalation, unauthorised -> 403 + audit [DT-AT-12]; audit-log retention >= 90 days.
- Conformance / interface-contract twin for the security/management boundary.

F-B5.4 Constraints

- Certificate-based mutual auth; default credentials invalid post-commissioning; tamper detection consumes A7 enclosure-seal state - depends on the A7 seal scope (pending REQ-5 split; stub as binary sealed/open at 1 Hz until resolved).

---

6. Digital Twin Scope

6.0 Two Twin Layers [NEW v0.3]

The term “digital twin” here denotes two distinct layers, built by different workstreams and defined below.

Twin layer	What it is	Who builds it	Pipeline?
Interface-contract twin	Behavioral simulation of each subsystem’s HAL contract - signals, FSM, timing, error modes - parameterized against stated performance bounds. Not physics simulation.	HV M0-M7 pipeline (REQ-11.2)	Yes - generated
Physics twin	Physics-based simulation of the §6.1 modules (atmospheric channel, optical aberration, gimbal/OPA transfer functions, thermal). Produces the performance-bound parameters the interface-contract twin consumes.	Physics/Simulation Engineering (bench-calibrated)	No - separate workstream

The two layers meet only at named seams governed by the versioned parameter-ingestion contract (REQ-12.2, §6.3). The interface-contract twin can be built and the software stack developed against it immediately; the fidelity of that development firms up as physics parameters advance through their provenance tiers. Whether physics-twin fidelity reaches a level that meaningfully reduces hardware iterations is an open engineering question (OQ-12).

6.1 Components Requiring Physical Simulation (Physics-Twin Workstream)

These components have physical behaviours that cannot be derived from software logic alone and constitute the physics-twin workstream. They are not pipeline-generated; their output is validated, versioned, provenance-tagged performance parameters consumed by the interface-contract twin (§6.3).

Component	What Must Be Modelled
Atmospheric channel	Beer-Lambert attenuation vs. weather/visibility; scintillation (Rytov variance) vs. path length and turbulence; rain attenuation; time-varying random processes. Parameterised for 1550 nm per ITU-R P.1817.
Optical terminal - transmit path	Laser source power, spectral width, beam divergence angle, collimation quality, far-field intensity profile.
Optical terminal - receive path	Aperture diameter, detector sensitivity curve, receiver noise floor, AGC response curve.
Beam divergence & pointing error	Angular error vs. vibration PSD input, wind load model, thermal expansion of mount.
Mirror gimbal / OPA steering	Transfer function from control signal to beam angle; latency; angular range; step-response characteristics.
Thermal envelope	Heat dissipation for electronics and optics; temperature rise vs. ambient and solar load; throttling thresholds.

6.2 Components That Are Pure Software (Direct Implementation)

These are implemented directly as running software (pipeline-generated) and do not require physical simulation. v0.3 adds the EVT software-of-hardware components (REQ-11).

Component	Notes
Beam acquisition & tracking control algorithm	Scan pattern generator, hill-climbing tracker, Kalman filter for stabilisation.
AGC & link margin computation	Signal processing from RSS to adaptation decision.
Atmospheric fault classifier	Signal statistics analyser; rule engine.
FEC encoder/decoder	Standard codec (Reed-Solomon, LDPC); testable against BER target.
Hitless switchover controller	State machine managing optical/RF/fibre path selection.
OTA firmware update manager	Download, verify, stage, apply, rollback workflow.
Management backend (cloud)	REST API, telemetry ingestion, alerting, RBAC, multi-tenancy.
Fleet management UI	Web front-end for operator and administrator roles.
Commissioning & alignment assist app	Mobile/tablet UI for field technicians.
Site survey tool	Link budget calculator using GPS + terrain data.
SNMP / NETCONF agent	Standards-compliant NMS integration module.
Hardware abstraction layer (HAL)	API surface exposing LED/port/IMU/seal state and steering contract.
Interface-contract twin (REQ-11.2) [v0.3]	Behavioral simulation of HAL contracts; consumes physics parameters via the ingestion contract.
HIL test harnesses (REQ-11.3) [v0.3]	Interface simulators presented identically by twin and hardware rig.

Component	Notes
Characterization/calibration tooling (REQ-11.4) [v0.3]	Captures bench data; emits versioned, provenance-tagged parameter sets.
Verification suite (REQ-11.5) [v0.3]	Requirement-traceable tests; run against twin and hardware.

6.3 Interfaces Between Simulated-Physical and Implemented-Software Components

v0.3 extends the interface table with the beam-steering HAL contract and the parameter-ingestion contract, and tags each interface by seam type: **PHY** (physics seam - IC software consuming physics parameters) or **SW** (software seam - cross-subsystem software dependency).

Interface	Simulated/Source Side	Software Side	Type / Seam
Received signal strength	Atmospheric + optical receive model	AGC / link margin engine	Float (dBm), 1 kHz . PHY
Beam pointing error	Gimbal/OPA + vibration model	Tracking control algorithm	Angular error vector (rad) . PHY
Thermal state	Thermal envelope model	Power/thermal manager	Temp (°C), 10 Hz . PHY
Atmospheric condition	Atmospheric channel model	Fault classifier	Attenuation (dB/km), visibility (m) . PHY
Optical output power	Laser model	Transmit power controller	Power setpoint (dBm) . PHY
IMU orientation	Vibration/mount model	Tracking feed-forward + commissioning app	Quaternion + accel (rad, m/s²), 100 Hz . PHY
Seal sensor state	Enclosure physical model	HAL / tamper detection	Binary (sealed/open), 1 Hz . PHY
Port link state	Physical connector model	HAL / network integration	Enum (up/down/disabled), event . PHY
Steering command + capability	Gimbal/OPA steering model (params)	Tracking control via steering HAL (GS-I1)	[v0.3] set_beam_angle / get_capabilities . SW + PHY
beam_safe_state interlock	(software) steering HAL	Tx-power controller (GS-S2/I3)	[v0.3] Binary interlock . SW
Parameter-ingestion contract	Physics workstream (§6.1)	Interface-contract twin (GS-I5)	[v0.3] params + physics_parameter_set_version + fidelity tier . PHY

6.4 Physics-Twin Requirements (Beam Steering - Worked Subset) [NEW v0.4]

NEW IN v0.4 Per-seam physics-twin requirements for the beam-steering subsystem. Each physics seam (see A1 / Appendix C) is specified like a build requirement: the phenomenon to model, the parameter delivered at the seam, a fidelity criterion, a validation protocol, the required-vs-current provenance tier (REQ-12.2), criticality, and status. This worked subset covers the beam-steering

(gimbal/OPA) seams; the remaining §6.1 modules - atmospheric channel (highest risk), optical Tx/Rx, thermal - follow on the same template.

