



ETSI White Paper No. 69

AI in the evolution of Autonomous Networks

ETSI perspectives and major achievements

First edition – November 2025

Authors: Raymond Forbes (Forbes Ltd.), Luigi Licciardi, Yoshihiro Nakajima (NTTdocomo), Nick Sampson (Orange), Faraz Naim (Accenture), Benoit Radier (Orange), Aldo Artigiani (Huawei), Olivier Ferveur (Post Luxembourg); Marcus Brunner (Huawei), Yuan Xie (Huawei), Fernando Camacho (Huawei), Yu Zeng (China Telecom), Ricard Vilalta (CTTC), Massimo Banzi (TIM), Christos Tranoris (University of Patras), Kostis Trantzas (University of Patras), Muslim Elkotob (Vodafone), Scott Cadzow (Cadzow Consulting), Shahar Steiff (Esthertech), Giulio Maggiore (Fibercop), Xueli An (Huawei), Haitao Xia (Huawei), DongJin Lee (SK Telecom).

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org



About the authors

Raymond Forbes
Luigi Licciardi
Yoshihiro Nakajima
Nick Sampson
Faraz Naim
Benoit Radier
Aldo Arigani
Olivier Ferveur
Marcus Brunner
Yuan Xie
Fernando Camancho
Yu Zeng
Ricard Vilalta
Banzi Massimo
Christos Tranoris
Kostis Trantzas
Muslim Elkoto
Scott Cadzow
Shahar Steiff
Maggiore Giulio Carmelo
Xiahaitao
Xueli An
DongJin Lee

Editors: Luigi Licciardi, Helene Schmidt



Contents

About the authors	2
Contents	3
Executive Summary	7
1 Introduction	8
2 The role of Artificial Intelligence in AN evolution	9
3 The evolution towards AN level 4: challenges and opportunities	10
3.1 Background on AN levels	11
3.2 Challenges in Achieving AN Level 4	11
3.2.1 Architectural complexity and integration challenges	11
3.2.2 Organisational and operational challenges	12
3.2.3 Technology maturity gaps	12
3.3 AN L4 Opportunities	12
3.3.1 Business transformation opportunities	13
3.3.2 Technical advancement opportunities	13
3.4 Moving from AN Level 3 to AN level 4 using AI	13
3.4.1 AI-enabled capabilities for Level 4	14
3.4.2 Implementation considerations	14
4 The innovative enablers	16
4.1 Network Digital Twin in AN	16
4.1.1 Core Technologies and Architectural Elements of Network Digital Twin	17
4.1.2 Enhanced Decision Making	18
4.1.3 Closed-Loop Automation Enablement	18
4.1.4 Continuous Optimisation	18
4.1.5 Testing	19
4.1.6 Benefits for Network Operators	20
4.2 GenAI for AN	20
4.2.1 The benefits and challenges of applying Generative AI in Autonomous Networks	20
4.2.2 Intent- Driven Network Management	22
4.2.3 Predictive Analytics and Optimisation	22
4.2.4 Predictive Analytics and Optimisation	23



4.2.5	Enhanced Anomaly Detection and Root Cause Analysis	23
4.2.6	Dynamic Security Policy Generation	24
4.2.7	Service Template and Code Generation	25
4.2.8	Intelligent Customer Support	25
4.3	AI agent for AN	25
4.3.1	AI agent Background	25
4.3.2	Runtime Control and Optimisation	26
4.3.3	Network Self-reflection and Self-evolving	26
4.3.4	Flexible Tool Usage for Future-Proof	27
4.3.5	Ultra-efficient Network Service	27
4.4	Autonomous Networks Data-Models and APIs	27
4.4.1	Data Models Defining Autonomous Networks	28
4.4.2	Key Stakeholders	29
4.4.3	APIs for Data Exchange	30
4.4.4	Use Cases for Data Exchange	30
5	Security and Privacy	32
5.1	Security and Privacy in AI-Driven Evolution of Autonomous Networks	33
5.1.1	The critical role of security in AN evolution	33
5.1.2	Emerging threat landscape	33
5.2	Security Challenges in Autonomous Networks	34
5.2.1	AI-driven cyber threats: The dual-edged nature of artificial intelligence	34
5.2.2	Securing network digital twins and AI agents	34
5.2.3	API security risks in autonomous networks	35
5.2.4	Zero Trust and adaptive security architectures	35
5.2.5	Privacy-preserving AI in autonomous networks	35
5.2.6	Securing generative AI in autonomous networks	36
5.3	AI-driven cybersecurity operations and automated response	36
5.4	Implementation recommendations	37
6	ETSI Technical Groups on AN: evolution and innovation	37
6.1	ISG Experiential Networked Intelligence (ISG ENI)	38
6.1.1	Technical innovations and architectural advances	38
6.1.2	New Proofs of Concept (PoCs)	39



6.1.3	Main achievements	39
6.2	ISG Zero touch network and Service Management (ISG ZSM)	39
6.2.1	Architectural innovations and frameworks	40
6.2.2	Proof of concept validation	40
6.2.3	Technical specifications and standards	41
6.3	ISG Network Functions Virtualisation (ISG NFV)	41
6.3.1	Innovative Perspectives	41
6.3.2	New Proofs of Concept (PoCs)	43
6.3.3	Main Achievements	43
6.4	TC Methods for Testing and Specifications (TC MTS)	43
6.4.1	Innovative perspectives	44
6.4.2	New PoCs	44
6.4.3	Main Achievements	44
6.5	TC Autonomic Management and Control Intelligence for Self-Managed Fixed & Mobile Integrated Networks (TC INT-AFI)	45
6.5.1	Innovative perspectives	45
6.5.2	New PoCs	46
6.5.3	Main Achievements	47
6.6	ISG 5th Generation Fixed Network (ISG F5G)	47
6.6.1	Overview of F5G Advanced and its relation to Autonomous Networks and AI	47
6.6.2	Innovative perspectives	49
6.6.3	F5G Advanced PoCs related to AN	49
6.7	TC Securing Artificial Intelligence (TC SAI)	50
6.7.1	Innovative perspectives	50
6.7.2	PoC related to AN	50
6.7.3	Main achievements	50
6.8	SDG TeraFlowSDN (SDG TFS)	51
6.8.1	Innovative perspectives	51
6.8.2	PoC related to AN	51
6.8.3	Main achievements	51
6.9	SDG OpenSlice (SDG OSL)	52
6.9.1	Innovative perspectives	52



6.9.2	PoC related to AN	53
6.9.3	Main achievements	53
7	ISG/TC/ SDG progress table	53
8	AN Ecosystem	57
9	Future perspectives and recommendations	58
10	Conclusions	60
11	References	60



Executive Summary

Modern communications networks are digital: they carry digital traffic and use digital signalling to control that traffic. The operators increasingly interact with each other and their customers in wholly digital modes. The digital transformation has impacted all of the supply chains and all of the stakeholders in networks. Autonomous Networks (AN) are going to enable the Digital Transformation by capturing detailed real time knowledge of the network to move control into the native behaviour of the network. This move to autonomy leverages Artificial Intelligence in the Network to offer savings through efficiency and targeted service offerings. Even if AN does not imply conceptually AI, being that the basic concepts (Self-X capabilities, Closed Loop, Intent driven, Network Intelligence, ...) are independent on AI, for sure AI represents an incredible enabler to fasten the path to reach full AN (corresponding AN Level 5). A recent questionnaire among the main Telco Operators shows the business value of moving forward AN level 4 first in order to achieve significant cost reduction, to improve sustainability and to open opportunities of new services to their customers.

The focus of this White Paper, that collects contributions of the ETSI Technical Groups (TC and ISG) and Software Development Groups (SDGs) involved in the evolution of AN is in the role that AI can play in the evolution of Autonomous Networks in particular to accelerate the path to achieve AN level 4 (as a first step) and to open the gateway to the Digital Transformation, with key business advantages for the whole ICT ecosystem and Enterprises.

With respect of the previous paper ETSI White Paper No. 56: "[Unlocking Digital Transformation with Autonomous Networks](#)," we focus here on the key innovative enablers, most of them supported by AI: Network Digital Twin, AI agents – AN agentic Network, Gen AI, Data models and API applied to AN evolution, by exploiting advantages, opportunities and their impacts in AN architecture.

AI is a topic where there is a worldwide debate on the correct usage of it, with reference of Security and Privacy, therefore the reader can find a dedicated chapter with analysis, observations, and suggestions. Artificial Intelligence in Autonomous Networks can transform the security landscape, introducing enhanced defensive capabilities and novel threat vectors. As networks evolve toward higher levels of autonomy, establishing robust security framework is mandatory to ensure reliable, trustworthy, and resilient network operations. Nevertheless, AI systems process subscriber data, network telemetry, and service assurance information, so that AN must implement privacy-preserving AI techniques, including federated learning, homomorphic encryption, and differential privacy, to ensure data confidentiality.

The innovation related to AI in Network evolution to move forward AN L4/ L5 brought new blood to most ETSI TCs/ ISGs so that the White Paper also reports the innovative perspectives, the new scenarios and Proof of Concepts (PoC) and the main achievements to the attention of the reader.



PoCs developed in ETSI on AI for AN achieved relevant interest in the ICT ecosystem and were shared with major Fora and standard organisations, including 3GPP, TM Forum, ITU-T and GSMA.

The recent evolution in ETSI on Software development with the creation of SDGs is well represented here, focusing on the use of LLMs for intent-driven networking, enabling operators to input high-level service requests in natural language, allowing AI-driven engines to interpret, classify, and translate these requests into configurations.

The ICT ecosystem is developing a significant effort on Autonomous Networks, most Fora, SDO and Alliances are investing on this evolution of the Network; opportunities of exchange of information, workshops, APIs development are active as well and ETSI is playing a significant role. AN can bring to 5G advanced/5.5 G and Optical Networks evolution (F5G) a significant added value. AN enhanced by AI capabilities is considered also as a possible requirement for 6G, that might be the first AN native technology.

1 Introduction

As the telecommunications landscape continues to evolve, the integration of Artificial Intelligence (AI) into autonomous networks has become a cornerstone for next-generation infrastructure development. Autonomous networks, characterised by their ability to operate independently and adapt to changing conditions, represent a fundamental transformation in how modern technological infrastructure functions.

AI, with its broad spectrum of capabilities including machine learning, deep learning, and cognitive computing, serves as the enabling force behind this network evolution. These technologies provide autonomous networks with the ability to discern meaningful patterns within vast datasets, make intelligent decisions, and continuously improve operations without, or with limited, human intervention.

An autonomous network can be considered as a network presenting the following properties:

- **Self-configuration:** The network can automatically configure its components and adapt to changes without human intervention.
- **Self-optimisation:** The network continuously monitors and optimises its performance to meet service requirements.
- **Self-healing:** The network can detect, diagnose, and recover from faults and failures.
- **Self-protection:** The network proactively identifies and mitigates security threats and vulnerabilities.
- **Self-learning:** The network learns from experience and improves its operations over time.



