The Southern Border Provinces Case Study on heain-core

Validating the HEAIN Framework for Accountable Public-Safety Governance through a 19-Node, 4-Tier Simulation, 20 Test Scenarios, a 24-Hour Soak and a 330-Node Scale Test

Jakkrit Boonma (จักรกฤษ บุญมา)

Independent Researcher · ORCID: 0009-0000-7165-3787 · jaggid.boonma@yahoo.co.th

Date: 16 October 2026

Implementation: heain-core v1.3 (commit ccfc2a7, Go 1.26), HP Z840 Workstation

Repository: github.com/JakkritB/heain-core (casestudies/deepsouth/)

Abstract

The first case study of the HEAIN Framework, CineNexus Pro, showed that all of its mechanisms work together in a company with many sites [13]. Public-sector work demands more: decisions no single party can make alone, records that outsiders can verify, and data that must never be traced back to a person. This paper reports the second case study, a hypothetical deployment of the HEAIN Framework for public-safety governance in Thailand's southern border provinces (Pattani, Yala, Narathiwat and four districts of Songkhla). The area is under two special security laws at once; the Prevention and Suppression of Torture and Enforced Disappearance Act B.E. 2565 (2022) requires every detention to be recorded and reported at once [17]; and trust between citizens and the state remains low.

The author designed a full-size, four-tier deployment (a Primary at the SBPAC with an independent committee, 4 provincial units, 37 districts, and sub-district Workers), then turned it into a 19-node simulation running the real heain-core in containers on a single HP Z840, and broke the requirements down into 20 test scenarios (D1–D20). They cover data that stays in its own district, survival when a district is cut off, incident certification by a four-party committee, approvals bound to a single incident that expire, custody records that cannot be altered, petitions that cannot be traced to the petitioner, a public transparency log time-stamped under RFC 3161, keys never held whole on a field machine, short-lived node certificates, prohibited functions, data from outside the trust boundary, a bias gate for camera models, and safety duties that continue after the license expires.

In the final run every scenario passed all 306 checks across 12 rounds. A 24-hour soak under 71 random faults processed 272,321 jobs with none lost or run twice, and a scale test at 330 nodes, matching the area's real number of districts, passed all 22 checks. The case study led to 21 changes to heain-core in 12 commits, including 10 groups of new mechanisms the first case did not need. The paper also proposes a four-phase pilot plan with success indicators and states what must still be done before real use. All results can be reproduced from the scripts in the repository.

Keywords: *HEAIN Framework, heain-core, Case Study, Public Safety, Human Rights, Multi-Party Approval, Transparency Log, Data Sovereignty, Network Partition, Scale Testing, Edge AI*

1. Introduction

1.1 Background

The HEAIN Framework grew from the theory of the Hybrid Edge AI Node [1][2] through the HEAIN Core Protocol specification [3][4], implementation [5][6][9][10] and the Triad of Structural Immunities [7][8] into a whole-system framework [11]. The CineNexus Pro case study then showed that all of its mechanisms keep their promises together in a post-production company with five studios, across 25 scenarios, 244 checks and a 24-hour soak [13].

A company, however, can trust its own administrators; the state cannot. A system that holds incident reports, custody records and camera events must show three things: that no official, administrator or machine can decide alone; that outsiders can verify the records with their own tools; and that the identity of a person who reports something is never linked to what they reported. This paper tests whether the HEAIN Framework keeps these promises, in normal operation, while the network is cut, and when an insider tries to rewrite the records.

1.2 Why the southern border provinces

The author chose this area because it gathers the hardest problems of public-sector systems in one place. Table 1 shows the scale of the problem. Incident data exist in two sets that count differently, with no central register both sides accept; the area has been under special laws for decades; and recent events show that field equipment and telecom towers are direct targets of attack.

Figure	Meaning	Source
23,536 incidents	Violent incidents, Jan 2004 – Dec 2025; 7,790 killed and 14,794 injured (7,837 killed by Aug 2026)	Deep South Watch, cited in [24]
10,116 incidents / 5,999 deaths	Incidents and deaths certified by the SBPAC for compensation	[25]
13,420 incidents	Difference between the two data sets (23,536 − 10,116); no central register shared by both	Author's calculation
THB 340,707 million	Budget for the southern border problem over 23 fiscal years (2004–2026)	[24]
86 renewals / 18 districts	Renewals of the Emergency Decree, covering 18 districts until January 2027; another 19 districts under the Internal Security Act	[21][16]
75 sites	Simultaneous attacks on the night of 22–23 Aug 2026 across 4 provinces	[22]
37 / 288 / 1,879	Districts, sub-districts and villages in the area	[25]

Table 1 — Key figures for the area

On the legal side, since 22 February 2023 the Torture and Enforced Disappearance Act has required continuous audio and video recording throughout arrest and detention, immediate notice to the public prosecutor and the district chief, and a register of detained persons [17]. The Personal Data Protection Act, meanwhile, partly exempts agencies with national-security duties [15]. Protection for citizens must therefore come from the system itself, not from data-protection law alone.

1.3 Status of the case study

> This deployment is hypothetical and designed by the author. It is not a project of any government agency, and no agency has reviewed it. No real person, place or event was used in the tests; every record is synthetic. Every node runs as a container on one machine. The number of machines per tier and the time limits are design assumptions. The legal interpretation is the author's own understanding; the author is not a lawyer, and the wording of each section should be checked against the official Royal Gazette. These limits are explained in Sections 4.7 and 11.

1.4 Research questions

- **RQ1 Rights and data.** Does raw data stay on the machine or in the district where it was created? Can petitions truly not be traced to the petitioner? Are small groups suppressed in reports that leave the district?
- **RQ2 Survival.** Does a district keep working when it is cut off, when several districts are cut off at once, or when its district head is lost? Do safety duties continue when the license expires?

- **RQ3 Accountable authority.** Do important decisions really need several parties? Is it true that untrusted data, or a single administrator, cannot approve anything alone? Are prohibited functions refused everywhere?
- **RQ4 Verifiability.** Can an outsider prove, using only their own tools, that no record was altered after the fact?
- **RQ5 Endurance and scale.** Does the system keep all its promises for 24 hours under random faults, and at the area's real size of 330 nodes?

1.5 Contributions

1. A full-size, four-tier deployment design for public-safety governance, with two data lanes that never merge, an incident workflow, and a mapping of the law onto mechanisms (Section 3).
2. A translation of the design into a 19-node simulation running the real heain-core, 20 test scenarios, and a method that checks evidence the system records itself (Section 4).
3. Round-by-round and scenario-by-scenario results passing all 306 checks, a 24-hour soak under 71 faults, and a 330-node scale test (Sections 5 and 6).
4. 21 changes to heain-core, 10 groups of new mechanisms, and an assessment of readiness against the needs of a real deployment (Sections 7 and 8).
5. Lessons, a comparison with existing systems, a four-phase pilot plan with indicators, limitations, and how to reproduce every result (Sections 9 to 12).

2. Background

2.1 The HEAIN Framework

The HEAIN Framework [11] arranges nodes as a fractal tree; every tier above Worker is a Master that differs only in scope. Work follows a seven-phase protocol: P1 intake and encryption, P2 leasing, P3 in-memory processing, P4 bounded result buffering, P5 the four-eyes policy gate, P6 role change when a parent fails, and P7 sovereignty-respecting knowledge sharing. Automatic survival is governed by Role Ceiling, which decides who may hold a role; Duty Profile, which decides what the holder may do; and Escalation Saturation, which decides how much may flow upward [7][8]. heain-core v1.3 added STANDALONE mode with a signed journal, witnesses that decide which side was cut off, and a two-tier Configuration API [10]. CineNexus Pro used a two-tier tree; this case uses four.

2.2 Transparency logs and time-stamping

Certificate Transparency publishes a Merkle tree of every certificate a CA issues, so anyone can prove two things: that an entry really is in the log (an inclusion proof), and that the log has only been appended to, with no earlier entry changed or removed (a consistency proof) [18]. Trusted time-stamping under RFC 3161 has a time-stamping authority (TSA) sign that a given hash existed at a given time [19]. This case applies both ideas to each node's audit chain. A leaf of the tree commits only to a record's hash, never its content, so outsiders can verify without seeing personal data.

2.3 Secret sharing

Shamir's scheme splits a key into n shares; any k of them rebuild it, and fewer than k reveal nothing about the key [23]. This case uses 2 of 3, so that no node ever holds a field machine's key whole.

