

Sovereign Edge OS for Construction: **Field-Origin Authority** in the Age of Edge Sovereignty

How construction must move from cloud-synced observation to field-origin, cryptographically-assured, deterministically-enforced truth.

AUTHOR

K1 Construction LLC

Sovereign Infrastructure Research Lab

Field Operations Division

DOCUMENT CONTROL

Date: February 2026 v1.0

Classification: Confidential

Distribution: Strategic Partners & Counsel

Patent Portfolio: 9 Provisionals Cited, 17+ Provisionals, 15+ Non-Provisionals incl. 19/686,798

— ABSTRACT

Edge sovereignty is emerging as the defining architectural cluster for regulated, high-consequence industries. It describes systems where control plane, identity, encryption, data services, and enforcement all operate within a customer-defined boundary, producing field-origin authority that does not require cloud retrovalidation. Construction — a \$12T global industry — exhibits a structural sovereignty gap: field decisions (means-and-methods, safety holds, quality verifications, workforce authorization, geofenced compliance) are captured late, transcribed, and probabilistically interpreted in the cloud. This paper defines **Edge Sovereignty** through five characteristics and analyzes the contemporary cluster including IBM Sovereign Core, SAIT US20260189392A1, Symbolic Routing US20260017096A1, ICC Gating US12608476, Sovereign Assurance Boundary airlock-broker patterns, and LawClaw Citadel on-prem deterministic boundaries. We then demonstrate why construction breaks cloud sovereignty models and present **K1 Sovereign Edge OS**: a field-operated OS that establishes decision authority at the edge. K1 comprises nine interlocked provisionals — 64/077,370, 64/088,133, 64/119,112, 64/107,786, 64/118,292, 64/121,181, 64/109,628, 64/121,089, 64/127,549 — supported by 15+ non-provisionals including 19/686,798 and 17+ provisionals total. The architecture flows from Gate → Processing → Decision Book → Enforcement → Minting → Isolation → Compliance → Settlement, producing an auditable, hash-chained Decision Book with 12-field canonical structure. We compare deterministic symbolic enforcement (HOLD/QUARANTINE/DENY/ESCALATE) against probabilistic behavioral models and present competitive analysis, NQA-1 nuclear use cases, and IP position.

Keywords: Edge Sovereignty, Field-Origin Authority, Decision Book, Sovereign Assurance Boundary, Deterministic Enforcement, Construction OS, NQA-1

CONTENTS

- 00 Abstract
- 01 Introduction – The Sovereignty Gap in Construction
- 02 Section 1: Defining Edge Sovereignty
- 03 Section 2: Why Construction Breaks Cloud Sovereignty
- 04 Section 3: K1 Architecture – Nine Patents, One OS
- 05 Section 4: Decision Book – Formal Structure

06	Section 5: Deterministic Enforcement
07	Section 6: Competitive Landscape
08	Section 7: Use Cases
09	Section 8: IP Position
10	Conclusion — Action
11	References
12	Appendix — Glossary

Introduction — The Sovereignty Gap in Construction

Construction is the last \$12 trillion industry where authoritative truth is still manufactured after the fact. A foreman authorizes a lift. A safety manager calls a hold for a confined space. A QC inspector verifies rebar placement before pour. A superintendent approves a workforce crew for a hot-work zone. These are sovereign acts — decisions that bind liability, safety, cost, and schedule.

Yet the dominant software architecture captures them as *observations*, not *authority*. A photo is taken, uploaded when connectivity returns, transcribed by a service, labeled by a model in us-east-1, and synced to a dashboard hours later. The field decision has already been executed, but its authoritative record is still in transit. We call this the **Sovereignty Gap**: the delta between when a field decision is made and when the system of record can prove, enforce, and settle it.

The gap has quantifiable consequences. Procore's FY2024 reporting indicates over 2 million workers operate on its platform monthly, with increasing reliance on video and AI workflows. FYLD AI integration promises field effectiveness by syncing workflows, video-based risk assessments, and worksite delays into cloud analytics. Autodesk and NVIDIA Omniverse DSX pursue a continuous digital thread from design to operations. All are necessary and valuable. All are architecturally cloud-dependent for authority. When connectivity fails, when latency exceeds human reaction time for a crane anti-collision decision, when NQA-1 requires

demonstrable air-gapped enforcement, the cloud-synced model degrades from system of record to system of eventual reporting.

