ZEROSTACK TECHNICAL WHITEPAPER SERIES · PART 2

ZeroStack: A Zero-Stall, O(1) Deterministic Zigbee 3.0 Stack

Part II: Beyond the Power Cycle — Eliminating Lockups, Brownout Corruption, and Remote Faults

Published by: SMLIGHT Engineering (`smlight.tech`)
Target Platform: 48 MHz 32-Bit ARM Cortex-M4F Wireless Microcontroller (IEEE 802.15.4 / Zigbee PRO R23 Coordinator)
Dataset: 6 November 2026 Adversarial Fault-Injection & Resilience Campaign — Legacy Reference Stack vs. ZeroStack Memory-Safe Rust NWK/APS/ZNP Engine

1. Executive Summary

Part 1 of this series (*Scaling Zigbee 3.0 / R23 Beyond the 100-Node Wall*) demonstrated that achieving *O(1)* deterministic execution time across coordinator address resolution, security processing, and memory management reduces worst-case processing latency by up to three orders of magnitude. Part 2 (*Beyond the Power Cycle*) addresses the complementary systems engineering question: **how does each stack fail under malformed over-the-air input, resource exhaustion, hostile serial framing, mesh broadcast storms, and mid-write power loss—and does it recover deterministically without a power cycle or memory leak?**

Using an identical 48 MHz ARM Cortex-M4F hardware-in-the-loop (HIL) testbed and cycle-accurate NOR flash brownout simulation harnesses, we evaluate a commercial Legacy Reference Stack (Zigbee 3.0) against **ZeroStack**, whose NWK, APS and ZNP layers use a memory-safe Rust protocol engine, across five operational fault domains:

- **Malformed, Truncated, & Tampered Over-the-Air Frames:** 3,255 adversarial and reference frames across the IEEE 802.15.4 MAC boundary, paired with 12 on-target NWK/APS fault classes covering malformed protocol headers, invalid routing subframes, truncated control commands, 392 cryptographic bit-flips (AAD, ciphertext, MIC-32), and a 1,000-frame replay flood evaluated on physical silicon at non-volatile table depth *D = 150*.
- **Resource Exhaustion & Unauthenticated Join Floods:** Software timer saturation, heap depletion down to `0` free bytes, and 50 back-to-back first-contact Trust Center Link Key (TCLK) misses against a 300-node coordinator table.
- **Host Serial Transport Framing Abuse:** Truncated host command frames, corrupted frame check sequences (FCS), maximum-length payload floods, and `300 × SOF` Start-of-Frame delimiter storms at 115,200 baud.
- **Non-Volatile Memory Power-Loss & Brownout Fuzzing:** Byte-by-byte power cuts across 22,565 compaction cut points and 394 record-update cut points against a physical NOR flash bit-AND model, verified alongside 2,000,000 randomized shadow-fuzz operations.
- **Mesh Broadcast Storms & Router Echo Amplification:** Back-to-back multi-router broadcast floods and 1,000-frame router rebroadcast echo storms at table depth *D = 150*.

Across all tested fault domains, ZeroStack achieves:

- **Zero CPU crashes across all 12 on-target malformed frame classes**, whereas the Legacy Reference Stack suffers a deterministic **remote CPU** **`HardFault`** **(**`Precise BusFault`**)** when presented with unauthenticated malformed secured frames.
- **9.8× to 402× lower CPU rejection cost** at table depth *D = 150* (`320–790 cycles` for malformed header drops, `1,550–1,568 cycles` for replay rejections and `4,731–4,771 cycles` for cryptographic MIC failures vs. `3,136 cycles` for a cleartext header drop and `143,058–144,412 cycles` for the others on the Reference Stack), draining a **1,000-frame replay flood in** `32.4 ms` **of CPU time vs.** `2.99 seconds`.
- **0 lost or corrupted non-volatile items across 22,959 power-cut points**, with **749× lower post-brownout flash write volume** following an interrupted write (`27 B` and `0` page erases vs. the Reference Stack's `20,232 B` and `62` page erases).
- **0 lost host commands under hostile UART framing** (`3–55 ms` recovery), where the Reference Stack suffers an **8.84-second serial link blackout** dropping 44 consecutive health checks.
- **7.7× faster control-plane recovery** during a 50-device unauthenticated join storm (`0.22 s` vs. `1.70 s`).
- **19.9×–20.3× lower broadcast storm CPU cost** at table depth *D = 150*, suppressing a **1,000-frame 50-router rebroadcast echo storm in** `151.16 ms` **of total CPU time (**`7,076 cycles` **/** `147 µs` **per echo) vs.** `3.00 seconds`

(`143,865 cycles` / `3.00 ms` per echo) on the Reference Stack, and completing a **64-frame post-outage unique broadcast flood in `18.87 ms` vs. `200.25 ms` (10.6× lower CPU time)** with `0` duplicate upper-layer deliveries and *Δheap = 0 B*.