The convergence of AI and autonomous networks represents a significant advancement in network automation and intelligence. While traditional networks rely on predetermined rules and algorithms, AI-enhanced autonomous networks introduce a new dimension of adaptability and intelligence. This combination enables networks to not only react to known scenarios but also to develop innovative responses to unprecedented situations. The potential applications span multiple domains, from dynamic network topology optimisation and predictive maintenance to adaptive security measures and intelligent resource allocation.

This White Paper explores how AI is transforming autonomous networks, examining both current implementations and future possibilities. The analysis covers the technical foundations, challenges, and opportunities that arise from this integration, with a particular focus on practical applications in telecommunications and enterprise networks. Through case studies and technical analysis, the paper demonstrates how this technological convergence is shaping the future of network automation and contributing to the evolution of AI driven network systems.

2 The role of Artificial Intelligence in AN evolution

The evolution of autonomous networks represents a fundamental shift in how telecommunications and network infrastructure operate, with artificial intelligence serving as the cornerstone of this transformation. AI is transforming network operations from reactive to cognitive, enabling the creation of fully autonomous networks, improving both efficiency and user experience. The following paragraphs demonstrate how AI is addressing the properties introduced in the previous clause [1], [2].

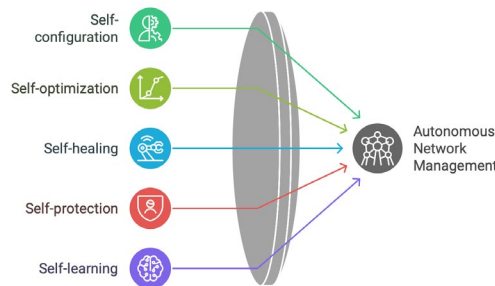


Figure 1: AN self-X capabilities

Self-configuration allows networks to automatically adapt to changes without human intervention. AI achieves this through machine learning algorithms that detect new network elements, understand their capabilities, and seamlessly integrate them into existing infrastructure. Deep learning models analyse network topology and traffic patterns to determine optimal configurations, significantly reducing the need for manual setup and maintenance.

Self-optimisation uses AI systems to continuously process vast amounts of performance metrics and telemetry data. Advanced analytics and reinforcement learning algorithms enable real-time decision-making for resource allocation, traffic routing, and quality of service management. Through Network Digital Twins, AI-powered simulations aid in network planning and predict the impact of changes before they're implemented, ensuring optimal performance.

Self-healing leverages AI's diagnostic capabilities through AIOps (AI for IT Operations). Machine learning models identify patterns in network behaviour that precede failures, enabling predictive maintenance. When issues occur, AI systems quickly isolate problems, determine root causes, and implement corrective actions. Natural language processing enhances this capability by analysing error logs and system messages for more accurate fault diagnosis [3].

Self-protection uses AI to strengthen network security through advanced threat detection and response mechanisms. Anomaly detection algorithms identify unusual patterns that may indicate security breaches, while behavioural analysis models track and flag suspicious activities. AI-powered security systems can automatically adjust security policies and implement countermeasures against emerging threats, though this raises important considerations about privacy and cybersecurity.

Self-learning represents AI's most transformative impact. Through continuous analysis of network operations and outcomes, AI systems build increasingly sophisticated models of network behaviour. These models improve over time through techniques like transfer learning and federated learning, allowing networks learning to adapt to new situations and requirements more effectively.

Industry frameworks guide the implementation of these autonomous capabilities. The TM Forum's Autonomous Network Framework defines six levels of automation, from fully manual (0) to fully autonomous (5), providing a roadmap for network evolution. Similarly, the NGMN Alliance offers guidance on use cases, requirements, and architectural principles for AI-based autonomous networks [4], [5].

3 The evolution towards AN level 4: challenges and opportunities

The evolution toward Autonomous Networks Level 4 (AN L4) represents a critical milestone in telecommunications infrastructure development, where networks achieve high-level autonomy with minimal human intervention while maintaining strategic oversight for complex decision-making. This transformation enables communications service providers (CSPs) to operate more efficiently, deliver enhanced customer experiences, and accelerate innovation through zero-touch, zero-wait, and zero-trouble service delivery.



3.1 Background on AN levels

The TM Forum IG1230 [49] framework defines six autonomous network levels (L0 to L5) based on the degree of human and system participation in network management workflows. TM Forum IG1252 AN Level Evaluation Methodology defines a classification system and evaluation guideline which provides a structured approach to understanding and implementing network autonomy progression.

The following figure shows a simplified view of AN levels.

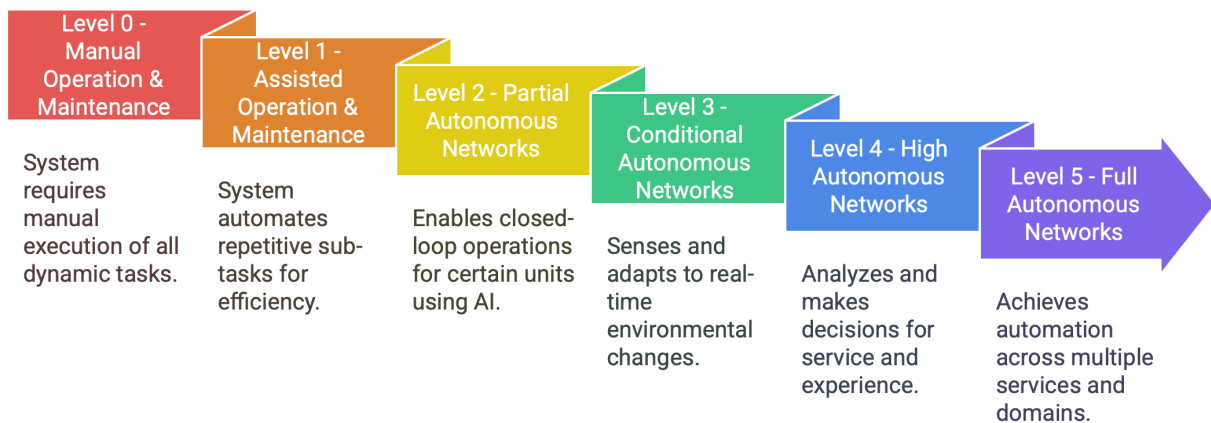


Figure 2: AN Levels features

3.2 Challenges in Achieving AN Level 4

The transition to AN L4 presents several technical and organisational challenges that CSPs must address systematically. CSPs leverage TM Forum's AN assessment e.g., GB1059A to evaluate their current AN level and identify gaps to achieve the AN L4 target state. Through this process, CSPs have also consensus on the key challenges that hinder progress toward L4.

Based on the TM Forum's work, various technology and network domain specific assessment and classifications are possible. For example, see in paragraph 7.6.2 the F5G AN definition and classification for the optical network domain.

3.2.1 Architectural complexity and integration challenges

Evolution path uncertainty: Approximately 50% of CSPs cite difficulties in integrating autonomous network layers and the absence of clear L4 end-to-end architecture evolution paths as primary obstacles. The complexity of transitioning from existing infrastructure while maintaining service continuity requires comprehensive migration strategies and intermediate architectural states.



Technology integration complexity: While enabling technologies such as machine learning, large language models, generative AI, and network digital twins are maturing rapidly, their effective integration to deliver measurable business value remains challenging. CSPs require clear implementation roadmaps that define technology deployment sequences, integration points, and success metrics.

3.2.2 Organisational and operational challenges

Operational silos: Traditional CSP organisational structures built around linear software processes managed by separate teams (fulfilment, service activation, assurance) present significant barriers to AN L4 implementation. The necessity of organisational restructuring, combined with skills gaps in automation and AI capabilities, represents a fundamental challenge requiring strategic workforce transformation.

Human-machine collaboration frameworks: While AN L4 aims to minimise human intervention, effective human oversight mechanisms remain essential for strategic decisions and exception handling. Developing robust frameworks for human-machine collaboration that ensure operators can intervene appropriately while maintaining system autonomy represents an ongoing challenge.

Operational skills: technologies are evolving at an impressive speed. It is mandatory for CSPs to keep its operational staff constantly updated to the evolution of these new technologies. Too much often the staff don't know how to handle these new tools: they use them rarely and often poorly. Continuous training is becoming more and more important to enable a full exploitation of the possibility offered by AI applied to ANs.

3.2.3 Technology maturity gaps

Cross-domain orchestration: Achieving seamless automation across multiple network domains (access, transport, core, cloud) requires sophisticated orchestration capabilities that can manage dependencies, resolve conflicts, and optimise resource allocation holistically.

Cognitive decision-making: Implementing AI systems capable of making complex, context-aware decisions across diverse scenarios while maintaining predictability and auditability remains technically challenging.

3.3 AN L4 Opportunities

Despite these challenges, AN L4 presents significant opportunities for competitive advantage and operational excellence.



3.3.1 Business transformation opportunities

Accelerated service delivery: AN L4 enables rapid service instantiation and modification, reducing time-to-market for new offerings and improving customer satisfaction through responsive service delivery.

Operational cost reduction: Automated fault resolution, predictive maintenance, and optimised resource utilisation contribute to substantial operational expenditure reductions while improving service reliability.

Innovation acceleration: The foundation provided by AN L4 enables CSPs to rapidly experiment with new services and business models, supporting digital transformation initiatives and market differentiation.

Effectiveness Metrics for AI-Enhanced AN Business Impact: A critical aspect is the measure of the impact that comes from introducing AI into AN to reach AN L4. There are several documents delivered by TM Forum on such aspects, contributed mainly by China Mobile and China Unicom (e.g., IG1256 Autonomous Networks Effectiveness Indicators, IG1256C China Unicom Practice on Autonomous Networks Effectiveness Indicators). These studies outline the effectiveness in investing to reach such a Network level of automation that is indeed a huge investment for a CSP.

3.3.2 Technical advancement opportunities

Enhanced customer experience: Proactive service optimisation, automated problem resolution, and personalised service delivery improve overall customer experience metrics and reduce service-affecting incidents.

Network optimisation: Continuous performance monitoring and automated optimisation deliver improved network efficiency, better resource utilisation, and enhanced service quality.

Scalability improvements: Automated scaling capabilities enable CSPs to handle traffic variations and service demand fluctuations more effectively while maintaining service quality.

3.4 Moving from AN Level 3 to AN level 4 using AI

The transition from Level 3 to Level 4 represents a fundamental shift from reactive awareness to proactive intelligence. While Level 3 provides management systems with situational awareness, Level 4 introduces AI-driven deep analysis and autonomous decision-making capabilities.



3.4.1 AI-enabled capabilities for Level 4

Predictive analytics: AI systems analyse historical and real-time data to predict network behaviour, service demand, and potential failures, enabling proactive management actions.