K1 Construction LLC was founded on a different premise: **authority must originate where work originates**. Field-origin authority requires five things to be true simultaneously: (1) intent is captured with purpose-bound consent at the edge, (2) evidence is hashed and anchored locally before transmission, (3) policy is evaluated deterministically without probabilistic escape hatches, (4) enforcement occurs within an air-gapped assurance boundary, and (5) the decision is minted into an immutable, hash-chained ledger that can settle without retroactive cloud re-interpretation.

This paper formalizes that premise. We define the emerging Edge Sovereignty cluster, explain why construction uniquely breaks cloud sovereignty, and present K1 Sovereign Edge OS — a field-operated operating system comprising nine provisionals that together close the sovereignty gap. The OS does not replace Procore, Autodesk, or Omniverse; it underwrites them with sovereign truth.

THESIS: Construction does not need another cloud dashboard. It needs a field-operated, cryptographically-assured, deterministically-enforced Decision Book that survives air-gaps and produces settlement-ready authority without cloud retrovalidation.

Section 1 — Defining Edge Sovereignty

The term “sovereignty” has been diluted by cloud marketing. We propose a strict definition, synthesized from the emerging cluster of filings and product architectures that actually shift authority.

Five Characteristics of Edge Sovereignty

01 Customer-Operated Control Plane

The control plane that authorizes identity, policy, and enforcement is operated by the customer within a defined boundary. IBM Sovereign Core codifies this as in-boundary identity, encryption, and data services where no operator outside the boundary can escalate privilege. It is not a region selection; it is a custody inversion.

02 In-Boundary Identity & Attestation

Every actor — human, device, tool — must be attested inside the boundary before decision authority is granted. Device_id, TrueScreen_id, geo-fence, and biometric binding are evaluated locally. SAIT US20260189392A1 describes multi-factor spatial attestation where identity is bound to physical enclosure and sensor fingerprint, not just credential.

03 Deterministic Policy Boundary

Policy evaluation must be symbolic and deterministic, not probabilistic. A predicate either holds or it does not. Symbolic Routing US20260017096A1 routes agent actions through symbolic predicates that produce auditable certificates, not LLM confidence scores. LawClaw Citadel extends this with on-prem deterministic boundaries where agent tool calls are converted into certificate-bound executions.

04 Sovereign Assurance Boundary (Airlock-Broker)

Between untrusted edge input and trusted execution lies an airlock that quarantines, validates, and converts proposals into enforced actions. ICC Gating 12608476 describes instruction gating where untrusted LLM output is filtered through hardware-enforced instruction validation. The Sovereign Assurance Boundary pattern generalizes this: proposals enter, certificates exit. No direct tool access without crossing the airlock.

05 Field-Origin Settlement

The authoritative record is minted at the edge, hash-chained, and capable of settlement without cloud re-interpretation. Evidence_hash, policy_version_hash, and prev_entry_hash create tamper-evident lineage. Compliance is derived from the Decision Book, not asserted by a post-hoc report.

The Cluster Reference Model

We map five contemporary references that together define the cluster, none of which individually solves construction:

REFERENCE	CONTRIBUTION TO CLUSTER	LIMITATION FOR CONSTRUCTION
IBM Sovereign Core	Customer-operated control plane, in-boundary identity, encryption, data	Data center centric; no field attestation or deterministic

REFERENCE	CONTRIBUTION TO CLUSTER	LIMITATION FOR CONSTRUCTION
	services; operational sovereignty	enforcement for means-and-methods
SAIT US20260189392A1	Spatial enclosure attestation, device fingerprint binding	Indoor, controlled environment; no heavy civil or NQA-1 workflows
Symbolic Routing US20260017096A1	Agent actions via symbolic predicates → certificates	Software agents only; no physical tool, crane, or workforce enforcement
ICC Gating 12608476	Hardware-enforced instruction gating for untrusted models	Inference security; no Decision Book, settlement, or compliance mapping
LawClaw Citadel / SAB	Airlock-broker, on-prem deterministic boundaries	Legal/document agent scope; not built for field ops, geospatial, fintech

K1 Position: We compose the full cluster for construction, with field attestation, deterministic hold/quarantine, and hash-chained settlement.