Headline Resilience Benchmark Summary

Operational Fault Domain	Legacy Reference Stack	ZeroStack Architecture	Measured Improvement
Malformed Secured OTA Frames	Unauthenticated remote CPU `HardFault` (`Precise BusFault`)	**`0` crashes** across all 12 fault classes (`320–6,631 cyc` rejection)	**Eliminates remote over-the-air coordinator crash**
1,000-Frame Replay & Tamper Flood (*D=150*)	`143,802 cycles` (`3.0 ms`) per replay; **`2.99 s` total CPU lockup**	**`1,550 cycles` (`32 µs`)** per replay; **`32.4 ms` total CPU**	**9.8×–402× lower CPU rejection cost**
Flash Power-Loss Recovery (22,959 Cuts)	Full 62-page flash compaction (`20,232 B` written) + `1` NOR verify conflict	`0` data loss across 22,959 cuts; **`27 B` written, `0` page erases**	**749× lower post-brownout boot flash write volume**
Serial Framing Abuse (`115,200` baud)	**`8.84 s` serial link blackout** (`44` consecutive lost pings)	**`0` lost pings** across all 6 abuse scenarios (`3–55 ms` recovery)	**Eliminates multi-second host-coordinator serial dropouts**
50-Device Unauthenticated Join / Miss Flood	`33.9 ms` stall per miss; **`1.70 s` total control-plane stall**	**`4 µs` miss lookup** (`208 cyc` ; `4.3 ms` wire ping); **`0.22 s` total**	**7.7× faster control-plane recovery during join storms**
Resource Exhaustion (`0 B` Free Heap)	Uncapped subsystem timer allocation	**Bounded resource capacity** + 100% recovery from `0 B` heap (*Δheap = 0 B*)	**Predictable degradation with zero memory leaks**
Mesh Broadcast Storm (*D=150*)	`143,865 cycles` (`3.00 ms`) per echo; **`3.00 s` total CPU** (`1,000` echoes)	**`7,076 cycles` (`147 µs`)** per echo; **`151.16 ms` total CPU** (`0` dup deliveries)	**19.9×–20.3× lower broadcast storm CPU time (`10.6×` on 64-frame flood)**

2. Methodology & Invariant Oracles

2.1 Experimental Architecture

Every fault-injection campaign evaluates the unmodified Legacy Reference Stack and ZeroStack under identical stimulus conditions. On-target hardware benchmarks execute on a single-board **48 MHz 32-bit ARM Cortex-M4F** wireless microcontroller (`1 µs = 48 CPU cycles`) over a 115,200 baud 8N1 UART control link, paired with an out-of-band Serial Wire Debug (SWD) probe that samples allocator watermarks, hardware cycle counters, fault status registers, and RTOS task state without perturbing runtime execution. Boundary state-space and power-loss campaigns execute deterministic protocol and NOR flash fault-injection harnesses with strict memory-safety and bit-level verification oracles.

2.2 The Four Universal Resilience Oracles

Resilience verification requires stronger guarantees than merely avoiding a CPU exception. After every injected fault or adversarial burst, the test harness enforces four strict post-fault invariants:

1. **Control-Plane Liveness & Reset Oracle:** The Device Under Test (DUT) must respond to synchronous host keepalive pings, and no CPU fault (`HardFault` / `BusFault`) or unsolicited reset indication may occur during or after fault injection.
2. **Zero-Leak Memory Oracle (SWD):** Once the fault stimulus is drained or released, out-of-band SWD inspection of total free heap memory must return to the exact pre-fault byte baseline (*Δ heap = 0 B*).
3. **State Immutability Oracle:** Cryptographic replay counters (NWK and APS frame counters), network information base (NIB) attributes, non-volatile flash records, active timer tables, and the 300-entry TCLK table must remain bit-for-bit unchanged by any rejected frame or failed resource allocation.
4. **Forward Progress Oracle:** The immediately following valid protocol operation (e.g., an encrypted frame with frame counter *FC = FC_{stored} + 1*, a valid non-volatile write, or a host command) must succeed on the first attempt.