How fidelity criteria are set. A parameter's required fidelity is derived backward from the acceptance test that consumes it: it must be accurate enough that the test returns the same pass/fail verdict on the interface-contract twin as it would on hardware. Fidelity is therefore "sufficient not to flip the verdict," not an absolute number; a parameter reaches the `validated` tier when its uncertainty is below that verdict-flipping threshold. The provisional numeric tolerances below are starting points pending per-test verdict-sensitivity analysis.

Status legend: Achievable = protocol and cost known. **Feasibility-open** = a conforming model cannot be confirmed to exist until characterization data exists. Writing the requirement locates and bounds the uncertainty; it does not by itself make hard physics tractable.

Status board

PT-REQ	Parameter (seam)	Criticality	Status
PT-REQ-1	Steering transfer function / settling (GS-N5, GS-P2)	Critical path	Achievable
PT-REQ-2	Mechanical bandwidth & resonance (GS-P3, GS-U4)	Medium	Achievable; site-dependent
PT-REQ-3	Gimbal actuator degradation signature (GS-F3)	Late (fault tests)	Harder but bounded
PT-REQ-4	OPA aperture-loss far-field (GS-F4)	Late (fault tests)	Feasibility-open
PT-REQ-5	Eye-safety envelope (GS-S4 -> GS-S2)	Critical (HW bring-up)	Achievable (regulated)
PT-REQ-6	Parameter-ingestion contract (GS-I5)	Critical path	Achievable (software)

PT-REQ-1 - Steering transfer function & settling (seam GS-N5, GS-P2)

Field	Detail
Phenomenon	Command-to-achieved-angle dynamics. Gimbal: second-order mechanical response (inertia, actuator bandwidth, damping). OPA: electronic phase-pattern reconfiguration latency.
Parameter delivered	Per-axis step response yielding slew rate (mrad/s), settling time to ±0.5 mrad (ms), angular resolution (µrad).
Fidelity criterion	Accurate enough that DT-AT-10 (steady-state pointing ≤ 0.5 mrad RMS) and SA-1.2.4 (fine-track convergence ≤ 3 s) return the same verdict on twin vs. hardware. Provisional: ≤ ±15% of bench step-response settling until verdict-sensitivity analysis fixes the bound.
Validation protocol	Actuator/encoder step-response characterization (gimbal); array reconfiguration-timing measurement (OPA), with interferometer/encoder ground truth.
Required vs. current tier	bench_measured required for DT-AT-10 / DT-AT-02; datasheet_estimate acceptable for early tracking-loop development. Current: datasheet_estimate.
Criticality	Critical path - needed to develop and tune the tracking control loop at all.
Status	Achievable - standard motor/optical characterization, known cost.

PT-REQ-2 - Mechanical bandwidth & resonance (seam GS-P3, GS-U4)

Field	Detail
Phenomenon	Structural and mount resonances, mechanical bandwidth, and the vibration-PSD-to-pointing transfer (wind, traffic, HVAC).
Parameter delivered	Resonant frequencies (Hz) and Q; vibration-to-pointing transfer function; mount-resonance signatures used as IMU validity gates (GS-U4).
Fidelity criterion	Resonance peaks and transfer gain accurate enough that DT-AT-10 under injected wind/HVAC PSD returns the same verdict on twin vs. hardware.
Validation protocol	Shaker-table characterization plus ambient-vibration capture at representative mounts.
Required vs. current tier	bench_measured for DT-AT-10; literature_model acceptable for initial feed-forward (REQ-1.5) design. Current: literature_model.
Criticality	Medium - needed for vibration-compensation tests, not for first lock.
Status	Achievable, but mount-resonance signatures are site-dependent and only finalize at install (partially feasibility-open per site).

PT-REQ-3 - Gimbal actuator degradation signature (seam GS-F3)

Field	Detail
Phenomenon	Actuator stall, backlash growth, and resonance excitation under wear.
Parameter delivered	Mapping from degradation state to observables (pointing-error variance, drive-current signature) feeding the `actuator_degraded` threshold.
Fidelity criterion	Signature fidelity sufficient that DT-AT-06 (fault-classification accuracy ≥ 95%) holds on the twin for gimbal hardware-fault scenarios, and that the threshold does not false-trigger switchover.
Validation protocol	Failure-mode bench testing with induced stall/backlash.
Required vs. current tier	bench_measured for DT-AT-06; not needed for nominal-path development. Current: none.
Criticality	Late - exercised only by fault-handling tests.
Status	Harder but bounded - requires deliberate failure injection on hardware.

PT-REQ-4 - OPA aperture-loss far-field (seam GS-F4)

Field	Detail
Phenomenon	Per-element failure producing sidelobe/grating-lobe growth, gain loss, and beam-shape change in the far field.
Parameter delivered	Mapping from aperture-health level to far-field degradation feeding `aperture_degraded(level)`.
Fidelity criterion	Degradation curve accurate enough that DT-AT-06 returns the same verdict for OPA aperture-loss scenarios and the level thresholds do not mis-trigger switchover.
Validation protocol	OPA far-field characterization with elements deliberately disabled (requires OPA prototype + optical bench).
Required vs. current tier	bench_measured required; current: datasheet_estimate (array-factor theory only).
Criticality	Late - fault-handling tests.

Field	Detail
Status	Feasibility-open - array-factor structure is known in theory, but real far-field under partial aperture loss with fabrication variation cannot be confirmed until OPA silicon exists. Principal residual of former OQ-12 on the steering side.

PT-REQ-5 - Eye-safety envelope (seam GS-S4 -> interlock GS-S2)

Field	Detail
Phenomenon	Optical power density as a function of beam divergence, steering angle, and range, versus the IEC 60825-1 Class 1 boundary.
Parameter delivered	Maximum permissible Tx power as a function of beam geometry/angle, supplied as the `beam_safe_state` interlock threshold.
Fidelity criterion	One-sided (safety): the bound must never under-estimate hazard; a conservative bound is acceptable and preferred. Validated against IEC 60825-1 methodology - not a verdict-matching tolerance.
Validation protocol	Optical power-density measurement per IEC 60825-1 at an accredited test lab.
Required vs. current tier	validated (safety-critical) before any on-air hardware; a conservative worst-case bound is acceptable for twin/software development. Current: conservative worst-case.
Criticality	Critical for hardware bring-up (safety gate); non-blocking for software development.
Status	Achievable - standardized methodology - but gated by regulatory testing, which is out of pipeline scope (§7.1).