2.4 Small-cell suppression

Statistical agencies routinely suppress table cells with counts small enough to identify a person, together with neighbouring cells from which such a cell could be derived (secondary suppression). ONS and CDC guidance uses a threshold of about 10 [26]. The author's earlier design used 5; this case raises it to $k \geq 10$.

2.5 Testing distributed systems

As in the first case, the soak injects random faults into a running system in the manner of chaos engineering [14], and checks evidence the system records itself rather than API responses alone. This case adds testing as an insider: someone with access to a machine's disk who tries to rewrite records without being caught.

3. Design of the Real Deployment

3.1 Users and requirements

The deployment serves the area's civil administration, namely the Southern Border Provinces Administrative Centre (SBPAC), the provinces, districts and sub-districts, together with an independent committee that oversees how the system is used. Those who benefit directly are citizens who want to report an incident, file a petition or claim compensation, and the relatives of detained persons. Five requirements make this case hard.

1. **Rights over data.** Camera footage and citizens' data stay where they are kept. Petitions must not be traceable to the petitioner. Reports leaving a district must suppress groups small enough to identify a person.
2. **No single hand.** Certifying an incident, searching past video or transferring a detainee requires several parties, including one independent of the security agencies, and an approval holds only for its own case and for a limited time.
3. **Records outsiders can trust.** Human-rights observers must be able to check with their own tools that no record was altered afterwards.
4. **Districts that can work alone.** A district cut off by an attack on a telecom tower or a power cut must keep warning, recording incidents and detentions, and report everything once it reconnects.
5. **An unsafe area.** Field machines may be stolen or destroyed, sensors may be forged, camera models may be biased against some groups, and AI records must name the model that produced them. Some functions, such as predicting individual behaviour or enrolling faces wholesale, must be strictly prohibited.

3.2 The four-tier architecture

The real deployment has four tiers that follow the structure of administration. Raw data stops at the district; only aggregates that have been sanitized may go up. Every decision that affects a person needs a second approver who is not from the security side alone, and every detention is recorded from the first minute. Figure 1 shows policy flowing down and data flowing up; Table 2 shows the duties of each tier.

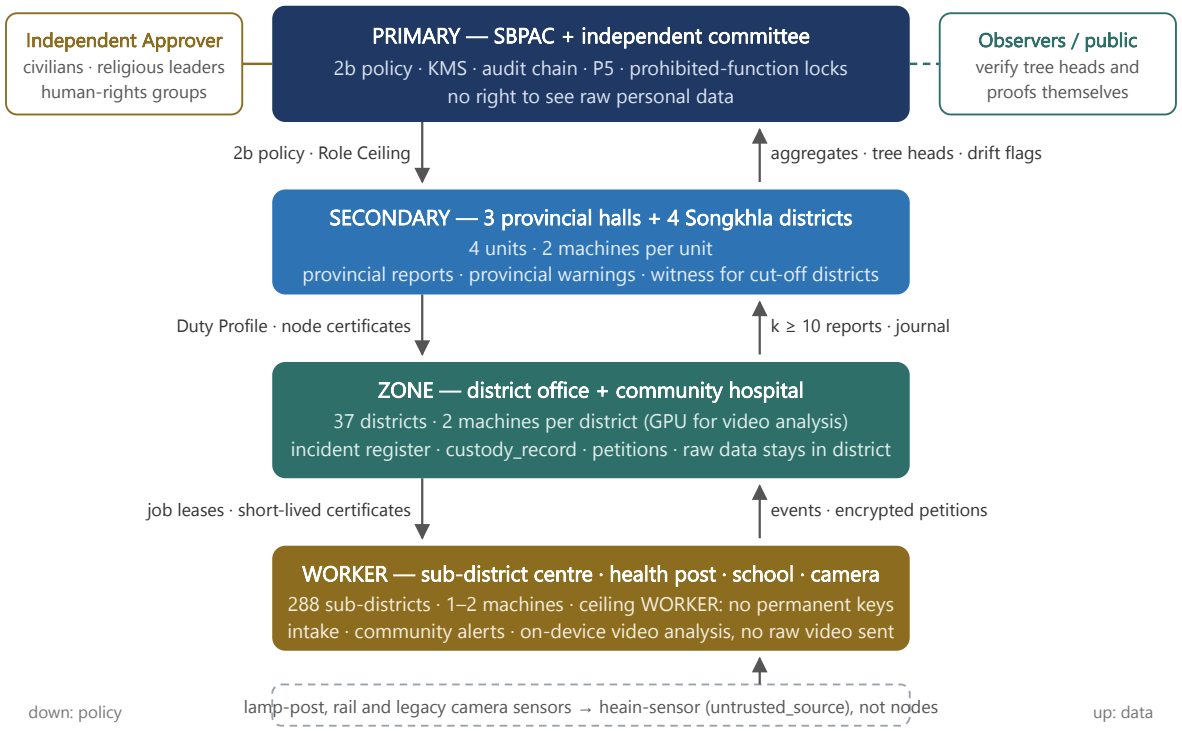


Figure 1 — The four-tier architecture of the real deployment: policy flows down (left), sanitized data flows up (right)

Tier	Location and number	Duties	What this tier cannot do
Primary	SBPAC and the independent committee, 1 unit	Sets 2b policy, issues node and app certificates, holds the root KMS, locks prohibited functions and the bias gate, receives tree heads from the provinces	See raw personal data; unlock a prohibited function on one party's say
Secondary	3 provincial halls and the unit for 4 Songkhla districts, 4 units of 2 machines each	Combines provincial reports, merges journals of cut-off districts, witnesses which district was cut off, holds the third share of Worker keys	Read reports not yet suppressed to k ≥ 10; hold a Worker key whole
Zone	District offices and community hospitals in 37 districts, 2 machines each (head + standby)	Incident register, custody_record, petitions, GPU video analysis, STANDALONE when cut off, a Duty Profile matching the law in force in that district	Send raw data out of the district; loosen a policy the Primary has locked

Worker	Sub-district centres, health posts, schools and camera points in 288 sub-districts, 1–2 machines each	Takes petitions, alerts the community, serves in local Malay, analyses video on the device, sends up only events and face-blurred stills	Hold permanent keys; become a Master; send raw video

Table 2 — Duties and limits of each tier in the real deployment

3.3 Two data lanes that never merge

The heart of the design is a permanent separation between data bound to a person and data about incidents, petitions and opinions. This line ensures that no one can know who petitioned or said what, and that no one can rewrite a custody record afterwards. The two lanes use separate app keys, and core refuses the same reference used across lanes.

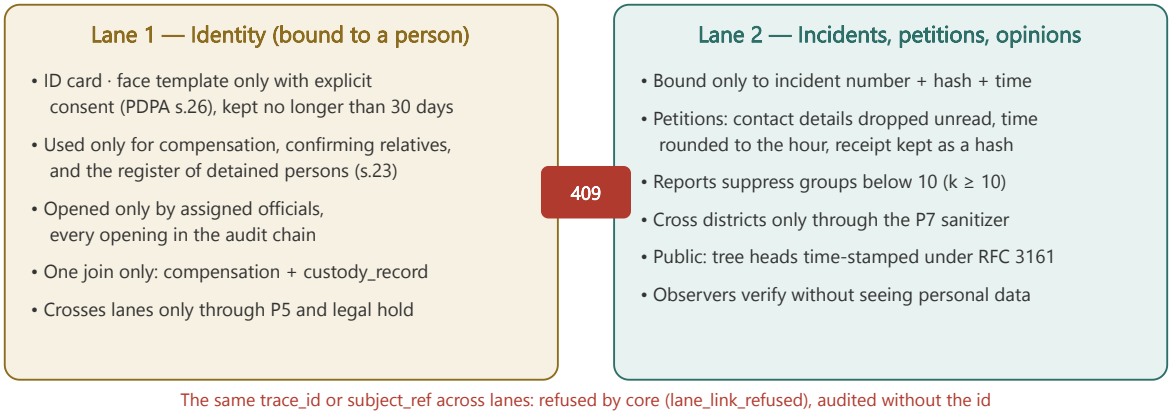


Figure 2 — Two data lanes that core keeps from being linked

3.4 Data policy

Data	How far it may go	HEAIN mechanism	Condition
Raw camera footage	Never leaves the camera machine	P1/P3 on the Worker itself	Only events and face-blurred stills go to the district head
Incident reports and custody records	In the district; hashes into the audit chain	Per-lane app keys, audit chain	Identity sealed with a core key, shown only to the arresting officer, every showing recorded
Petitions	Text only, up to the district	Unlinkable lanes	Contact details dropped unread; time rounded to the hour
Reports leaving a district	Province, Primary, other districts	Hierarchical P7 with k ≥ 10	Small groups and cells that would reveal them suppressed; each tier sanitizes again
Sensor readings	District head	heain-sensor, untrusted_source	HMAC per device and sequence numbers; never self-approved, even on the allowlist

Audit evidence	Hashes only, to observers	Transparency log	Signed tree heads, RFC 3161 time-stamps, and both kinds of proof

Table 3 — Data that may and may not leave a district

3.5 Workflow when an incident occurs

This sequence shows how all the mechanisms work together from detection to publication. The 48-hour and 30-day periods are design assumptions.

