CONFIGURATION MANAGEMENT & KM BRIEFING

OKF-CM: Open Knowledge Format for Configuration Management

Bringing Zero-Trust Baseline Assurance, PQC Attestation, and Cryptographic Integrity to AI Agent Workflows

Presenters **Jeff Heisler & Larry Gurule** I-INFUSION® Intelligent Process Solutions | Meta-Governance.com

Target Body **SAE S-19 Digital Engineering Committee** In Coordination with SAE G-33 Configuration Management

Specification Version **Draft Standard v1.0** NIST FIPS 204 (PQC) Compliant

The AI Ingestion Crisis & The OKF-CM Solution

The Ingestion Crisis

Un-Governed Context Causes Hallucinations: AI agents and generative tools suffer from severe execution errors when ingesting raw, un-curated file trees.

Lack of File-Level Assurance: Standard file systems lack a native cryptographic specification to enforce baseline integrity, leaving AI tools exposed in zero-trust environments.

Obsolete Document Risk: Operating on un-versioned drafts or deprecated specifications leads to non-deterministic behavior in safety-critical aerospace systems.

OKF-CM Aerospace Profile

Aerospace-Hardened Profile: Extends Google's open-source Open Knowledge Format (OKF) with zero-trust cryptographic rigor.

Formal Boundary Conditions: Enforces mandatory metadata wrappers, ownership chains, and schema rules via .okf.md manifests.

Deterministic Verification: Replaces loose text ingestion with Merkle-tree baseline hashing (KOH) to transform enterprise data into a trusted knowledge engine.

Pillar 1: Safe Boundaries & Directory Traversal Guard OKF-CM-001

Configuration Management as AI Guardrail

AI agents rely entirely on Configuration Management boundaries to establish factual accuracy and prevent malicious file system escapes.

·**Standard Manifest (.okf.md):** Every Knowledge Object directory is anchored by an .okf.md manifest file containing YAML frontmatter and Markdown.

·**Path Security Boundary:** Parser enforces zero-tolerance checks against relative directory traversal attempts (e.g., ../.. escaping).

·**Strict Schema Validation:** Enforces semantic versions, ULIDs, ISO 8601 UTC timestamps, and explicit artifact inventories.

// Safe Boundary Directory Tree

```
root-directory/
├── .okf.md (OKF-CM-001 Manifest)
└── src/
    ├── main.py
    ├── agent.py
    └── config/
        └── schema.json
```

// Security Guard Traversal Test

CHECK_PATH: "../../etc/passwd"

EXECUTION: [OKF_ERR_PATH_TRAVERSAL]

// Ingestion immediately blocked at boundary!

Pillar 2: Version Authority & Baseline Lifecycle Gates

APPROVED

Active baseline authorized for AI model training, context ingestion, and execution.

DEPRECATED

Historical artifact. AI agents are alerted and barred from active reasoning contexts.

SUPERSEDED

Replaced baseline. Ingestion parser automatically resolves pointer to active replacement.

Fail-Fast Ingestion Gate

If an engineering baseline is modified out of state or fails status validation, OKF-CM triggers an immediate fail-fast error, preventing model contamination and context corruption.

SYSTEM LOG — INGESTION_GATE_FAILURE

```
[INTEGRITY_ERR] OKF_ERR_KOH_MISMATCH
status_enum: REJECTED
ingestion_gate: FAILED_FAST
reason: "modified_out_of_state"
// Action: Blocked from AI context memory
```

Pillar 2: 3-Tier Merkle Tree & NIST PQC Attestation OKF-CM-002

Deterministic State (KOH) Computation

OKF-CM computes a single 32-byte **Knowledge Object Hash (KOH)** to verify complete repository integrity before AI ingestion:

$$KOH = SHA256 (H_{manifest} \| H_{artifacts})$$

- **Tier 1 ($H_{\text{artifacts}}$):** Concatenated byte-hashes of all payload files sorted lexicographically.
- **Tier 2 (H_{manifest}):** Normalized line endings of .okf.md excluding signature block.
- **Tier 3 (Root KOH):** Binds manifest metadata and payload contents together.

Federal PQC & FIPS 204 Compliance

NIST FIPS 204 Approved Suite: Direct integration with Cloudflare's CIRCL library implementing ML-DSA (CRYSTALS-Dilithium) and SLH-DSA (FIPS 205).