PT-REQ-6 - Parameter-ingestion contract (seam GS-I5)

Field	Detail
Phenomenon	None - this seam is pure software design.
Parameter delivered	The ingestion schema carrying parameter values plus `physics_parameter_set_version` and provenance/fidelity tier (REQ-12.2).
Fidelity criterion	Not physics; correctness = schema validation and DT-AT-14 (provenance traceability) passing.
Validation protocol	Software test (DT-AT-14); M7 enum-completeness check on the fidelity-tier enum.
Required vs. current tier	N/A (software). Current: specified.
Criticality	Critical path - the conduit through which every other parameter reaches the twin.
Status	Achievable - pure software; the one seam in this list that the pipeline itself builds.

Residual feasibility-open items

PT-REQ-4 (OPA aperture-loss far-field) is the one steering-seam parameter whose model cannot be confirmed until OPA silicon and an optical bench exist. PT-REQ-2 is achievable but its mount-resonance signatures are site-dependent and finalize at install. These - together with the not-yet-covered atmospheric channel, the system's highest fidelity risk (it underwrites DT-AT-03 availability and DT-AT-05 BER) - are the real content of the former OQ-12, now expressed as a staged engineering plan rather than a single open question.

7. Constraints and Exclusions

7.1 Scope Boundary

Scope boundary. In scope: the operational software and the EVT/software-of-hardware layer (System A epics, F.3) - HAL, interface-contract twin, HIL harnesses, characterization/verification software. Adjacent but not pipeline-delivered: the physics-twin modules (§6.1), a separate bench-calibrated workstream feeding parameters across named seams. Out of scope: anything that requires atoms.

Explicitly out of scope (pipeline delivery):

- Physical fabrication of optical terminals, lenses, mirrors, or OPA photonic chips.
- Procurement or qualification of laser sources, detectors, or optical components.
- Mechanical enclosure design, IP65 testing, or environmental qualification.
- Regulatory compliance testing (IEC 60825 eye safety, FCC/ETSI type approval, national spectrum filings).
- Civil installation works (mounting structures, power infrastructure, cabling).
- Third-party RF or fibre backup medium procurement or integration beyond the software interface contract.
- Physics-twin model construction and calibration (§6.1) - a separate workstream, not a pipeline output; it supplies parameters consumed across the seams of §6.3.

The physical hardware timeline is out of scope: lead time, fabrication cycles, and EVT/DVT phases are neither modelled nor accelerated, and the M4/M5 estimation model does not apply to hardware programs. Whether physics-twin fidelity can reach a level that reduces hardware iterations is an open question, structured parameter-by-parameter in §6.4 (OQ-12).

7.2 Technical Constraints the Implementation Must Respect

- **Open protocols preferred:** Management plane shall use SNMP v2c/v3 and/or NETCONF/YANG; proprietary NMS protocols are not acceptable for the integration layer.
- **Ethernet hand-off standard:** Data plane must present IEEE 802.3-compliant interfaces; no proprietary framing.
- **Target deployment platforms:** Cloud backend deployable on standard cloud infrastructure (containerised, Kubernetes-compatible); no single-cloud proprietary managed-service dependency in the critical path.
- **Wavelength band:** 1535-1565 nm C-band NIR is fixed; the physics-twin atmospheric model must be parameterised for this band.
- **Eye safety:** IEC 60825-1 Class 1 transmit-power and beam-geometry constraints are hard limits on the transmit-power controller and the steering beam_safe_state interlock.
- **No NLOS:** LOS-only. Mesh routing, reflective, or scatter-based non-line-of-sight modes are excluded.
- **HAL opacity:** Variant-specific hardware behavior must be expressible behind the HAL as parameters and a unified fault taxonomy; application logic must not depend on variant-raw health (each epic F.4; see Appendix D).

---

8. Open Questions and Assumptions

OQ-3 is reclassified in v0.3 from BLOCKING to Resolved (pending parameters) on the strength of the Appendix C worked decomposition. OQ-11 and OQ-12 are new; in v0.4 OQ-12 is dissolved into the §6.4 Physics-Twin Requirements annex. All others carry forward as M0-pass-with-notes items.

#	Status	Question / Ambiguity	Assumption / Resolution
OQ-1	Note	Beam acquisition angular search range (azimuth x elevation) not specified.	Assumed ±5° azimuth, ±3° elevation. Needs confirmation.
OQ-2	Note	Backup medium interface contract (connector, signalling, switchover API) not defined.	Assumed standard Ethernet port with LACP or carrier-detect failover.
OQ-3	Resolved (pending parameters)	OPA vs. mirror control software: one beam-steering control agent or two.	[v0.3] ONE control agent behind a parameterized HAL with a unified fault taxonomy + per-variant capability/parameter descriptor (subsystem A1; worked in Appendix C). Condition: HAL opacity (F-A1.4), enforced by DT-AT-13. Remaining dependency tracked as OQ-11.
OQ-4	Note	Atmospheric model fidelity (fog onset, duration, seasonal variation) must be agreed.	ITU-R P.1817 and Kruse visibility model assumed as baseline.
OQ-5	Note	Multi-hop / relay topology unspecified.	Single-hop point-to-point assumed; multi-hop excluded.
OQ-6	Note	Management backend deployment model (operator-hosted, Rincon SaaS, or both).	Operator-hosted containerised deployment assumed as primary.
OQ-7	Note	Commissioning self-test pass/fail thresholds require stakeholder sign-off.	Thresholds in B3 / F-B3.3 and Appendix B; flagged for sign-off.
OQ-8	Note	Tamper-detection hardware mechanism (reed switch, microswitch, accelerometer, seal) unspecified.	Assumed microswitch with secure-element attestation log. Hardware team to confirm.
OQ-9	Note	End-to-end latency SLA for enterprise customers not bounded (physical layer ≤ 1 ms is set).	Physical layer ≤ 1 ms assumed sufficient; end-to-end SLA deferred to operator.
OQ-10	Note	Data sovereignty and telemetry retention policy unspecified.	90-day rolling telemetry retention assumed; jurisdiction flagged for legal review.
OQ-11	Note	Per-variant parameter & fault sets for gimbal vs. OPA (the descriptor populated behind the HAL).	[v0.3] Physics workstream to deliver, advancing through provenance tiers (REQ-12.2). Not blocking single-agent resolution; required for full twin fidelity.
OQ-12	Structured (§6.4)	Physics-twin fidelity sufficiency: can it reach a level that meaningfully reduces hardware iterations?	[v0.4] Dissolved into per-seam Physics-Twin Requirements (§6.4), beam-steering subset, each with a backward-derived fidelity criterion, validation protocol, and required-vs-current tier. Residual feasibility-open (steering): OPA aperture-loss far-field (PT-REQ-4), pending OPA prototype. Highest remaining system risk - atmospheric channel - to be specified next on the same template.