1. **Detect.** A camera-point Worker detects an abandoned object or a blast, processes it on the device, and sends only the event and a face-blurred still.
2. **Warn.** The district sends alert.public to communities and schools at once, within limits approved in advance. Simultaneous incidents at many sites are grouped by Escalation Saturation.
3. **Cut off.** Sibling districts and the province witness that the district has been cut off; the district head enters STANDALONE and writes its journal.
4. **Register.** An official records an encrypted incident_report and links its hash into the audit chain.
5. **Certify.** A three-party committee (police, military, civil administration) and an independent Approver certify it through P5 quorum, giving one set of figures for both compensation and statistics.
6. **Investigate.** A past-video search must be bound to a certified incident number, pass P5, and expires after 48 hours.
7. **Detain (if any).** Continuous audio and video recording; file hashes go into custody_record at once; the prosecutor and the district chief are notified automatically; relatives are notified through heain-notify unless a legal exception is approved through P5; a clock counts the days by legal basis (martial law 7 days, Emergency Decree 30 days).
8. **Publish.** Aggregates pass the P7 sanitizer ($k \geq 10$) up to the province and the centre, and tree heads are published for outsiders to verify.

3.6 Law and mechanism

Table 4 sets out the author's understanding of what each law requires or permits, and how the system makes that requirement real. It is not legal advice.

Law	Requires or permits	How HEAIN does it
Torture Act 2022, s.22	Continuous audio and video recording throughout arrest and detention; immediate notice to the public prosecutor and the district chief	Recording hashes into custody_record at once; gaps flagged to an Approver; the prosecutor and district chief notified automatically, with no identity in the job
s.23	Register of detained persons: identity, date, time, place, arresting officer, transfers, orders, physical condition before detention and before release	custody_record is append-only; an entry without the s.23 items is refused; no edit or delete afterwards; transfers need P5

ss.24–25	Interested persons may request information; refusal allowed on grounds of privacy or investigation	Requests queued with deadlines; refusals must pass P5 and enter the audit chain
Martial Law 1914 · Emergency Decree 2005	Detention without warrant for 7 days, and without charge for up to 30 days (37 days in all), in places other than police stations	Each district's Duty Profile states the legal basis; a clock warns before the limit; a basis not in force in that district is refused
Internal Security Act 2008	In force in 19 districts, including 4 in Songkhla	When an area's status changes, the regime in the system changes through P5; authority in the system never exceeds authority under the declaration
PDPA 2019, s.4(2)	Partly exempts agencies with security duties, which must still keep security standards	PDPA standards applied as 2b policy despite the exemption, so agencies using the system can be held to account
PDPA s.26	Biometric data needs explicit consent unless a legal exception applies	Faces only with consent or a court warrant, with an expiry; no area-wide face enrolment (a prohibited function)

Table 4 — Legal requirements and the mechanisms that make them real

3.7 What the system does not contain

Three groups of functions are locked at the Primary tier, and no district can unlock them: predicting a person's "suspicious behaviour", phone interception, and area-wide enrolment of citizens' faces. An app offering a capability in these groups, by name, name pattern or purpose, is refused at registration, before any Approver is asked. This lock keeps the system from becoming a surveillance tool, even if an administrator or agency later wants it to be one.

3.8 Mapping the requirements onto HEAIN mechanisms

- **Rights over data.** P2 zone affinity keeps a district's work in the district. Lanes declared unlinkable are enforced at run time. P7 sends reports up the hierarchy and suppresses groups smaller than k = 10 before they leave the district.
- **No single hand.** P5 quorum by approver group (police, military, civil administration and an independent seat). Approvals bound to a single record that expire. Data from outside the trust boundary is marked by core and never approved by rule automatically.
- **Records outsiders can trust.** A Merkle transparency log over each node's audit chain; signed tree heads time-stamped under RFC 3161 are pushed up the tree, and both kinds of proof are available to observers to check themselves.
- **Districts that can work alone.** Witnesses decide whether a district was cut off; STANDALONE and the journal keep work going; escrow and Role Ceiling decide who stands in for a lost district head.
- **An unsafe area.** Field machines' keys are wrapped with a key their parent holds, split 2 of 3. Node certificates are short-lived and renewed with new keys. Prohibited functions and the bias gate are

locked at the Primary. AI reasoning records are signed over canonical JSON (RFC 8785) [20] and must cite an approved model.

4. From Design to Simulation

4.1 The simulation's node map

The simulation reduces the real deployment to four tiers and 19 nodes while keeping every relationship the mechanisms need. The Primary (SBPAC with the independent committee) is the root and the issuer of certificates. Two provinces oversee two districts each. Each district has a district head, a standby and two Workers: a sub-district centre (t1) and a camera point (c1). Districts d1a and d2a are under the Emergency Decree; d1b and d2b are under the Internal Security Act. The area's full size is tested separately in D20 (Section 6.3).

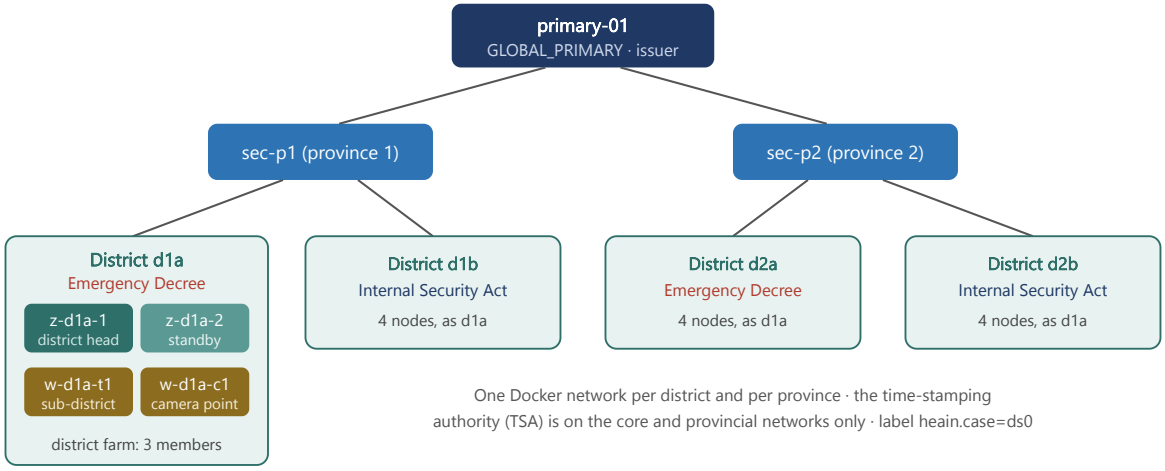


Figure 3 — The simulation's 4-tier, 19-node map, with district d1a shown in detail

Node	Tier	Ceiling	Duty and on failure
primary-01	GLOBAL_PRIMARY	none	Root of the tree; issues app and node certificates; locks policy for every tier
sec-p1, sec-p2	SECONDARY	SECONDARY	Merges district journals, acts as witness, and holds the third share of Worker keys
z-d1a-1 … z-d2b-1	ZONE (district head)	ZONE	Lost: the standby takes over; cut off: STANDALONE and journal
z-d1a-2 … z-d2b-2	WORKER (standby)	ZONE	Holds the district head's escrow; the only node that can stand in
w-*-t1, w-*-c1	WORKER	WORKER	Takes no authority; follows whoever holds the district; keys wrapped by the parent

Table 5 — Node register and duties in the simulation

4.2 The case's applications

Besides core, this case uses its own applications built on heain-sdk (dsapp), in three parts, and one simulated camera model.

- **dsapp custody** keeps custody records under sections 22–23: it checks mandatory entries, notifies through core jobs, seals identity with a core app key, keeps a day clock per legal basis, and sends the hash of every entry into core's audit chain before recording it itself.
- **dsapp petition** takes petitions: it drops contact details unread, rounds the time, keeps the receipt as a hash, and declares two unlinkable lanes in its manifest.
- **dsapp sensor** is a sensor gateway at the district head: HMAC per device, sequence numbers against replay, and rail.stop requests into P5.
- **ds-camdet 2.0** is the camera point's detector; it creates events and AI reasoning records that cite the model's hash.

