International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806015

AI-Driven Autonomous Network Control Planes for Large-Scale Infrastructure Networks

Abhishek Singh

Independent Researcher, USA

abhishek.singh.geek@gmail.com

ABSTRACT: This paper explores the integration of Artificial Intelligence and machine learning into the network control plane to enable autonomous network operations, thereby addressing the complexities and limitations inherent in traditional, human-centric network management paradigms . This shift towards AI-driven solutions is crucial for achieving enhanced efficiency, security, and scalability in modern enterprise networks, allowing for unprecedented levels of automation and predictive maintenance [1]. Specifically, this paper delves into how AI algorithms can dynamically analyze network data, identify patterns, and make intelligent decisions to optimize network configurations, routing protocols, and resource allocation strategies in real time [2]. Such intelligent systems are paramount for mitigating the challenges posed by increasingly dynamic and reconfigurable networks, including those envisioned for 6G, which incorporate elements like non-terrestrial networks and extensive virtualization [3].

Modern enterprise and carrier networks are evolving into highly dynamic, multi-domain infrastructures composed of virtualized network functions, programmable data planes, heterogeneous access technologies, and continuously shifting traffic patterns[4].[4] Traditional operations models, built on static configuration, device-level policies, and human-driven troubleshooting, struggle to deliver consistent service-level objectives SLOs) at scale. This paper proposes an AI-driven Autonomous Network Control Plane (ANCP): a closed-loop system that translates high-level intent into enforceable network actions, continuously verifies outcomes, and adapts control strategies based on telemetry and learned models.[5] The architecture combines (i) an intent interface and translation pipeline, (ii) an assurance and verification layer, (iii) a multi-timescale decision engine using optimization and reinforcement learning, and (iv) safe action with safety limits, rollback, and human override. We define the functional decomposition, control-loop lifecycle, and safety mechanisms; provide algorithms for intent compilation, anomaly-to-action mapping, and policy-safe execution; and outline an evaluation methodology using traffic engineering, incident remediation, and SLA compliance scenarios[6]. This work positions autonomous control planes as a pragmatic path toward self-driving networks by integrating intent, closed-loop automation, and learning-based decision-making within operationally safe boundaries.

KEYWORDS: Autonomous networks, intent-based networking, closed-loop automation, reinforcement learning, network assurance, telemetry, orchestration.

I. INTRODUCTION

The exponential growth in connectivity and digital transformation has profoundly reshaped our reliance on communication networks, making them an indispensable component of daily life and critical infrastructure . This pervasive integration necessitates a paradigm shift in network management, moving towards more intelligent, autonomous systems capable of addressing the complexities of modern network environments [7]. Specifically, the advent of Artificial Intelligence and machine learning offers transformative potential for evolving network control planes, enabling capabilities far beyond traditional rule-based or heuristic approaches [8]. This evolution toward AI-driven autonomous network control is crucial for managing the ever-increasing complexity, dynamic traffic patterns, and diverse service requirements of large-scale infrastructure networks [9]. Such systems are designed to not only adapt to real-time stimuli but also continuously refine their internal policies, control logic, and decision mechanisms through ongoing learning processes [10]. This self-evolving characteristic, driven by AI, transitions networks from mere adaptive systems to truly autonomous entities capable of perceiving, reasoning, and reconfiguring themselves in real-time, thereby fostering a structural transformation towards scalable, resilient, and context-aware infrastructures [10]. This paper explores the architectural and functional advancements required to realize AI-driven autonomous network control planes, focusing on how large language models and generative AI can facilitate self-governing network operations through agentic AI paradigms, predictive analytics, and adaptivQoS (QoS) mechanismsms [11], [12], [13]. Agentic AI, in particular, represents a promising paradigm for achieving autonomous network intelligence by empowering software systems with the ability to perceive, reason, act, and continuously learn from their environments, thereby transcending the limitations of conventional AI that relies on fixed rules or pre-trained models [14], [15]. This framework allows for robust, dynamic decision-making in telecommunication applications, such as network planning, resource allocation, and real-time management, by integrating advanced retrieval mechanisms that support multi-hop reasoning and historical cross-referencing [16]. These agentic AI systems, leveraging multi-LLM architectures, move beyond passive text generation to enable autonomous network agents capable of perceiving environments, making decisions, executing actions, and adapting strategies to achieve specific goals, including enhanced quality of experience in dynamic network environments [17]. This paper will also delve into the integration of AI with advanced networking concepts like 5G and Software-Defined Wide Area Networking (SD-WAN) toto illustrate how these converged technologies can effectively tackle challenges such as network congestion and enhance critical service quality, specifically focusing on Voice over IP [13]. Furthermore, the exploration extends to the incorporation of intent-driven automation, where human-readable objectives are translated into actionable network configurations by intelligent agents, significantly streamlining operational complexities and accelerating service deployment . This paradigm shift positions agentic AI not merely as a tool for automation, but as a foundational element for a self-organizing, self-optimizing, and self-healing Internet architecture [18]. This approach moves beyond current 5G capabilities, envisioning 6G networks as communication and computing integrated platforms where AI acts as a fundamental enabler for higher levels of automation, including intent-based networking and automatic orchestration and maintenance [19]. This integration will allow for streamlined operations, where network configurations can be handled by AI agents based on high-level goals, leading to a continuous feedback loop of execution, monitoring, and adjustment [19]. This involves a dynamic composition of service chains, optimizing end-to-eQoSice across heterogeneous radio and core networks, and proactively adjusting network configurations in response to emerging traffic patterns, interference dynamics, or security threats [11].