Appendix A - Acceptance Traceability Index

System-level acceptance targets (formerly §5.1) mapped to the epic that owns them and the feature where the test is written. This index is for human verification that every system-level target has a home; the test definitions themselves live inline in each F-X.3.

Target	Owning epic	Feature
Max data rate >= 20 Gbps (LB) / 25 Gbps (Beam)	A4 Link / Modem	F-A4.3
Max link range 20 km (LB) / 10 km (Beam)	A3 Optical Receive	F-A3.3
Link availability >= 99.9% (LT-1)	A5 Link Adaptation	F-A5.3
Link availability >= 99.999% (LT-1P)	A5 Link Adaptation	F-A5.3
Beam acquisition (cold start) <= 20 s	A1 Beam Steering	F-A1.3
Fine-track convergence <= 3 s	A1 Beam Steering	F-A1.3
Link re-acquisition (warm) <= 5 s	A1 Beam Steering	F-A1.3
Hitless switchover latency <= 50 ms	A5 Link Adaptation	F-A5.3
Optical-to-backup restoration <= 100 ms	A5 Link Adaptation	F-A5.3
Post-FEC BER <= 1e-12	A4 Link / Modem	F-A4.3
FEC overrun frame loss < 0.001%	A4 Link / Modem	F-A4.3
One-way physical-layer latency <= 1 ms	A4 Link / Modem	F-A4.3
Frame-forwarding latency <= 500 us	A4 Link / Modem	F-A4.3
Carrier-detect de-assertion <= 100 ms	A4 Link / Modem	F-A4.3
Typical power <= 40 W	A6 Power	F-A6.3
Peak power <= 60 W	A6 Power	F-A6.3
Operating temp -20..+55 C (+65 C solar)	A7 Thermal	F-A7.3
Fog tolerance to 30 dB/km	A5 Link Adaptation	F-A5.3
Pointing accuracy <= 0.5 mrad RMS	A1 Beam Steering	F-A1.3
Link-margin estimate latency <= 10 ms	A3 Optical Receive	F-A3.3
Telemetry delivery latency <= 5 s	B2 Fleet Backend	F-B2.3
Telemetry granularity 1 s	B2 Fleet Backend	F-B2.3
Fault classification latency <= 2 s	B4 Fault (system-level)	F-B4.3
TLS 1.2 minimum	B5 Security	F-B5.3
Audit-log retention >= 90 days	B5 Security	F-B5.3
Installation time <= 4 h (two-person)	B3 Field Install	F-B3.3
Commissioning self-test thresholds	B3 Field Install	F-B3.3

Note: per-subsystem fault *detection* latency is owned in each epic's F.3; the <= 2 s bound above is B4's classified-output latency only, to avoid double-counting.

Appendix B - Performance Targets & Acceptance Criteria (Reference)

These targets are binding acceptance criteria for both hardware qualification and the Digital Twin test suite. Digital Twin test cases (§5.2) are cross-referenced against performance targets (§5.1).

5.1 Performance Targets

Parameter	Target	Notes
Maximum data rate	≥ 20 Gbps FDX (LT-1); ≥ 25 Gbps (Beam)	IEEE 802.3 framing, at Ethernet hand-off
Maximum link range	20 km (LT-1); 10 km (Beam)	Clear-air, flat terrain, LOS
Link availability (LT-1)	≥ 99.9% annual	Excludes scheduled maintenance
Link availability (LT-1P)	≥ 99.999% annual	Including hitless backup switchover credit
Beam acquisition time (cold start)	≤ 20 s	Clear-air, correct coarse alignment pre-set
Fine-tracking convergence	≤ 3 s from first signal detection	Clear-air
Link re-acquisition (warm restart)	≤ 5 s	After transient obstruction or brief power cycle
Hitless switchover latency	≤ 50 ms packet loss window	Optical-to-backup transition
Optical-to-backup restoration	≤ 100 ms	Backup-to-optical restoration
Bit error rate (post-FEC)	≤ 10^{-12}	At minimum link margin (30 dB/km, 1 km)
FEC overrun frame loss	< 0.001% of frames	Under clear-air conditions
Latency (one-way, physical layer)	≤ 1 ms	Optical propagation + processing, excl. IP routing
Frame forwarding latency	≤ 500 µs	Data port input to optical modulator
Carrier detect de-assertion on loss	≤ 100 ms	After optical link drop
Typical power consumption	≤ 40 W per terminal	Both mirror and OPA variants
Peak power consumption	≤ 60 W per terminal	Worst-case thermal and beam-steering load
Operating temperature	−20°C to +55°C; +65°C w/ solar	Per IP65 enclosure
Fog tolerance	Operational to ≤ 30 dB/km attenuation	Beyond this, switchover engaged
Beam wavelength	1535-1565 nm (C-band NIR)	Eye-safe, unlicensed
Pointing accuracy (steady-state)	≤ 0.5 mrad RMS	Under normal vibration conditions
Link margin estimate latency	≤ 10 ms	From optical signal change to computed value

Parameter	Target	Notes
Telemetry delivery latency	≤ 5 s	Terminal measurement to backend ingestion
Telemetry granularity	1 s minimum reporting interval	RSS, BER, throughput, temperature
Fault classification latency	≤ 2 s	From triggering event to classified record
Subsystem restart on fault	≤ 3 attempts before escalation	Software fault recovery
TLS version	TLS 1.2 minimum	Management plane encryption
Audit log retention	≥ 90 days	Management access events
Installation time (two-person crew)	≤ 4 hours per link	Includes commissioning self-test
HAL abstraction opacity (binding)	No application-layer reference to variant-raw hardware health	[v0.3] Enforced by DT-AT-13; REQ-12.1 / OQ-3
Physics parameter provenance	Each set tagged: datasheet_estimate / literature_model / bench_measured / validated	[v0.3] REQ-12.2; recorded in test evidence

5.2 Digital Twin Acceptance Tests

Each test is linked to the performance target it validates. DT-AT-13 through DT-AT-16 are new in v0.3 and validate the hardware-adjacent track.

