EXECUTIVE SUMMARY

As the Global Energy Grid, Industrial, and Manufacturing sectors transition to AI Inference at the Edge, a systemic **Trust Gap** has emerged: OS-level security alone cannot satisfy Sovereign AI requirements. If firmware or silicon integrity is compromised, AI systems become operational liabilities.

AXIS establishes the **Immutable Handshake** between Red Hat Device Edge (MicroShift) and physical silicon —ensuring every AI inference is cryptographically anchored to a verified hardware root of trust.

This transforms AI from a probabilistic system into a **deterministic, auditable, and sovereign execution layer**.

SAFE-GRID STACK — TECHNICAL ARCHITECTURE

AXIS operates as a **Red Hat Certified Operator (Security Grade A)** bridging Red Hat Device Edge and hardware Trusted Execution Environments (TEE).

Execution Flow (Deterministic Pipeline):

- **Orchestration Layer:** Red Hat MicroShift manages lifecycle, scheduling, and containerized AI workloads
- **Trust Handshake Layer:** AXIS SWGI Operator validates firmware, TPM, and TEE integrity prior to execution
- **Execution Layer:** AI inference runs inside a secure, software-wrapped enclave (SGX/TDX enforced)
- **Accountability Layer:** Hardware-signed SHA-256 receipts are generated (~0.25ms) for every execution event

Result: A closed-loop system where no workload executes without verification, and every output is provable.

CORE VALUE PROPOSITIONS

1. Pre-Built Sovereign Compliance (NIST AI RMF / 600-1)

AXIS enforces execution only on verified hardware, converting compliance into a **runtime-enforced control**, not a post-process requirement.

2. Deterministic Low-Latency Governance

~0.25ms hardware-triggered enforcement enables:

- Real-time safety cutoffs
- Grid stabilization responses

- Industrial fail-safe automation

This avoids the latency penalties of traditional software-based security overlays.

3. Sovereign Audit & Forensic Layer

Every inference produces a **hardware-anchored SHA-256 receipt**:

- Tamper-resistant (firmware-level anchoring)
- Immutable execution record
- Suitable for national security and regulated environments

AXIS SOVEREIGN EDGE NODE v1 — HARDWARE SPECIFICATION

Manufacturer: Axis Property Solutions LLC
Product Classification: Sovereign AI Edge Compute Node
Certification Target: Red Hat Enterprise Linux (RHEL) 9.x / Red Hat Device Edge

---

I. CORE HARDWARE ARCHITECTURE

- **Processor:** Intel® Xeon® D-2700 Series (edge-optimized, high I/O throughput, deterministic compute profile)
- **Memory:** 32GB ECC DDR4/DDR5 (fault-tolerant, mission-critical stability)
- **Storage:** 256GB NVMe M.2 Industrial SSD (low-latency, write-intensive endurance class)
- **Networking:**
- 2x 10GbE SFP+ (high-throughput data plane)
- 2x 1GbE RJ45 (segregated management plane)
- **Form Factor:** Ruggedized, fanless chassis
- Operating range: -40°C to +75°C
- Designed for edge-critical deployments (grid, field, industrial)

II. SILICON-ANCHORED TRUST LAYER (ROOT OF TRUST)

- **Trusted Execution:** Intel® SGX (secure enclave execution)
- **Workload Isolation:** Intel® TDX (hardware-enforced isolation domains)
- **Hardware Identity:** TPM 2.0 (aligned to FIPS 140-3 Level 3 target profile)
- **Attestation Engine:** Hardware-backed "Proof-of-Life" validation for all AI execution threads

AXIS Enforcement Rule: No verified silicon → No execution.

III. PERFORMANCE & GOVERNANCE METRICS

- **Remediation Latency:** ~0.25ms (hardware-triggered governance interrupt under optimized conditions)
- **Telemetry Throughput:** Up to 1M SHA-256 receipt events/sec (pipeline-optimized)
- **Execution Control:** Deterministic allow/deny enforcement at operator level

Integration Interfaces:

- Red Hat Advanced Cluster Management (ACM) — fleet orchestration and governance
- Security telemetry integration ready (SIEM/XDR compatible architecture)

Compliance Alignment:

- NIST AI RMF (AI 600-1) — Sovereign AI readiness
- NIST 800-171 / 800-172 — controlled and high-security environments

---

IV. SOFTWARE & ORCHESTRATION STACK

- **Operating System:** Red Hat Enterprise Linux (RHEL) 9.x
- **Edge Runtime:** Red Hat Device Edge (MicroShift) / OpenShift compatibility
- **Container Standard:** OCI-compliant runtime

Governance Layer: AXIS SWGI Operator (v1.0.0)

- Pre-execution verification (firmware + TPM + TEE)
- Continuous runtime governance loop
- Hardware-anchored cryptographic receipt generation
- One-click deployment model (fully hardened baseline)

V. SYSTEM ROLE IN RED HAT ECOSYSTEM

AXIS Sovereign Edge Node v1 functions as a **hardware-verified execution boundary** within Red Hat Device Edge.

- Anchors MicroShift workloads to trusted silicon
- Enforces trust before orchestration
- Converts AI inference into verifiable, auditable transactions

Positioning: Default **trust and governance layer** for Red Hat Industrial Edge AI patterns.