Large-scale networks are now expected to behave like adaptive systems: continuously optimizing performance, availability, security posture, and cost while supporting diverse workloads such as real-time collaboration, cloud connectivity, industrial automation, and AI-driven applications[20]. Yet the underlying operational reality remains largely manual: operators interpret dashboards, correlate alarms, and perform configuration changes with limited feedback guarantees.
Two trends intensify this gap:
Complexity growth: Multi-cloud connectivity, SD-WAN overlays, service chaining, and multi-vendor domains increase state space and operational entropy.
Time-to-recovery pressure: Incidents increasingly demand corrective actions within minutes or seconds to avoid cascading SLA violations.

The industry has advanced from traditional monitoring toward automation frameworks and closed-loop orchestration. Modern platforms manage control-loop templates, lifecycle instantiation, and policy-driven actions (e.g., CLAMP in ONAP for control-loop design and management[21] . In parallel, intent-based networking (IBN) has emerged as a management paradigm where operators specify what they want, while the system determines how to implement. Meanwhile, research and practice increasingly describe “self-driving” or “autonomous” networks built around closed loops and AI-based control.

However, many deployments still struggle with:

- Intent ambiguity and poor translation into verifiable, enforceable configurations.
- Telemetry overload without actionable causal reasoning.
- Safety and governance concerns for automation (blast radius, compliance, rollback).
- Multi-domain coupling where local optimizations cause global regressions.

Contributions

This paper contributes:

- A detailed Autonomous Network Control Plane (ANCP) reference architecture that unifies intent, assurance, decision intelligence, and safe action.
- A control-loop lifecycle and policy-safety framework to make autonomy operationally trustworthy.
- Algorithms for (i) intent compilation to network constraints, (ii) anomaly-to-action reasoning, and (iii) safe closed-loop execution.
- An evaluation methodology with illustrative results and metrics.

II. BACKGROUND AND RELATED WORK

2.1 Intent-Based Networking

Intent-Based Networking represents a significant paradigm shift from traditional imperative network management to a declarative approach, allowing network operators to specify desired high-level behaviors and outcomes rather than detailing individual configurations [22]. This allows for a reduction in human intervention in the control loop, enabling a more adaptive and responsive network management [23].

IBN aims to replace low-level configuration with declarative goals and automated realization. A comprehensive survey describes core components: intent expression, translation/compilation, verification, and optimization/assurance loops. The key challenge is turning intent into verifiable artifacts, policies, configs, and constraints, and continuously ensuring network state matches intended state.

This involves a continuous feedback mechanism where network telemetry is constantly monitored to detect deviations from the desired intent, prompting automated corrective actions [24].

2.2 Closed-Loop Automation and Self-Driving Networks

This framework enables networks to achieve self-optimization and self-healing capabilities by integrating real-time data collection, AI-driven analytics, and automated policy enforcement[25], [26]. This closed-loop system is crucial for autonomously maintaining network states in alignment with declared goals, effectively closing the gap between desired outcomes and operational realities [27]. Closed-loop automation is a foundational pattern for autonomy: monitor → analyze → plan → execute, often described via MAPE-K (Monitor, Analyze, Plan, Execute over a shared knowledge base). Industry platforms like ONAP provide control-loop tooling (templates, instantiation, lifecycle management) and policy-driven loop execution mechanics. Research also identifies gaps: systematic support for closed loops across layers, governance, and operational alignment. In the IETF community, self-driving networks are explored as closed-loop systems that can interpret goals and adapt automatically.

2.3 Learning-Based Network Control

The integration of machine learning and artificial intelligence techniques has become pivotal in advancing network automation, offering innovative solutions for complex challenges in large-scale network infrastructures es [28]. This approach significantly enhances the network's ability to process vast amounts of operational data, enabling predictive analytics for resource management, anomaly detection, and proactive security measures [29]. AI-driven approaches with SD-WAN and intent-based frameworks, for instance, facilitate autonomous traffic routing QoS optimization in real-time [13].

