Project GAINS

(Generative AI for Network Sustainability)

Deliverable D3.2

Technical Report on Network Orchestrator Design and Implementation

Giordano, A. – Basile, L. – De Giacomo, A. – Haider, B. – Paesani, M.
2026-01

Work Package: WP3 Design, Prototype implementation and Evaluation of Agents

Status: Final | Version: 1.0

Classification: internal project use; controlled sharing with partners as needed.

Abstract

The operational management of networks and digital infrastructures of the new generation requires increasingly fast, controllable, and auditable change processes, in the face of growing complexity due to technological heterogeneity, variable traffic dynamics, security constraints, and sustainability requirements. In this context, traditional automation based on playbooks and static rules shows structural limitations: it struggles to generalize across domains and vendors, does not robustly make decision assumptions explicit, and rarely natively integrates an accountability model that links decisions, evidence, configurations, and impact. This deliverable presents the design and reference implementation of the Network Orchestrator, a software agent oriented toward intent-based networking and change governance, designed to transform operational intents into candidate configurations and execution plans, integrating knowledge grounding and estimation of energy impact in a traceable and reproducible manner. The proposed approach combines deterministic control components with assistive components based on language models, constrained by schemas and validation rules. The Network Orchestrator operates as a stateless API service with external persistence of state and artifacts, introducing an explicit and idempotent job lifecycle, capable of managing end-to-end the submit–context–generation–validation–impact–documentation–approval chain. The architectural core is an agentic pipeline that: normalizes the intent into a canonical representation; performs applicable retrieval from a knowledge store using hard filters on vendor, role, and version; produces structured artifacts that include explicit references to the sources used; enforces deterministic security and compliance policies; performs syntactic and semantic validations on configuration and change plan; estimates energy impact as-is/to-be/delta via telemetry and models, making explicit confidence, method, and assumptions; and finally generates an operational explain pack oriented toward review, audit, and human decision-making. The use of an external OpenAI-compatible LLM endpoint is confined to non-authoritative tasks such as assisted parsing, variable binding, and controlled enrichment of the plan, with minimization of context, preventive drafting, and schema-based post-validation, mitigating risks of prompt injection and data leakage. The main contribution is a replicable implementation model that makes change generation “decidable”: each output is packaged into versioned and hashed artifacts, linked to knowledge references and evidence references, and accompanied by validation reports and verifiable rollback conditions. This approach enables change

governance consistent with industrial requirements of traceability, operational risk reduction, and compliance control, and introduces a first level of sustainability by design thanks to the systematic production of impact estimates and the explicit management of uncertainty. Evaluation is defined through a multi-level suite of unit tests, schema contract tests, integration and regression tests, including quantitative metrics on correctness, security, auditability, and performance, as well as adversarial tests for robustness. The Network Orchestrator constitutes a key building block for the industrialization of agent-based architectures applied to networks and infrastructures, in line with digital and sustainable transition goals: it reduces time-to-change, increases the quality and verifiability of decisions, and prepares controlled integration toward execution systems and closed-loop monitoring, while keeping reproducibility, accountability, and data protection at the center. [15][22][23][27]

Table of Contents