Test ID	Description	Pass Criterion	Target Ref
DT-AT-01	Cold-start acquisition across 1,000 randomised atmospheric realisations (clear-air & 10 dB/km fog)	All runs lock within 20 s	§5.1 acquisition
DT-AT-02	Warm-restart re-acquisition across 500 transient obstruction events	All within 5 s	§5.1 re-acquisition
DT-AT-03	30-day availability run with ITU-R P.1817 fog/rain injection	Availability ≥ 99.9%	§5.1 availability
DT-AT-04	Hitless switchover across 100 consecutive fog-onset events	All within 50 ms loss window	§5.1 switchover
DT-AT-05	BER at minimum link margin (30 dB/km, 1 km)	Post-FEC BER ≤ 10^{-12}	§5.1 BER
DT-AT-06	Fault classification vs. labelled fault set (50 atmospheric, 50 hardware)	Accuracy ≥ 95%	§5.1 fault class.
DT-AT-07	OTA firmware update cycle (download, verify, stage, apply, reboot, re-acquire)	Link re-established within budget; rollback on injected signature failure	§5.1 re-acquisition
DT-AT-08	Telemetry delivery latency across 10,000 events under normal load	99th pct ≤ 5 s	§5.1 telemetry
DT-AT-09	Power budget across all states (cold start, steady, throttle, shutdown)	Never > 60 W; steady ≤ 40 W	§5.1 power
DT-AT-10	Steady-state pointing under injected vibration PSD (wind/HVAC)	RMS pointing ≤ 0.5 mrad	§5.1 pointing

Test ID	Description	Pass Criterion	Target Ref
DT-AT-11	Commissioning self-test logic vs. injected hardware faults	Each fault produces correct fail state + corrective message	§5.1 commissioning
DT-AT-12	RBAC across all features (REQ-1-REQ-12) with read-only/operator/admin	No role exceeds privilege; all unauthorised return 403 + audit event	§5.1 TLS/RBAC
DT-AT-13	HAL opacity - static + runtime check that the application layer never references variant-raw health (aperture/actuator)	No raw-health reference above HAL; build fails otherwise (M7 architecture enforcement)	REQ-12.1 / OQ-3
DT-AT-14	Parameter-set version & provenance traceability across twin-based runs	Every run records physics_parameter_set_version + fidelity tier; reproducible against the exact set	REQ-12.2
DT-AT-15	Interface-contract twin conformance - full stack runs against twin pre-hardware, same suite re-runs against hardware	Suite passes on twin; on hardware, divergences flagged as calibration findings (not silent re-baseline)	REQ-11.2 / 11.5
DT-AT-16	Cross-subsystem seam integration - eye-safety interlock (steering-Tx-power) + commissioning seams end-to-end	Each software seam exercised end-to-end; a seam satisfiable only in isolation fails the gate	REQ-12.3

Appendix C - Beam Steering Worked Decomposition & OQ-3 Resolution

NEW IN v0.6 This worked example applies the M3 six-category decomposition to a single subsystem - beam steering - chosen because it spans a software-control layer and an electromechanical/optical physics layer, and because it is the subsystem behind OQ-3 (OPA vs. mirror control software). It is both a proof of the interface-contract/physics scope boundary and the analysis that resolves OQ-3.

Legend and traceability

Each activity is tagged by the workstream that owns it, so the scope line is visible in the artifact itself:

- **[IC]** Interface-Contract layer - pipeline-generated (HAL, FSM, behavioral sim, HIL harness, tests).
- **[PHY]** Physics layer - physics-twin workstream, out of pipeline; produces parameters the IC layer consumes.
- **[SEAM]** an [IC] activity that consumes a [PHY]-supplied parameter - a named handoff point between the two workstreams.

This `[IC]/[PHY]/[SEAM]` tagging is defined in the legend above and applies to any subsystem decomposition.

Traceability anchors: maps to REQ-1 (Beam Acquisition & Tracking), REQ-5.3/5.6 (orientation + alignment assist), REQ-11 (EVT software), REQ-12 (co-design), §6.1 (gimbal/OPA + vibration

physical-sim modules) and §6.3 (interface table). Consuming roles (M2): Tracking-Control (sw), Commissioning/Field-Tech, Systems-Integration, Test/Validation.

Category remap (M3 six categories, applied to hardware)

M3 software category	Hardware-adjacent analog
Positive / nominal flow	Nominal steering operation
Negative / error flow	Failure modes & degradation (FMEA)
Permission check	Safety interlock & command authority
Usability pattern	Serviceability / commissioning / observability
Performance consideration	Performance margin & timing bounds
Integration touchpoint	Interface points (HAL + cross-subsystem)

Category 1 - Nominal steering operation

- **GS-N1 [IC]:** Accept a commanded pointing setpoint (az, el) via the steering HAL; acknowledge with sequence + timestamp.
- **GS-N2 [IC]:** Report estimated beam angle + actuator/element state at the loop feedback rate (≥ 1 kHz).
- **GS-N3 [IC]:** Execute operating-mode FSM transitions (idle, scan, acquire, fine-track, hold), emitting a mode-change event on each transition.
- **GS-N4 [PHY]:** Convert commanded angle to physical deflection - gimbal: mirror actuator through the mechanical transfer function; OPA: phase-pattern synthesis across the emitter array to form the far-field beam.
- **GS-N5 [SEAM]:** Simulate command-to-achieved-angle in the interface-contract twin using slew-rate / settling-time / resolution parameters supplied by the physics workstream.