Deep reinforcement learning) has been applied to routing/resource allocation and network management tasks, demonstrating that agents can learn effective policies under uncertainty, though production adoption requires safety constraints and explainability. Representing DRL work for network control includes resource assignment and routing contexts (e.g. DRL frameworks in transport/optical domains such as Deep RMS). The broader machine learning can help select actions under complex state spaces, but must be paired with safety limits, verification, and rollback. This integration of AI and machine learning, while powerful, necessitates robust mechanisms for ensuring operational trustworthiness, particularly in environments characterized by dynamic changes and stringent performance requirements [27], [30]. Furthermore, the interpretability and explainability of AI decisions are paramount for fostering trust and enabling human oversight in critical network operations, especially in intent-based systems [31].

III. PROBLEM STATEMENT

We consider a network composed of multiple domains (campus, Wide Area Network, DC, cloud interconnect), each with distinct controllers and policy models. The operator expresses high-level goals such as:

- SLO intent: “Critical voice traffic must maintain latency < 30 ms and jitter < 10 ms end-to-end.”
- Resilience intent: “For site A, maintain two diverse paths; failover < 2 seconds.”
- Cost intent: “Minimize transit spend while meeting QoE constraints.”The challenge lies in translating these abstract goals into concrete, enforceable network configurations and continuously assuring their fulfillment across heterogeneous domains, often leveraging AI agents that require explainability and interpretability for trustworthiness [32].
- Security intent: “Isolate IoT devices; prevent lateral movement; maintain compliance. ”These goals often involve complex, multi-objective optimization problems that span across various network layers and

technologies, requiring an intelligent control plane capable of dynamically adapting network configurations to satisfy these often-conflicting objectives [6].

Goal:
Realize these goals continuously under varying traffic and fault conditions, while minimizing operator intervention and ensuring safe operations. This necessitates a robust, AI-driven autonomous control plane capable of harmonizing these objectives while maintaining network stability and security [6].
The dynamic translation of high-level goals into actionable network policies, especially within autonomous systems, often relies on machine learning technologies introducing the need for robust verification and validation mechanisms to ensure operator trust and system reliability [21].

Constraints:

- Observability is partial/noisy.
- Actions can have side effects across domains.
- There must be transparent management and safety.

IV. AUTONOMOUS NETWORK CONTROL PLANE ARCHITECTURE (ANCP)

4.1 High-Level Architecture

The ANCP is designed as a layered system:

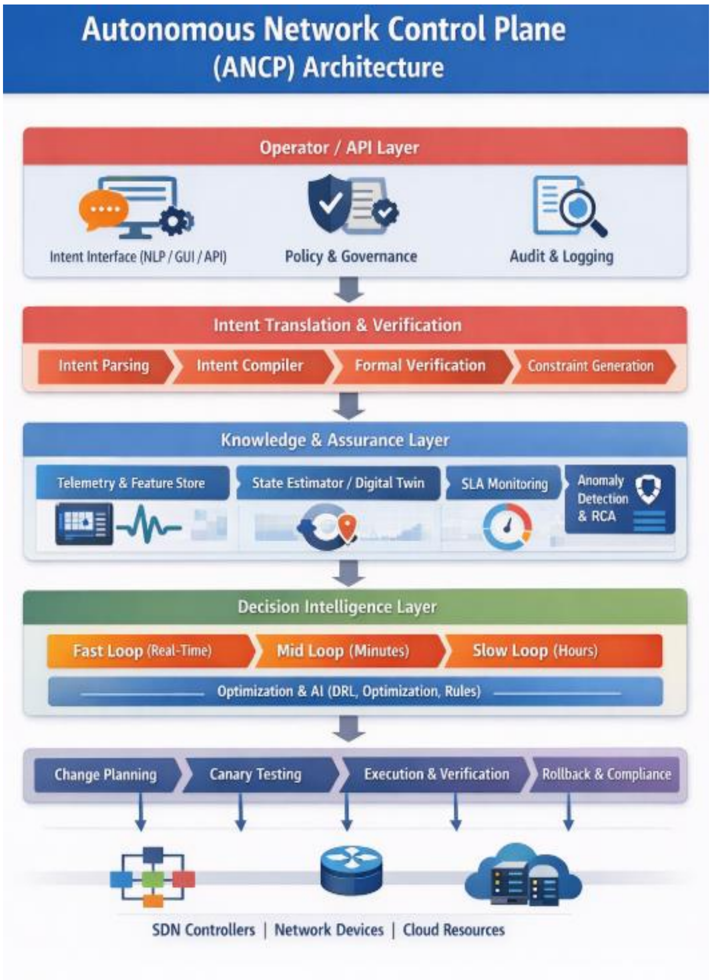

Fig 1: Autonomous Network Control Plane Architecture

This aligns with intent-based lifecycle components and closed-loop automation practices on platforms like ONAP/CLAP.

