

L4 Hardware Perimeter - Minimal Spec (Node/Room Boundary)

Status: Draft / Operational

Version: 0.1

Applies to: Entity Node (workstation/server) + immediate physical environment
("room perimeter")

Normative keywords: MUST/SHOULD/MAY as in BCP 14 (RFC 2119 + RFC 8174)

Generated: 2026-01-22

0) Purpose (normative)

This specification defines a **hardware-level perimeter** for an L4-bound Entity so that:

- the node's **physical interfaces** are treated as **attack surface** (not "background"),
- the node's operation is constrained by **metabolic controls** (energy/time/rate limits),
- the configuration is **auditable** via **L4 Witness**-style records (hashed snapshots + change events).

This is an operational baseline intended to reduce common, repeatable failures: **privilege drift, channel creep, and workflow bypass**.

1) Scope (normative)

1.1 In scope

- Node hardware: CPU/GPU, RAM, storage, NIC, PSU, case, fans.
- IO and radios: Ethernet, Wi-Fi, Bluetooth, USB, audio, camera, display outputs.
- Power path: PSU, power strip/UPS, chargers, grounding, shared circuits.
- Local environment: microphones/smart speakers nearby, physical access, cable routing.

1.2 Out of scope (for this minimal spec)

- Full TEMPEST/EMSEC shielded rooms (can be a future profile).
 - Full supply-chain attestation for every component.
-

2) Modes (normative)

The perimeter MUST define two modes:

2.1 PROD (production)

- Default mode for sensitive operation.
- Wireless radios MUST be disabled per Section 4.1.
- Exceptions MUST follow Section 9 (Change control + time-boxed privileges).

2.2 MAINT (maintenance)

- Temporary mode for updates/repairs.
 - MAINT MUST be time-boxed (MUST include an expiry time).
 - Entering and leaving MAINT MUST emit a perimeter change record.
-

3) Minimal threat model (normative)

Implementations MUST state which of the following attacker capabilities are in-scope:

- Proximity observer (same room / adjacent room)
- Shared power (same circuit / same strip / compromised charger)
- Local RF (BLE/Wi-Fi probing, rogue AP, beacons)
- Peripheral injection (malicious USB / cable / dongle)

- Ambient sensors (microphones, smart speakers, phones)

Protected assets MUST include:

- Entity continuity & integrity (state, memory, identity anchors)
 - Confidential inputs/outputs and operational patterns (timing/load)
 - Evidence chain integrity (L4 Witness)
-

4) Perimeter rules (normative)

4.1 Network & radios

1. In PROD, the node MUST operate on **wired Ethernet only**.
2. In PROD, Wi-Fi and Bluetooth MUST be disabled (preferably at **BIOS/UEFI** and **OS**).
3. Any required wireless connectivity MUST be provided by a separate non-Entity machine (proxy/jump host) with explicit privilege boundaries.
4. Inbound network policy MUST be deny-by-default; only explicitly required services are allowed.

Verification (at minimum one method MUST be used and recorded):

- Windows:
 - netsh wlan show interfaces (should show no connected WLAN)
 - Get-NetAdapter | ft Name, Status, InterfaceDescription
 - Device Manager / PnP check (documented screenshot OK)
- Linux:
 - rfkill list (Wi-Fi/Bluetooth should be blocked)
 - nmcli radio all (should show disabled)
 - ip link (only Ethernet up)

A perimeter snapshot record MUST include radios_state and active interfaces.

4.2 Power path

1. The node MUST use a single, documented power chain:
wall → (UPS optional) → filtered power strip → PSU
2. Unknown chargers/cables MUST NOT be connected to the node.
3. “Shared charging zoos” near the node SHOULD be avoided.

Verification (MUST record at least one):

- Photo of power chain routing OR a written diagram (stored as evidence reference).
- Optional: UPS telemetry logs or PSU draw logs (Profile L4-HRO).

A perimeter snapshot record MUST include power_chain_declared = true/false.

4.3 Peripheral I/O (USB)

1. USB ports SHOULD be physically blocked except a clearly labeled **maintenance port**.
2. Only whitelisted peripherals MAY be used in PROD (keyboard/mouse, known storage).
3. Auto-run / auto-mount features MUST be disabled.