Category 2 - Failure modes & degradation (FMEA)

- **GS-F1 [IC]:** Reject out-of-range / malformed command; hold last valid setpoint.
- **GS-F2 [IC]:** Detect feedback fault (stale / implausible / missing state telemetry); FSM to fault/safe.
- **GS-F3 [SEAM]:** Gimbal-specific - actuator stall / backlash / resonance excitation. Physics characterizes the signature; IC exposes `actuator_degraded` + detection threshold.
- **GS-F4 [SEAM]:** OPA-specific - emitter-element failure, sidelobe/grating-lobe growth, gradual aperture loss. Physics characterizes far-field impact; IC exposes `aperture_degraded(level)`.
- **GS-F5 [IC]:** Emit a unified fault taxonomy {command_invalid, feedback_lost, range_exceeded, actuator_degraded, aperture_degraded, over_temp} to the tracking agent. <-- OQ-3 hinge.

Category 3 - Safety interlock & command authority

- **GS-S1 [IC]:** Enforce angular soft-limits in the HAL; clamp/reject and log out-of-envelope commands.
- **GS-S2 [IC]:** Expose `beam_safe_state` interlock so the Tx-power controller cannot drive a power/geometry combination outside IEC 60825-1 Class 1 (cross-subsystem; links REQ-2.4.2, REQ-4.6).
- **GS-S3 [IC]:** Command authority - only the tracking agent / authorized commissioning role may issue setpoints; manual override needs operator-role auth + audit log (REQ-10.3).
- **GS-S4 [PHY]:** The physical eye-safety envelope (power density x divergence x angle) is a physics output; IC consumes it as the interlock threshold.

Category 4 - Serviceability / commissioning / observability

- **GS-U1 [IC]:** Expose az/el/tilt from IMU at 10 Hz via commissioning API (= SA-5.3.1).
- **GS-U2 [IC]:** Alignment-assist hook - stream pointing-quality score from steering feedback + RSS (= REQ-5.6).
- **GS-U3 [IC]:** Report steering self-test (range sweep + feedback continuity) in commissioning self-test (= REQ-8.4).
- **GS-U4 [SEAM]:** IMU plausibility bounds (±16 g, ±2000 °/s, SA-5.3.3) + mount-resonance signatures come from physics; IC uses them as validity gates.

Category 5 - Performance margin & timing bounds

- **GS-P1 [IC]:** Assert command-to-ack latency bound at the HAL.
- **GS-P2 [SEAM]:** Assert step-response settling within fine-track convergence budget (≤ 3 s, SA-1.2.4) and steady-state pointing ≤ 0.5 mrad RMS (SA-1.3.4) - bounds from physics, asserted by the IC test suite.
- **GS-P3 [PHY]:** Slew rate, mechanical bandwidth, OPA reconfiguration time, resonant frequencies, thermal-drift rate.
- **GS-P4 [IC]:** Verify the control loop sustains ≥ 1 kHz correction rate against the twin (SA-1.3.1).

Category 6 - Interface points (auto-injected; spans ≥ 3 layers)

- **GS-I1 [IC]:** Steering HAL contract - `set_beam_angle(az,el)` / `set_steering_vector(...)`, `get_beam_state()`, `get_capabilities()`, `subscribe_faults()`. <-- central artifact.
- **GS-I2 [IC]:** Tracking-control to steering - angular-error feedback loop (matches §6.3 “beam pointing error” row).
- **GS-I3 [IC]:** Steering to Tx-power controller - `beam_safe_state` interlock (software seam).
- **GS-I4 [IC]:** Steering to commissioning app - orientation + alignment-assist (software seam).
- **GS-I5 [SEAM]:** Steering to physics twin - the parameter-ingestion contract (carries version + fidelity tier per REQ-12.2).

Interface Contract - Beam Steering HAL (buildable specification) [NEW v0.5]

The decomposition above yields the contract below: the actual HAL surface a coding swarm builds against - method signatures, data types, the operating-mode state machine, the fault enum, performance bounds, and the physics seams consumed. This is the buildable unit; every other subsystem follows the same contract template.

HAL methods

Method (signature)	Description
`set_mode(mode: Mode, seq: u32) -> Ack`	Request an operating-mode transition (see FSM below).
`set_beam_angle(az_mrad: f32, el_mrad: f32, seq: u32) -> Ack`	Command an absolute pointing setpoint; rejected with RANGE_EXCEEDED if outside the configured envelope.
`get_beam_state() -> BeamState`	Current angle estimate, mode, abstracted actuator/element state, RSS, timestamp; pollable at the control-loop rate (>= 1 kHz).
`get_capabilities() -> Capabilities`	Per-variant descriptor (range, resolution, slew, settle, supported fault codes). The only place variant differences surface.
`subscribe_faults(cb: fn(FaultEvent)) -> SubId`	Register for asynchronous fault events drawn from the unified taxonomy.

Data types

Type	Definition	Units / range / note
BeamAngle	`{ az_mrad: f32, el_mrad: f32 }`	az: +/-5 deg (+/-87.3 mrad); el: +/-3 deg (+/-52.4 mrad), per OQ-1; resolution <= 0.05 mrad
Mode	`enum { IDLE, SCAN, ACQUIRE, FINE_TRACK, HOLD, FAULT, SAFE }`	operating-mode FSM states
ActuatorState	`enum { NOMINAL, DEGRADED, FAULT }`	abstracted; never raw per-element health (REQ-12.1)
BeamState	`{ angle: BeamAngle, mode: Mode, actuator_state: ActuatorState, rss_dbm: f32, ts_utc: i64, seq_ack: u32 }`	returned by get_beam_state()
Capabilities	`{ variant: {GIMBAL|OPA}, az_range_mrad, el_range_mrad, resolution_mrad, max_slew_mrad_s, settle_ms, supported_faults: FaultCode[] }`	populated from physics parameters (REQ-12.2)
FaultCode	`enum { COMMAND_INVALID, FEEDBACK_LOST, RANGE_EXCEEDED, ACTUATOR_DEGRADED, APERTURE_DEGRADED, OVER_TEMP }`	unified taxonomy (GS-F5); the only health surface
Ack	`{ seq: u32, accepted: bool, reject: FaultCode? }`	acknowledgement for every commanded call

Operating-mode FSM (transition table)