3. Non-Volatile Storage Power-Loss, Torn Writes, and Brownout Recovery

3.1 Deterministic Byte-Level NOR Flash Brownout Simulation

A Zigbee coordinator relies on non-volatile flash storage to persist the active network key, network state, address bindings, and hundreds of per-device Trust Center Link Keys (TCLKs) alongside their monotonic frame counters. In field deployments, power interruptions frequently coincide with periods of elevated flash activity—such as multi-device commissioning bursts or background flash page compaction.

We evaluate both the Legacy Reference Stack's flash translation layer and ZeroStack's storage engine against a deterministic NOR flash hardware simulator configured to match a production **128 KB (`64 × 2 KB` page)** flash geometry:

- **Physical NOR Bit-AND Semantics:** Erased flash pages initialize to `0xFF`. Programming any byte executes a bitwise `AND` (`flash[addr] &= data`). Any software bug that attempts to flip a `0` bit back to `1` without an intervening page erase leaves the physical bit at `0`, fails hardware read-back verification, and records a **NOR write conflict**.
- **Exhaustive Cut-Point Replay:** A brownout interposer sits on the flash bus. If a composite storage operation executes *K* primitive byte-writes and page-erases, the harness replays the workload *K* times from a clean pre-operation snapshot—severing power immediately after primitive *1, 2, …, K*, cold-booting the storage driver, and verifying every logical record against the expected transactional state.
- **Correctness Criterion ("Bad"):** Any cut point that yields a lost record, stale value, checksum error, torn payload, resurrected tombstone, or boot initialization error is classified as **Bad**.

3.2 Cut-Point Scan Results

Brownout Scan Scenario	Stack Arm	Total Cut Points Tested	Bad Outcomes	Post-Reboot State Detail
Mid-Compaction Power Cut *(64 variable-length records, 32 updated, 1 deleted, interrupted at every byte/erase of compaction)*	Legacy Reference Stack	`20,511`	`0`	**`1` NOR hardware write-verify conflict** observed.
Mid-Compaction Power Cut	**ZeroStack**	**`22,565`**	**`0`**	`0` items lost, `0` NOR conflicts, `0` boot errors across all 22,565 cuts.
Torn Tail, Large Record *(Update existing multi-hundred-byte record, cut power after every programmed byte)*	Legacy Reference Stack	`380`	`0`	Every cut resolves deterministically to either the intact prior record or the complete new record (`0` torn payloads).
Torn Tail, Large Record	**ZeroStack**	**`380`**	**`0`**	Every cut resolves deterministically to either the intact prior record or the complete new record (`0` torn payloads).
Torn Tail, Small Record *(Single-word counter update, cut power after every programmed byte)*	Both Arms	`14`	`0`	Every cut resolves deterministically without torn state.

3.3 Post-Brownout Boot Recovery Cost (Flash Wear & Boot Amplification)

Transactional atomicity requires that no committed data is lost, but **the volume of flash writes and page erases triggered during the subsequent reboot** dictates whether repeated power glitches prematurely wear out NOR flash cells or stall coordinator startup:

Boot Scenario Following Power Cut	Legacy Reference Stack: Flash Bytes Written (Mean / Max)	Legacy Reference Stack: Page Erases (Mean / Max)	ZeroStack: Flash Bytes Written (Mean / Max)	ZeroStack: Page Erases (Mean / Max)
Boot After Mid-Compaction Power Cut	`19,377 B` / `22,458 B`	`62` / `64`	**`19,405 B`** / **`20,529 B`**	**`56`** / **`63`**
Boot After Torn Record Tail	**`20,232 B`** / **`20,447 B`**	**`62`** / **`63`**	**`27 B`** / **`27 B`** **(749× lower)**	**`0`** / **`0`**

3.4 Black-Box Evaluation of Post-Brownout Recovery

1. **Zero Data Loss Across 22,959 Cut Points:** Across all `22,565` mid-compaction cuts, `394` record-update byte cuts, and `2,000,000` randomized shadow-fuzz operations, ZeroStack experiences `0` **lost, stale, or corrupted records and** `0`

NOR hardware write-verify conflicts (compared to `1` hardware write-verify conflict in the Reference Stack).

