A Governance Plane for AI-Native 6G Architectures Under Intermittent Connectivity

J.D. "Pepper" Petersen
Aristotle Agentic, Helena, Montana, USA
jdpepper@aristotleagentic.com

Abstract

6G architecture roadmaps increasingly describe networks as AI-native systems that converge communication, compute, sensing, and distributed intelligence across terrestrial and non-terrestrial domains. In this setting, deep-edge nodes and non-terrestrial network elements may host autonomous agents that make operational decisions under intermittent backhaul. Intermittency creates an accountability gap. If connectivity to the operator domain is degraded or unavailable, institutional policy and auditability may fail to follow the agent.

This paper proposes a Governance Plane (G Plane) as a first-class architectural layer that complements the data plane (transport) and the management plane (configuration and monitoring). The G Plane provides delegated authority as Policy as Code, runtime constraint enforcement, explicit safety fallback modes, escalation logic, and cryptographic attestation of decisions for deferred audit and synchronization after reconnection. We define four Governance Plane functional entities, describe their sequence of operations during backhaul loss, and map candidate interfaces into the 3GPP service-based architecture and the O-RAN near-real-time RIC. The contribution is architectural. It does not claim new radio techniques. Instead, it frames governance as an interoperable control surface needed to make AI-native 6G deployable in mission-critical and intermittently connected environments.

Keywords: 6G architecture, AI-native networks, governance plane, intermittent connectivity, non-terrestrial networks, intent-driven management, Policy as Code, attestation, standardization

I. Introduction

6G is commonly framed as more than a throughput upgrade. It is a shift toward programmable architectures that integrate distributed intelligence, compute-connectivity convergence, and new service classes across the deep-edge-to-cloud continuum. At the same time, 6G visions place non-terrestrial networking and three-dimensional coverage on the critical path for resilience, remote operations, and public-safety use cases. The IMT-2030 framework highlights ubiquitous connectivity and resilience as system objectives that must hold even under disruption [1]. Intermittent connectivity is therefore not a corner case but a defining deployment condition.

Architecture discussions already include data-plane functions, management and orchestration, and multiple forms of AI enablement, including analytics functions in the core and operator intent-based automation [2], [3]. European roadmap work emphasizes modular cloud-native architectures and AI-native capabilities as first-order design principles [4]. However, many descriptions of AI-native operation still assume that the controlling authority remains continuously reachable. In practice, a deep-edge node may run autonomously for meaningful periods while its operator domain is unreachable. During that period, an agent can drift from institutional policies, either due to benign optimization pressure or adversarial influence.

The core claim of this paper is simple. AI-native 6G needs a governance surface that remains enforceable when backhaul is degraded. We call this surface the Governance Plane (G Plane). The G Plane is not intended to replace existing management, intent, or analytics components. Instead, it provides a formal and interoperable mechanism for delegated authority, local-first constraint enforcement, safety fallback behavior, and cryptographic attestation of actions so that accountability survives disconnection.

This paper is conceptual and architectural in scope. It does not propose a new protocol, mandate, or normative standard, but instead frames governance as a missing abstraction layer suitable for future standardization.

The contributions are:

• a plane-level framing for governance in AI-native 6G architecture
• four Governance Plane functional entities and their responsibilities
• a mission sequence that makes intermittent connectivity a first-class requirement
• an authority-envelope concept implemented as Policy as Code
• safety fallback modes that bound behavior under degraded connectivity
• a standardization discussion that connects the concept to existing 3GPP SBA and O-RAN automation surfaces

---

II. Background and Related Work

Zero-touch and autonomous networking are active standardization and industry topics. ETSI ISG ZSM has defined requirements and a reference architecture for end-to-end zero-touch network and service management [5], [6]. 3GPP has studied and specified enablers for network automation and analytics functions, including the NWDAF architecture for analytics services in the 5G core [2], [3]. NGMN has published an autonomous system and network automation framework that emphasizes interoperable, market-enabling specifications and a system-wide perspective [7].