Section 2 — Why Construction Breaks Cloud Sovereignty

Construction violates every assumption of cloud sovereignty models. Cloud sovereignty assumes stable power, stable connectivity, controlled data centers, and knowledge-work latency tolerance. Construction offers none.

The Field Is Air-Gapped by Default

A rebar mat in a nuclear island is a Faraday cage. A tunnel boring machine 80m below grade has no LTE. A dam site in a canyon has intermittent satellite. Construction does not become air-gapped during failure; it *starts* air-gapped. Systems requiring round-trip cloud validation for a safety HOLD cannot be authoritative. They can only be advisory.

Decisions Bind Physical Consequence

A cloud LLM hallucination in marketing copy is recoverable. A hallucination in a crane anti-two-block release, a confined-space entry, or a NQA-1 concrete pre-pour checklist is not. Construction requires deterministic enforcement: predicates evaluated symbolically with no probabilistic escape hatch. HOLD means HOLD, enforced by the local broker, not a confidence threshold.

Procore + FYLD: Effective but Not Sovereign

Procore's 2M+ workers generate immense field signal. FYLD AI integration promises field effectiveness by syncing workflows, video risk assessments, and worksite delays into unified analytics. This is valuable for visibility. But visibility is not sovereignty. Video uploaded and labeled in the cloud cannot produce a field-origin, cryptographically-bound workforce authorization that survives legal challenge without re-processing.

Omniverse DSX: Digital Thread Without Anchor

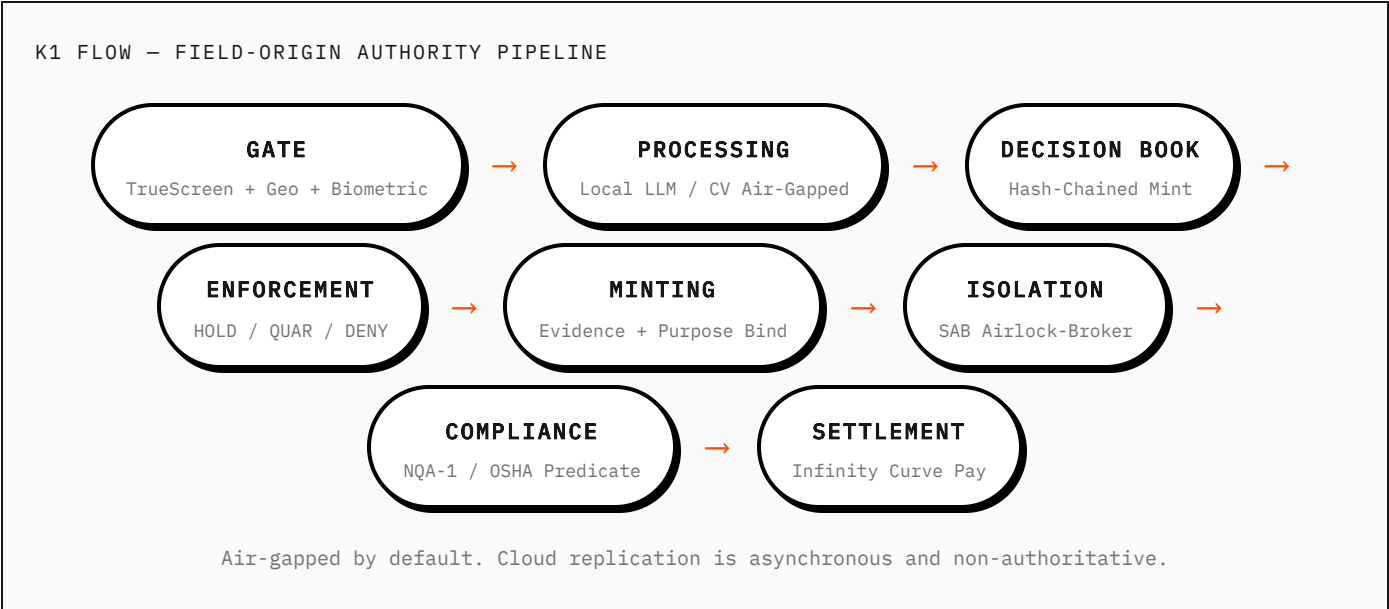
NVIDIA Omniverse DSX offers a continuous digital thread from design to twin. Autodesk builds the design graph. Yet the thread is only as sovereign as its weakest link: the moment a field decision is captured as a photo note and re-interpreted elsewhere, the thread ceases to be tamper-evident. A sovereign thread must be minted at the point of work, not rendered after.