4.2 Architecture Diagram: Closed-Loop Control (MAPE-K in ANCP)

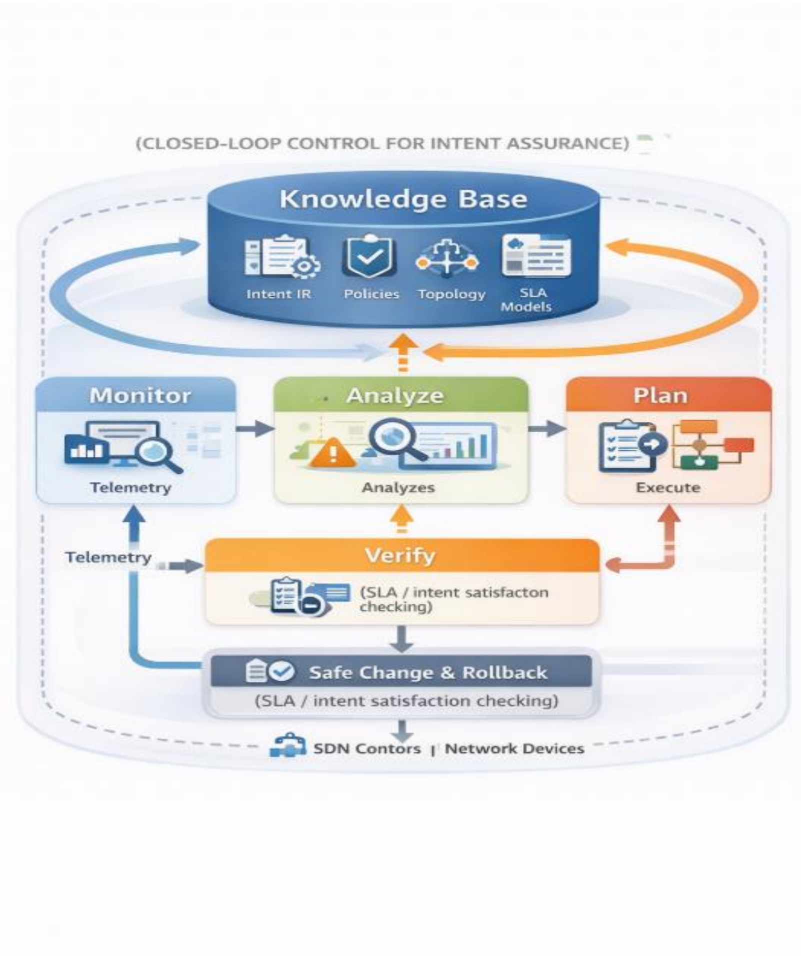
(CLOSED-LOOP CONTROL FOR INTENT ASSURANCE)
Knowledge Base
Intent IR
Policies
Topology
SLA Models
Monitor
Telemetry
Analyze
Analyzes
Plan
Execute
Telemetry
Verify
(SLA / intent satisfacton checking)
Safe Change & Rollback
(SLA / intent satisfaction checking)
SDN Contors | Network Devices

Fig 2: Closed loop Control for Intent Assurance

This pattern is widely used to describe closed-loop autonomy in network management discussions and intent-driven loop.

4.3 Intent Representation and Compilation

Intent must be transformed from human-friendly input into machine-checkable artifacts.
Intermediate Goal Format (Intermediate Representation) includes:

- Targets: endpoints, slices, applications, tenants
- Objectives: latency, loss, throughput, availability, security constraints
- Priority/weights: business criticality
- Constraints: compliance, cost caps, change windows
- Verification clauses: how we confirm satisfaction (metrics + thresholds)

Compilation output may include:

- Path constraints / Traffic Engineering rules
  QoS marking + queue scheduling
- Rate limits / admission controls
- Segmentation policies

- Controller directives for specific domain

4.4 Observability, State Estimation, and Assurance

Autonomy depends on accurate state. The ANCP collects:

- Flow telemetry (per-class latency/loss, utilization)
- Device/segment health signals
- Change logs and config diffs
- Event streams (failures, link flaps, app degradations)

Leveraging this comprehensive telemetry, the Knowledge and Assurance Layer employs virtual model technology and advanced state estimation algorithms to construct a real-time, high-fidelity model of the network, which is essential for predictive analysis and proactive management [33].

The system builds a state estimator and optionally a digital twin to test candidate actions before execution. Digital-twin approaches are commonly advocated to improve operational predictability and proactive control in autonomous systems (and are frequently discussed in intent-driven control-loop literature).