6G architecture work from the European research ecosystem summarizes architectural building blocks and convergences expected for 6G, including AI-native aspects and non-terrestrial integration [4]. Space and non-terrestrial networking

is treated as a major component of the 6G era, with recent surveys and roadmaps in the Proceedings of the IEEE covering technical and system challenges for space communications and multi-layer integration [8].

These efforts support closed-loop automation, analytics, and intent-based control. However, governance in the sense used here is often implicit. In many architectures, policy enforcement is treated as a management function, a security function, or a product feature. The telecom architecture problem differs. A network node may need to keep operating when oversight is unavailable, and the operator must later prove what happened and why in a way that is auditable across vendors and domains.

This paper does not claim that governance is absent in all forms. Attestation, remote verification, and policy enforcement are mature themes in security. The point is that AI-native 6G architectures currently lack a plane-level, interoperable abstraction for delegated authority and deferred accountability under intermittent connectivity.

III. Problem Statement and Requirements

Consider a deep-edge 6G node operating as part of a non-terrestrial-network-supported service chain. It hosts one or more autonomous agents that can take actions such as slice prioritization, radio-resource-management decisions, edge-compute scheduling, and routing or caching adjustments. The operator provides intents and constraints. The node experiences intermittent backhaul due to satellite visibility, weather, interference, disaster, or energy constraints.

During a backhaul outage, three architectural requirements become acute.

R1. Delegated authority must remain enforceable locally.
The node must be able to determine what it is allowed to do without querying the core.

R2. Safety must degrade predictably.
Under degraded connectivity, the system must enter known-good fallback states rather than improvising.

R3. Accountability must be provable after the fact.
The operator must be able to audit a tamper-evident record of decisions made during autonomy.

Secondary requirements follow: minimal overhead, interoperability across vendors, support for multiple policy sources (operator, regulator, application), and compatibility with existing intent-based workflows and security models, including zero-trust approaches.

IV. Governance Plane Concept

We define the Governance Plane as the architectural layer that encodes what is permitted and how accountability is produced when autonomous agents act. It is distinct from the data plane, which transports information, and the management plane, which supports configuration and monitoring. The Governance Plane focuses on delegated authority, runtime constraint checks, safety fallback logic, escalation triggers, and attested records of autonomous behavior.

Figure 1 (conceptual): a vertical stack with Autonomous AI Agents proposing actions, the Governance Plane mediating, and underlying data and management planes. A dotted arrow from the Governance Plane to the operator domain indicates deferred synchronization after reconnection.

V. System Architecture and Functional Entities

To operationalize the plane concept, we introduce four Governance Plane Functional Entities (FEs). The naming is descriptive rather than normative.

Authority Orchestration Function (AOF)
Translates operator intent and institutional policy into signed Authority Envelopes distributed to governed nodes.

Runtime Constraint Monitor (RCM)
A high-priority local gate that validates proposed actions from agents against the active Authority Envelope.

Escalation Logic Controller (ELC)
Handles governance-driven state transitions when constraints block an agent's action or when backhaul is lost.

Attestation and Logging Function (ALF)
Produces cryptographic attestation that the node's decision history has not been tampered with and synchronizes evidence after reconnection.

The AOF is typically centralized in the operator domain, while the RCM, ELC, and ALF are instantiated at the edge node. During outages, the governed node relies on cached envelopes and local enforcement.

VI. Governance Plane vs Management and Security Planes

Table I. Plane Comparison

Plane	Primary Objective
Management Plane	Configure, optimize, and monitor network and service operation
Security Plane	Protect identity, confidentiality, integrity, and access control

Plane	Primary Objective
Governance Plane (proposed)	Enforce delegated institutional authority and preserve auditability for autonomous decisions

The Governance Plane consumes cryptographic primitives but is not itself a security plane. Security planes address identity, confidentiality, integrity, and access control. The Governance Plane addresses operational authority, intent compliance, and institutional accountability for autonomous actions.