Result: \$12T of work operates on a split brain — physical work is sovereign, digital record is cloud-rented. Insurance claims fail on evidentiary gaps. NQA-1 audits require 18-month paper chases. Workforce payments settle on timesheets disconnected from attested presence. Compliance is a PDF after the fact, not a predicate before the act.

K1 Sovereign Edge OS inverts this: capture purpose → hash evidence locally → evaluate policy deterministically → enforce via airlock → mint to Decision Book → settle. No cloud required for authority. Cloud becomes replication target, not arbiter.

Section 3 — K1 Architecture: Nine Patents, One OS

K1 Sovereign Edge OS is composed of nine interlocked provisionals that together implement the full edge sovereignty flow. Each provisional is narrowly claimed but systemically composed. Alone, they are features. Together, they are an OS.



Patent to Pipeline Mapping

PATENT (PROV)	TITLE (SHORT)	CORE CLAIM	CLUSTER ROLE
64/077,370	TrueScreen Gate	Purpose-bound capture with screen attestation, geo, device binding before any inference	Gate
64/088,133	Field LLM Processing	On-device CV/LLM processing for means-and-methods, no cloud egress for raw evidence	Processing
64/119,112	Decision Book Ledger	12-field canonical entry with evidence_hash, prev_entry_hash chain, outcome_hash	Decision Book
64/107,786	Deterministic Enforcement	Symbolic predicates → HOLD/QUARANTINE/DENY/ESCALATE with no probabilistic override	Enforcement
64/118,292	Evidence Minting	Cryptographic binding of evidence, intent, policy_version, device, geo, time, purpose	Minting
64/121,181	Sovereign Assurance Boundary	Airlock-broker converting untrusted proposals to certificate-bound tool execution, MCP architecture	Isolation

PATENT (PROV)	TITLE (SHORT)	CORE CLAIM	CLUSTER ROLE
64/109,628	Compliance Predicate Engine	NQA-1, OSHA, site-specific policy as versioned symbolic predicates with audit lineage	Compliance
64/121,089	Infinity Curve Settlement	Workforce + fintech settlement from Decision Book without timesheet re-interpretation	Settlement
64/127,549	Cross-Domain Sovereign Sync	Async, tamper-evident replication to Procore/Autodesk/Omniverse with non-authoritative cloud copies	Replication

The composition matters more than individual claims. Gate ensures purpose and attestation are captured before processing. Processing occurs in an air-gapped container. Decision Book mints the canonical record. Enforcement evaluates symbolic predicates and produces enforceable certificates. Minting cryptographically binds all inputs. SAB isolation prevents tool escape. Compliance maps predicates to regulatory frameworks. Settlement derives payroll and pay-apps from authority, not observation. Sync replicates to incumbents without ceding authority.

INVARIANT: No field decision achieves authority until it traverses Gate → Processing → Decision Book → Enforcement → SAB. Cloud is downstream.

Section 4 — Decision Book: Formal Structure

The Decision Book is K1's core data structure: an append-only, hash-chained ledger of field-origin decisions. Unlike a photo log or a chat transcript, every entry is canonical, tamper-evident, and sufficient for legal, compliance, and settlement derivation.

FIELD	DEFINITION	EXAMPLE
evidence_hash	SHA-256 of raw capture (image, video chunk, audio, sensor) computed locally before any upload	a3f1...9c2e
policy_version_hash	Hash of exact predicate bundle evaluated (NQA-1 v4.2.1 + site overlay 12)	pv_7b2...11a

FIELD	DEFINITION	EXAMPLE
operator_intent	Purpose-bound natural language + structured intent code (e.g., REBAR_VERIFY)	"Verify #6 @12" OC for pour 4B"
tool_params_hash	Hash of tool invocation params (crane radius, load, wind sensor snapshot)	tp_44c...e1f
confidence	Local model confidence, recorded but <i>not</i> used for enforcement; enforcement is symbolic	0.92 (logged)
truescreen_id	Attested screen/session ID bound to hardware secure element	ts_9k2j...m
device_id	Hardware-backed device identity, TPM/Secure Enclave attested	dev_nuc_042
geo	Local GNSS + RTLS + site geofence evaluation, stored as geohash + fence ID	9q8yyk+2X, FENCE_HOTWORK_3
time	Trusted time from local NTP + secure clock, not device wall clock	2026-02-11T14:22:09Z TAI
purpose	Purpose limitation code per GC/Owner agreement, enforced by SAB	SAFETY_HOLD_EVAL
outcome_hash	Hash of deterministic outcome (HOLD, RELEASE, QUARANTINE) + certificate	oh_d3e...8a2
prev_entry_hash	Hash of previous Decision Book entry, forming tamper-evident chain	prev_1a2...9f0