From	Event	To	Guard / note
IDLE	activate	SCAN	after calibration state loaded (SA-1.1.1)
SCAN	signal_detected	ACQUIRE	RSS > acquisition threshold (SA-1.1.3)
SCAN	scan_timeout	FAULT	emits FEEDBACK_LOST / peer-not-found (SA-1.1.4)
ACQUIRE	converged	FINE_TRACK	pointing error < 0.5 mrad (SA-1.2.1)
ACQUIRE	converge_timeout	SCAN	> 5 s without lock (SA-1.2.3)
FINE_TRACK	link_loss	SCAN	RSS below floor > 100 ms; warm restart (SA-1.4.1)
FINE_TRACK	hold_requested	HOLD	operator / maintenance
HOLD	resume	FINE_TRACK	-
(any)	unrecoverable_fault	FAULT	hardware fault; may trigger switchover (REQ-9.4)
(any)	safe_requested	SAFE	eye-safety interlock (GS-S2)
FAULT / SAFE	reset	IDLE	operator-cleared

Performance bounds (contract acceptance)

Bound	Value	Reference
Scan-to-lock (cold start)	<= 20 s	§5.1 / SA-1.1.5
Fine-track convergence	<= 3 s	§5.1 / SA-1.2.4

Bound	Value	Reference
Warm re-acquisition	<= 5 s	§5.1 / SA-1.4.4
Steady-state pointing	<= 0.5 mrad RMS	§5.1 / SA-1.3.4
Control-loop correction rate	>= 1 kHz	SA-1.3.1
Command-to-ack latency	bound from physics (PT-REQ-1)	GS-P1 / §6.4

Physics seams consumed (via the parameter-ingestion contract, REQ-12.2)

Parameter	Type	Source
Slew rate / settling / resolution	f32 each	PT-REQ-1 (§6.4)
Resonance / mechanical bandwidth	f32[]	PT-REQ-2
Actuator degradation curve (gimbal)	curve	PT-REQ-3
Aperture-loss far-field map (OPA)	curve	PT-REQ-4
Eye-safety envelope	fn(geometry)	PT-REQ-5

Conformance to REQ-12. The application layer consumes only `BeamState` and `FaultCode` - never raw per-element or per-actuator health (HAL opacity, REQ-12.1, enforced by DT-AT-13). All variant difference lives in `Capabilities` and the physics parameters (REQ-12.2). The steering-to-Tx-power and steering-to-commissioning seams are integration-tested end-to-end (REQ-12.3). From the tables above a swarm builds the HAL stub, the interface-contract twin, the HIL harness, and the verification suite directly.

The scope line

Everything `[IC]` is what the pipeline builds from an ICD + Behavioral Spec: one HAL, one FSM, the behavioral twin, the HIL harness, the verification suite. Everything `[PHY]` (GS-N4, the F3/F4 signatures, S4, P3, U4 bounds) is the bench-calibrated physics workstream - it never rides the pipeline; it only feeds parameters across the five `[SEAM]` points. The seams are few and named - that small, explicit integration surface is the argument.

Resolution of OQ-3

Walking the nominal path and the FSM (GS-N1-N3, GS-I1-I2), setting an angle, reading back state, and transitioning modes are variant-agnostic - nothing in the control logic differs between a two-mirror gimbal and a 1,000-emitter OPA. Every real divergence lands in exactly two places: the failure-mode set (GS-F3 vs. F4) and the performance/degradation parameters (GS-P3, F3/F4 curves) - both expressible as a unioned fault taxonomy (GS-F5) plus a capability/parameter descriptor (GS-I1 `get_capabilities()`) behind one contract.

Answer: one beam-steering control agent, not two, behind a parameterized HAL carrying (i) the unified fault taxonomy and (ii) a per-variant capability/parameter descriptor populated by the physics workstream.

Condition (falsifiable, enforced): the HAL abstraction must remain opaque (REQ-12.1) - the tracking agent consumes only the unified taxonomy and abstracted state, never variant-raw health (`aperture_degraded(level)` and `actuator_degraded` are the only health signals it sees, symmetrically across variants). This is enforced at build time by DT-AT-13. If any nominal or FSM activity had required variant-specific control logic rather than just parameters, the single-agent hypothesis would break - the decomposition shows it does not.

This converts OQ-3 from BLOCKING to resolved-pending-parameters: the remaining dependency is the physics workstream supplying the per-variant parameter and fault sets (tracked as OQ-11).

Appendix D - Verification & Evaluation Criteria (applied per epic)

The generic verification & evaluation criteria (former REQ-11) and architecture constraints (former REQ-12), retained as the reference checklist each epic instantiates in its F.3 and F.4.

REQ-11 | Epic: Engineering Validation & Test (EVT) Software [NEW v0.3]

Scope: The per-subsystem verification & evaluation artifacts: HAL conformance checks, the interface-contract twin (also the pre-hardware development substrate), HIL test harnesses, characterization/calibration tooling, the requirement-traceable verification suite, and manufacturing/commissioning test sequences.

Cross-cutting verification & evaluation criteria. REQ-11 and REQ-12 are not themselves build targets; they are the criteria applied to every hardware subsystem to ensure the right test and evaluation artifacts get written against that subsystem's detailed interface contract. The buildable component specification is the interface contract itself (HAL API, FSM, fault taxonomy, seams, bounds) - beam steering in full in Appendix A, the others (optical Tx/Rx, thermal, IMU/orientation, enclosure/seal, ports) on the same template. REQ-11 mandates the verification artifacts and the substrate they run on; REQ-12 the architecture properties they must enforce. Applied to a contract, these criteria yield that subsystem's acceptance tests (cf. §5.2).

- **REQ-11.1** For each hardware subsystem, the build shall provide a HAL conformance check that verifies the implemented HAL against the subsystem's interface contract (signatures, operating-mode FSM, fault taxonomy). The HAL contract itself is defined in that interface contract (Appendix A and equivalents), not here.
- **REQ-11.2** The system shall provide an interface-contract digital twin for each hardware subsystem: a behavioral simulation reproducing the subsystem's contract (signals, state machine, timing, error modes), parameterized against performance bounds supplied by the physics workstream (§6). This interface-contract twin is explicitly distinct from the physics-simulation modules of §6.1.
- **REQ-11.3** The system shall provide hardware-in-the-loop (HIL) test harnesses - interface simulators for each hardware boundary - enabling the complete software stack to execute and be verified before physical hardware exists.
- **REQ-11.4** The system shall provide characterization and calibration-capture tooling that records bench-measured hardware behavior and emits parameter sets (carrying version and provenance/fidelity tier per REQ-12.2) consumable by the interface-contract twin.
- **REQ-11.5** The system shall provide a verification suite generated from the activity decomposition (§4) and traceable to requirements, runnable against both the interface-contract twin and physical hardware, asserting that software conforms to the interface contract.
- **REQ-11.6** The system shall provide manufacturing and field commissioning test sequences (self-test, range sweep, interface continuity) that reuse verification-suite assertions where applicable to support production and bring-up.