Cognitive decision-making: Machine learning algorithms process complex, multi-dimensional data to make informed decisions across scenarios where rule-based systems prove insufficient.

Cross-domain intelligence: AI enables intelligent coordination across network domains, optimising end-to-end service delivery while managing resource dependencies and constraints.

3.4.2 Implementation considerations

Scenario-based deployment: Initial AN L4 implementations typically focus on well-defined scenarios with limited decision-making scope, gradually expanding to more complex use cases as confidence and capabilities mature. TM Forum IG1339 shows the 20 high-value scenarios identified as priorities for the next two years. The following Table associates AI capabilities to the mentioned scenarios.

Table 1: AI enabling capabilities for the priority Operations scenarios

AI enabling capabilities	Service Operation Scenarios	Network Operation Scenarios
AI-driven demarcation and diagnosis, self-guided assistance, and minimal dispatch based on autonomous rectification	<ul style="list-style-type: none"> Individual Service Complaint Handling Home Broadband Complaint Handling 5G2B Service Complaint Handling IoT Service Complaint Handling 	<ul style="list-style-type: none"> Wireless Network Fault Management Core Network Fault Management Transport Network Fault Management Optical Network Fault Management IP Network Fault Management
AI/GenAI- enabled closed-loops to ensure intent fulfilment	<ul style="list-style-type: none"> Individual Service Assurance Home Broadband Service Assurance Enterprise Private Line Service Assurance 5G2B Service Assurance IoT Service Assurance 	<ul style="list-style-type: none"> Wireless Network Quality Optimisation Transport Network Quality Optimisation IP Network Quality Optimisation Wireless Network Energy Efficiency Optimisation Optical Network Energy Optimisation
AI-powered Cognitive decision-making, effect simulation	<ul style="list-style-type: none"> Enterprise Private Line Service Provisioning 5G2B Service Provisioning 	<ul style="list-style-type: none"> Core Network Change Transport Network Change IP Network Change

Regulatory compliance: Many scenarios require human validation of AI-generated decisions due to regulatory requirements, requiring efficient human-in-the-loop processes that maintain autonomy benefits while ensuring compliance.

Risk management: Comprehensive validation, testing, and rollback capabilities ensure that AI-driven decisions maintain network stability and service quality.



The evolution to AN L4 represents a significant opportunity for reducing operational costs and improving service delivery, positioning CSPs for success in increasingly competitive telecommunications markets while establishing the foundation for eventual progression to full autonomy.

The usage of AI capabilities in autonomous networks requires careful consideration of several factors, concerning Data Privacy and Security (see Chapter 6) and Validation and Safety.

“Organisations must establish safeguards when training AI models on network data, ensuring proprietary configurations and operational parameters remain protected. Data privacy protocols must include access controls, encryption standards, and anonymisation techniques preventing unauthorised infrastructure access.

Secure customer data processing demands privacy-preserving AI techniques such as federated learning, differential privacy, and homomorphic encryption. These approaches enable valuable insights from customer patterns while maintaining privacy protection and regulatory compliance with GDPR and telecommunications-specific standard.

Ensuring AI-generated network configuration reliability requires systematic validation processes verifying accuracy before production implementation. Organisations must establish testing frameworks evaluating configurations against network requirements, compatibility constraints, and performance benchmarks through automated testing and human verification protocols.

Clear escalation procedures define when automated decisions require human intervention, establish approval workflows, and ensure critical issues receive qualified personnel attention. These procedures specify AI system decision boundaries and maintain stakeholder communication for significant modifications.

Particular care should be applied to *Resource and Model management*: Effective Generative AI deployment requires balancing computational requirements with available network resources, ensuring AI processing doesn't impact core network functions. Resource allocation strategies must reserve computational capacity for AI operations while maintaining adequate resources for primary services and emergency response.

Regular model updating and fine-tuning ensures continued effectiveness as conditions evolve. This involves monitoring performance metrics, identifying prediction accuracy degradation, and implementing retraining procedures incorporating new data while preserving learned behaviours.

Addressing algorithmic bias requires diverse training data representing full operational scenarios. Organisations should establish quality monitoring identifying bias sources, implement correction mechanisms ensuring fair decisions, and maintain assessment programs detecting emerging issues.

Model deployment optimisation involves efficient distribution mechanisms, edge computing capabilities reducing latency, and monitoring systems tracking production performance while considering topology constraints and scalability needs” [6].

4 The innovative enablers

In AN framework especially L4 Reference Architecture, full-stack AI is introduced as an important concept, it means AI will be used in each operation layer for implementing intelligent applications or management services, and the effective cross-layer AI collaboration will make it possible to complete increasingly complex tasks. Figure 3 provides an example of a high-level illustration of the capabilities provided by an Autonomous Networks, in which the related innovative enablers are described in the following sections.

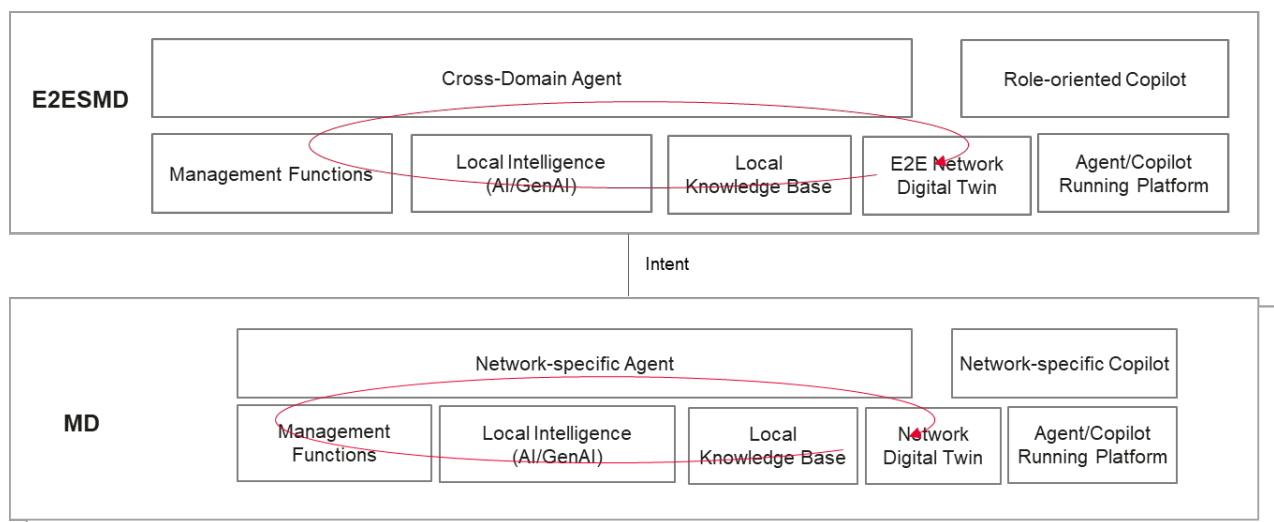


Figure 3: High-level illustration of capabilities of AN L4 Framework

The Cross-Domain (AN) Agent manages provisioning, assurance, and quality supervision with continuously closed-loop using AI-driven logic. While the Network-specific Agent optimises configurations, diagnose faults, and tune performance parameters dynamically. These agents implement network or service scenario (e.g., service assurance, network fault management) autonomously assuring by AI/GenAI, Knowledge, Network Digital Twin, etc.

4.1 Network Digital Twin in AN

A Network Digital Twin (NDT) enhances autonomous network operations by providing a virtual replica of a communications network, enabling advance modelling, simulation and decision-making:

Modeling and Simulation: NDTs simulate various network scenarios and operations, predicting outcomes and impacts before execution on the actual network. This allows for informed decision-making and risk mitigation.



Dynamic Behaviour Modeling: NDTs continuously update their models based on real-time data from sensors, telemetry, and anomaly detection systems, reflecting the ever-changing state of the physical network environment.

Automation Support: NDTs provide information to automated operations systems, enabling them to make decisions and take actions based on predicted outcomes and real-time network conditions.

Adaptive to Variations: NDTs are designed to handle variations in network size, equipment types, and data sources, ensuring accurate modeling regardless of the specific physical network configuration.

In essence, NDTs empower autonomous networks by providing a virtual sandbox for experimentation, predictive insights for informed decision-making, and a framework for continuous optimisation and adaptation. By leveraging advanced simulations, AI-driven modeling, and closed-loop automation, NDTs empower networks to become self-healing, self-optimising, and self-configuring, ultimately leading to higher reliability, efficiency, and operational agility—without risking live network disruptions. This makes the NDTs a key enabler for autonomous networks.

4.1.1 Core Technologies and Architectural Elements of Network Digital Twin

At the heart of autonomous network transformation, the Network Digital Twin [7] relies on a synergy of advanced technologies and architectural principles. Central to its construction are robust data acquisition mechanisms that continuously harvest telemetry, sensor outputs, and historical performance metrics across the network's breadth. This diverse data landscape is fundamental for accurate modelling and simulation.

A layered AI analytics stack sits atop these data streams, employing machine learning and deep learning algorithms to uncover patterns, detect anomalies, and generate predictive insights. The integration of real-time data pipelines ensures that the digital twin remains a living, adaptive entity—capable of reflecting the ever-evolving reality of the physical network.

Scalable computing infrastructure, often cloud-native, powers the twin's simulation engines, enabling rapid experimentation with new configurations or operational strategies. Modular microservices orchestrate the twin's virtual components, providing flexibility and extensibility as network requirements shift. The architecture embraces a closed-loop paradigm: insights gained through simulation directly inform automated decision systems, which in turn feed new outcomes and data back into the twin for continuous refinement.

Security and privacy considerations are woven into every layer, safeguarding sensitive network information while enabling transparent collaboration between network operators and AI-driven management platforms. Through standardised APIs and interoperable interfaces, the Network Digital Twin integrates seamlessly with existing orchestration and management tools, fostering a holistic approach to autonomous operations.

Ultimately, these architectural elements position the Network Digital Twin not just as a static model, but as an intelligent, dynamic partner in the pursuit of operational excellence—laying the foundation for the advanced capabilities described in subsequent sections.

4.1.2 Enhanced Decision Making

NDTs go beyond simply mirroring the current network state. They leverage historical data, real-time telemetry, and machine learning algorithms to predict future network behaviour. This includes forecasting traffic patterns, identifying potential bottlenecks, and anticipating equipment failures before they occur.

Furthermore, Operators can use NDTs to explore different operational scenarios such as changes in traffic load, configuration adjustments, or even simulated outages without affecting the live network. This allows for risk assessment and optimisation of configurations before implementation.

4.1.3 Closed-Loop Automation Enablement

NDTs play a crucial role in enabling zero-touch network management by continuously feeding real-time insights into closed-loop automation systems. For example:

- If an NDT predicts congestion on a specific link, it can automatically trigger traffic rerouting or resource allocation adjustments in the physical network.
- An NDT detecting a potential hardware failure can initiate automated repairs or software updates, minimising downtime and service disruptions.