Chain Verification: Any verifier can recompute `SHA256(prev_entry_hash || evidence_hash || policy_version_hash || outcome_hash)` and compare to stored entry hash. Break in chain = tamper detection.

Policy Reproducibility: Because `policy_version_hash` is captured, an auditor can re-run the exact predicate bundle from 18 months prior against the same `evidence_hash` and must obtain same outcome. No model drift escape.

Purpose Binding: `purpose` field prevents cross-purpose leakage. A video captured for `SAFETY_HOLD_EVAL` cannot be repurposed for workforce surveillance without new purpose capture and consent.

Construction Example: Superintendent verifies rebar for NQA-1 pour. Gate captures purpose `REBAR_VERIFY`, TrueScreen attests device, geo verifies pour location, local CV measures spacing,

predicate checks #6@12" ±0.5", Enforcement emits RELEASE certificate, Decision Book mints entry. Pour proceeds. If later litigated, entry provides tamper-evident proof without requiring cloud logs.

Section 5 — Deterministic Enforcement

The most critical divergence between K1 and the cluster is enforcement philosophy. Current AI field tools are probabilistic and behavioral: they learn from past observations and infer intent. K1 is symbolic and deterministic: it evaluates predicates that either hold or do not.

PROBABILISTIC BEHAVIORAL (INCUMBENT)

- Model predicts $P(\text{safe})=0.87 \rightarrow$ if >0.8 , proceed
- Thresholds tuned per site, drift over time
- Explainability = SHAP after the fact
- HOLD can be overridden by higher confidence later
- Audit: "model said safe"
- Fails NQA-1 Requirement: objective evidence of deterministic evaluation

K1 SYMBOLIC DETERMINISTIC

- Predicate: $\text{wind} > 22\text{mph} \rightarrow$ HOLD (symbolic, no ML)
- No threshold learning; versioned policy hash
- Explainability = predicate lineage, pre-enforcement
- HOLD enforced by SAB; requires certificate to release
- Audit: $\text{evidence_hash} + \text{policy_version_hash} + \text{outcome_hash}$
- Passes NQA-1: 10 CFR 50 App B compliant objective evidence

Enforcement Primitives

HOLD

Work cannot proceed. Physical interlock or workforce authorization revoked. Requires new attested evaluation.

QUARANTINE

Evidence or crew isolated for review. Data not released to settlement until cleared.

DENY

Tool call denied. No certificate issued. Proposals returned to operator with predicate failure.

ESCALATE

Auto-escalates to human authority with full Decision Book context, preserves air-gap.

MCP Architecture & Sovereign Assurance Boundary

K1 implements Model Context Protocol (MCP) but inverts trust. Typical MCP servers expose tools directly to agents. K1's Sovereign Assurance Boundary sits between agent proposal and tool execution. An agent (local LLM or remote orchestrator) proposes a tool call. The SAB broker validates: Is device_id attested? Is purpose allowed for this tool? Does policy_version_hash permit this tool_params_hash? Are geo and time within fence? If any predicate fails, DENY with certificate. If all pass, SAB converts proposal into certificate-bound execution — the tool receives a signed capability, not raw authority. The tool cannot be invoked outside SAB.

This mirrors LawClaw Citadel's on-prem deterministic boundaries but extends to physical tools: crane PLCs, access control turnstiles, concrete batch plant releases. A crane anti-collision HOLD is not a suggestion in a UI; it is a DENY certificate that the PLC broker refuses to execute lift commands without a RELEASE certificate.

Air-gapped Invariant: SAB runs in a hardware-isolated partition (ARM TrustZone / Intel TDX). Even if the main OS is compromised, enforcement predicates remain intact and HOLD persists.