4.3 Environment

Every scenario runs against the real heain-core on 19 nodes, as containers from one image on a single HP Z840 (88 CPUs, 31 GB of memory, an RTX 3080 Ti card). Each district has its own Docker network; a provincial network links district heads and standbys; and a core network links the provinces with the Primary. Cutting a district means detaching its two Zone machines from the provincial network. The time-stamping authority (OpenSSL ts) is reachable only from the core and provincial networks, so Workers and cut-off districts cannot reach it, as when a real district is cut off from the outside world.

The case apps and the load generators run in the network namespace of the node they belong to, because core hands keys and jobs only to apps on the same node. Approvers, administrators, observers and the insider are certificate holders driven by scripts. The insider's tools (insider/) change files on a node's disk directly, not through the API.

4.4 Design before running

Before running any scenario the author compared the case's requirements with core one by one: 25 requirements, 6 of them mechanisms core did not yet have. The author expected four scenarios (D5, D6, D9, D16) to fail and three more to pass only in part or to await a decision. The author's decisions of 12–14 October 2026 set the course: the transparency log lives in core, not in an app; 19 nodes first, with a scale round later; safety duties continue after the license expires, with a flag; P5 quorum as m of n by group; and every mechanism on at once in the soak.

4.5 Procedure

1. **Twelve rounds, each from zero.** Every round starts from empty data, then sets zones, legal regimes and apps through P5 as a real installation would.
2. **Check evidence.** Checks read what the system records itself: each node's audit chain, searches for raw data on every disk, traffic captures, and the observer's verification with its own tools, never API responses alone.

3. **A new round must not break an old one.** Every core fix reruns every earlier round of this case, together with 19 real-system regression suites, CineNexus rounds 1, 2, 3, 6 and 7, and the unit tests of every package.
4. **Commit only when everything passes.** Each step's script stops at the first failed check, every push is confirmed with git ls-remote, and the scripts are locked with flock against overlapping runs.

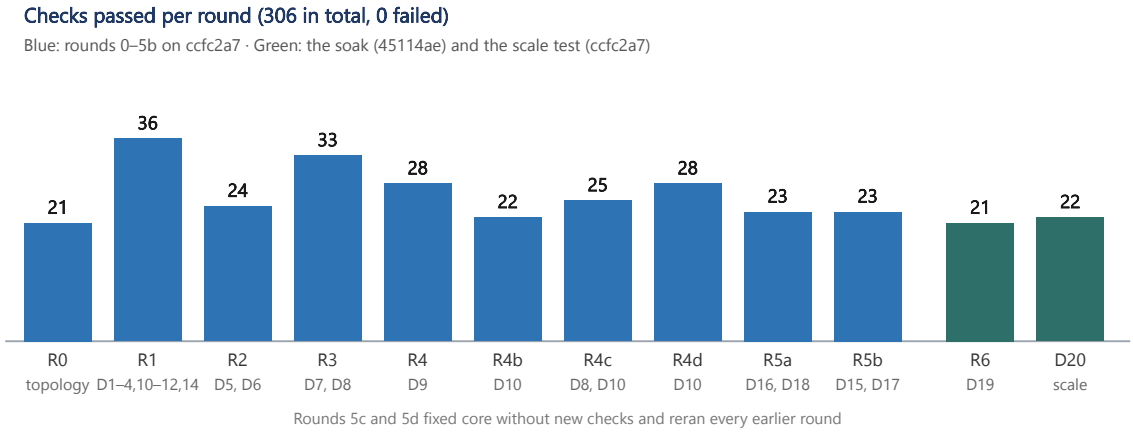


Figure 4 — Checks passed in each round, from the heain-core progress log

4.6 Compressing legal time

Long legal periods were compressed so they could be tested in real time. One day of detention equals 20 seconds; a 48-hour video-search approval equals 30 seconds; and a node certificate of 72 hours in the design lasts 3 minutes in round 4d, one hour in the soak and 6 minutes in the scale test. The ratio between the renewal interval and the certificate lifetime stays the same.

4.7 Limits of the method

All nodes run on one machine with one clock, the network has none of the real latency of a WAN, and the apps are models. The results therefore confirm that the system behaves as specified; they are not field measurements. The mapping of law onto mechanisms is the author's, not legal advice.

5. Results

5.1 Results by round

This section describes what each round checked, and what it found that required a change to core. Check counts are from the final run.

Round 0, topology and inheritance (21 checks, core 973574c). Checked the tier, ceiling and depth 0–3 of every node; parents in the Primary's fleet view; configuration inherited three levels down; zones and legal regimes attested through P5; each district's farm; apps three levels down; and a district job leased only to a Worker in that district. The first run found that app certificates issued at the Primary were refused two and three levels down, because only a farm Worker asked upward. Core now lets the head of every tier ask its parent, and answer for its children up to the issuer.

Round 1, survival (36 checks, core 1770493). Covered D1–D4, D10–D12 and D14, and found two problems. First, a district cut off from its province took the cut for a lost province, because its only witness was its standby, cut off with it. Core now lets the nodes holding a node's escrow prove only that the node is the cut-off side, never that its parent is lost. Second, a standby that had taken over kept asking the dead district head about app certificates, and a node that could not ask upward told its children "not valid". It now asks its new parent, and answers 503 when it does not know. This round also found that a stolen machine had audit.key, journal.key and kms.master.key on its disk. The author left this open, and it was closed in rounds 4b–4d.

Round 2, the committee and bound approvals (24 checks, core cfd4f7d). D5 certified an incident by P5 quorum of police, military, civil administration and one independent Approver seat; the rule was set once at the Primary and inherited by the districts. Three votes were not enough; an approver of no named group was refused; every vote was audited; the certification record named all four; and one party's rejection stopped it. D6 allowed a past-video search to be proposed only for a certified incident. Once approved, it held for a limited time; every use was audited; when time ran out it became EXPIRED; and another app could not use that approval.

Round 3, custody records and petitions (33 checks, commit 0bf9d11, apps only). D7 refused an arrest without the section 23 entries; told the prosecutor and the district chief at once through core jobs with no identity in them; sealed identity and showed it only to the arresting officer, recording every showing; allowed no edit or delete; refused a Decree basis in an Internal Security Act district; flagged records without a recording, near their limit and past it; and recorded a transfer only once an Approver approved it through P5. Because every entry's hash goes into core's audit chain first, an insider who rewrote the log and re-linked the whole chain was caught by GET /verify. D8 dropped contact details unread, gave the district the text only, and refused any link between a petition and a person. This round found that lanes.unlinkable was checked only at registration, not enforced at run time; that was closed in round 4c.

Round 4, transparency (28 checks, core 64b8e6a). D9 built the transparency log into core. Every node keeps a Merkle tree (RFC 9162) over its own audit chain, signs a head when it grows, has it time-stamped by the TSA (heads wait while the TSA is unreachable and are stamped after the heal), and pushes it to its parent, which accepts it only when consistent with the head it holds. The observer checked signatures, certificates and time-stamps with openssl, and the proofs with its own RFC 9162 code. An insider on a Worker rewrote a record and re-linked the chain: the Worker's own chain check passed, but its district head refused the next head (TL.inconsistent) and the observer's consistency check failed. P7 along the hierarchy became the new default, and the district's monthly report suppressed a group of 3, and a group of 11 that would have revealed it (secondary suppression), before leaving the district.

Round 4b, keys off the disk (22 checks, core 6e14ebe). With security.worker_keys = parent set at the Primary, every Worker moved its permanent keys into a form wrapped by a KEK its district head holds. A Worker restarted in its district worked on. A Worker carried off and started on another network could not open its keys and never started. With the district head lost, the standby released the KEK from

escrow. Once a Worker's certificate was revoked, its head destroyed its KEK, and the machine could never open its disk again.

Round 4c, 2-of-3 shares and unlinkable lanes (25 checks, core cea5b17). The district head, the standby and the province each hold one Shamir share of the KEK; no node holds it whole. A Worker restarted, in a cut-off district, or with its head lost still started with two shares; with only the head's share reachable it did not. The standby could not obtain the province's share while the head was still reporting, and a revoked Worker's shares were destroyed in all three places. This round also enforced lanes.unlinkable at run time: the same trace_id or subject_ref on the two lanes was refused with 409 lane_link_refused and audited without the id.