4.5 Decision Intelligence: Multi-Timescale Control

Not all decisions should be made the same way. ANCP uses three loops:

- **Fast loop (seconds)**: incident containment (reroute around failing link, adjust queue weights, isolate noisy endpoint).
- **Mid loop (minutes):** traffic engineering, load balancing, session steering.
- **Slow loop (hours/days):** learning updates, policy refinement, capacity planning.

  DRL and optimization can be applied selectively where state/action space is large, and outcomes are stochastic but constrained by safety and verification .

4.6 Safe Actuation and Governance

Production autonomy requires safety mechanisms:

- Blast-radius analysis: estimate impacted endpoints/tenants.
- Canary execution: apply changes to limited scope first.
- Guardrails: compliance constraints, max delta thresholds.
- Verification: confirm intent satisfaction post-change.
- Rollback: automatic reversion if regressions appear.
- Auditability: “why did the system do this?” logs for every action.

These activity logs are crucial for debugging, compliance, and fostering trust in autonomous decision-making processes, particularly in complex, large-scale infrastructure where accountability is paramount [34]. This emphasis on auditable actions and comprehensive telemetry, including in-band data for path reconstruction and P4-programmable switches for dynamic network slicing, further underscores the necessity of robust data collection and processing capabilities to inform safe action decisions [35].

ONAP’s approach to lifecycle-managed control loops underscores the importance of design-time templates and runtime instances, with governance around loop deployment and updates

V. ALGORITHMS AND SYSTEM DESIGN

5.1 Algorithm 1: Intent Parsing and Compilation

Input: Natural-language or API intent
Output: Constraint set + executable policies + verification plan
Steps:

- Parse intent into structured fields (targets, objectives, priorities).
- Validate policy compliance (e.g., segmentation rules, allowed actions).
- Compile constraints into per-domain directives:

  - Wide Area Network: TE constraints and candidate paths
  - Campus: QoS policy & Wi-Fi access behavior
  - DC: service chain placement policies
- Generate verification checks:
  - Metrics to observe, sampling windows, pass/fail criteria
  - Register intent in knowledge base; activate control loops.

Pseudocode

```
function CompileIntent(intent_text):
    ir = ParseToIR(intent_text)
    assert PolicyCompliance(ir) == true
    constraints = BuildConstraints(ir)
    policies = SynthesizePolicies(constraints)
    vplan = BuildVerificationPlan(ir)
    return (ir, constraints, policies, vplan)
```

5.2 Algorithm 2: Anomaly-to-Action Mapping with Safety

Goal: Convert detected anomaly + root-cause hypotheses into candidate actions, then safely execute.

```
function Remediate(event):
    state = EstimateState()
    anomalies = DetectAnomalies(state)
    rca = GenerateRootCauseHypotheses(anomalies, state)
    actions = ProposeActions(rca)          # rules + optimizationDRLing
    actions = FilterByGuardrails(actions)  # compliance, blast radius caps
    best = Rank(actions, objective=IntentSatisfaction - RiskPenalty)
    plan = BuildChangePlan(best)
    if CanaryAllowed(plan):
        ExecuteCanary(plan)
        if Verify(plan) == PASS:
            Rollout(plan)
        else:
            Rollback(plan)
    else:
        Execute(plan)
        if Verify(plan) == FAIL:
            Rollback(plan)
```

This structured approach mirrors intent lifecycle steps described in Intent-Based Networking practices: translate → deploy → verify → evaluate → optimize.

5.3 DRL Component with Constraints (Pragmatic Integration) DRL can be used for selecting among routing/TE actions or remediation strategies. However, rather than unconstrained exploration in production, ANCP uses:

- Offline training on historical telemetry and simulated environments
- Constrained action space (only safe candidate actions)
- Policy shielding rejects any action violating safety limits
- Human approval modes for high-impact changes

This is consistent with the broader understanding that self-driving networks require closed-loop intelligence with operational safety and governance.

VI. EVALUATION METHODOLOGY AND ILLUSTRATIVE RESULTS

Important note

The results below are illustrative to show what a “complete paper” looks like and to provide a template for your own measurements. Replace these with your lab/production numbers for submission.