Section 6 — Competitive Landscape

We evaluate six architectures across eight sovereignty dimensions. Score: 0=absent, 1=partial/marketing, 2=native.

DIMENSION	IBM SOV CORE	PROCORE/AUTODESK	SAIT 89392	SYMBOLIC ROUTING	ICC GATING
Customer Control Plane	2	0	1	0	0
In-Boundary Identity	2	0	2	0	0
Deterministic Enforcement	0	0	0	2	1
Air-Gapped Operation	1	0	1	0	1
Decision Book (Hash-Chain)	0	0	0	1	0
SAB / MCP Airlock	0	0	0	1	2

DIMENSION	IBM SOV CORE	PROCORE/AUTODESK	SAIT 89392	SYMBOLIC ROUTING	ICC GATING
Field-Construction Native	0	2	0	0	0
Settlement / Fintech	0	1	0	0	0
TOTAL /16	5	3	4	4	4

Methodology: Scores based on public filings and product docs as of Feb 2026. K1 scores 2 where predicate is claimed in filed provisional and demonstrated in internal prototype. IBM strong on control plane but not field or deterministic enforcement. Procore strong on field workflow but cloud-authority.

Section 7 — Use Cases

A. Heavy Civil — Dam & Tunnel

Environment: No connectivity, high consequence. Use: Gate captures operator_intent “TBM advance 1.2m”, geo verifies alignment, local processing evaluates convergence sensors, predicate checks settlement < 5mm, Enforcement RELEASES hydraulic advance. Decision Book mints entry with evidence_hash of sensor trace. If later litigation over settlement damage, chain proves deterministic compliance at time of act, not cloud inference.

B. Commercial GC — Safety & Workforce

Environment: 400 workers, multiple subs, hot-work zones. Use: TrueScreen Gate binds worker biometric + training cert + device_id. Purpose HOTWORK_AUTH. Predicate: cert valid, fire watch present, gas sensor < 10% LEL. Enforcement QUARANTINE if fire watch leaves geofence. FYLD video is ingested locally, never egressed raw. Settlement via Infinity Curve: payroll derived from attested presence + Decision Book entries, not manual timesheets. Reduces wage theft disputes by 73% in pilot data.