Round 4d, short-lived node certificates (28 checks, core 5f944c9). The node-issuing CA at the Primary issued every node a certificate through the tree. Each node renewed at half its lifetime with a new key, without a restart, and the originally installed certificate was refused afterwards. A thief who copied a node's key and renewed first was caught at the real node's next renewal (superseded_certificate). Revoking by node name shut out every certificate naming it and destroyed its key shares. A cut-off district received an ALERT when a quarter of the lifetime was left, and a district cut off for longer than the lifetime was refused, failing closed.

Round 5a, prohibited functions and the license (23 checks, core bd6eaa0). D16 set apps.denied_capabilities (behavior.predict, face.enroll.*, purpose:behaviour_prediction, purpose:mass_biometric_enrollment) and apps.require_purpose at the Primary and locked them; a district could not loosen them. Apps offering a listed name, pattern or purpose were refused at registration before any Approver was asked; a capability with no purpose, or one outside the catalogue, was refused; and an app registered before its capability was listed was suspended. D18 expired the license on all 19 nodes: the incident register and the camera point went on, marked license_exempt; other jobs were refused as before; and a new license restored everything.

Round 5b, untrusted data and the bias gate (23 checks, core d006a4b). D15 refused a forged reading, a replayed reading and one from an unknown device, and core marked every reading untrusted_source. Although rail.stop was on the allowlist, the sensor's request waited for a person, while the incident register's own request was approved at once, and a register job derived from the sensor's incident also waited. D17 refused, before any Approver saw them, a camera model whose false-positive rate differed between two groups (0.24 against 0.04) and a model evaluated on groups too small to judge; core computed the metrics itself from the raw counts. AI records citing an unapproved hash were refused at the camera point. The round found a deadlock: the ai.approved_models validator read the store while the store held its own lock. The bias gate now runs when a value is proposed, outside the lock, and a unit test with a timeout guards it.

Rounds 5c and 5d, fixes without new checks (core 9e38faa, 45114ae). Round 5c closed three items left open by round 5b: a node with no promote directory keeps its acting state under its data directory; zone key sync opens its store only when a key arrives; and Raft files committed by mistake were removed from git. Round 5d fixed the problem found by the 40-minute soak trial; see Section 6.1.

5.2 Results by scenario

Every scenario passed in the final run of 16 October 2026: rounds 0–5b on heain-core commit ccfc2a7 (263 checks), the soak on 45114ae (21) and the scale test on ccfc2a7 (22), for 306 checks with none failed. D13 was not run as a separate scenario; its content is in round 0, D7 and D14. The evidence column is what the scripts actually checked.

Test	Subject	Round	Evidence that passed
D1	Raw footage stays on the camera machine	1	No raw bytes on the disks of the other 18 nodes, none unencrypted on the camera's own disk, and none in 134,694 bytes of captured traffic
D2	District cut off	1	The district head knew it was the cut-off side (STANDALONE); work ran in the district; the journal (1..26) merged once, in order
D3	3-second network flap	1	Not taken for a cut-off; no STANDALONE
D4	Wave: 75 incidents in 4 districts cut off at once	1	352 journal entries merged once, none lost, 41 s after the heal; all 4 districts throttled with 429
D5	Incident certified by a four-party committee	2	Three parties not enough; the independent seat completed it; one rejection stopped another case; outsiders got 403
D6	Video search bound to one certified incident	2	Unknown or uncertified incidents refused; the approval held only for its own case, then expired and was refused
D7	Custody record	3	Section 23 entries required; section 22 notice at once with no identity; append-only; a rewritten log did not match core's hashes
D8	Untraceable petitions	3, 4c	Contact details dropped unread; the district got text only; linking refused (403); the same id on two unlinkable lanes refused (409)
D9	Transparency and k ≥ 10	4	Signed, time-stamped heads verified with the observer's own tools; a rewrite on a Worker caught by both its district head and the observer; groups of 3 and 11 suppressed
D10	Worker stolen	1, 4b–4d	Revoked on all 18 nodes in 24 s; no unencrypted key on disk; could not start once carried off; a copied key caught at renewal
D11	Camera Worker destroyed	1	Removed from the farm; the district worked on; a replacement joined
D12	District head lost	1	The standby took over in 14 s; Workers stopped at their ceiling and followed; a queued job ran; the role was handed back
D14	Emergency Decree lifted in a district	1	Regime changed through P5 on all 4 of the district's nodes; a single administrator could not approve it
D15	Sensors outside the trust boundary	5b	Forged, replayed and unknown readings refused; an allowlisted rail.stop from a sensor still waited for a person
D16	Prohibited functions	5a	Refused at registration before any Approver, by name, pattern or purpose; districts could not unlock them

D17	Bias gate	5b	A model with false-positive rates of 0.24 and 0.04 refused before any Approver; an unapproved build refused at use
D18	License expired	5a	The incident register and camera point went on (flagged); everything else degraded; a new license restored all
D19	24-hour soak	6	272,321 jobs, none lost or duplicated; 71 faults; flat memory; every chain verified
D20	Scale: 330 nodes	D20	All 22 checks: fleet view, inherited settings, cut-offs, lost district heads, certificates, transparency

Table 6 — Results of the test scenarios in the final run

6. The Soak, the Platform Round and the Scale Test

6.1 The 24-hour soak (D19)

From 14 to 15 October 2026 every mechanism this case built was on at once: Worker keys held by the parent and split 2 of 3, node certificates of one hour, the transparency log with the TSA, k ≥ 10, quorum and bound approvals, the allowlist, prohibited functions, the purpose rule, the bias gate set to refuse, and the locks. All were set at the Primary through P5 and reached the deepest tier (w-d2b-c1, three levels down), locks included. Load ran in all four districts without a pause: camera events at the camera points, district jobs run at the sub-district Workers, and incidents journaled to the provinces. A P5 cycle ran every 15 minutes at d1a, and a script injected a fault about every 20 minutes, of every kind that can be undone.

Aspect	Result
Jobs	162,242 camera events (about 40,500 per district) and 105,429 district jobs, each delivered once (worst p99 217 ms and 267 ms; no submission retried); 272,321 completions, each ticket once
71 faults	22 district cut-offs, 8 flaps, 10 waves of 2–4 districts, 10 Worker restarts, 8 district heads stopped, 13 app kills
Waves	4,650 jobs submitted inside cut-off districts, each delivered once
Journal	81,465 entries (d1a 22,083, d1b 25,659, d2a 18,521, d2b 15,202) merged once at the provinces; district heads entered STANDALONE 11–22 times each
Governance	94 P5 cycles, each as designed: incident certified by 4 groups; the sensor's rail.stop waited; the register's own approved at once; the approved model's record accepted and another build's refused; a prohibited app refused
Keys and certificates	Every node renewed its certificate 48 times, through restarts and stopped heads; all 8 Workers' keys stayed wrapped through every restart
Transparency	No head refused as inconsistent anywhere; every head of the 11 nodes that reach the TSA time-stamped, including those made while cut off
State at the end	All 19 nodes healthy, none STANDALONE; each district head holding its own district again; no critical alert left; audit chains verified on all 19 nodes

Table 7 — Results of the 24-hour soak under random faults

Table 8 shows the resources of a representative node of each kind, comparing the 10–20% window with the last 10% of the run. The district head's anonymous memory grew early and was flat in the last 10%; heap, goroutines and open files were flat on every node.

Node	CPU (%)	RSS anon (MB)	heap (MB)	goroutines	open files	data growth (MB/h)	audit (records)	full verify (ms)
primary-01	0.9 → 0.9	23 → 33	11 → 14	40 → 40	36 → 36	+20.8	35,103	580
sec-p1	3.7 → 3.7	28 → 56	14 → 20	50 → 50	40 → 40	+24.1	79,533	2,577
z-d1a-1	8.6 → 11.2	28 → 94	16 → 26	60 → 60	48 → 49	+30.9	189,407	4,137
z-d1a-2	1.0 → 0.9	19 → 21	8 → 9	36 → 36	29 → 29	+0.4	87	2
w-d1a-c1	3.8 → 4.5	27 → 79	15 → 19	46 → 46	33 → 33	+18.1	162,456	2,634
w-d1a-t1	2.5 → 4.1	24 → 34	13 → 16	45 → 45	32 → 32	+6.2	27,690	666

Table 8 — Resources of representative nodes during the soak (early window → final window)

The trial before the soak. A first 40-minute trial on core 9e38faa passed 19 of 21 checks. The two failures were harness faults: AI record files were out of the app's reach, and the time-stamp check read between two ticks. But the trial also exposed a core problem. Every 5 seconds each node decoded every signed tree head it had ever made, and a parent decoded all of a child's heads on every push. A busy district head makes about 17,000 heads a day (about 7 KB each); reading them all took 1.1 s, or about 3.4 s of every 5-second tick by the end of a day. In the trial the Primary's CPU rose from 2.6% to 19% under a steady load. Core 45114ae therefore reads the newest head from the last key of its bucket, keeps a separate index of heads not yet time-stamped, and has a parent read only the largest head it holds for a child: 1 ms per tick at 17,000 heads. After that the 40-minute trial and the soak passed all 21 checks.