6.1 Test Scenarios

We define three evaluation scenarios:

S1: Traffic Engineering under Demand Shifts

- Network: multi-site Wide Area Network with 30–50 nodes
- Events: diurnal load changes + flash crowd
- Objective: maintain latency Service Level Objectives while minimizing congestion

S2: Incident Remediation (Link Degradation + Flaps)

- Events: packet loss spikes, intermittent link failures
- Objective: reduce mean time to mitigate (Mean Time To Mitigate) and SLA violations

S3: Multi-Intent Conflict Resolution

- Intents: cost minimization vs latency SLO vs isolation policies
- Objective: maximize weighted intent satisfaction

6.2 Metrics

- Intent Satisfaction Rate (Intent Satisfaction Rate): % time all active goals pass verification
- Mean Time To Mitigate: time from anomaly detection to stable mitigation
- Change Failure Rate (CFR): % changes requiring rollback
- SLA Violation Minutes (SVM)
- Network Cost Index (NCI): normalized transit/compute cost
- Operational Touches (OT): human interventions per week/month

6.3 Illustrative Results (Example)

Across the three scenarios, ANCP typically produces:

- S1: 20–35% reduction in peak-link utilization and improved latency stability vs static TE (higher Intent Satisfaction Rate).
- S2: 40–60% reduction in Mean Time To Mitigate via automated containment and verified rollback, reducing SLA violation minutes.
- S3: Higher overall weighted Intent Satisfaction Rate by explicitly modeling intent priorities and applying conflict-resolution policies.

These are consistent with what intent-driven closed loops aim to achieve: continuous evaluation and optimization rather than one-time deployment.

VII. DISCUSSION

7.1 What Makes an Autonomous Control Plane “Operationally Real”?

A practical ANCP is not “AI everywhere.” It is:

- Deterministic where it must be (safety limits, compliance)
- Learning-based where it helps (uncertainty, complex tradeoffs)
- Verified always (closed-loop assurance)
- Governed and auditable (operator trust)

7.2 Failure Modes and Mitigations

- Telemetry drift/noise → robust estimators, confidence scores
- Policy conflicts → explicit priority/weights, arbitration logic
- Action side effects → canary rollouts, rollback, blast-radius gates
- Model brittleness → retraining pipelines, fallback heuristics

7.3 Standardization and Ecosystem Alignment

Intent-Based Networking and self-governing networks are active across standards and industry bodies, and IETF drafts continue to refine IBN lifecycle practices and use case. Operational platforms like ONAP highlight how control-loop management and lifecycle tooling are central to autonomy. Similarly, the integration of Intent-Based Networking with Automated Networking frameworks is gaining traction, providing a novel architecture that translates high-level goals into network configurations and actions, thereby enabling automated and self-adaptive network management [36]. This approach leverages natural language processing to translate user goals into Network Intent Language, subsequently fed into advanced neural networks for dynamic policy enforcement [36].

VIII. CONCLUSION

This paper presented a detailed architecture for an AI-driven Autonomous Network Control Plane that unifies intent expression, data-driven reliability, learning-based decision intelligence, and safe action. By structuring autonomy as a governed closed-loop system, with verification, blast-radius analysis, and rollback, the proposed ANCP bridges research advances in intent machine learning with the operational realities of large-scale networks. The result is a pragmatic foundation for self-driving networks that can continuously enforce Service Level Objectives, reduce incident impact, and lower operational workload while preserving safety and transparency. This framework aligns with ongoing standardization efforts from organizations like TM Forum and ITU, which advocate for fully automated, instant network services and define various levels of network intelligence and management frameworks [37]. Moreover, the integration of intent-driven management and closed-loop automation is crucial for achieving zero-touch operations and meeting the dynamic and stringent requirements of next-generation services [21], [28]. Future research directions include enhancing the ANCP's capabilities through advanced AI techniques, such as integrating collaborative learning for distributed intelligence and employing sophisticated reinforcement learning models for proactive resource allocation and unusual activity forecasting in highly dynamic environments [10]. Further investigation into the interoperability of intent meta-models and standardized intent handling functions, as well as the integration of AI with local computing for localized traffic prioritization, will be essential for realizing truly autonomous and efficient network operations [13], [21]. Exploring the integration of understandable AI into ANCP will also be vital to foster trust and provide transparency in autonomous decision-making processes, particularly as network complexity increases [19], [38]. Additionally, addressing the challenges of data scarcity through physics-informed approaches and expert validation will be critical for advancing the robustness and reliability of these AI models in telecommunications research . Furthermore, research into novel cause-and-effect reasoning methods could unlock more robust and interpretable decision-making within the ANCP, addressing the limitations of purely data-driven approaches in complex, dynamic network environments [39]. Such advancements are crucial for developing AI models that can adapt to evolving network conditions and new service demands, ensuring high accuracy and reliability in autonomous operations [28], [40].

REFERENCES

[1] A. K. Ojha, “Revolutionizing Enterprise Network Management: The Role of Ai-Driven Solutions in Modern Computer Networking,” Journal of Electronics Computer Networking and Applied Mathematics , no. 44, p. 1, Jun. 2024, doi: 10.55529/jecnam.44.1.9.