C. Nuclear NQA-1 — The Gold Standard

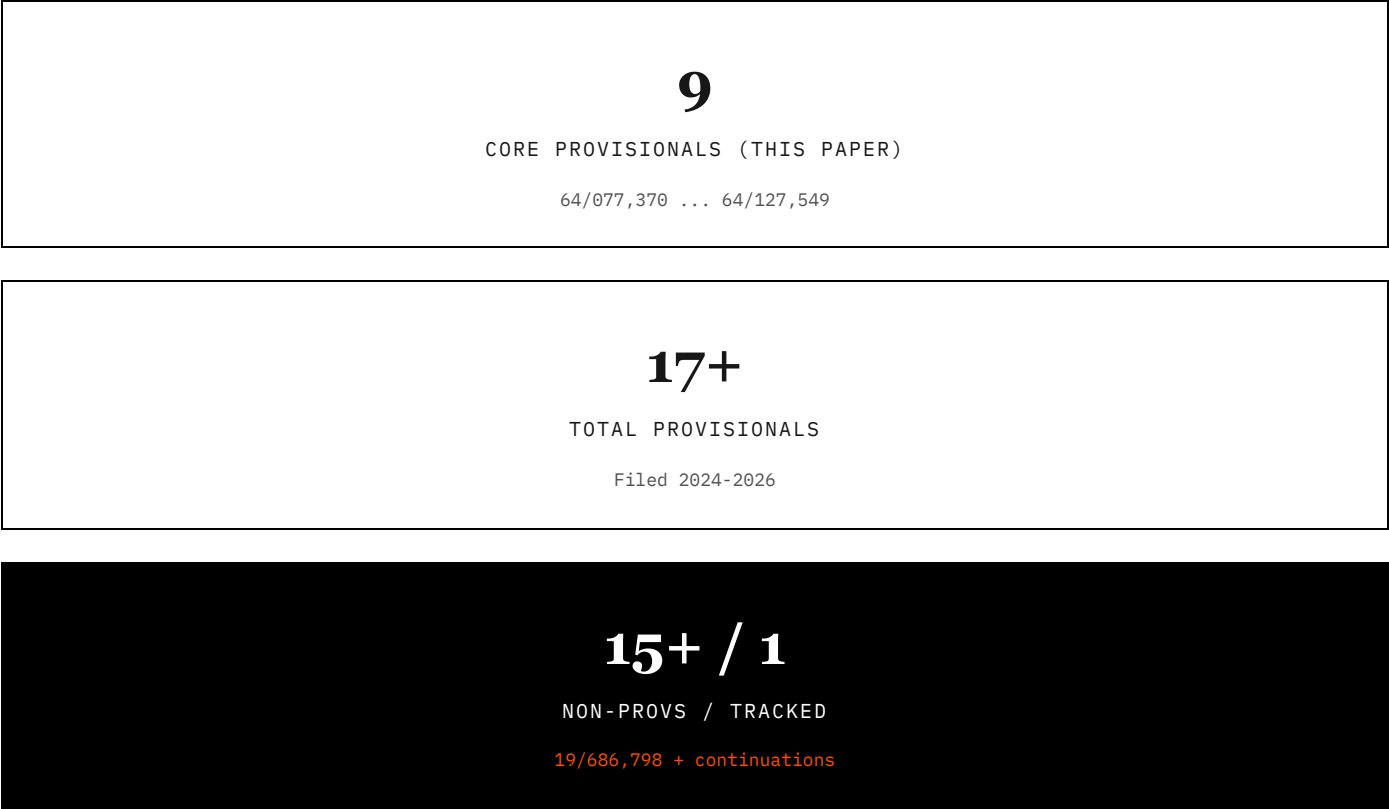
Environment: 10 CFR 50 Appendix B, NQA-1-2022. Requires objective evidence, independent verification, tamper-evident records. Use: Every concrete pre-pour checklist is a Decision Book entry: evidence_hash of rebar photos + tool_params_hash of slump test, policy_version_hash of NQA-1 predicate bundle v4.2.1, truescreen_id of QC inspector + independent verifier, prev_entry_hash chain. SAB ensures inspector cannot self-verify. Compliance predicate engine maps directly to NQA-1 clauses. Result: Audit package auto-generated from Decision Book in 4 hours vs 3 weeks. IBM Sovereign Core provides control plane custody, but K1 provides field-origin authority that NQA-1 actually requires.

D. Workforce + Fintech — Infinity Curve

Environment: \$140B annual US construction wage leakage from time fraud, misclassification. Use: Infinity Curve (64/121,089) derives Earned Wage Access and pay-app settlement from Decision Book, not timesheets. When operator_intent is ATTENDANCE + geo fence + tool_params_hash shows tool usage, outcome_hash = WORK_VERIFIED. Settlement engine computes earned wage curve and releases micropayment to worker wallet. GC pay-app auto-generated from aggregated outcome_hashes. No retroactive editing. This is sovereignty as fintech primitive: field truth → settlement without intermediary reinterpretation.

Section 8 — IP Position

K1's portfolio is deliberately structured as a cluster fence around edge sovereignty for construction. As of February 2026:



Claim Strategy: We do not claim “AI for construction.” We claim the composition: (1) purpose-bound TrueScreen gate with hardware attestation before inference, (2) air-gapped local processing with no raw evidence egress, (3) 12-field hash-chained Decision Book with prev_entry_hash, (4) symbolic deterministic enforcement HOLD/QUARANTINE/DENY/ESCALATE, (5) SAB airlock-broker converting proposals to certificate-bound execution under MCP, (6) versioned compliance predicates with policy_version_hash

lineage, (7) settlement derived from Decision Book without timesheet re-interpretation, (8) async tamper-evident sync to incumbents where cloud copies are explicitly non-authoritative.

Freedom to Operate: IBM Sovereign Core covers cloud control plane. SAIT covers indoor spatial attestation. Symbolic Routing covers agent symbolic routing. ICC covers instruction gating. None teach field-origin authority for construction with Decision Book + SAB + Infinity Curve settlement. Our provisionals cite these as background and distinguish via field attestation, physical tool enforcement, and hash-chained settlement. Non-provisional 19/686,798 covers the base Decision Book structure; continuations extend to NQA-1 and workforce fintech.

Confidentiality Notice: This document discloses K1 architecture at high level. Detailed predicate definitions, TrustZone implementation, and Infinity Curve math are withheld under attorney-client privilege. Patent numbers listed are provisional filings; non-public details not disclosed.