In addition, NDTs play a crucial role in intent-based network management. Operators define desired outcomes (intentions), and the NDT can be used to explore multiple solutions to find the best operational strategy to implement those intentions into the network infrastructure.

4.1.4 Continuous Optimisation

NDTs analyse current and predicted traffic conditions to determine the optimal routing paths, bandwidth allocation, network configurations and resource distribution. This improves Quality of Service (QoS) and ensures efficient network utilisation.

Moreover, NDTs can incorporate feedback from real-world network operations, refining their models and decision-making algorithms over time. This enables the network to learn from past events and adapt to changing traffic patterns, user demands, and emerging threats.



4.1.5 Testing

NDT is also a key issue for testing AN and innovative Networks (5G, F5G, 6G); the most significant use cases for testing purposes are the following:

1. Pre-deployment Testing

Before rolling out new network services or configurations, NDTs allow engineers to *validate changes virtually*. For example, an operator can test new 5G slicing strategies, routing policies, or QoS configurations in the twin without risking disruption in the production environment.

2. Performance Benchmarking

NDTs can replicate various traffic loads, device failures, or congestion scenarios to evaluate system resilience. They allow benchmarking of throughput, latency, jitter, and packet loss under controlled yet realistic conditions.

3. Failure and Fault Testing

Injecting faults into a live network is impractical, but in a digital twin, operators can *simulate failures* (e.g., link breakdowns, DDoS attacks, or equipment outages) to evaluate recovery mechanisms, redundancy planning, and self-healing protocols.

4. Security Testing

Cyberattacks such as man-in-the-middle, DoS, or malware propagation can be simulated in the NDT to assess network defenses. This helps in *validating intrusion detection systems (IDS), firewalls, and zero-trust models* before deployment.

5. Regression Testing After Updates

Whenever software upgrades or patches are rolled out, NDTs enable regression testing by mirroring the pre- and post-update network state. This ensures backward compatibility and operational stability.

6. Benefits of Using NDT for Testing

- *Risk-Free Environment*: Safe testing of changes without impacting live networks.
- *Cost-Efficiency*: Reduces need for expensive lab setups and physical testbeds.
- *Scalability*: Supports large-scale and complex test scenarios that would be impractical in real deployments.
- *Predictive Insights*: AI-driven analytics help forecast performance under future workloads.
- *Faster Innovation*: Accelerates service rollout by enabling rapid prototyping and validation.



4.1.6 Benefits for Network Operators

Key benefits for operators include:

- Reduced downtime: Proactive fault detection and automated remediation minimise service interruptions.
- Improved Resource Utilisation: Dynamic allocation of resources based on real-time demand optimises network efficiency.
- Enhanced Security: NDTs can identify anomalies and potential security threats, allowing for quicker response and mitigation efforts.
- Higher level of network autonomy: Automated workflows and centralised monitoring reduce the complexity of managing large and complex networks.

For AN and the new network technologies NDTs are expected to evolve *from testing tools into decision-making companions* for network operators. They will enable continuous validation, proactive fault prevention, and closed-loop automation. Testing standardisation efforts in **ETSI** can move towards the Specific Digital Twins for the component under evaluation, *providing a virtual test environment* that mirrors the real network. Instead of executing test specifications on hardware or live infrastructure, they are executed through NDT.

- This allows *repeatability* of tests.
- Tests can be run *on a scale and under diverse conditions* (e.g., high traffic, fault injection, security attacks).
- The risk of production is eliminated, the quality of test specification and feedback to base standards increase.

4.2 GenAI for AN

4.2.1 The benefits and challenges of applying Generative AI in Autonomous Networks

Generative AI (GenAI) represents a transformative advancement in enabling and enhancing Autonomous Networks (AN) by improving their intelligence, adaptability, and interaction capabilities. By leveraging Large Language Models (LLMs) and other generative capabilities, GenAI significantly enhances network automation, optimisation, and self-management across multiple domains.



Benefits:

GenAI introduces natural language interfaces that dramatically simplify complex network management tasks, enabling operators to interact with network systems using intuitive conversational commands rather than complex technical syntax. The technology demonstrates remarkable ability to generate adaptive responses to novel network conditions that fall outside predetermined rule sets, providing flexibility in managing unexpected scenarios and emerging challenges.

The sophisticated pattern recognition capabilities inherent in GenAI significantly enhance anomaly detection systems, identifying subtle deviations in network behaviour that traditional monitoring systems might overlook. Enhanced context-aware decision-making enables networks to consider broader operational contexts when making autonomous decisions, leading to more intelligent and appropriate responses to complex situations.

Automated documentation and knowledge management capabilities ensure that network configurations, changes, and operational procedures are continuously documented and updated, reducing the burden on human operators while maintaining comprehensive operational records. Improved human-machine collaboration emerges through intuitive interfaces that bridge the gap between technical complexity and operator understanding, enabling more effective partnership between human expertise and machine intelligence.

Challenges and LLM Limitations:

Scale and Processing Constraints: Current LLMs have context windows that are insufficient for processing the massive volumes of data generated by large-scale networks. Even advanced models struggle to simultaneously analyse comprehensive network states, forcing implementations to rely on selective data sampling that may miss important patterns.

Computational Requirements: The computational demands of running sophisticated LLMs for network operations are substantial, creating both economic and practical deployment challenges, particularly for edge network components where resources are limited.

Performance Considerations: Network operations often require near-instantaneous decision-making, but current LLM inference times introduce latency that may be unacceptable for time-critical functions, necessitating architectural compromises.

Domain Knowledge Gaps: While LLMs exhibit impressive general capabilities, they often lack specialised telecommunications knowledge, requiring fine-tuning on domain-specific datasets and integration with existing systems.

Reliability Concerns: LLMs are prone to hallucinations that could lead to incorrect network configurations. This necessitates verification mechanisms and appropriate human oversight for critical operations.



To address these challenges, practical implementations typically employ a layered approach combining specialised models for real-time operations with larger models for planning and analysis tasks, along with hybrid architectures that leverage traditional rule-based systems for critical functions while incorporating GenAI capabilities where appropriate.

4.2.2 Intent- Driven Network Management

GenAI models, particularly LLMs [7], together with agentic technologies, enable a more intuitive way for network operators to express requirements and goals using natural language instructions rather than low-level technical commands. These models can interpret high-level business intents like "optimise the network for video streaming during peak hours" and automatically translate them into detailed network policies, configurations, and quality of service parameters. This abstraction layer significantly reduces management complexity while ensuring business objectives are accurately reflected in network operations.

4.2.3 Predictive Analytics and Optimisation

By analysing vast amounts of historical and real-time network data, GenAI models and AI agents can:

- Predict future network behaviour and potential issues before they occur;
- Generate synthetic data to simulate various scenarios;
- Create more accurate predictions of network behaviour and scale;
- Develop sophisticated "what-if" scenarios for capacity planning;
- Generate adaptive thresholds for performance monitoring, network scale and security requirements.

This enables proactive network management and continuous optimisation without impacting live operations.

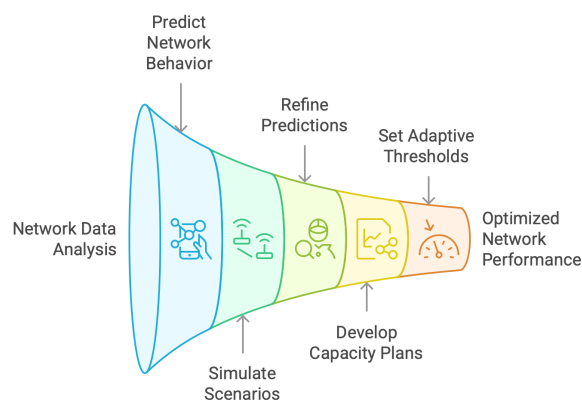


Figure 4: Predictive analytics for Network Optimisation

4.2.4 Predictive Analytics and Optimisation

GenAI and multiple AI agents are used to assist in the task of network planning by:

- Generating optimal network topologies based on projected demand;
- Creating capacity plans considering geographic, political and legal constraints;
- Developing equipment configurations and upgrades aligned with business objectives;
- Exploring multiple design options rapidly;
- Recommending cost-effective and performant solutions.

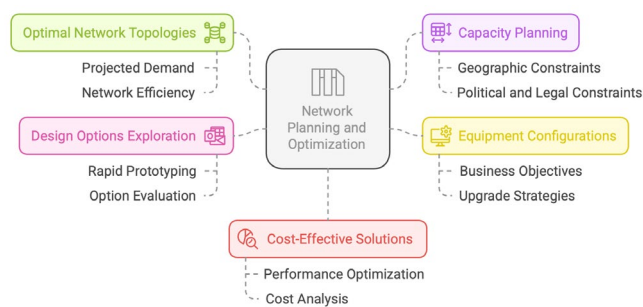


Figure 5: Gen AI for Network planning

4.2.5 Enhanced Anomaly Detection and Root Cause Analysis

GenAI models and AI agents learn complex patterns in network behaviour to detect subtle anomalies that traditional rule-based systems might miss. When issues occur, GenAI enhances self-healing capabilities by: Generating detailed problem descriptions from network symptoms; proposing potential solutions based on historical resolution data; creating step-by-step remediation plans; documenting incident responses for future reference.

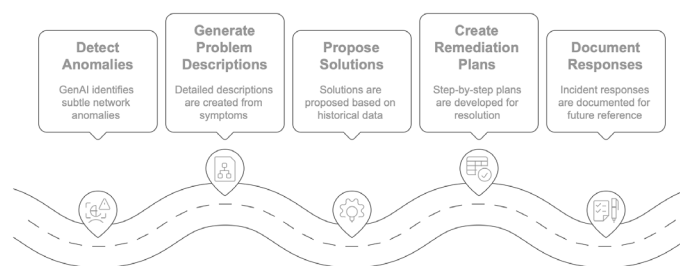


Figure 6: Gen AI for self-healing

This can significantly reduce the mean time to repair (MTTR).

4.2.6 Dynamic Security Policy Generation

As network threats evolve, AI can strengthen network security by enhancing threat intelligence and policy management capabilities. When properly configured and with appropriate oversight, AI systems can: Analyse and identify network threats in real time; provide recommendations for security policy updates; generate potential adaptive firewall rules and access controls; support the development of intrusion detection signatures; offer policy conflicts resolution strategies.

It is imperative to note that the actual implementation of AI-generated security policies, particularly those involving firewall rules and access controls, should remain within the decision-making authority of network administrators. Organisations should carefully evaluate their risk tolerance, compliance requirements, and operational context when determining the appropriate level of autonomy granted to AI systems for security policy management.

Network administrators may choose different approaches based on their specific environments: **Recommendation-only mode:** AI systems analyse threats and suggest policy changes, but all implementations require explicit human approval.

Supervised autonomy: AI can implement low-risk changes automatically while escalating significant policy modifications for human review.