2. ***O(1)* Torn-Write Recovery vs. Full-Volume Compaction (`27 B` vs. `20.2 KB`):** As shown in Table 3.3, when power fails during an ordinary record update outside of compaction, **the Legacy Reference Stack falls back to a full-volume flash compaction on the very next boot**, writing `20,232 B` and erasing `62` flash pages. In contrast, **ZeroStack recovers in *O(1)* flash I/O (`27 B` written, `0` page erases)**—eliminating unnecessary flash wear and boot-time compaction stalls after transient power brownouts.

4. Host Serial Transport Framing Abuse

4.1 Motivation: Host-Coordinator Serial Link Availability

In production smart-home gateways, the host application processor communicates with the Zigbee coordinator over an asynchronous serial framing protocol. In the field, this UART/TCP-serial boundary is exposed to baud-rate transients during host reboots, operating-system serial probe strings, container restarts that sever an outbound frame mid-transmission, and electrical line noise. If malformed byte sequences lock the coordinator's serial receiver, the host controller declares the radio unresponsive and restarts the entire Zigbee network.

4.2 Hardware Test Protocol

Executed on target hardware at `115,200` baud (5 seeded repetitions per scenario). In each trial, the test harness transmits a hostile byte sequence into the coordinator's UART RX line and immediately polls the coordinator with back-to-back synchronous `PING` commands (`200 ms` timeout per attempt, up to `100` attempts) until a valid response frame is received, followed by SWD verification of free heap memory.

4.3 Empirical Hardware Results

Adversarial UART Input Scenario	Legacy Reference Stack: Pings Lost	Legacy Reference Stack: Recovery Time	ZeroStack: Pings Lost	ZeroStack: Recovery Time	SWD Heap Δ (Both Arms)
512 B random noise (excluding `SOF`)	`0`	`48 ms`	`0`	`47 ms`	`0 B`
10 × `PING` frames with corrupted FCS checksum	`0`	`6 ms`	`0`	`9 ms`	`0 B`
Max-length header + 256 B garbage body	`0`	`25 ms`	`0`	`25 ms`	`0 B`
Truncated frame (cut mid-payload)	**`1` (every rep)**	`203 ms`	`0`	`3 ms`	`0 B`
SOF Delimiter Storm (`300` × `SOF` back-to-back)	**`44` (every rep)**	`8,840 ms` (`8.84 s`)	`0`	`29 ms`	`0 B`
512 B unconstrained random noise (including `SOF`)	**`30`, `4`, then `0`**	`6,000 ms` (`6.0 s`)	`0`	`47–55 ms`	`0 B`

(Note: Baseline recovery times of `25–55 ms` on 512-byte injections reflect the physical wire serialization duration of the hostile burst itself at 115,200 baud: 5120 bits / 115,200 bps ≈ 44.4 ms.)

4.4 Empirical Link Availability Comparison

- **Legacy Reference Stack Serial Blackout (`8.84 Seconds`):** Following a truncated frame, the Reference Stack drops the immediately following host command (`203 ms` recovery delay on every trial). Following a Start-of-Frame delimiter storm (`300 × SOF`) or unconstrained line noise, the Reference Stack suffers a prolonged serial link blackout—**dropping up to `44` consecutive `PING` health checks over `8.84 seconds`** before answering the host.
- **ZeroStack Immediate Recovery (`0` Pings Lost):** ZeroStack resynchronizes at wire speed across all six fault classes, losing **zero host commands** (`3–55 ms` total recovery time) with zero heap drift (*Δheap = 0 B*).

5. Resource Exhaustion & Unauthenticated Join Floods

5.1 Test Protocol

To evaluate graceful degradation under extreme load, the test harness drives the coordinator into three resource-exhaustion regimes while probing control-plane survival and verifying 100% resource reclamation via SWD once the load is released:

1. **Timer Saturation:** Allocate software timers until the subsystem refuses additional timers (or hits the 255-timer harness cap).
2. **Heap Exhaustion to Zero Free Bytes:** Allocate memory blocks until allocation returns `NULL` (stepping through controlled free-memory watermarks of `2,048 B`, `512 B`, `128 B`, and `0 B`), test control-plane liveness, and issue an in-band release command to verify zero-leak recovery.
3. **50-Device First-Contact TCLK Miss Flood (*D = 300*):** With a full 300-entry TCLK table populated in non-volatile memory, inject 50 back-to-back link-key lookups for unknown 64-bit IEEE addresses (modeling a burst of 50 unprovisioned devices attempting to join or exchange security frames simultaneously), measuring control-plane ping stall latency after each miss.