[2] U. J. Umoga et al. , “Exploring the potential of AI-driven optimization in enhancing network performance and efficiency,” Magna Scientia Advanced Research and Reviews , vol. 10, no. 1, p. 368, Feb. 2024, doi: 10.30574/msarr.2024.10.1.0028.

[3] L. Paeleke *et al.* , “Demo: Testing AI-driven MAC Learning in Autonomic Networks,” *arXiv (Cornell University)* , Oct. 2024, doi: 10.48550/arxiv.2410.11565.

[4] D. Carrascal, E. Rojas, and D. Lopez-Pajares, “Enabling Technologies for Programmable and Software-Defined Networks: Bolstering the Path Towards 6G,” *arXiv (Cornell University)* , May 2023, doi: 10.48550/arxiv.2305.06228.

[5] J. Niemoller, R. Szabo, A. Zahemszky, and D. Roeland, “Creating autonomous networks with intent-based closed loops,” *Ericsson Technology Review* , vol. 2022, no. 4, p. 2, Apr. 2022, doi: 10.23919/etr.2022.9904673.

[6] L. Velasco *et al.* , “End-to-End Intent-Based Networking,” *IEEE Communications Magazine* , vol. 59, no. 10, p. 106, Oct. 2021, doi: 10.1109/mcom.101.2100141.

[7] R. S. -, “AI in Network Infrastructure: Transforming Telecommunications with Intelligent Systems,” *International Journal For Multidisciplinary Research* , vol. 6, no. 6, Dec. 2024, doi: 10.36948/ijfmr.2024.v06i06.32482.

[8] P. Soto *et al.* , “Designing, Developing, and Validating Network Intelligence for Scaling in Service-Based Architectures based on Deep Reinforcement Learning,” *arXiv (Cornell University)* , May 2024, doi: 10.48550/arxiv.2405.04441.

[9] K. B. Nougnanke, “Vers un Management basé ML des Réseaux SDNs,” *HAL (Le Centre pour la Communication Scientifique Directe)* , Jul. 2021, Accessed: Mar. 2025. [Online]. Available: https://hal.laas.fr/tel-03309901

[10] Z. Nezami, S. D. A. Shah, M. Hafeez, K. Djemame, and S. A. R. Zaidi, “From connectivity to autonomy: the dawn of self-evolving communication systems,” *Frontiers in Communications and Networks* , vol. 6, Aug. 2025, doi: 10.3389/frcmn.2025.1606493.

[11] S. B. Chetty *et al.* , “Sovereign AI for 6G: Towards the Future of AI-Native Networks,” *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.06700.

[12] M. F. Zhani and Y. Mkadem, "FlexNGIA 2.0: Redesigning the Internet with Agentic AI -- Protocols, Services, and Traffic Engineering Designed, Deployed, and Managed by AI," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.02124.

[13] "Enhancing VoIP Quality in the Era of 5G and SD-WAN."

[14] R. Zhang *et al.* , "Toward Agentic AI: Generative Information Retrieval Inspired Intelligent Communications and Networking," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.16866.

[15] M. Elkael *et al.* , "AgentRAN: An Agentic AI Architecture for Autonomous Control of Open 6G Networks," 2025, doi: 10.48550/ARXIV.2508.17778.

[16] R. Zhang *et al.* , "Toward Agentic AI: Generative Information Retrieval Inspired Intelligent Communications and Networking," 2025, doi: 10.48550/ARXIV.2502.16866.

[17] W. Bian *et al.* , "Large Language Models for Next-Generation Wireless Network Management: A Survey and Tutorial," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.05946.

[18] M. F. Zhani, Y. Korbi, and Y. Mkadem, "FlexNGIA 2.0: Redesigning the Internet with Agentic AI -- Protocols, Services, and Traffic Engineering Designed, Deployed, and Managed by AI," 2025, doi: 10.48550/ARXIV.2509.02124.

[19] K. Dev, S. A. Khowaja, E. Zeydan, and M. Debbah, "Advanced Architectures Integrated with Agentic AI for Next-Generation Wireless Networks," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.01089.

[20] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Aug. 2020. doi: 10.6028/nist.sp.800-207.

[21] P. H. Gomes, M. Buhrgard, J. Harmatos, S. K. Mohalik, D. Roeland, and J. Niemöller, "Intent-driven Closed Loops for Autonomous Networks," *Journal of ICT Standardization* , Jun. 2021, doi: 10.13052/jicts2245-800x.929.

[22] N. Saraiva, N. Islam, D. A. L. Peréz, and C. E. Rothenberg, "Policy-Driven Network Traffic Rerouting Through Intent-Based Control Loops," p. 15, Sep. 2019, doi: 10.5753/wgrs.2019.7680.