Domain-restricted autonomy: AI is permitted to manage policies in specific network segments while critical infrastructure remains under direct human control.

Full autonomy: In highly specialised cases, AI may be trusted to implement policies directly, but with comprehensive audit trails and rollback capabilities.

The appropriate balance between AI assistance and human oversight should be determined by each organisation's security governance framework, with clear boundaries established for AI systems' authority to modify security policies. This approach ensures that network security benefits from AI's analytical capabilities while maintaining appropriate human judgment for critical security decisions.

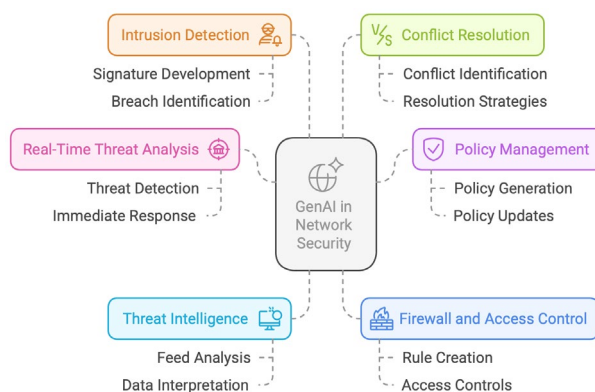


Figure 7: Gen AI for Network Security



4.2.7 Service Template and Code Generation

GenAI accelerates network automation by: Generating service definitions based on customer requirements; creating adaptable templates for various network conditions; developing test cases to validate service functionality; producing scripts and proposing code for common automation tasks; generating documentation for service deployment and maintenance.

4.2.8 Intelligent Customer Support

GenAI and agent enabled systems provide personalised, context-aware support by: Understanding complex queries from customers and operators; accessing relevant knowledge bases; generating clear, actionable responses; processing unstructured data sources like trouble tickets; providing context-aware assistance in troubleshooting see [9] Master of Code - Generative AI in Telecom.

4.3 AI agent for AN

4.3.1 AI agent Background

The NGMN White Paper [10] describes new use cases and services that need to be supported by 6G networks. These new use cases and services require 6G networks to provide ultra-high performance while connecting humans, machines and various other entities. This calls for a variety of new capabilities and requires 6G networks to have enhanced on-demand customisation capabilities to adapt to the wide range of applications autonomously. These include immersive multimedia and multi-sensory interactions, highly intelligent industrial applications, integration of physical and virtual worlds through digital twins, and ubiquitous intelligence and computing.

As described by ITU M.2160-0 [11], it is expected to integrate sensing and intelligence capabilities, empowered with AI and machine learning, into networks to keep up with the steady progress and fast spread of such. As stated in the same document, [11] could serve as an AI-enabling infrastructure that can provide services for intelligent applications listed above. Therefore, 6G networks are expected to face great challenges in the future as intelligent applications will take numerous forms and may be triggered based on user intents.

5G systems are known for their heterogeneity in service categories, such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and massive Machine Type Communications (mMTC). Such a broad diversity in service requirements calls for customised solutions by 5G network operators for their customers, which has primarily been addressed via the network slicing concept. Together with Network Function Virtualisation (NFV), network slicing allows the 5G mobile network operators to build dedicated, virtualised and logical networks on a common physical infrastructure to meet the diverse communication requirements of their customers.



In contrast to 5G networks, which are designed for providing only communication service to their users, 6G networks are envisioned to extend their services beyond connectivity. More specifically, 6G networks are expected to add AI, compute, and sensing to their services on top of connectivity, introducing new types of resources, new functionalities, and design considerations. This calls for a more flexible, autonomous, and generalisable network slicing framework for the configuration, deployment and management of such slices of new type. Since this comes with increased complexity rendering the conventional methods insufficient, the deep integration of AI agents into 6G networks offers a promising solution [49].

An example use case to be studied for the adoption of AI agents in 6G core is the optimal and flexible design of End-to-End (E2E) network slices. In such a setting, AI agents that are empowered with Large Language Models (LLMs) can be employed as an interface to support human operators in defining high-level intents and setting up optimisation tasks as external input.

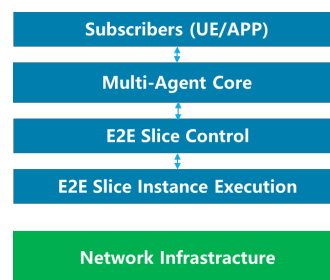


Figure 8: AI agents for AN

4.3.2 Runtime Control and Optimisation

AI agents can be introduced to 6G networks to generate the service networks on-the-fly that integrate network functions and tools provided by third parties as well as associated resources based on the intents of subscribers.

During the execution process of the service networks, AI agents can sense the changes of network environments and status autonomously, and adjust the functions, tools and resources dynamically to guarantee the QoS (Quality of Service).

4.3.3 Network Self-reflection and Self-evolving

AI agents can be used to improve the network performance continuously by: Interacting with the external environments to obtain feedback from the environments; retrieving the contextual information and combining the external feedback to check the previous decisions and performing self-reflection to generate better decisions; adopting reinforcement learning algorithms to fine-tune their local model so as to improve their capabilities.



4.3.4 Flexible Tool Usage for Future-Proof

The 6G network can integrate various kinds of tools, including network functions, application functions, and APIs, to enrich services provided by the network. One important feature of AI agents is that they can execute the tasks (e.g. through invoking tools) by themselves to achieve the goal. Facing with different tasks, the AI agents can flexibly assemble and invoke various tools to perform the tasks. Leveraging this feature, AI agents can enable the plug-and-play of new tools to make the network future-proof and make the network flexible and extensible.

4.3.5 Ultra-efficient Network Service

AI agents make network management and control completely autonomous and intelligent. When they notice that there are services in the network, they will allocate the resources on-demand for the execution of services. When they percept that the services are completed, they will recycle the resources automatically so as to save energy consumption and avoid wasting resources, achieving the goal of zero-bits-zero-watt.

4.4 Autonomous Networks Data-Models and APIs

Traditionally, Operators are embracing platform business models like network-as-a-service (NaaS) to simplify and abstract the complexity of the underlying network, leveraging APIs such as the TM Forum Open APIs. These APIs adopt a layered architecture pattern stratified into a business, service, and resource operations layer. The efficient separation of the operating domains is a prerequisite for the AN framework, providing each domain the ability to operate autonomously based on independent inputs. The precision of the latter is of utmost importance for effective closed-control loop automation. The advent of GenAI significantly infuses these inputs with the elements of creativity and improvisation, leading to an efficient way of expressing requirements, goals and constraints through Intents. Each operational layer may be subject to Intent, therefore the interaction between them is achieved through standardised interfaces and models, such as TMF921 Intent Management [13]. The Intent is equally portable across vertical operational layers and federated autonomous domains, enabling intent-drive closed loops.

Leveraging the advanced Agentic AI (i.e. AI agent) technologies, the 6G network is expected to become a service innovation platform that generates highly customised XaaS (Everything as a Service), which can flexibly assemble network functions, 3rd party application functions and APIs to provide customised services according to users' intents.

Autonomous Networks (AN) rely on well-defined data models and APIs to enable effective communication and coordination between various network components, systems, and stakeholders. This ecosystem comprises several key data models and interfaces that facilitate autonomous operations.

4.4.1 Data Models Defining Autonomous Networks

The data models for Autonomous Networks are essential for representing network elements, configurations, services, and operational states. They provide a common framework that various stakeholders can utilise to ensure consistency in data representation across diverse network environments and operational contexts.

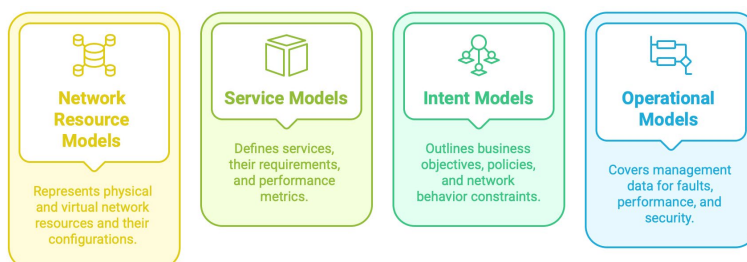


Figure 9: AN data models

Network Resource Models encompass comprehensive representations of both physical and virtual network infrastructure components, incorporating configuration parameters, operational constraints, and performance metrics essential for autonomous decision-making. These models capture resource dependencies and relationships between network components, enabling autonomous systems to understand infrastructure interconnections and optimise resource allocation through capacity and utilisation metrics that support predictive analytics and proactive management strategies.

Service Models define comprehensive service specifications including functional requirements, Quality of Service parameters, and Service Level Agreements that autonomous systems can interpret and enforce. These models explicitly capture service dependencies and customer experience metrics, enabling intelligent orchestration, conflict resolution, and autonomous optimisation decisions that maintain committed performance standards while enhancing user satisfaction.

Intent Models translate high-level business objectives and strategic policies into machine-readable formats, capturing network behaviour constraints, performance goals, security requirements, and compliance rules. These models ensure that autonomous decisions align with organisational policies and regulatory requirements while providing measurable objectives that guide optimisation processes and maintain mandatory protection mechanisms throughout autonomous operations.

Operational Models provide comprehensive frameworks for managing day-to-day network operations, encompassing fault management data, performance management metrics, security management policies, configuration management parameters, and accounting information.

These models enable autonomous healing capabilities, predictive maintenance, automated security responses, structured configuration management, and resource consumption monitoring that supports both operational efficiency and revenue management activities.

4.4.2 Key Stakeholders

Several stakeholders utilise and exchange the data represented by these data models:

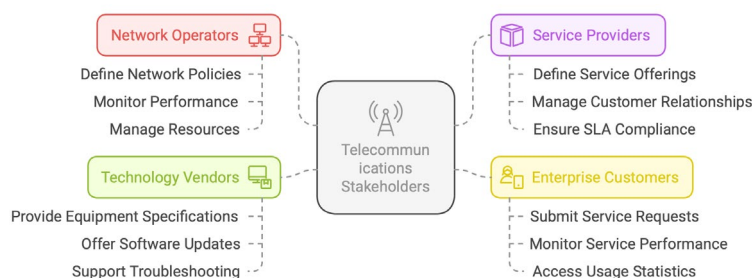


Figure 10: Key stakeholders

Network Operators (who can also assume the role of Service Providers) serve as the primary administrators of autonomous network infrastructure, defining comprehensive network policies and intents that guide automated decision-making processes. They continuously monitor network performance through sophisticated analytics platforms, manage network resources across multiple domains, handle complex service provisioning workflows, and oversee security operations to ensure robust protection against evolving threats while maintaining operational excellence and regulatory compliance.