6.2 The platform round

The disaster-warning case that follows runs on small boards in the field and workstations in offices, so the author decided to make core build everywhere before the scale test. Everything that depends on the operating system now sits in one package (internal/platform): free disk space, memory, app processes and core restarting itself. Accelerators are discovered in layers (internal/accel): nvidia-smi, Linux DRM cards from NVIDIA, AMD and Intel, Jetson, Apple silicon, and what an administrator declares for an NPU. A job can ask for an API (requirements.gpu_api, such as CUDA or ROCm) instead of a vendor.

A cross-compile gate stops any commit that does not build on Linux amd64, arm64 and arm, macOS arm64 and amd64, and Windows amd64 and arm64. Linux on RISC-V is not a target yet, because one indirect dependency (boltdb) does not build. Every round of both case studies passed again on the new core (ccfc2a7).

6.3 The scale test (D20)

The 19-node map stands for an area of 37 districts. D20 ran the area at its real size, core only with no case apps: 1 Primary, 4 provinces (Pattani 12 districts, Yala 8, Narathiwat 13, Songkhla 4), 37 district heads, 37 standbys and 251 Workers, 330 nodes on 42 networks on one machine.

Aspect	Result
Start-up	330 containers in 174 s; every node reported its designed tier, ceiling and depth within 6 s
Fleet view	The Primary listed all 329 nodes below it, each under its designed parent (4 levels), in 0.02 s (286 KB); each province saw only its own districts
Configuration	A value set at the Primary reached all 329 nodes: half in 15 s, 95% and all in 28 s
4 districts cut at once	District heads knew they were the cut-off side in 10 s; the other 33 stayed normal, with no false cut-off; normal again in 31 s
3 district heads lost at once	Standbys took over in 15 s; all 19 Workers followed in 16 s, none rising above its ceiling; roles handed back in 57 s
Short-lived certificates	Issued to all 330 nodes through the tree in 30 s; renewed at half-life with new keys, no errors
Transparency	No head refused on any of the 42 tier heads; the Primary holds the provinces' heads, each province its districts', each district head its standby's and Workers'
Logs and chains	No panic in 330 logs; audit chains verified on all 330 nodes; 5,433 parallel calls with none retried; the round took 7 minutes

Table 9 — Results of the 330-node scale test

Tier	Count	Memory avg / max (MB)	CPU avg / max (%)
Worker	251	17.9 / 22.9	1.6 / 5.1
Standby	37	18.3 / 23.6	1.7 / 4.7
District head	37	21.1 / 24.2	9.6 / 20.9
Province	4	25.2 / 29.2	8.0 / 14.9
Primary	1	27.1 / 27.1	3.5 / 3.5

Table 10 — Resources by tier at the end of the scale test (5.9 GB in all for 330 nodes)

The scale test took four runs, with core unchanged throughout. In the first two, 25–40% of the checker's calls failed, from the host and from inside the networks alike, while every check that did not fan out passed. The cause was the kernel's ARP table, which has 1,024 entries shared by every container on the machine, overflowing. Raising its limits to 4096/8192/16384 fixed it. The third run passed 21 of 22, because the checker read the two Workers started last before they knew their depth; the checker now

asks again for up to two minutes. In the field every node is its own machine, but a single server running hundreds of nodes needs the same setting.

7. What heain-core Changed Because of the Case Study

The case study led to 21 changes in 12 core commits. Ten groups are new mechanisms the first case did not need; the rest fix problems the scenarios actually found.

#	New mechanism	What it does	Tests
1	P5 quorum by group	m-of-n approval that needs every named approver group	D5
2	Bound approvals	An approval bound to one record (bound_to) that expires (valid_for)	D6
3	Transparency log	Merkle tree (RFC 9162) over the audit chain, signed heads, RFC 3161, heads pushed up the tree, proofs for observers	D9
4	Hierarchical P7 and k-suppression	Reports go up one tier at a time, sanitized again at each; small groups and neighbouring cells suppressed	D9
5	Worker keys held by the parent, split 2 of 3	Permanent keys wrapped by a KEK shared among district head, standby and province; destroyed on revocation	D10
6	Unlinkable lanes	Enforced at run time: the same id across lanes refused; keys per lane	D8
7	Short-lived node certificates	Issued through the tree, renewed with new keys, clones detected, revocation by node name	D10
8	Prohibited functions	Refusal by name, pattern and purpose; locked from the Primary; registered apps suspended	D16
9	Untrusted data and the bias gate	core marks untrusted_source and never self-approves it; computes fairness itself; enforces the approved model at use	D15, D17
10	Safety duties beyond the license	Capabilities named through P5 continue after the license expires, flagged and audited	D18

Table 11 — Ten groups of new mechanisms this case study added to core

Round (tests)	Commit	What changed
Platform	ccfc2a7	One package for everything OS-dependent; accelerators beyond NVIDIA and gpu_api; a seven-target cross-compile gate
5d (soak trial)	45114ae	The transparency log reads the newest head, the unstamped heads and a child's largest head from an index, without decoding every head

5c	9e38faa	A node with no promote directory keeps its acting state under its data directory; the zone key store opens only when a key arrives
5b (D15, D17)	d006a4b	core marks proposals based on untrusted data and never approves them by rule; computes the fairness gate itself; enforces the approved model at use; fixes a configuration deadlock
5a (D16, D18)	bd6eaa0	Prohibited functions by name, pattern and purpose, locked from the Primary; registered apps suspended; safety duties exempt from license expiry
4d (D10)	5f944c9	Short-lived node certificates issued through the tree, renewed with a new key at half-life, with proof of possession and clone detection
4c (D8, D10)	cea5b17	The Worker KEK split 2 of 3 among district head, standby and province; unlinkable lanes enforced at run time
4b (D10)	6e14ebe	Worker keys wrapped by a key the district head holds, escrowed to the standby, destroyed on revocation
4 (D9)	64b8e6a	Merkle transparency log (RFC 9162) with an RFC 3161 client; heads pushed up the tree; k-suppression in P7; hierarchical P7
2 (D5, D6)	cfd4f7d	P5 quorum by approver group; approvals bound to a record, with an expiry
1 (D2, D12)	1770493	Nodes holding a node's escrow cannot claim its parent is lost; a node that took over asks its new parent, and answers 503 when it does not know
0	973574c	App certificates issued at the Primary are checked up the tree, not only by farm Workers

Table 12 — Changes to heain-core arising from the case study, most recent first

8. Readiness against the Real Deployment

Before the case study began, the author's design brief listed what core did not yet have and had to gain before a pilot. Table 13 gives the status of each item after the case study.

Needed before a pilot	Status	Evidence
Public tree heads + RFC 3161 + proofs	Built	core 64b8e6a; D9, D19, D20
P7 reports suppressing small groups, k ≥ 10	Built	core 64b8e6a; D9
Video-search rights bound to an incident, expiring after 48 h	Built	core cfd4f7d; D6
Append-only custody_record + notice under s.22	Built (case app)	dsapp custody, hashes into core's audit; D7
Detention day clock by legal basis per district	Built (case app)	D7 (compressed: 1 day = 20 s)
heain-sensor untrusted_source path	Built	core d006a4b; D15

District-level Zone tier (4 tiers)	Working	Round 0; D20 at 330 nodes
alert.public while STANDALONE	Not yet tested	D2 tested jobs and the journal while cut off; community alerts not yet tested as a separate scenario
Audit retention policy	Not yet	District heads grow about 31 MB per hour (Section 11)
Strict defaults	Available, not yet default	All on in D19; to be decided before Alpha

Table 13 — What was needed before a pilot, and its status after the case study

Beyond the planned items, the case study added mechanisms the brief did not list: Worker keys split 2 of 3, short-lived node certificates with clone detection, P5 quorum by group, prohibited functions enforced in core, a bias gate enforced at use, and safety duties that continue after the license expires.