5.2 Hardware Results

Exhaustion / Flood Vector	Legacy Reference Stack	ZeroStack	Operational Outcome
Timers held until allocation refusal	Uncapped up to harness limit (`255`)	**Bounded capacity refusal** (`194` timers, then `NO_TIMER_AVAIL`)	Runaway timer use is refused cleanly at a bounded limit instead of exhausting memory.
Control-plane `PING` while max timers held	`5 / 5` answered	`5 / 5` **answered**	Timer saturation does not impair serial command processing on either stack.
`PING` survival at `2,048` / `512` / `128 B` free	`5/5`, `5/5`, `5/5`	`5/5`, `5/5`, `5/5`	Both stacks preserve 100% control-plane responsiveness down to `128 B` of free heap.
Heap exhausted to `0` (`keep = 0`)	No crash; `5/5` pings	**No crash;** `5/5` **pings**	Clamping the system heap to `0 B` leaves ZeroStack's host command path answering; the in-band release command recovers 100% (*Δheap = 0 B*).
In-band release command after `0 B` heap	**Recovers 100%** (*Δ heap = 0 B*)	**Recovers 100%** (*Δ heap = 0 B*)	Both stacks execute the release command and return to their exact pre-test byte watermark.
Single TCLK Miss (`300` entries): `PING` stall (`p50` / `max`)	**`33.9 ms` (`34.9 ms`)**	**`4.3 ms` (`4.4 ms`)**	On every unknown-device miss, the Reference Stack incurs a `~31 ms` processing stall (+*3 ms* UART wire time); ZeroStack resolves a miss in ***4 µs*** (`208` cycles; *4.3 ms* is pure UART round-trip time).
50 Back-to-Back TCLK Misses + Ping	**`1.70 s`** (`1,700 ms`)	**`0.22 s`** (`220 ms`, **7.7× faster**)	A 50-device first-contact miss burst stalls the Reference Stack control plane for 1.7 seconds; ZeroStack remains continuously responsive.

6. Malformed, Truncated, and Tampered Over-the-Air Frames

6.1 IEEE 802.15.4 MAC Boundary State-Space Verification

Prior to upper-layer protocol processing, the 802.15.4 MAC receive boundary is verified across 3,255 adversarial and reference frames (1,085 malformed vectors interleaved with 2,170 valid verification frames). The test suite sweeps the IEEE 802.15.4 MAC Header (MHR) state space—covering truncated and oversized frame lengths, bit-flipped control fields, reserved frame-type and version combinations, invalid addressing modes, and compressed PAN identifier permutations. Across all 3,255 vectors, ZeroStack exhibits **zero memory safety faults, zero leaks, and zero state corruption**, while accepting every interleaved valid frame on the first attempt.

6.2 On-Target NWK/APS Malformed Frame & 1,000-Frame Replay Flood (*D = 150*)

6.2.1 HARDWARE INJECTION METHODOLOGY

To evaluate the upper protocol layers (NWK header parsing, routing headers, CCM* security unsealing, replay protection, and APS dispatch) on identical silicon across both stacks, the harness injects 12 fresh-boot classes of malformed, truncated, bit-flipped, and replayed frames on the 48 MHz ARM Cortex-M4F testbed with non-volatile table depth populated to *D = 150* devices. Each class begins from a clean boot, records hardware cycle counts for two sequential pipeline stages—the MAC-to-NWK handoff (`handoff p50`) and the NWK/APS frame processing execution (`total p50`)—verifies SWD heap stability (*Δ heap*) and security state integrity, and confirms that the immediately following valid encrypted frame is accepted.