Service Providers focus on the commercial and customer-facing aspects of autonomous network operations, defining innovative service offerings that leverage autonomous capabilities to deliver enhanced value propositions. They manage comprehensive customer relationships through automated engagement systems, monitor service quality metrics to ensure consistent user experiences, handle billing and accounting processes through integrated revenue management platforms, and ensure SLA compliance through continuous monitoring and automated remediation mechanisms.

Enterprise Customers represent the end-users of autonomous network services, actively submitting service requests through self-service portals and automated interfaces that leverage natural language processing capabilities. They monitor service performance through customised dashboards and analytics tools, report issues through integrated ticketing systems that trigger autonomous resolution processes, access detailed usage statistics for capacity planning and cost optimisation, and configure service parameters through intuitive management interfaces that translate business requirements into technical implementations.



Technology Vendors provide the foundational technologies and ongoing support that enable autonomous network operations, supplying detailed equipment specifications and technical documentation that inform autonomous configuration and optimisation processes. They develop and maintain management interfaces that enable seamless integration with autonomous orchestration platforms, deliver software updates and patches through automated distribution mechanisms, provide expert troubleshooting support for complex technical issues, and share performance metrics and analytics that contribute to continuous improvement of autonomous network capabilities.

4.4.3 APIs for Data Exchange

Management APIs provide comprehensive interfaces for network configuration and control, service provisioning and modification, resource allocation and optimisation, performance monitoring and reporting, and security policy enforcement. These APIs enable autonomous systems to manage complex network operations through standardised protocols that ensure consistent behaviour across multi-vendor environments.

Service APIs facilitate service ordering and activation, service modification and termination, SLA monitoring and reporting, usage tracking and billing, and customer support integration. These APIs enable seamless interaction between customer-facing systems and underlying network infrastructure, supporting automated service lifecycle management and customer experience optimisation.

Integration APIs enable cross-domain orchestration, multi-vendor interoperability, third-party system integration, analytics and reporting, and automation workflow management. These APIs provide the essential connectivity that allows autonomous networks to coordinate across different technology domains and vendor solutions while maintaining unified operational visibility and control.

The APIs follow a layered architecture, including business layer APIs, service layer APIs, and resource layer APIs, as exemplified by the TM Forum Open APIs.

4.4.4 Use Cases for Data Exchange

The need for exchanging data within Autonomous Networks spans multiple use cases across diverse operational domains.

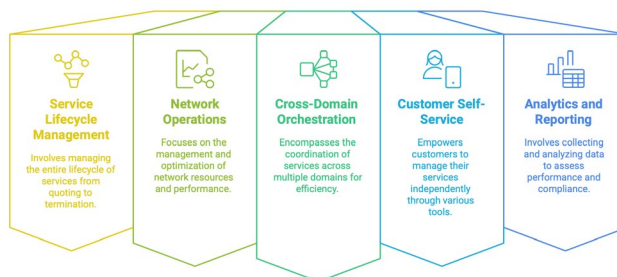


Figure 11: Data exchange operational domains

Service Lifecycle Management encompasses comprehensive quote management through Configure, Price, Quote (CPQ) systems, complete service ordering and provisioning workflows, dynamic service modification and scaling capabilities, efficient service termination and resource release processes, continuous SLA monitoring and enforcement, detailed usage tracking across all service components, and comprehensive settlement processes including invoicing, reconciliation, and payment management. These use cases require seamless data exchange between customer-facing systems, service orchestration platforms, and underlying network infrastructure to ensure efficient service delivery and customer satisfaction.

Network Operations involve sophisticated resource allocation and optimisation algorithms, comprehensive performance monitoring and troubleshooting capabilities, automated fault detection and resolution mechanisms, systematic configuration management across multi-vendor environments, and robust security policy enforcement throughout the network infrastructure. These operations depend on real-time data exchange between monitoring systems, management platforms, and network elements to maintain optimal performance and security posture.

Cross-Domain Orchestration enables multi-domain service provisioning across heterogeneous network technologies, intelligent inter-domain resource management that optimises utilisation across different network segments, comprehensive end-to-end service monitoring that provides unified visibility, coordinated cross-domain fault management that ensures rapid issue resolution, and federated security enforcement that maintains consistent protection policies. These capabilities require standardised data exchange protocols that enable seamless coordination between different network domains and management systems.

Customer Self-Service provides intuitive service catalogue browsing experiences, streamlined order placement and tracking capabilities, real-time performance monitoring dashboards, efficient issue reporting and tracking systems, and transparent usage and billing information access. These self-service capabilities rely on APIs that enable customers to interact directly with network services while maintaining appropriate security and access controls.



Analytics and Reporting encompass comprehensive performance metrics collection from all network elements, detailed resource utilisation monitoring across infrastructure components, continuous service quality assessment that informs optimisation decisions, security event tracking that enables threat detection and response, and compliance reporting that ensures regulatory adherence. These analytics capabilities require robust data aggregation and processing systems that can handle large volumes of network data while providing actionable insights.

The standardisation of these data models and APIs is crucial for achieving interoperability in autonomous networks. Industry organisations like TM Forum, ETSI, MEF, and IETF play key roles in defining standard models and interfaces. For example, TM Forum's Open APIs provide a framework for service management, while ETSI's ZSM and ENI specifications define models for automated network operations.

To ensure effective implementation, organisations should adopt industry standard data models where available, define clear data governance policies that ensure data quality and consistency, implement robust security measures that protect sensitive information, maintain comprehensive documentation and version control systems, and provide adequate training and support for technical teams. These practices ensure that data exchange capabilities support organisational objectives while maintaining security and operational excellence.

As autonomous networks continue to evolve, these data models and APIs will need to adapt to support new capabilities and use cases while maintaining backward compatibility and security. By establishing robust data models and APIs, Autonomous Networks can achieve greater interoperability, flexibility, and efficiency in managing complex network environments. This foundation is critical for realising the full potential of autonomous operations in the telecommunications landscape.

5 Security and Privacy

The integration of Artificial Intelligence in Autonomous Networks fundamentally transforms the security landscape, introducing both enhanced defensive capabilities and novel threat vectors. As networks evolve toward higher levels of autonomy, establishing robust security frameworks becomes paramount to ensuring reliable, trustworthy, and resilient network operations.



5.1 Security and Privacy in AI-Driven Evolution of Autonomous Networks

5.1.1 The critical role of security in AN evolution

Security serves as the foundational cornerstone for successful autonomous network deployment. AI-driven mechanisms that enhance self-optimisation, self-healing, and self-management capabilities across mobile, transport, access, OSS/BSS, and core network domains introduce new attack surfaces while simultaneously providing advanced defensive capabilities. The increased reliance on AI for real-time decision-making raises fundamental concerns about trustworthiness, accountability, and explainability in critical network operations.

To ensure secure autonomous network evolution, a comprehensive security framework must integrate Zero Trust principles, AI-driven threat intelligence, and Minimum Baseline Security Standards (MBSS) across 5G, 6G, and cloud-native telecommunications infrastructures [14], [15]. This framework must address the dual nature of AI as both a security enabler and potential vulnerability.

5.1.2 Emerging threat landscape

AI-powered autonomous networks face an evolving threat landscape characterised by sophisticated adversaries leveraging AI to automate cyber-attacks, create advanced evasion techniques, and manipulate AI models governing critical network functions.

Key threat categories include:

Adversarial AI attacks: Sophisticated manipulation of machine learning models through data poisoning, model inversion, and adversarial examples that can compromise network slicing, service orchestration, and Open RAN controllers.

AI-driven automation exploitation: Attacks targeting flaws in AI-based automation systems, potentially leading to unauthorised access, service disruption, and compromised network integrity.

Supply chain vulnerabilities: Autonomous networks rely on complex software and hardware ecosystems involving multiple vendors, creating opportunities for supply chain attacks that can cascade into system-wide failures or introduce persistent backdoors [16], [17].

Dynamic attack adaptation: The self-adjusting nature of autonomous networks provides attackers with opportunities to exploit orchestration layers, APIs, and inter-domain communications to gain persistent access to network resources.



Case study: AI-manipulated network slicing attack

Consider a scenario where an autonomous network employs AI-driven network slicing to dynamically allocate resources for different services, such as Ultra-Reliable Low-Latency Communications (URLLC) for autonomous vehicles and enhanced mobile broadband (eMBB) for streaming services. An adversary who successfully injects false data into the AI model managing network slicing could cause the system to allocate excessive bandwidth to non-critical applications, thereby disrupting latency-sensitive services and potentially endangering autonomous vehicle operations. Mitigation strategies must include continuous AI model validation, real-time anomaly detection, and strict access control mechanisms.

5.2 Security Challenges in Autonomous Networks

5.2.1 AI-driven cyber threats: The dual-edged nature of artificial intelligence

AI plays a paradoxical role in autonomous network security, simultaneously strengthening defensive mechanisms while being leveraged by attackers to bypass traditional security controls. Adversarial AI attacks, including model poisoning and adversarial examples, can distort network behaviour by manipulating AI-driven decision-making systems that govern dynamic network slicing, RAN automation, and SDN-based transport networks.

Attackers can exploit vulnerabilities in machine learning models to generate deceptive anomalies, leading to false positives in security systems or enabling evasion of detection mechanisms. Protecting AI components in autonomous networks requires implementing adversarial robustness techniques, continuous model retraining, and explainability mechanisms to ensure transparency in AI-driven security decisions [18], [19].

5.2.2 Securing network digital twins and AI agents

Network Digital Twins (NDTs) provide critical real-time simulations, predictive analytics, and automated responses for RAN, core networks, and service orchestration. However, compromised NDTs can lead to incorrect security configurations, faulty network predictions, and unauthorised access to sensitive network data.

Security mechanisms for NDTs must include strong identity and access controls, encrypted data exchange protocols, and continuous validation of simulation results. Similarly, AI agents that autonomously manage network functions require protection against adversarial inputs, unauthorised reconfiguration attempts, and API exploitation to ensure the integrity of automated decision-making processes [20], [21].



Case study: Malicious manipulation of network digital twin

In a practical scenario, a telecommunications operator deploys an NDT to simulate network behaviour and predict congestion in a 5G Standalone (SA) Core network. If an attacker gains unauthorised access and modifies the twin's parameters, the operator might receive misleading congestion predictions, leading to incorrect traffic rerouting decisions and subsequent service degradation. Preventing such risks requires implementing strict NDT access controls, cryptographic integrity verification mechanisms, and anomaly detection systems within simulation models.

5.2.3 API security risks in autonomous networks

APIs serve as the fundamental communication backbone for autonomous networks, enabling seamless interaction between different network components. However, insecure APIs can expose sensitive network configurations, allow unauthorised data access, and create privilege escalation opportunities. Common API vulnerabilities include weak authentication mechanisms, improper access controls, and injection vulnerabilities that can lead to severe security breaches. Implementing robust API security measures requires deploying OAuth 2.0 authentication, mutual TLS encryption, rate limiting, and comprehensive anomaly detection systems. Organisations must also conduct regular security assessments and implement API gateways with built-in security controls [22], [23].

