Progetto GAINS

(Generative AI for Network Sustainability)

Deliverable D3.2

Technical Report su Progettazione e Implementazione Network Orchestrator

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

Work Package: WP3 Progettazione, Implementazione Prototipale e Valutazione degli Agenti

Stato: Definitivo | Versione: 1.0

Classificazione: uso interno di progetto; condivisione controllata con partner su necessità.

Abstract

La gestione operativa delle reti e delle infrastrutture digitali di nuova generazione richiede processi di change sempre più rapidi, controllabili e auditabili, a fronte di una complessità crescente dovuta a eterogeneità tecnologica, dinamiche di traffico variabili, vincoli di sicurezza e requisiti di sostenibilità. In questo contesto, l'automazione tradizionale basata su playbook e regole statiche mostra limiti strutturali: fatica a generalizzare tra domini e vendor, non esplicita in modo robusto le assunzioni decisionali, e raramente integra in modo nativo un modello di accountability che colleghi decisione, evidenze, configurazioni e impatto. Questo deliverable presenta la progettazione e l'implementazione di riferimento del Network Orchestrator, un agente software orientato a intent-based networking e governance del change, progettato per trasformare intent operativi in configurazioni candidate e piani di esecuzione, integrando knowledge grounding e stima dell'impatto energetico in modo tracciabile e riproducibile. L'approccio proposto combina componenti deterministiche di controllo con componenti assistive basate su modelli linguistici, vincolate da schemi e regole di validazione. Il Network Orchestrator opera come servizio API stateless con persistenza esterna di stato e artefatti, introducendo un lifecycle del job esplicito e idempotente, capace di gestire end-to-end la catena submit–context–generation–validation–impact–documentation–approval. Il cuore architetturale è una pipeline agentica che: normalizza l'intent in una rappresentazione canonica; effettua retrieval applicabile da un knowledge store mediante filtri hard su vendor, ruolo e versione; produce artefatti strutturati che includono riferimenti espliciti alle fonti usate; applica policy deterministiche di sicurezza e conformità; esegue validazioni sintattiche e semantiche su configurazione e change plan; stima l'impatto energetico as-is/to-be/delta tramite telemetria e modelli, esplicitando confidenza, metodo e assunzioni; infine genera un explain pack operativo orientato a revisione, audit e decisione umana. L'uso dell'endpoint LLM esterno OpenAI-compatibile è confinato a task non-authoritative come parsing assistito, binding di variabili e arricchimento controllato del piano, con minimizzazione del contesto, redazione preventiva e post-validazione a schema, mitigando rischi di prompt injection e data leakage. Il

contributo principale è un modello implementativo replicabile che rende la generazione di change “decisionabile”: ogni output è pacchettizzato in artefatti versionati e hashati, collegati a knowledge references ed evidence references, e accompagnati da report di validazione e da condizioni di rollback verificabili. Questa impostazione abilita governance del change coerente con requisiti industriali di tracciabilità, riduzione del rischio operativo e controllo di conformità, e introduce un primo livello di sostenibilità by design grazie alla produzione sistematica di stime d’impatto e alla gestione esplicita dell’incertezza. La valutazione è definita tramite una suite multilivello di test unitari, contract test degli schemi, test di integrazione e regressione, includendo metriche quantitative su correttezza, sicurezza, auditabilità e prestazioni, oltre a test avversari per robustezza. Il Network Orchestrator costituisce un tassello chiave per l’industrializzazione di architetture agentiche applicate a reti e infrastrutture, in linea con gli obiettivi di transizione digitale e sostenibile: riduce il time-to-change, aumenta la qualità e la verificabilità delle decisioni, e prepara l’integrazione controllata verso sistemi di esecuzione e closed-loop monitoring, mantenendo al centro riproducibilità, accountability e protezione dei dati. [15][22][23][27]

Indice