6.2.2 EMPIRICAL HARDWARE RESULTS (*D = 150*)

Fault Class & Description	Vectors	Legacy Reference Stack Outcome (`total p50` / `handoff p50` cycles)	ZeroStack Outcome (`total p50` / `handoff p50` cycles)	Rejection Speedup
Malformed Cleartext Header	`16`	`0` delivered, *Δheap = 0 B*, state intact, next ok (`3,136` / `1,031` cyc)	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`320` / `253` cyc)**	**9.8×**
Malformed Secured Frame — Class A	`14`	**CRASH: `HardFault` (`Precise BusFault` on unauthenticated input; `143,345` cyc)**	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`357` / `291` cyc)**	**∞ (`402×` cyc)**
Malformed Secured Frame — Class B	`19`	**CRASH: `HardFault` (`Precise BusFault` on unauthenticated input; `144,412` cyc)**	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`4,731` / `337` cyc)**	**∞ (`30.5×` cyc)**
Malformed Upper-Layer Stub	`8`	`0` delivered, *Δheap = 0 B*, next ok (`144,290` / `1,437` cyc)	**`0` delivered, *Δheap = 0 B*, next ok (`6,312` / `330` cyc)**	**22.9×**
Malformed Routing Header	`9`	**BUG: Accepts malformed frame, mutates security state, & delivers to app!** (`144,127` / `1,728` cyc)	**`0` delivered (all 9 rejected), *Δheap = 0 B*, state intact, next ok (`790` / `394` cyc)**	**182×**
Truncated Control Command — Class A	`3`	`0` delivered, *Δheap = 0 B*, next ok (`149,862` / `1,465` cyc)	**`0` delivered, *Δheap = 0 B*, next ok (`6,631` / `347` cyc)**	**22.6×**
Truncated Control Command — Class B	`3`	Accepted without drop (`152,069` / `1,444` cyc)	**`0` delivered, *Δheap = 0 B*, next ok (`6,269` / `335` cyc)**	**24.3×**
Authenticated Header Bit-Flips	`240`	All invalid AAD bit-flips rejected, *Δheap = 0 B*, next ok (`143,065` / `1,587` cyc)	**All invalid AAD bit-flips rejected, *Δheap = 0 B*, next ok (`4,760` / `357` cyc)**	**30.1×**
Ciphertext Bit-Flips	`120`	`0` delivered, *Δheap = 0 B*, state intact, next ok (`143,060` / `1,587` cyc)	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`4,768` / `358` cyc)**	**30.0×**
Authentication Tag Bit-Flips	`32`	`0` delivered, *Δheap = 0 B*, state intact, next ok (`143,058` / `1,587` cyc)	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`4,771` / `357` cyc)**	**30.0×**
Cryptographic Replay Flood *(1,000 back-to-back replayed frames, FC ≤ FC_{stored})*	`1,000`	`0` delivered, *Δheap = 0 B*, state intact, next ok (`143,802` / `1,589` cyc; **`~2.99 s` total CPU**)	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`1,550` / `355` cyc; `~32.4 ms` total CPU)**	**92.8×**
Boundary Replay Check *(Exact duplicate FC = FC_{stored} and FC = 0)*	`2`	`0` delivered, *Δheap = 0 B*, state intact, next ok (`143,775` / `1,586` cyc)	**`0` delivered, *Δheap = 0 B*, state intact, next ok (`1,568` / `355` cyc)**	**91.7×**

(Note: on both stacks `total p50` starts once the MAC has placed the frame in the stack's buffer and measures the stack's handling of it, at `48 MHz` (`1 µs = 48 cycles`). The `handoff p50` measurement boundaries differ between the two stacks, so the two `handoff` columns are not like-for-like.)

6.2.3 BLACK-BOX ANALYSIS OF ON-TARGET FRAME FAULT FINDINGS

1. UNAUTHENTICATED REMOTE OVER-THE-AIR `HARDFAULT` ELIMINATION

In **Malformed Secured Frame — Class A** and **Class B**, the Legacy Reference Stack suffers a deterministic **CPU `HardFault` (`Precise BusFault`)** triggered by unauthenticated over-the-air input prior to message authentication tag verification—meaning any unauthenticated transmitter within radio range holding no network keys can halt a Reference Stack coordinator or router. ZeroStack rejects all 33 malformed secured vectors in **`357–4,731` cycles (`7–99 µs`)** with zero faults, zero state mutation, and zero heap movement.

2. MALFORMED ROUTING HEADER REJECTION (`182×` FASTER)

In the **Malformed Routing Header** class, the Legacy Reference Stack fails to reject an invalid routing header structure, spending `144,127 cycles` (`3.0 ms`) processing the frame, mutating security state, and delivering the malformed packet to the application layer. ZeroStack drops all 9 invalid vectors in **`790 cycles` (`16 µs` —182× faster)** with zero state mutation.