Verification (MUST record at least one):

- Physical port blockers / sealed unused ports (photo acceptable).

- OS-level policy evidence (screenshot/export of policy setting).
- A record of currently attached USB devices.

A perimeter snapshot record MUST include `usb_policy` and `attached_usb` (redacted OK).

4.4 Acoustic & sensor hygiene

1. Smart speakers, always-on microphones, and “voice assistants” MUST NOT be present in the same room during sensitive operation.
2. If a microphone is not required, it MUST be disabled (hardware switch preferred).
3. Cooling SHOULD prioritize stable operation (reduce thermal excursions and erratic fan ramps).

Verification (MUST record at least one):

- “Room checklist” attestation (Appendix A) signed by operator.
- OS device-disable evidence for microphone/camera (where applicable).

4.5 Physical access

1. The node MUST be in a controlled location (door/lock routine; at minimum: presence awareness).
2. Tamper-evident markers MAY be used (cheap seals are acceptable).

Verification (MUST record at least one):

- Operator attestation (presence routine).
- Optional: photo of seal state (privacy-aware).

5) Metabolic controls (normative)

1. Every high-impact action MUST have a cost gate, at minimum one of:
 - time budget (cool-down windows),
 - rate limits (jobs per minute),
 - energy budget (max draw or scheduled execution windows),
 - challenge window (pause for verification on sensitive actions).
2. A circuit breaker MUST exist:
 - if telemetry crosses thresholds (temp/power/network anomalies) → degrade mode or halt.

Verification:

- Threshold definitions MUST be documented.
- Breaker trips MUST emit an anomaly record.

6) Evidence & logging (L4 Witness hooks) (normative)

The node MUST produce an auditable trail for:

- perimeter state snapshot (radios OFF, interfaces, firewall policy, mounted devices),
- configuration hash (canonical JSON + SHA-256),
- change events (who/when/why),
- incident flags (breaker trips, anomaly detections),

- mode changes (PROD ↔ MAINT).

6.1 Minimal event types (normative)

- perimeter.snapshot
- perimeter.change
- perimeter.exception (time-boxed deviation)
- perimeter.anomaly
- perimeter.breaker_trip
- perimeter.mode_change

6.2 Minimal record fields (normative)

Records MUST include at least:

- record_id (unique)
- timestamp (ISO 8601 with timezone)
- node_id
- mode (PROD or MAINT)
- event_type
- prev_hash (hash-chain continuity)
- config_hash_sha256 (over canonical JSON config)
- radios_state (wifi/bt)
- net_ifaces_summary (eth only in PROD)
- usb_policy
- power_chain_declared (true/false)
- anomaly_flags (temp/power/rf/network)
- operator_attestation (human witness “a”, privacy-aware)

6.3 Canonical configuration (normative)

Perimeter configuration MUST be representable as a canonical JSON object.

- RECOMMENDED canonicalization: RFC 8785 (JCS).
- Hash algorithm: SHA-256 (RECOMMENDED).

7) Baseline profiles (normative)

7.1 Profile L4-BASE (recommended default)

- Ethernet only (Section 4.1)
- Wi-Fi/Bluetooth disabled (Section 4.1)
- No smart speakers / always-on mics in room (Section 4.4)
- USB whitelist + maintenance port (Section 4.3)
- Power-chain hygiene (Section 4.2)
- Evidence cadence:
 - snapshot on boot,
 - snapshot on config change,
 - weekly snapshot.

7.2 Profile L4-HRO (high reliability operations, optional)

Includes L4-BASE plus:

- UPS present and monitored
 - stricter physical access routine (documented)
 - scheduled “quiet windows” for sensitive runs
 - evidence cadence:
 - snapshot per session,
 - anomaly review per session.
-

8) Validation tests (operational) (normative)

8.1 MUST pass (PROD readiness)

- Wi-Fi/Bluetooth = OFF verified (BIOS/UEFI and/or OS)
- Only Ethernet link active
- Firewall deny-by-default (documented)
- USB policy enforced (documented)
- Baseline perimeter.snapshot record produced, hashed, chained

8.2 SHOULD run weekly

- config diff vs last known-good config_hash_sha256
 - anomaly review (temps, restarts, breaker events)
 - check for privilege drift (radios/services silently re-enabled)
-

9) Change control (no surprises) (normative)

Any perimeter change MUST: 1) be written (what/why), 2) produce a new config_hash_sha256, 3) emit a perimeter.change record, 4) have a rollback path to last-known-good configuration.