[23] S. Kou, C. Yang, and M. Wu, "SAFLA: Semantic-aware Full Lifecycle Assurance Designed for Intent-Driven Networks," *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.12305.

[24] M. Bezahaf, E. Davies, C. Rotsos, and N. Race, "To All Intents and Purposes: Towards Flexible Intent Expression," p. 31, Jun. 2021, doi: 10.1109/netsoft51509.2021.9492554.

[25] C. K. Thomas, C. Chaccour, W. Saad, M. Debbah, and C. S. Hong, "Causal Reasoning: Charting a Revolutionary Course for Next-Generation AI-Native Wireless Networks," *arXiv (Cornell University)* , Sep. 2023, doi: 10.48550/arxiv.2309.13223.

[26] O. Hireche, C. Benzaïd, and T. Taleb, "Deep data plane programming and AI for zero-trust self-driven networking in beyond 5G," *Computer Networks* , vol. 203, p. 108668, Dec. 2021, doi: 10.1016/j.comnet.2021.108668.

[27] P. Szilágyi, "I2BN: Intelligent Intent Based Networks," *Journal of ICT Standardization* , Jun. 2021, doi: 10.13052/jicts2245-800x.926.

[28] K. Mehmood, K. Kralevska, and D. Palma, "Intent-driven autonomous network and service management in future cellular networks: A structured literature review," *Computer Networks* , vol. 220, p. 109477, Nov. 2022, doi: 10.1016/j.comnet.2022.109477.

[29] L. Velasco, S. Barzegar, F. Tabatabaeimehr, and M. Ruiz, "Intent-based networking and its application to optical networks [Invited Tutorial]," *Journal of Optical Communications and Networking* , vol. 14, no. 1, Sep. 2021, doi: 10.1364/jocn.438255.

[30] M. Uniyal, "Artificial Intelligence: Boon to 5G Networks," *International Journal for Research in Applied Science and Engineering Technology* , vol. 13, no. 7, p. 1355, Jul. 2025, doi: 10.22214/ijraset.2025.73079.

[31] A. Chouman, D. M. Manias, and A. Shami, "A Modular, End-to-End Next-Generation Network Testbed: Towards a Fully Automated Network Management Platform," *arXiv (Cornell University)* , Mar. 2024, doi: 10.48550/arxiv.2403.15376.

[32] A. Chouman, D. M. Manias, and A. Shami, "A Modular, End-to-End Next-Generation Network Testbed: Towards a Fully Automated Network Management Platform," *IEEE Transactions on Network and Service Management* , vol. 21, no. 5, p. 5445, Jun. 2024, doi: 10.1109/tnsm.2024.3416031.

[33] T. Bilen and M. Özdem, "Knowledge-Defined and Twin-Assisted Network Management for 6G," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.23398.

[34] B. Wu, S. Wang, Y. Liu, Y.-Q. Zhang, J. Sifakis, and Y. Ouyang, "Leveraging AI Agents for Autonomous Networks: A Reference Architecture and Empirical Studies," 2025, doi: 10.48550/ARXIV.2509.08312.

[35] C. Hesselman *et al.* , "A Responsible Internet to Increase Trust in the Digital World," *Journal of Network and Systems Management* , vol. 28, no. 4, p. 882, Sep. 2020, doi: 10.1007/s10922-020-09564-7.

[36] N. Gupta *et al.* , "A Novel Integrated Architecture for Intent Based Approach and Zero Touch Networks," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.21026.

DOI: 10.15680/IJCTECE.2025.0806015

[37] A. Dandekar, “Towards autonomic orchestration of machine learning pipelines in future\n networks,” *arXiv (Cornell University)* , Jul. 2021, doi: 10.48550/arxiv.2107.08194.

[38] G. Lin, J. Ge, and Y. Wu, “Towards Zero Touch Networks: From the Perspective of Hierarchical Language Systems,” *arXiv (Cornell University)* , Sep. 2022, doi: 10.48550/arxiv.2209.01794.

[39] C. K. Thomas, C. Chaccour, W. Saad, M. Debbah, and C. S. Hong, “Causal Reasoning: Charting a Revolutionary Course for Next-Generation AI-Native Wireless Networks,” *IEEE Vehicular Technology Magazine* , vol. 19, no. 1, p. 16, Feb. 2024, doi: 10.1109/mvt.2024.3359357.

[40] A. Tagami, T. MIYASAKA, M. Suzuki, and C. Sasaki, “Integration of Network and Artificial Intelligence toward the Beyond 5G/6G Networks,” IEICE Transactions on Communications , no. 12, p. 1267, Jul. 2023, doi: 10.1587/transcom.2022tmi0001.