3. CRYPTOGRAPHIC REPLAY FLOOD ABSORPTION (`32.4 MS` VS. `2.99 S` CPU LOCKUP)

At table depth *D = 150*, the Legacy Reference Stack expends **`143,058–144,412 cycles` (`~3.0 ms` of solid CPU execution)** for every single tampered or replayed packet—burning **`2.99 seconds` of continuous CPU time** during a `1,000`-frame replay flood. ZeroStack rejects replayed frames in **`1,550–1,568 cycles` (`32–33 µs`)** and tampered frames in **`4,760–4,771 cycles` (`99 µs`)**, absorbing the same 1,000-frame replay flood in **`32.4 ms` (`93×` faster)** while keeping the coordinator responsive.

7. Mesh Broadcast Storms & Router Echo Amplification (*D = 150*)

7.1 Motivation: Whole-Mesh Broadcast Amplification Lockups

In large residential and commercial Zigbee networks (100–300+ nodes with 40–80 mains-powered routers), **mesh-wide broadcast storms are the primary trigger of coordinator lockups following mains power restoration or rapid discovery bursts**. Under the Zigbee PRO specification, every router rebroadcasts a broadcast frame up to `nwkMaxBroadcastRetries` times while tracking passive acknowledgments from neighboring routers in its Broadcast Transaction Table (BTT). When dozens of routers simultaneously announce themselves or echo broadcast frames back toward the coordinator within the broadcast delivery window (`nwkBroadcastDeliveryTime`), the coordinator is subjected to both BTT capacity saturation and intense back-to-back duplicate echo storms.

7.2 Empirical Hardware Results (*D = 150*)

Broadcast Storm Scenario (*D = 150*)	Vectors	Legacy Reference Stack Outcome (`total p50` / `handoff p50` cycles)	ZeroStack Outcome (`total p50` / `handoff p50` cycles)	Measured Improvement
Unique Broadcast Saturation Flood *(64 back-to-back unique NWK broadcasts, `DstAddr = 0xFFFC`, `MAC DstAddr = 0xFFFF`, `radius = 30`, modeling simultaneous post-outage router announcements)*	`64`	`30 / 64` delivered (BTT capacity = `30`), *Δheap = 0 B*, next unicast ok `144,858` / `1,623` cyc (`154,705` accepted p50; `144,644` shed p50) **`200.25 ms` total CPU** (`2.16 ms` post-burst ping)	**`40 / 64` delivered (BTT capacity = `40`, `+33%`), *Δheap = 0 B*, next unicast ok** **`16,710` / `357` cyc** (`17,699` accepted p50; `8,341` shed p50) **`18.87 ms` total CPU** (`2.15 ms` post-burst ping)	**10.6× lower total CPU time** **17.3× faster overflow shedding** (`174 µs` vs. `3.01 ms`)
50-Router Echo Amplification Storm *(1,000 frames: 20 unique broadcasts × 50 copies each — 1 origin + 49 router rebroadcast echoes per broadcast)*	`1,000`	`20 / 20` delivered (`0` dup echoes), *Δheap = 0 B*, next unicast ok `143,866` / `1,621` cyc (`152,887` origin p50; `143,865` / `152,526` echo p50 / p99) **`3,004.97 ms` (`3.00 s`) total CPU** (`2.56 ms` post-burst ping)	**`20 / 20` delivered (`0` dup echoes), *Δheap = 0 B*, next unicast ok** **`7,079` / `357` cyc** (`16,808` origin p50; **`7,076` / `7,335` echo p50 / p99**) **`151.16 ms` total CPU** (`2.16 ms` post-burst ping)	**19.9× lower total CPU time** (`151 ms` vs. `3.00 s`) **20.3× faster per-echo suppression** (`147 µs` vs. `3.00 ms`)

(Note: as in Table 6.2.2, the `handoff` measurement boundaries differ between the two stacks, so the `handoff` columns are not like-for-like.)