REQ-12 | Epic: Interface & Architecture Constraints [NEW v0.3]

Scope: The interface and architecture constraints the build must satisfy: HAL opacity, the versioned parameter-ingestion contract, and end-to-end integration of cross-subsystem seams.

Cross-cutting. These are the testable architecture properties the verification must enforce on every subsystem interface contract (Appendix A and the rest); each maps to an acceptance test in §5.2.

- **REQ-12.1** Each hardware-software abstraction (HAL) shall remain opaque: application-layer logic shall consume only the abstracted state and the unified fault taxonomy, never variant-raw hardware health signals. This opacity is enforced as a build-time architecture check (DT-AT-13) and is the condition under which a single control agent serves multiple hardware variants (see OQ-3).
- **REQ-12.2** The parameter-ingestion contract between the physics workstream and the interface-contract twin shall carry a `physics_parameter_set_version` and a provenance/fidelity tier (`datasheet_estimate → literature_model → bench_measured → validated`); test-run evidence records shall record both so results are reproducible against a known fidelity level.
- **REQ-12.3** Cross-subsystem software seams shall be implemented and integration-tested end-to-end - not stubbed within a single subsystem - so the integration gate exercises each seam rather than allowing it to be siloed.

REQ-11 | Engineering Validation & Test (EVT) Software [NEW v0.3]

REQ-11.1 - HAL Conformance Check

- **SA-11.1.1 (Normal):** The conformance check verifies the implemented HAL against the subsystem's interface contract (commands, state, events, FSM); an implementation that diverges from the contract fails the check.
- **SA-11.1.2 (Integration):** HAL contracts are published as machine-readable schemas (e.g. OpenAPI/IDL) consumed by both the interface-contract twin and the verification suite.
- **SA-11.1.3 (Access):** HAL contract changes are versioned and gated; a breaking change increments the major contract version and triggers a re-verification run.

REQ-11.2 - Interface-Contract Twin

- **SA-11.2.1 (Normal):** For each hardware subsystem, the twin reproduces the HAL contract behaviorally - state machine transitions, timing, and error modes - driven by physics-workstream parameters ingested per REQ-12.2.
- **SA-11.2.2 (Normal):** The twin records the `physics_parameter_set_version` and fidelity tier in use and stamps it onto any test run executed against it.
- **SA-11.2.3 (Failure):** If a required parameter is missing or its fidelity tier is below a configured floor for a given test, the twin refuses the run and emits an "insufficient parameter fidelity" event rather than producing a misleading pass.

REQ-11.3 - HIL Test Harnesses

- **SA-11.3.1 (Normal):** Each hardware boundary has an interface simulator that the full software stack binds to in place of physical hardware, enabling end-to-end execution pre-hardware.
- **SA-11.3.2 (Normal):** The harness can inject fault and degradation scenarios at the interface (e.g. feedback loss, range exceedance) to exercise negative paths.
- **SA-11.3.3 (Integration):** The same harness interface is presented by the physical hardware test rig, so a test binds to twin or hardware without modification.

REQ-11.4 - Characterization & Calibration Tooling

- **SA-11.4.1 (Normal):** The tooling captures bench-measured behavior (e.g. step response, range, degradation curves) and emits a parameter set tagged with version and provenance/fidelity tier.

- **SA-11.4.2 (Normal):** Successive captures advance a parameter's fidelity tier (datasheet_estimate, literature_model, bench_measured, validated) with an audit trail of when and how each was produced.
- **SA-11.4.3 (Integration):** Emitted parameter sets are published to the parameter-ingestion contract (REQ-12.2) and become available to the interface-contract twin.

REQ-11.5 - Verification Suite

- **SA-11.5.1 (Normal):** Test cases are generated from the §4 activity decomposition and carry a traceability reference to the originating requirement/activity.
- **SA-11.5.2 (Normal):** The suite runs identically against the interface-contract twin and physical hardware; a per-run report records pass/fail, measured value, and the parameter-set version/fidelity in effect.
- **SA-11.5.3 (Failure):** A test that passes against the twin but fails against hardware is flagged as a contract/reality divergence (calibration finding) and routed to the physics workstream, not silently re-baselined.

REQ-11.6 - Manufacturing & Commissioning Test Sequences

- **SA-11.6.1 (Normal):** Production and field bring-up sequences (self-test, range sweep, interface continuity) reuse verification-suite assertions where applicable to avoid divergence between lab and field criteria.
- **SA-11.6.2 (Integration):** Sequence results are recorded against the unit's build/commissioning record (links REQ-8.4).

REQ-12 | Interface & Architecture Constraints [NEW v0.3]

REQ-12.1 - HAL Opacity Invariant

- **SA-12.1.1 (Access):** Application-layer logic consumes only abstracted state and the unified fault taxonomy; variant-raw health signals (e.g. per-element aperture health, raw actuator backlash) are not exposed above the HAL.
- **SA-12.1.2 (Normal):** The invariant is symmetric across variants - it applies equally to OPA aperture-health and gimbal actuator-health signals.
- **SA-12.1.3 (Failure):** A build whose application layer references variant-raw health fails the architecture-enforcement check (DT-AT-13) and is not packaged.

REQ-12.2 - Versioned Parameter-Ingestion Contract

- **SA-12.2.1 (Normal):** Every parameter set carries `physics_parameter_set_version` and a provenance/fidelity tier; the twin and verification suite stamp both onto each run's evidence record.
- **SA-12.2.2 (Integration):** The fidelity-tier enum is closed and validated wherever a parameter set is consumed, so an unrecognised tier is rejected.

REQ-12.3 - Cross-Subsystem Seam Integration

- **SA-12.3.1 (Integration):** Cross-subsystem seams (e.g. steering-to-Tx-power eye-safety interlock; steering-to-commissioning app) are implemented and exercised as real cross-subsystem integrations, not stubbed within one subsystem.
- **SA-12.3.2 (Failure):** Integration-gate verification exercises each software seam end-to-end; a seam that is satisfiable only within a single subsystem in isolation fails the gate.

End of Document - Version 0.6-2 - System/Subsystem Reorganization (Lossless, M0-Ready)