VII. Policy as Code and Authority Envelopes

A Governance Plane requires policies that are unambiguous and machine-enforceable. We therefore treat delegated authority as Policy as Code. The policy artifact is signed, versioned, and deployable with explicit provenance.

We define an Authority Envelope (AE) as the signed Policy-as-Code bundle applied to a governed node for a time-bounded mission interval. An AE includes permissible action space, constraints and invariants, fallback states for degraded operation, escalation triggers, expiration logic, and attestation requirements.

Policy distribution can reuse secure configuration channels and zero-touch workflows. The Governance Plane contribution is the semantics of the artifact for autonomy and intermittent connectivity.

VIII. Safety Fallback Modes and Priority Precedence

State S0. Connected Normal
Link_Status = 1, normal autonomy within AE_0.

State S1. Degraded Autonomy
Link_Status = 0, autonomy continues but within AE_degraded.

State S2. Hold Safe
Link_Status = 0 and a defined risk threshold is exceeded. Freeze to a known-good configuration and preserve priority services.

State S3. Stop and Report
Forced termination of autonomous actions. Preserve evidence and await reconnection or human decision.

Link_Status is a local reachability signal asserted by the node's transport-monitoring function and consumed by the ELC.

A legitimate conflict exists when a governance constraint blocks an action that an agent deems necessary for system survival. The Governance Plane therefore requires an explicit priority-precedence model encoded into the Authority Envelope.

Tier 1. Physical Safety
Tier 2. Life-Critical Services
Tier 3. Institutional Policy

Tier 1 overrides ensure that autonomous RRM and edge-control decisions never violate hard-coded safety constraints such as regulatory spectral masks, maximum EIRP limits, and platform safety controls that must remain enforceable even during disconnected operation.

IX. Attestation and Deferred Accountability

Logging alone is not sufficient because a compromised node can rewrite its history. The ALF therefore produces attestation evidence.

At minimum, the ALF maintains a hash-chained journal where each entry binds the previous digest, a timestamp, and decision context. The chain is periodically signed using a device identity key. Where available, hardware roots of trust can protect keys and strengthen identity. After reconnection, the operator verifies that the journal is complete and untampered.

ETSI architectural work on artificial intelligence in networks discusses governance interfaces and traceability, reinforcing the need for explicit architectural hooks for accountability [9].

X. Mission Sequence Under Intermittent Connectivity

Connected Phase

1. G-AOF → RCM: Gov_Policy_Distribute(AE_0, AE_degraded, signature, validity)
2. RCM: Validate_Signature and Cache(AE_0, AE_degraded)
3. ALF: Init_Journal(policy_version, journal_root)
4. AI Agent → RCM: Gov_Validation_Req(action, context_hash)
5. RCM → AI Agent: Gov_Validation_Rsp(approve)

Link Loss Phase

6. Transport monitor → ELC: Link_Status = 0
7. ELC: State_Transition(S0 → S1)
8. AI Agent → RCM: Gov_Validation_Req(action, context_hash)
9. RCM → AI Agent: Gov_Validation_Rsp(approve or reject, constraint_id)
10. RCM → ELC: Constraint_Violation(constraint_id, risk_score)
11. ELC → Node control: Enforce_Fallback(S1 or S2)
12. ALF: Append_Event(hash_chain, signature)

Link Restoration Phase

13. Transport monitor → ELC: Link_Status = 1
14. ELC: State_Transition(S1 → S0)

15. ALF → G-AOF: Gov_Attestation_Push(journal_root, signature, policy_version)
16. G-AOF: Verify_Chain and Generate_Compliance_Report

XI. Mapping to 3GPP SBA and O-RAN

In 3GPP Service-Based Architecture terms, Governance Plane functions can be realized as Network Functions exposed over Service-Based Interfaces. The Authority Orchestration Function aligns most closely with an extension of the Policy Control Function, producing signed governance artifacts analogous to policy rules. The Attestation and Logging Function can be implemented as a specialized sidecar to the Unified Data Repository or as a policy-governed extension to the NWDAF analytics pipeline.