5.2.4 Zero Trust and adaptive security architectures

Legacy telecommunications networks designed without Zero Trust principles prove insufficient for securing AI-driven autonomous networks, where real-time automation and dynamic interactions require continuous trust verification. Zero Trust Architecture (ZTA) ensures that no entity, whether inside or outside the network perimeter, receives inherent trust privileges.

AI enhances Zero Trust security implementations by enabling automated authentication processes, continuous behavioural monitoring, adaptive access control based on real-time risk assessment, and dynamic micro-segmentation. The combination of AI capabilities with Zero Trust principles allows autonomous networks to dynamically enforce security policies, significantly reducing risks associated with unauthorised access and insider threats [24], [25].

5.2.5 Privacy-preserving AI in autonomous networks

As AI systems process extensive amounts of subscriber data, network telemetry, and service assurance information, privacy concerns arise regarding data collection, processing, and sharing practices. Autonomous networks must implement privacy-preserving AI techniques, including federated learning, homomorphic encryption, and differential privacy, to ensure data confidentiality while enabling AI-driven insights.

Regulatory compliance with frameworks such as GDPR, CCPA, and telecommunications-specific privacy standards (including ETSI NFV security and ETSI SAI security specifications) must be enforced to protect sensitive user and operational data within autonomous network environments [26], [27].

5.2.6 Securing generative AI in autonomous networks

As autonomous networks leverage generative AI for adaptive decision-making and predictive modeling in network optimisation and security automation, securing these models becomes imperative. Attackers can exploit vulnerabilities in decision logic, data sources, and policy enforcement layers to introduce unintended behaviours in network operations.

Implementing robust security measures requires deploying explainable AI policies, conducting comprehensive security validation procedures, and ensuring decision auditability mechanisms. Regulatory frameworks should mandate transparency and accountability in automated security operations to maintain trustworthy autonomous network functions [28], [29].

Case study: AI-generated phishing in telecommunications networks

Consider a scenario where malicious actors leverage generative AI to create highly realistic phishing attacks targeting telecommunications engineers managing autonomous networks. These AI-generated attacks could exploit compromised credentials to manipulate network policies or exfiltrate sensitive subscriber data. Effective mitigation strategies include implementing AI-driven anomaly detection systems, deploying user behaviour analytics, and establishing robust validation mechanisms for AI-generated content.

5.3 AI-driven cybersecurity operations and automated response

Autonomous networks must adopt comprehensive automated cybersecurity operations (AutoSecOps) to predict, prevent, detect, and respond to threats without human intervention. Security Operations Centers (SOCs) enhanced with advanced observability capabilities can leverage sophisticated security analytics, behavioural modeling, and real-time risk assessments to automate incident response workflows.

AutoSecOps enhances cyber resilience through continuous learning from attack patterns, proactive vulnerability identification, and autonomous countermeasure enforcement. Machine learning models analyse network behaviours, identify anomalies, and generate automated response actions to neutralise threats before they can escalate into significant incidents.

The integration of AI-powered Security Orchestration, Automation, and Response (SOAR) systems with User and Entity Behaviour Analytics (UEBA) platforms enables real-time incident handling, substantially reducing response times to security events. Integrating AI capabilities with existing cybersecurity frameworks ensures proactive threat mitigation while minimising downtime and service disruptions in autonomous networks [10], [30].



5.4 Implementation recommendations

The successful integration of AI in autonomous networks requires a balanced approach that addresses both security opportunities and challenges. Network operators should:

1. **Implement layered security architectures** that combine traditional security controls with AI-enhanced detection and response capabilities.
2. **Establish comprehensive governance frameworks** for AI model development, deployment, and lifecycle management.
3. **Deploy continuous monitoring systems** that provide real-time visibility into AI decision-making processes.
4. **Maintain human oversight mechanisms** for critical security decisions while preserving autonomous operational benefits.
5. **Ensure regulatory compliance** through regular audits and assessments of AI-driven security systems.
6. **Implement Continuous Auditing** to validate and track the "choices" made by AI. Ensuring the traceability and verification of AI-driven choices is fundamental for preventing problems or, in the last resort, identifying responsibilities.

The evolution toward secure autonomous networks requires collaborative efforts among industry stakeholders, regulatory bodies, and cybersecurity researchers to develop standardised security frameworks that address the unique challenges of AI-driven network evolution while enabling the full potential of autonomous operations.

6 ETSI Technical Groups on AN: evolution and innovation

ETSI's comprehensive approach to Autonomous Networks spans multiple Technical Committees, Industry Specification Groups and Software Development Groups, each contributing specialised expertise and solutions. This section presents a synthesis of the most significant new achievements and recent ongoing developments across ETSI's AN-focused initiatives, in scope with the focus of the current White Paper (AI on the evolution of AN and the road toward AN L4), highlighting project progress, architectural innovations, practical implementations, and future evolution pathways.

The following analysis is authored by relevant technical experts from each TC/ISG and SDGs, primarily Chairs and Vice-chairs, ensuring the representation of each group's contributions to the autonomous network's ecosystem.

6.1 ISG Experiential Networked Intelligence (ISG ENI)

ISG ENI focuses on defining Cognitive Network Management architectures that enhance operator experience through advanced cognition capabilities. Cognition, defined as the process of acquiring and understanding data to produce new knowledge, represents the foundation for intelligent network operations.

6.1.1 Technical innovations and architectural advances

Hybrid learning approach for cognitive modeling: ENI implements a sophisticated hybrid learning methodology using deep reinforcement learning (DRL) agent frameworks to realise cognition models. DRL agents demonstrate data-driven adaptability, continuously updating policies based on environmental observations and rewards. This approach enables optimisation of complex reward functions that encode safety constraints, fairness criteria, and multi-objective trade-offs for refined behaviour management.

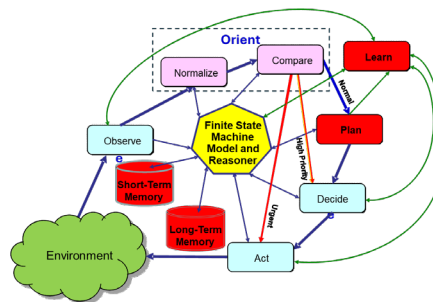


Figure 12: ENI Cognition Model as an Extension of the OODA Control Loop [18], [48]

Generative AI integration for network management: ENI has pioneered the integration of Generative AI models in network management applications, enabling autonomous detection and resolution of network issues while optimising performance and minimising downtime. By analysing extensive network data, generative AI predicts potential failures and recommends proactive maintenance strategies. The integration enhances network security through real-time threat identification and mitigation, while AI-driven automation streamlines configuration management, reducing human error and ensuring consistent policy enforcement.

Advanced AI model implementations: ENI's research encompasses three primary generative model categories:

Generative Adversarial Networks (GANs): Generate realistic network traffic patterns through adversarial training between generator and discriminator networks, enabling network debugging and intrusion detection system development.

Variational Auto Encoders (VAEs): Learn underlying probability distributions of network data using probabilistic latent spaces, enabling generation of new data samples that resemble original network patterns.



Transformers and Large Language Models: Process sequential network data using self-attention mechanisms to capture long-range dependencies, enabling advanced natural language processing for network management tasks.

6.1.2 New Proofs of Concept (PoCs)

ENI maintains an active portfolio of 23 proof-of-concept ETSI GS ENI 006 [77], [Ongoing PoCs](#) projects that validate theoretical frameworks through practical implementations. These PoCs demonstrate the feasibility and effectiveness of cognitive networking approaches across diverse network scenarios and operational environments, autonomous network space-ground co-operation, including slicing and satellites.

6.1.3 Main achievements

Comprehensive specification portfolio: ENI has published a number of technical deliverables, including:

- ETSI GS ENI 005 Functional Architecture, cognitive networking, Generative AI, Semantics, policy models, [32]
- ETSI GS ENI 019 Models (Data & Information), Interfaces and APIs, [78]
- ETSI GR ENI 051 Agentic AI [33]
- Multiple White Papers: Including White Papers 22: 44 ENI vision [31], 51 Cognitive network management [46], 64 AI technologies [34] for Autonomous operations

Autonomy level definitions: ENI has developed critical deliverables for AN capability assessment, including ETSI GR ENI 007 [35], ETSI GR ENI 010 [36] (recently revised), ETSI GR ENI 035 [37], and ETSI GR ENI 049 [38], providing frameworks for evaluating and implementing autonomous network capabilities.

Release 4 developments: Current work focuses on architectural enhancements, AI agent integration, and expanded cognitive capabilities, with deliverables available in the ENI Open Area for community review and feedback [32], [33], [37], & [38].

The release 4 documents not yet published are all in the [ENI Open Area](#).

6.2 ISG Zero touch network and Service Management (ISG ZSM)

ISG ZSM develops comprehensive end-to-end automation frameworks optimised for AI-driven decision-making, targeting elimination of manual intervention in network operations through "zero-X" operational goals: zero wait, zero touch, and zero trouble.



6.2.1 Architectural innovations and frameworks

Intent-driven closed-loop systems: ZSM's framework employs declarative intent specifications as key enablers for autonomous network and service management. Natural language processing and machine-readable policy engines translate service-level agreements into dynamic resource allocation patterns using reinforcement learning models that optimise latency, throughput, and energy efficiency.

Network Digital Twin integration: The ZSM framework positions NDTs as management services, specifically analytics services, extending capabilities to support risk prediction, network visualisation, synthetic data generation, and historical incident analysis within autonomous network architectures.

Hierarchical closed-loop architecture: Building upon the Observe-Orient-Decide-Act (OODA) model, ZSM implements nested control loops operating across microsecond to hour-level timescales. Localised loops handle rapid state changes while strategic loops optimise long-term resource Utilisation across multi-vendor environments through novel escalation matrices.

Cross-domain service fabric: ZSM's service-based architecture dissolves traditional network boundaries through unified abstraction layers, enabling autonomous service composition across virtualised network functions, physical infrastructure, and edge computing nodes via standardised APIs.

Ethical AI governance: Addressing explainability challenges in autonomous systems, ZSM incorporates explainable AI modules with blockchain-anchored audit logs for tracking model versioning, data provenance, and policy compliance, ensuring accountability in critical operations.

6.2.2 Proof of concept validation

Intent-driven energy optimisation: Deutsche Telekom and Huawei demonstrated intent-driven energy saving in radio networks, including intent expression for RAN energy efficiency targets, fulfillment reporting, and effect evaluation while maintaining user experience quality.

Cloud AR/VR service deployment: Telefónica and Huawei validated cloud-based AR/VR service creation on CAMARA platforms using ZSM frameworks, demonstrating service lifecycle management through CAMARA APIs.

Trustworthy network management with explainable AI: EURECOM implemented closed-loop control mechanisms for anomaly detection and resolution with human-friendly explanations, integrating AI for detection, explainable AI for root cause analysis, and LLMs for user-friendly explanations.