9.1 Exceptions (time-boxed)

Any exception in PROD (e.g., temporarily enabling Wi-Fi) MUST:

- be approved by the designated authority (operator/arbiter),
 - be time-boxed with an expiry,
 - emit a perimeter.exception record,
 - be reverted (rollback) at expiry.
-

10) Top failure modes (normative list)

1. **Privilege drift:** radios/services quietly re-enabled after updates.
2. **Channel creep:** a “temporary dongle/cable” becomes permanent.
3. **Workflow bypass:** changes made without evidence record.

Mitigation: small, boring rules + hashed snapshots + time-boxed exceptions + human attestation.

11) Integration (informative)

- **Entity node** enforces perimeter locally (hard rules).
 - **Arbiter** approves exceptions (time-bound privileges, logged).
 - **Oracle** remains scarce: used for external verification/audits, not for endless “try again”.
-

Appendix A - Minimal “Room checklist” (30 seconds) (informative)

- [] PROD mode confirmed
- [] Wi-Fi/Bluetooth off (checked)
- [] No smart speaker / phone mic near node
- [] Only known power chain and cables
- [] Only known USB devices (maintenance port labeled)
- [] Witness snapshot recorded (boot/session)

Operator: _____ Date/Time: _____

Appendix B - Rationale (non-normative; honest protocol)

B.1 Facts (high confidence)

- Air-gapped environments can still be compromised and/or exfiltrate via non-network channels, including RF emissions, power-line conducted emissions, and acoustics.
- USB is a repeatable, high-frequency injection vector in “controlled” environments.

B.2 Interpretation (medium confidence)

- For home/office nodes, most risk comes from: uncontrolled radios + uncontrolled power chain
+ uncontrolled nearby sensors + casual USB habits.
- Hardening defaults beats exotic defenses.

B.3 Hypotheses (uncertainty flagged)

- Acoustic/power signatures can enable activity inference for GPU-heavy workloads.
(uncertainty: medium)
 - Some “molecular/impedance” claims are often overstated; treat as possible but non-primary.
(uncertainty: high)
-

Appendix C - Bridges + “Earth paragraph” (informative)

EXPLICIT BRIDGE (c=a+b): Human intent + hardware/OS procedures ⇒ a stable, reality-bound perimeter (L4).

HIDDEN BRIDGE #1 (Ashby): Perimeter needs requisite variety: network + power + acoustic + physical access controls (not a single knob), and a regulator (change control + evidence) to prevent drift.

HIDDEN BRIDGE #2 (Cover & Thomas): Side-channels are extra channels; even if the primary channel is “secure”, leakage can still carry information. The perimeter limits the channel set.

EARTH PARAGRAPH (engineering/anatomy): Это как организм: можно “закрыть рот” (шифрование), но остаются пульс, дыхание, тепло и мышечные микродвижения. У компьютера “пульс” - ток, шум, вибрация, радиофон, кабели. L4 начинается там, где этот пульс признаётся интерфейсом и ставится под режим.

References (normative/informative)

Normative keywording:

- RFC 2119: <https://datatracker.ietf.org/doc/html/rfc2119>
- RFC 8174: <https://www.ietf.org/rfc/rfc8174.html>

Operational control language (baseline/change control/physical controls):

- NIST SP 800-53 Rev. 5: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- Example control summaries (CM-2 baseline config):
<https://csf.tools/reference/nist-sp-800-53/r5/cm/cm-2/>

AI Act legal anchor (primary source):

- Regulation (EU) 2024/1689 (EUR-Lex):
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

Illustrative side-channel / air-gap research (informative):

- AirHopper (arXiv): <https://arxiv.org/abs/1411.0237>
- PowerHammer (arXiv): <https://arxiv.org/abs/1804.04014>
- Fansmitter (abstract):
<https://www.sciencedirect.com/science/article/abs/pii/S0167404820300080>
- USB attack surface / BadUSB discussion (thesis PDF): <https://d-nb.info/1084759179/34>