VI. DEPLOYMENT MODEL

- **One-Click Operator Deployment:** Instant provisioning of hardened, compliant environments
- **Air-Gapped Capable:** Fully operable in disconnected / classified environments

- **Fleet-Scale Governance:** Managed via Red Hat ACM across distributed nodes

---

VII. AXIS STANDARD (DECLARATIVE FRAMEWORK)

AXIS enforces three non-negotiable execution conditions:

1. **Verify Before Execute**
   Firmware, TPM, and silicon integrity must be cryptographically validated

2. **Govern During Execution**
   Continuous enforcement via hardware-aware policy loop

3. **Prove After Execution**
   Immutable SHA-256 receipts generated for every inference

Outcome: A closed-loop, hardware-anchored AI governance system aligned with sovereign infrastructure requirements.

STRATEGIC OBJECTIVE

Integrate AXIS into **Industrial Edge AI Validated Patterns** as the default trust layer.

- **Vision:** Every substation, factory, and critical node running Edge operates with AXIS-enabled hardware trust
- **Outcome:** Reduced infrastructure risk, enforceable AI governance, and verifiable execution across global edge networks

---

OPENSHIFT PLATFORM 4 — TWIN ARCHITECTURE (DATACENTER / HYBRID CLOUD)

EXECUTIVE SUMMARY

For centralized, hybrid, and multi-cluster environments, the Trust Gap persists at scale: cluster-level security cannot attest to node firmware integrity or guarantee that AI workloads execute on verified silicon.

AXIS extends the **Immutable Handshake** into **Red Hat OpenShift Platform 4**, binding Kubernetes orchestration to hardware-rooted trust across clusters. Every inference is executed, governed, and recorded against a verifiable silicon baseline.

SAFE-GRID STACK — OPENSHIFT 4 PROFILE

AXIS operates as a **cluster-wide governance operator** within OpenShift 4, integrating with native control planes and policy engines.

Execution Flow (Cluster Deterministic Pipeline):

- **Cluster Orchestration:** OpenShift 4 (Kubernetes) manages scheduling, scaling, and multi-tenant workloads
- **Node Attestation Layer:** AXIS SWGI Operator performs node-level verification (firmware/TPM/TEE) prior to pod admission
- **Admission Control:** AXIS enforces allow/deny via admission webhooks / policy bindings (only verified nodes admit sensitive workloads)
- **Secure Execution:** AI workloads run in enclave-backed contexts (SGX/TDX) on attested nodes
- **Accountability:** Hardware-anchored SHA-256 receipts emitted per execution event (~0.25ms) and indexed for cluster-wide audit

Result: Policy-driven, hardware-verified execution across single and multi-cluster OpenShift deployments.

CORE VALUE PROPOSITIONS (OPENSHIFT 4)

1. Cluster-Enforced Sovereign Compliance

Hardware attestation is enforced at **admission time**, ensuring NIST AI RMF (AI 600-1) controls are applied before scheduling.

2. Policy-Driven Governance at Scale

Integration with OpenShift policy frameworks enables deterministic governance across namespaces, tenants, and clusters without introducing latency-heavy sidecars.

3. Federated Sovereign Audit Trail

Per-inference receipts are aggregated across clusters, providing **tamper-resistant, fleet-wide provenance** suitable for regulated and national security workloads.

OPENSHIFT 4 — SOFTWARE & INTEGRATION

- **Platform:** Red Hat OpenShift Container Platform 4.x
- **Operator Model:** AXIS SWGI Operator (cluster-scoped + node agents)
- **Policy Integration:** Kubernetes admission controllers / policy bindings (enforce verified-node scheduling)
- **Cluster Governance:** Red Hat Advanced Cluster Management (ACM) for multi-cluster policy distribution and visibility

- **Telemetry:** Exportable to SIEM/XDR pipelines; receipt indexing for audit and forensics

---

NODE PROFILE (COMPATIBILITY)

Optimized for **AXIS Sovereign Edge Node v1** and compatible RHEL 9 worker nodes with: - TPM 2.0 enabled - SGX/TDX-capable processors - Secure boot and measured boot enabled

Nodes failing attestation are **quarantined from sensitive workload pools**.

DEPLOYMENT MODEL (OPENSHIFT 4)

- **Operator Install:** One-click via Operator Lifecycle Manager (OLM)
- **Day-0/Day-2:** Baseline hardening at install; continuous verification post-deploy
- **Air-Gapped Support:** Disconnected catalogs and local registries supported
- **Multi-Cluster:** ACM-driven rollout of policies and operator configuration

---

AXIS STANDARD — OPENSHIFT ENFORCEMENT

1. **Verify Before Schedule**
   Nodes must pass attestation before pods are admitted

2. **Govern During Runtime**
   Continuous policy enforcement without performance-degrading wrappers

3. **Prove Per Execution**
   Immutable, hardware-anchored receipts for every inference

Outcome: OpenShift becomes a **sovereign, hardware-verified execution fabric** for AI workloads.

STRATEGIC OBJECTIVE (OPENSHIFT 4)

Position AXIS as the **default trust and governance operator** for OpenShift-based AI platforms (enterprise, defense, and regulated industries).

- **Vision:** All AI workloads on OpenShift execute only on attested nodes with provable outputs
- **Outcome:** Reduced platform liability, enforceable compliance at admission, and verifiable execution across hybrid cloud

---

NEXT STEPS (OPENSHIFT 4)

- Demonstrate OLM-based deployment and admission control enforcement
- Validate multi-cluster policy propagation via ACM
- Provide certification-aligned artifacts for OpenShift Operator and RHEL 9 node compliance

---

Canvas Notes: - Mirror Edge layout; label this as “OpenShift 4 (Cluster Profile)” - Diagram: Control Plane → Admission (AXIS) → Attested Nodes → Enclave Execution → Receipt Bus - Emphasize “Verify Before Schedule” as the OpenShift-specific control point