Cryptographic Agility: Decoupled signature block allows instant algorithm migration without breaking manifest structure.

Executive Order 14412 Ready: Fully satisfies federal post-quantum cryptography mandates, NSM-10, and CNSA 2.0 standards for air-gapped attestation.

Pillar 3: Bridging the Aerospace Vault with Google OKF

Google's OKF Baseline

Google introduced the Open Knowledge Format (OKF) as an open, minimally opinionated standard for human and AI Markdown knowledge bases.

Aerospace OKF-CM Profile

OKF-CM extends Google's format with zero-trust cryptographic rigor, multi-tier Merkle trees, and explicit graph semantics required for defense and engineering.

Zero-SaaS Local-First

Operates entirely local-first, in-memory, and air-gapped. Enables local AI agents and MCP servers to query knowledge safely without cloud SaaS lock-in.

Pillar 3: ORDER Graph Semantics & Local Traversal OKF-CM-003

Directed Multi-Graph Model $G=(V,E)$

OKF-CM-003 defines **Ordered Relationships & Directed Execution (ORDER)** to map complex engineering dependencies directly inside file manifests.

```yaml
# .okf.md Frontmatter Relationships Block
relationships:
- target: "ko:01J9876543210ZYXWVUTSRQPONM"
type: satisfies
- target: "../Standards/ISO-27001"
type: depends_on
```

Canonical Edge Taxonomy & Inverses

Edge Type	Inverse Type	Semantic Meaning
depends_on	required_by	Functional dependency
satisfies	satisfied_by	Compliance requirement
supersedes	superseded_by	Lifecycle replacement

Local Impact & Blast-Radius Analysis

AI agents perform offline transitive dependency closure calculations directly across local folders—no external SQL or graph databases required.

Aerospace Capability Feature Comparison

Capability / Feature	Raw Directory Trees	Google OKF Baseline	OKF-CM Aerospace Profile
Target Consumer	Human File Browsing	General AI Agents & LLMs	**Mission-Critical Aerospace & Defense AI**
Directory Traversal Security	None ✗	Unenforced —	✓ **Strict Guard (OKF_ERR_PATH_TRAVERSAL)**
Cryptographic Integrity	None ✗	None ✗	✓ **3-Tier Merkle Tree (KOH)**
Post-Quantum Attestation	None ✗	None ✗	✓ **NIST FIPS 204 (ML-DSA / CIRCL)**
Graph Semantics & Impact	None ✗	Freeform Links —	✓ **Strict Multi-Graph & Inverses**

Dual-Committee Governance & Synergies

SAE S-19 (Digital Engineering)

Primary Technical Authoring Body:

- Authors and maintains technical schema specifications (OKF-CM-001/002/003).
- Validates parser execution rules, directory traversal security, and Merkle tree hashing.
- Integrates OKF-CM into modern MBSE digital thread software toolchains.

SAE G-33 (Configuration Management)

Co-Sponsoring Policy Authority:

- Validates alignment with EIA-649-C Configuration Management principles.
- Ensures strict baseline control and version authority across defense supply chains.
- Reasserts CM as the core gatekeeper for enterprise AI reliability and governance.

Four-Phase Standardization Roadmap

PHASE 01

PAR Launch

Submit formal Project Authorization Request (PAR) to launch OKF-CM as an Aerospace Information Report (AIR).

PHASE 02

Spec Refinement

Refine modules: 001 Manifest/Parser, 002 ADS Hashing & PQC, and 003 ORDER Graph Semantics.

PHASE 03

Reference CLI

Deliver open-source reference Go CLI / parser for automated schema validation and KOH computation.

PHASE 04

ARP Transition

Transition document to an Aerospace Recommended Practice (ARP) as industry adoption expands.

ACTION REQUESTED TODAY

Formalizing OKF-CM as an SAE Aerospace Standard

1. Joint Task Group Approval

Approval to form a joint working task group between **SAE S-19** (technical execution) and **SAE G-33** (governance oversight).

2. PAR Authorization

S-19 sponsorship for an SAE Aerospace Information Report (AIR) Project Authorization Request (PAR) to formalize OKF-CM.

Thank you for your leadership and consideration.