7.3 Black-Box Analysis of Broadcast Storm Resilience

1. 20.3× FASTER DUPLICATE ECHO SUPPRESSION (`151 MS` VS. `3.00 SECONDS` CPU TIME)

Under the Zigbee PRO security model, NWK encryption is applied hop-by-hop: every router that rebroadcasts a broadcast frame re-encrypts the payload with its own outgoing NWK security frame counter while preserving the original NWK source address and broadcast sequence number inside the encrypted header. Consequently, the receiving coordinator must authenticate and decrypt each incoming router echo before inspecting its broadcast sequence number against the Broadcast Transaction Table (BTT).

- **Legacy Reference Stack (`3.00 Seconds` CPU Time):** At non-volatile table depth *D = 150*, the Reference Stack's per-echo processing cost (**`143,865 cycles` / `3.00 ms` p50**, `152,526 cycles` p99) and BTT overflow drop cost (**`144,644`**

`cycles` / `3.01 ms` **p50**) match its per-frame replay rejection cost in Table 6.2.2 (`143,802 cycles` / `3.00 ms`) within `0.6%`—consuming `3,004.97 ms` (`3.00 seconds`) **of continuous CPU execution** across the 1,000-frame storm.

- **ZeroStack (`151.16 ms` CPU Time):** ZeroStack authenticates and suppresses each duplicate router echo in `7,076 cycles` (`147 µs` p50, `7,335 cycles` / `153 µs` p99)—a **20.3× per-echo speedup** that absorbs the entire 1,000-frame, 50-router echo storm in `151.16 ms` **of total CPU time (19.9× lower)** with `0` duplicate application deliveries and *Δheap = 0 B*.

2. 10.6× LOWER CPU COST & 17.3× FASTER OVERFLOW SHEDDING UNDER POST-OUTAGE FLOODS (`18.87 MS` VS. `200.25 MS`)

When 64 unique NWK broadcasts arrive back-to-back (modeling simultaneous router announcements and route discovery bursts immediately after mains power restoration):

- **Legacy Reference Stack (`200.25 ms` CPU Time):** Admits the first `30 / 64` unique broadcasts (`154,705 cycles` / `3.22 ms` p50, BTT capacity = `30`) and still spends `144,644 cycles` (`3.01 ms` p50) on each of the 34 shed overflow broadcasts—consuming `200.25 ms` **of total CPU time**.
- **ZeroStack (`18.87 ms` CPU Time):** Admits `40 / 64` unique broadcasts in `17,699 cycles` (`369 µs` p50, **BTT capacity = `40`, `+33%`**) and sheds the remaining 24 overflow broadcasts in `8,341 cycles` (`174 µs` p50 — **17.3× faster**), completing the entire 64-frame flood in `18.87 ms` **(10.6× lower total CPU time)** with `0` allocator errors, *Δheap = 0 B*, and immediate acceptance of the following encrypted unicast frame.

8. Architectural Conclusion & Road Ahead

The empirical data in Part 2 demonstrates a second fundamental systems truth: **coordinator lockups, post-brownout flash amplification, and serial dropouts in production Zigbee networks are not random hardware glitches—they are the measurable consequence of how a protocol stack handles malformed input, power interruptions, and adversarial traffic bursts.** When a single malformed over-the-air frame can trigger an unauthenticated CPU `HardFault`, a 1,000-frame replay or 50-router broadcast echo storm can saturate the CPU for `2.99–3.00 seconds`, a burst of 50 unknown-device join attempts can stall the control plane for `1.70 seconds`, a stream of serial framing delimiters can black out the host link for `8.84 seconds`, and an interrupted flash write forces a 62-page (`20,232 B`) full-volume compaction on reboot, field reliability collapses long before the hardware reaches its physical limits.

Across all five fault domains—eliminating remote over-the-air crashes (`0` faults across 12 on-target fault classes and 3,255 MAC vectors), cutting malformed-frame, replay and broadcast storm CPU time by `9.8×–402×`, accelerating join-storm control-plane recovery by `7.7×`, maintaining `0` lost host commands under hostile UART framing, and recovering from torn flash writes in `27 B` (`749×` lower write volume with `0` page erases across 22,959 power-cut points)—ZeroStack turns fault survival and deterministic recovery into a verified hardware invariant.

COMING NEXT IN THIS SERIES

- **Part 3 — Multi-Node Mesh & End-to-End Hardware-in-the-Loop (HIL) Soak Testing:** Real-world throughput, packet delivery ratio (PDR), many-to-one source routing stability, and 300-node commissioning storms under continuous RF load.