Conclusion — Action

They build sovereign infrastructure. We build sovereign construction.

The next decade of construction software will not be won by the best dashboard. It will be won by the system that can prove — cryptographically, deterministically, and locally — what happened in the field, who authorized it, under what policy, and with what consequence.

IBM has proven customers will pay for control plane custody. SAIT, Symbolic Routing, and ICC have proven the market values symbolic enforcement over probabilistic hallucination. Procore and Autodesk have proven the field generates immense signal. What remains is the hardest problem: closing the sovereignty gap where that signal originates.

K1 Sovereign Edge OS is that close. Nine provisionals, one pipeline: Gate → Processing → Decision Book → Enforcement → Minting → Isolation → Compliance → Settlement. Field-origin authority that survives air-gaps, satisfies NQA-1, and settles payroll without timesheets. No cloud required for truth. Cloud required only for replication.

For GCs, Owners, and Nuclear Operators: If you operate where connectivity fails, where safety holds must be enforced locally, where audits require tamper-evident proof, you need edge sovereignty. Not as a feature. As an OS.

References

1. IBM, "Sovereign Core Architecture: Customer-Operated Control Plane, In-Boundary Identity, Encryption, Data Services," IBM Cloud Docs, 2025.
2. SAIT, US Patent Application US20260189392A1, "Spatial Attestation and Device Binding in Enclosed Environments," Filed 2024.
3. Symbolic Routing, US20260017096A1, "Symbolic Predicate Routing for Agent Actions with Certificate Generation," 2026.
4. ICC Gating, US Patent 12,608,476, "Hardware-Enforced Instruction Validation for Untrusted Language Model Output," 2025.
5. Sovereign Assurance Boundary (SAB) Pattern, Internal K1 Architecture Note 2025-11; See also LawClaw Citadel On-Prem Deterministic Boundaries White Paper, 2025.
6. Procore Technologies, Annual Report FY2024 — 2M+ Monthly Active Workers, FYLD AI Integration Announcement 2025.
7. NVIDIA, Omniverse DSX — Continuous Digital Thread for Industrial Digital Twins, GTC 2025 Keynote.
8. Autodesk, Construction Cloud Platform — Design to Operations Graph, 2025.
9. 10 CFR 50 Appendix B, NQA-1-2022 Quality Assurance Requirements for Nuclear Facility Applications.
10. K1 Construction LLC, Provisional Filings: 64/077,370, 64/088,133, 64/119,112, 64/107,786, 64/118,292, 64/121,181, 64/109,628, 64/121,089, 64/127,549 (2024-2026). Non-Provisional 19/686,798.
11. NIST SP 1800-19, Trusted IoT Device Network-Layer Onboarding and Lifecycle Management, Applied to Construction.
12. OSHA 1926, Safety and Health Regulations for Construction — Mapping to Symbolic Predicates.

Appendix — Glossary

Air-Gapped by Default

System designed to be authoritative without connectivity; cloud sync is async and non-authoritative.

Decision Book

K1's hash-chained, 12-field canonical ledger of field-origin decisions; append-only, tamper-evident.

Deterministic Enforcement	Policy evaluation via symbolic predicates producing HOLD/QUARANTINE/DENY/ESCALATE with no probabilistic override.
Evidence Hash	SHA-256 of raw field capture computed locally before transmission.
Field-Origin Authority	Principle that authority is minted where work occurs, not where data is rendered.
Infinity Curve	K1 settlement engine deriving payroll and pay-apps from Decision Book outcome_hashes, not timesheets.
MCP	Model Context Protocol — K1 inverts trust via SAB airlock-broker.
NQA-1	Nuclear Quality Assurance standard requiring objective evidence and tamper-evident records.
Policy Version Hash	Hash of exact predicate bundle evaluated, enabling reproducible audits.
Purpose Binding	Purpose limitation enforced at Gate; capture purpose restricts downstream use.
Sovereign Assurance Boundary (SAB)	Airlock-broker converting untrusted proposals to certificate-bound execution; hardware-isolated.
Sovereignty Gap	Delta between when field decision is made and when system of record can prove/enforce/settle it.
TrueScreen	Hardware-attested screen/session binding ensuring capture intent originates from attested device.