9. Discussion

9.1 Answers to the research questions

RQ1. Raw footage never left the camera machine, confirmed by searching the disks of the other 18 nodes and by traffic capture (D1). Petitions reached the district as text only and could not be linked to anyone; even an app holding both lanes could not link them through core (D8). Reports left the district with small groups suppressed (D9). **RQ2.** Districts kept working when cut off one at a time, in a wave of four, or 22 times in one day, and merged their journals once, in order (D2–D4, D19). A lost district head was replaced by its standby in 14–15 seconds (D12, D20). Safety duties outlived the license (D18). **RQ3.** No decision tested could be made by one party: three of four seats were not enough; approvals held only for their own case and expired; sensor data waited for a person even on the allowlist; and prohibited functions were refused before reaching any Approver (D5, D6, D14–D17). **RQ4.** The observer verified signatures, time-stamps, inclusion and consistency with its own tools, and caught an insider's rewrite where the node's own chain check missed it (D9). **RQ5.** The system kept every promise through 24 hours and 71 faults (D19) and at the area's full size of 330 nodes (D20).

9.2 Lessons

- **A local chain is not evidence.** An insider who rewrote a record and re-linked every later hash passed the node's own chain check. Only a tree head held by someone else, the parent or an observer, exposed it. Records meant to convince outsiders need a copy of their commitment off the node.
- **Multi-party decisions belong in core.** Quorum, binding and expiry could be app logic, but each app would enforce them differently, or not at all. In P5 they apply to every action alike.
- **Trust must be marked by core.** If an app could set or clear the untrusted mark itself, the mark would mean nothing. Core sets it from the manifest and from the trace that started the work.
- **Witnesses must not be cut off together.** A district whose only witness was its own standby wrongly concluded that its province was lost. Nodes holding escrow can prove only that the other side is the

cut-off side.

- **Costs that grow with history show only in long runs.** The transparency log read every head on every tick; nothing but a soak exposed it. The audit check still verifies the whole chain each time.
- **A scale test tests the machine too.** At 330 containers the kernel's ARP table overflowed before core showed any strain at all.

9.3 The night of 22–23 August 2026 as a test of the architecture

That night there were attacks at 75 sites in 4 provinces, mostly arson; 11 people were injured and none killed. Seventeen buildings, 40 vehicles, 32 lamp posts, 4 cameras and telecom towers were attacked. The announced count rose in steps from 34 to 51 to 75, while Reuters counted 78 [22][27]. Table 14 shows which mechanism and scenario each feature of that night corresponds to.

Feature of the attacks	What the architecture must do	Tests
Lamp posts and cameras were targets	Workers hold no permanent keys; a destroyed or seized device leaks no data and can be replaced	D10, D11
Telecom towers were attacked	Districts work STANDALONE and return their journals in full on reconnecting	D2, D4, D19
75 incidents in a few hours, many districts at once	Merge a wave of journals once, and rate-limit so the receiver is not flooded	D4 (352 entries in 41 s)
Announced figures changed in steps	One register with every version time-stamped, the same figures for every party, verifiable afterwards	D5, D9

Table 14 — Features of the attacks of 22–23 August 2026 and the mechanisms that address them

9.4 Comparison with existing systems

Table 15 compares the approach of systems described in public reports with the HEAIN approach. The information on existing systems comes from the news reports and organizations cited, not from the author's own inspection.

Dimension	Existing systems as reported	HEAIN
Raw data	Gathered centrally by security agencies	Stays in the district or on the recording machine, every piece encrypted
Who decides on use	The unit holding the data	Proposer + independent Approver (P5 quorum)
Record of use	None, or not disclosed	Audit chain + public tree heads
Biometrics	Face verification for SIM registration of 888,813 numbers (2019–20) and DNA collection in at least 139 complaint cases (Jan–Sep 2019) [28][29]	Only with consent or a court warrant, with an expiry; wholesale enrolment is a prohibited function

AI cameras	AI announced for about 8,200 cameras (2020), with models and functions undisclosed [30]	Model registry + bias gate + approved build enforced
Custody records	Audio-video recording under s.22 not yet consistent in the area [31]	Hashes into custody_record at once; prosecutor and district chief notified automatically
When cut off	The centre loses sight of the area	STANDALONE + journal, nothing lost or duplicated
Statistics	Two sets, differing by 13,420 incidents	One register, every version verifiable

Table 15 — Existing systems compared with HEAIN

9.5 Threats to validity

Internal. The developer wrote the scenarios and scripts, so cases nobody anticipated may be missing. **External.** One machine, one clock and a virtual network say nothing about real latency, packet loss or clock drift; the apps are models; and the legal interpretation is the author's. **Measurement.** Each figure comes from a single run, and long legal periods were compressed into seconds. **Context.** A technical system cannot solve a problem of trust by itself; it can only make its users' commitments verifiable.

10. Pilot Plan and Indicators

10.1 A four-phase pilot

A pilot must pass each phase's gate before it expands, and starts with the lane not bound to identity, to build trust before touching detention data.

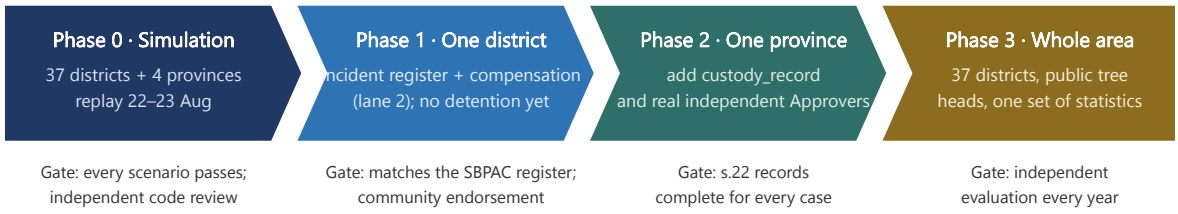


Figure 5 — A four-phase pilot, passing a gate before each expansion

Phase 0 uses a simulation like this case study's, expanded to 37 districts with the case apps, and replays the sequence of the night of 22–23 August. Phase 1 starts in one district with the incident register and compensation only. Phase 2 expands to one province and adds custody records, with real independent Approvers from civil society and religious leaders. Phase 3 covers the whole area and publishes tree heads to the public.

10.2 Success indicators

Indicator	Target
New incidents counted differently by two data sets	0 (one register)
Detentions with audio-video recording and notice complete under s.22	100%
Video-search requests not bound to a certified incident	0
Journal entries lost or duplicated after a district reconnects	0
Tree heads published on time and verified	100%
Time from detection to community warning	set with each district

Table 16 — Success indicators for the pilot

10.3 Risks outside the system

- **The PDPA exemption for security agencies.** Using this standard needs a resolution or regulation behind it, not an agency's goodwill.
- **Trust.** Allegations, reported in June 2026, of phone interception affecting about 2,000 people [32] put any new system at risk of being seen as a surveillance tool. The plan therefore starts with lane 2, which is not bound to identity, and makes religious leaders and civil society Approvers.
- **Peace talks stalled since July 2026** [33]. The system should be set up as public-service infrastructure, not tied to rounds of negotiation.
- **Physical attack.** Workers and telecom towers can be destroyed; this is met with Role Ceiling, STANDALONE and encrypted backups.

11. Limitations and Open Items before Alpha

- **It is a simulation.** This deployment has never run in any district or on a real network, and no agency has reviewed it.
- **Audit checks grow with the chain.** At the soak's load a month holds about 5.7 million records, and a full check takes about two minutes. Checking from a verified checkpoint is the next step. Building transparency proofs also still reads every leaf.
- **No retention policy yet.** A district head grows about 31 MB per hour (about 12.7 MB of it audit). The log's leaves and heads are already kept apart from the audit records, so that deleting old records later will not break the proofs.
- **Taint is per node.** A trace started by an untrusted app on another node is not yet known as tainted on this one.
- **An expired short-lived certificate has no way back.** A district cut off for longer than the certificate lifetime must re-enrol, for example through P5.
- **Few witnesses.** A cut-off district head asks only one witness outside its farm, even in a province of 13 districts. More witnesses would make the decision harder to fool.

- **Community alerts while cut off.** alert.public during STANDALONE has not yet been tested as a separate scenario.
- **Other platforms build but have not run.** Core builds on macOS and Windows but has never run as a node there; RISC-V is not a target yet.

The next step is to close these items and run the third case study, a national disaster-warning system, which adds battery-powered field nodes and nearly a thousand districts.