Runtime Constraint Monitor and Escalation Logic Controller are edge-resident micro-network functions consuming governance services via service-based interfaces. This placement preserves SBA semantics while introducing governance-specific service primitives without requiring new transport protocols.

In O-RAN, the Near-RT RIC executes control actions over the E2 interface toward E2 nodes while the Non-RT RIC provides policy guidance to the Near-RT RIC over the A1 interface. Authority Envelopes align naturally with A1 policy payloads that bound optimization behavior under degraded connectivity.

XII. Validation Approach and Metrics

This paper outlines a validation plan rather than claiming completed measurements. The Governance Plane can be evaluated in an emulated NTN or degraded-connectivity testbed.

Metrics include governance decision latency, prevented policy violations, continuity for priority services during outages, integrity verification success for attestation journals, and overhead in compute and storage footprint.

XIII. Use Case. NTN Emergency Services Under Disaster Conditions

A representative use case is an emergency response network deployed after a major earthquake or wildfire where terrestrial infrastructure is damaged and backhaul is available only through intermittent low-earth-orbit satellite passes.

A portable 6G base station and edge-compute node provide connectivity for first responders, medical telemetry, and situational-awareness drones. Autonomous agents dynamically prioritize traffic, allocate spectrum, and schedule edge inference workloads for victim detection and hazard mapping.

During satellite blackouts, the Governance Plane enforces a pre-distributed Authority Envelope that restricts autonomous actions to life-critical slices, caps transmit power to avoid interference with aeronautical systems, and freezes nonessential optimization loops.

If an AI agent proposes a spectrum reallocation that would starve medical telemetry, the Runtime Constraint Monitor blocks the action locally and the Escalation Logic Controller transitions the node into a hold-safe configuration. All decisions and overrides are recorded in a hash-chained journal by the Attestation and Logging Function.

When satellite connectivity resumes, the evidence is synchronized to the operator domain, which verifies that all autonomous actions remained within the delegated authority for emergency conditions.

XIV. Conclusion

Intermittent connectivity is a defining feature of non-terrestrial and deep-edge deployments. If 6G architectures delegate meaningful authority to autonomous agents, then policy enforcement and auditability must survive disconnection.

This paper proposed a Governance Plane as a first-class architectural layer for AI-native 6G. We defined functional entities, introduced Authority Envelopes as Policy as Code, specified safety fallback modes, described attestation for deferred accountability, and demonstrated applicability through an NTN emergency-services use case. Next work is to prototype minimal interfaces in an NTN-oriented testbed and use the results to inform standardization.

Acknowledgment

The author used generative AI tools to assist with drafting and editing portions of this manuscript. The author reviewed and revised all content and is responsible for the final submission.

References

[1] ITU-R Recommendation M.2160-0, Framework and overall objectives of the future development of IMT for 2030 and beyond, Nov. 2023.
[2] 3GPP TR 23.791, Study of Enablers for Network Automation for 5G, Release 16 Technical Report.
[3] 3GPP TS 23.288 (v18.x), Architecture enhancements for 5G System to support network data analytics services, Release 18.
[4] Hexa-X-II Consortium, 6G Architecture Vision, Deliverable D2.1, 2024.

[5] ETSI GS ZSM 001 V1.1.1, Zero-touch network and Service Management Scenarios and requirements, Oct. 2019.
[6] ETSI GS ZSM 002 V1.1.1, Zero-touch network and Service Management Reference Architecture, Aug. 2019.
[7] NGMN Alliance, Autonomous System and Network Automation Framework, Version 1.0, 29 Sept. 2022.
[8] K. Ntontin et al., “A Vision, Survey, and Roadmap Toward Space Communications in the 6G and Beyond Era,” Proceedings of the IEEE, Early Access 2024.
[9] ETSI GR ENI 005, System Architecture for Artificial Intelligence in Networks, 2021.