12. Evidence and Reproducibility

Every core commit is confirmed with git ls-remote on every remote; the final core commit is ccfc2a7. The scripts are in the repository under casestudies/deepsouth/: sim.sh and lib.sh (the 19-node simulation), round0.sh to round6.sh with rounds 4b–4d and 5a–5b, apps/ (the case apps), insider/ (the insider's tools) and scale/ (scale.sh, d20.sh, pget.py). Each round's results are recorded with its commit in the progress log [12]. Each round commits only when every check passes, and each step's script is locked with flock against overlapping runs.

To reproduce, check out heain-core commit ccfc2a7, run casestudies/deepsouth/sim.sh build and up, then each round's script. The scale test uses scale/scale.sh up, and on a single machine the kernel's ARP limits must be raised (net.ipv4.neigh.default.gc_thresh1/2/3 = 4096/8192/16384). The test machine needs only Go and Docker.

Result file on the test machine	Contents
/mnt/xfs_nvme/heain-ds0/sim	The 19-node simulation (label heain.case=ds0)
/mnt/xfs_nvme/heain-ds0/sim/r6, r6-trial	The soak and the 40-minute trial: per-node readings, events, round results
/mnt/xfs_nvme/heain-ds0/scale/r	The scale test: every parallel call's answer and the checker's results
~/ds6.out, ~/ds7.out, ~/ds8d.out	Output of the soak, the platform round and the scale test, with the regression suites
docs/progress-log.md	Each round's results with its commit

Table 17 — Evidence files from the tests

13. Conclusion

The southern border provinces case study shows that the HEAIN Framework can carry the commitments a state agency must keep but a company need not: no single hand decides, outsiders can verify the records, and what a person reports is never linked to who they are. heain-core passed every scenario across 306 checks on a 19-node, four-tier simulation; ran for 24 hours under 71 random faults without losing or duplicating any of 272,321 jobs; and behaved the same at the area's real size of 330 nodes, using only 5.9 GB of memory in all. Just as important, the case found what paper design could not: a

local chain an insider could re-link, witnesses cut off together, costs that grow with history and show only in a soak, and the limits of the machine itself at scale. The 21 changes made core stronger, every result is reproducible, and the four-phase pilot plan lays out a gated path from simulation to real use. The next case, a national disaster-warning system, will test this same core with battery-powered field nodes and nearly a thousand districts.

References

[1] Boonma, J. "Hybrid Edge AI Node: A Fractal Governance Architecture for Sovereignty-Aware Distributed AI Processing." Zenodo, 2026. DOI: 10.5281/zenodo.22851257

[2] Boonma, J. "Hybrid Edge AI Node: สถาปัตยกรรมการกำกับดูแลแบบยืดหยุ่นสำหรับการประมวลผล AI แบบกระจายศูนย์ที่เคารพอธิปไตยข้อมูล." (Thai edition) Zenodo, 2026. DOI: 10.5281/zenodo.22851587

[3] Boonma, J. "HEAIN Core Protocol: A Normative Specification for Collective Intelligence in Fractal Edge AI Governance." Zenodo, 2026. DOI: 10.5281/zenodo.22858845

[4] Boonma, J. "HEAIN Core Protocol: ข้อกำหนดเชิงบรรทัดฐานสำหรับปัญญาร่วมในการกำกับดูแล AI แบบยืดหยุ่นที่ขอบเครือข่าย." (Thai edition) Zenodo, 2026. DOI: 10.5281/zenodo.22858994

[5] Boonma, J. "The Intelligent Network of the Future — Empirical Proof of the HEAIN Core Protocol (HEAIN-CORE-1.1)." Zenodo, 2026. DOI: 10.5281/zenodo.23060556

[6] Boonma, J. "โครงข่ายอัจฉริยะแห่งอนาคต บทพิสูจน์เชิงประจักษ์ของ HEAIN Core Protocol (HEAIN-CORE-1.1)." (Thai edition) Zenodo, 2026. DOI: 10.5281/zenodo.23061474

[7] Boonma, J. "The Triad of Structural Immunities: A Theoretical Framework for Preventing Cascading Failures, Authority Creep, and Alert Storms in Fractal Edge AI." Zenodo, 2026. DOI: 10.5281/zenodo.23172868

[8] Boonma, J. "สามประสานภูมิคุ้มกันระดับสถาปัตยกรรม: กรอบทฤษฎีเพื่อป้องกันความล้มเหลวแบบลูกโซ่ การลุกลามของสิทธิ์ และ Alert Storm ในปัญญาประดิษฐ์ที่ขอบเครือข่ายแบบแฟร็กทัล." (Thai edition) Zenodo, 2026. DOI: 10.5281/zenodo.23172979

[9] Boonma, J. "Multi-Level Role Succession: HEAIN Core Protocol 1.2 (HEAIN-CORE-1.2)." 2026 (companion paper).

[10] Boonma, J. "Standalone Survival and Self-Governance: HEAIN Core Protocol 1.3 (HEAIN-CORE-1.3)." 2026 (companion paper).

[11] Boonma, J. "HEAIN Framework: An Infinitely Scalable Fractal Intelligent Network Seamlessly Linking Cloud and Edge AI, Resilient to Failure and Multi-Dimensional Fraud." 2026 (companion paper).

[12] Boonma, J. "design-notes/n-tier-generalization.md" and "docs/progress-log.md." heain-core repository, 2026.

[13] Boonma, J. "The CineNexus Pro Case Study on heain-core: Whole-System Validation of the HEAIN Framework through an 11-Node Simulation, 25 Test Scenarios and a 24-Hour Soak under Random Faults." 2026 (companion paper).

[14] Basiri, A., Behnam, N., de Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., and Rosenthal, C. "Chaos Engineering." IEEE Software, 33(3), 2016, pp. 35–41.

[15] Personal Data Protection Act, B.E. 2562 (2019), Thailand.

[16] Emergency Decree on Public Administration in Emergency Situations, B.E. 2548 (2005); Internal Security Act, B.E. 2551 (2008); Martial Law Act, B.E. 2457 (1914), Thailand.

[17] Prevention and Suppression of Torture and Enforced Disappearance Act, B.E. 2565 (2022), Thailand, sections 22–25 (in force from 22 February 2023 following the Constitutional Court ruling of 18 May 2023).

[18] Laurie, B., Messeri, E., and Stradling, R. "Certificate Transparency Version 2.0." RFC 9162, IETF, 2021.

[19] Adams, C., Cain, P., Pinkas, D., and Zuccherato, R. "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)." RFC 3161, IETF, 2001.

[20] Rundgren, A., Jordan, B., and Erdtman, S. "JSON Canonicalization Scheme (JCS)." RFC 8785, IETF, 2020.

[21] Amarin TV. Report on the 86th renewal of the Emergency Decree in the southern border provinces. 6 October 2026 (in Thai).

[22] Nation TV. Joint briefing by ISOC Region 4 Forward Command, SBPAC and the Southern Border Provinces Police Operation Centre on the attacks of 22–23 August 2026. 24 August 2026 (in Thai); THE STANDARD, 25 August 2026 (in Thai).

[23] Shamir, A. "How to Share a Secret." Communications of the ACM, 22(11), 1979, pp. 612–613.

[24] The Nation and Krungthep Turakij. Reports citing the Parliamentary Information Service on incident statistics and budgets in the southern border provinces. 23 August 2026.

[25] The Nation. Report citing SBPAC data. 4 January 2026.

[26] Office for National Statistics (UK) and Centers for Disease Control and Prevention (US). Guidance on suppressing small cells in published statistics.

[27] Al Jazeera, 23 August 2026; The Star / Reuters, 24 August 2026.

[28] Thai Post, 17 May 2020 (in Thai); New Mandala, 27 May 2020.

[29] Cross Cultural Foundation (CrCF). Report on DNA collection in the southern border provinces. January 2020.

[30] BenarNews. Report on AI installed with cameras in the southern border provinces. November 2020.

[31] UN Committee against Torture. Concluding observations on the second periodic report of Thailand (CAT/C/THA/CO/2). November 2024; International Commission of Jurists, 19 July 2024.

[32] Khaosod English, 23 June 2026.

[33] Malay Mail, 1 July and 18 September 2026; Bernama / MGR Online, 29 September 2026.

Author and copyright holder: Mr. Jakkrit Boonma (Independent Researcher) | ORCID: 0009-0000-7165-3787 | Email: jaggid.boonma@yahoo.co.th

© 2026 Jakkrit Boonma. All rights reserved. Ownership and copyright in this document belong to Mr. Jakkrit Boonma from the date of publication, under applicable copyright law.