Intent-based RAN resource management: DOCOMO and NTT verified RAN management domain feasibility checking for intent delivery from end-to-end management domains, utilising 3GPP TS 28.312 [39] intent-driven management services.

6.2.3 Technical specifications and standards

ZSM has developed comprehensive specifications covering:

- Reference Architecture ETSI GS ZSM 002 [40]
- Cross-domain E2E service lifecycle management ETSI GS ZSM 008 [41]
- Closed-Loop Automation series ETSI GS ZSM 009 [42]
- Intent-driven Closed Loops ETSI GS ZSM 016 [43]
- Enablers for Artificial Intelligence-based Network and Service Automation ETSI GS ZSM 012 [44]
- Network Digital Twin for enhanced zero-touch network and service management [ETSI GS ZSM 018](#) [45]

6.3 ISG Network Functions Virtualisation (ISG NFV)

6.3.1 Innovative Perspectives

ETSI ISG NFV addresses long-term evolution of NFV towards telco cloud, proposing a new architectural design based on key architectural principles, objectives that align with the current and future trends in the telco cloud industry. The study is proceeded and concluded in the following Release 6 group report ETSI GR NFV-IFA 054 [59].

The new architecture for Telco Cloud targets to support long-term evolution of the Telco Cloud from cloud-native to AI-native, which helps the Telco Cloud develop towards a high-level of autonomy (e.g., ADN level 4). It has two aspects of implication: AI4Cloud and Cloud4AI. AI4Cloud focuses on improving the Operations, Administration and Management (OAM) aspects (e.g., fault root cause diagnosis and resolution) of the Telco Cloud with assistance of advanced achievements of AI technologies, and builds a more intelligent OAM system for the Telco Cloud. Cloud4AI makes use of the diversified, heterogeneous resources and data from cloud infrastructure and platform, to provide a solid base to support AI models training and the deployment of AI-based applications.

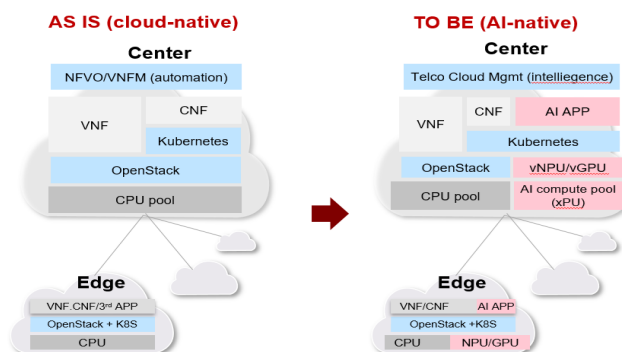


Figure 13: NFV architecture evolution due to AI

Associated with the above AI-native visions, ETSI ISG NFV is proceeding the following innovative trend/scenario study in Release 6:

New infrastructure resources for NFV: This study focuses on the aspects about enabling in the NFV architectural framework with new dimensions to extend and evolve the NFVI. One dimension is about new kinds of NFV infrastructure resources like the notation “xPU”, in which “x” represents a specialised processing unit for a certain “x” domain. The examples of “xPU” include Graphics Processing Unit (GPU), Data Processing Unit (DPU), Tensor Processing Unit (TPU) or Neural Processing Unit (NPU), and they can be composed of dedicated AI related computing resources in the NFVI. These new kinds of computing resources can be more efficient than the CPU in handling compute-intensive AI task requirements, as well as the infrastructure basis to support the NFV architecture to deploy new AI-based applications like large language models.

Serverless and other application virtualisation forms in NFV: This study encompasses the computing paradigm of Serverless and a variety of application virtualisation technologies, both of which are related to AI and can serve as a practice for Cloud4AI. Compared to traditional applications (e.g., network function), the deployment of AI-based application faces new challenges. For instance, the environment that AI-based application rely on is more complex. Different AI frameworks, xPU drivers, and xPU hardware can lead to AI-based application compatibility issues. WebAssembly (WASM), a new type of virtualisation technology, holds promise for addressing the compatibility issues in AI-based application deployment. By utilising the WASM virtual machine sandbox technology, WebAssembly not only abstracts away the differences in underlying runtime environments but also enhances the security of the runtime environment. Moreover, the virtual instruction set of WebAssembly can significantly reduce the size of software images while providing near-native execution speed, making it particularly suitable for deploying AI inference tasks at edge sites with limited resources and low latency tolerance.

Model-as-a-Service (MaaS) in NFV: This study investigates Model-as-a-Service (MaaS) for AI-based applications in the context of telco cloud management. It describes and analyses a set of relevant use cases, with a focus on the definition and role of MaaS within telco cloud management. Additionally, the report explores potential enhancements to the NFV framework to better support MaaS-based telco cloud management.

MaaS provides AI models and their capabilities as reusable services, enabling users to quickly build, deploy, monitor, and invoke models without the need to develop and maintain underlying infrastructure. MaaS supports techniques such as Retrieval-Augmented Generation (RAG), coordination between large models and smaller domain-specific models, and plugin orchestration, enhancing model adaptability and application efficiency. In telco cloud management, MaaS enables intelligent maintenance knowledge retrieval, data analysis, network fault sensing, event localisation, and automated fault resolution, significantly improving automation and intelligence in telco cloud operations.

6.3.2 New Proofs of Concept (PoCs)

ETSI ISG NFV added AN to the list of hot topics on which the community is invited to submit PoC proposals. PoCs on AN-in-NFV can be setup according to the generic NFV PoC framework specifications in the following Group Specification:

- ETSI GS NFV 005, “Network Functions Virtualisation (NFV); Proofs of Concept; Framework”.

6.3.3 Main Achievements

Key accomplishments of ISG NFV Release 6 in the autonomous networks’ domain include:

- ETSI GR NFV-IFA 054 [59] “Network Functions Virtualisation (NFV) Release 6; Architecture; Report on the architectural support for NFV evolution” (published).
- ETSI GR NFV-EVE 023 [60] “Network Functions Virtualisation (NFV) Release 6; Evolution and Ecosystem; Report on new infrastructure resources for NFV” (published).
- ETSI GR NFV-EVE 025 “Network Functions Virtualisation (NFV) Release 6; Evolution and Ecosystem; Report on Serverless and other application virtualisation forms in NFV” (ongoing).
- ETSI GR NFV-EVE 027 “Network Functions Virtualisation (NFV) Release 6; Evolution and Ecosystem; Report on Model-as-a-Service (MaaS) in NFV” (ongoing).

6.4 TC Methods for Testing and Specifications (TC MTS)

In general, the Technical Committee “Methods for Testing and Specification (MTS)” focuses on the development of testing methodologies and frameworks to ensure the quality, reliability, and interoperability of autonomous network systems. The committee plays a crucial role in establishing standardised approaches for testing autonomous network capabilities and validating their performance against specified requirements.



6.4.1 Innovative perspectives

TC MTS is developing innovative testing approaches specifically tailored for autonomous networks:

Model-Based Testing for Autonomous Systems: Development of testing methodologies that leverage formal models to verify autonomous network behaviours and decision-making processes.

AI-Driven Test Generation: Creation of intelligent test case generation systems that can adapt to evolving network conditions and requirements.

Runtime Verification Techniques: Development of methods to continuously monitor and verify autonomous network operations in real-time.

These testing frameworks are designed to address the unique challenges of validating self-* properties (self-configuration, self-optimisation, self-healing, etc.) in autonomous networks.

6.4.2 New PoCs

TC MTS is working on several Proof of Concepts implementations focused on testing autonomous network capabilities:

Automated Test Suite Generation: PoC demonstrating AI-powered generation of comprehensive test suites for autonomous network features.

Performance Testing Framework: Implementation of specialised tools for measuring and validating the performance of self-optimising network functions.

Security Testing Platform: Development of testing methodologies specifically focused on validating the security aspects of autonomous networks.

6.4.3 Main Achievements

Key accomplishments of TC MTS in the autonomous networks domain include:

Development of ETSI TS 104 008: A comprehensive testing framework for autonomous network systems that provides guidelines for test specification and execution (doc. In progress).

Creation of ETSI TR 103 910 [61]: Technical report outlining testing methodologies for various aspects of autonomous networks including robustness, trustworthiness, and compliance.

Establishment of standardised metrics and KPIs for evaluating autonomous network performance and reliability.

Definition of testing approaches for validating AI/ML components in autonomous networks.

These achievements have contributed significantly to ensuring the reliable and secure implementation of autonomous network capabilities across the industry.

6.5 TC Autonomic Management and Control Intelligence for Self-Managed Fixed & Mobile Integrated Networks (TC INT-AFI)

TC INT AFI WG is developing a framework for autonomic management and control (AMC) Intelligence for self-managed fixed & mobile Integrated networks and services (AFI); the Generic Autonomic Network Architecture (GANA).

Develop use cases and requirements for autonomous networks and services; ETSI TS 103 194 [62].

Develop test frameworks and test specifications for autonomous networks architectures (Self-Adaptive Networks); ETSI EG 203 341 [63].

Develop business drivers for autonomous network ETSI TS 103 195-1 [64],


Develop a generic architectural reference model for Autonomous cognitive management and control of networks and services ETSI TS 103 195-2 ETSI White Paper no. 16 [69]: and its instantiations onto various types of network architectures (BBF ETSI TR 103 473 [66], 3GPP Access, Backhaul & Core ETSI TR 103 404 [67] ; Wireless Ad-hoc/Mesh ETSI TR 103 495 [68] , ...)

Drive a 5G PoC Program/Project on GANA Autonomics in 5G Network Slices Creation, Autonomic & Cognitive Management & E2E Orchestration; with Closed-Loop (Autonomic) Service Assurance of IoT 5G Slices; Accepted PoC proposals - INTwiki. [Accepted PoC proposals - INTwiki](#).

GANA defined the key AI cognition module Decision-making Element (DE) required to drive an autonomous network at the GANA Node level and the GANA Knowledge Plane level thanks to the use case and requirement analysis. Autoconfiguration and auto-discovery management DE, resilience management DE fault management DE, and the security management DE with lower management DEs for multi-optimisations management DE(s) defined according to the needs of provider with no conflict by designed and interoperable with multi-vendor multi-domain systems.

6.5.1 Innovative perspectives

With no trusted data no AI, and with no trusted AI no data could be shared with AI (for inference or training), if the data could be not consumed by AI then AI could not drive the autonomous network.

A blue network diagram is positioned in the top right corner. It features a series of interconnected nodes and lines, forming a complex web that represents a network structure.

Big Data Analytics with massive and wide outreach to data parameters allows CSPs to increase their levels of autonomy (especially when it comes to dynamics metric and parameter values and certain context information) and to monetise on the large scale and variety of data they have access to. No stakeholder has more access to such a wide range of contextualised data as a CSP. Guaranteeing the confidentiality and sovereignty of data is essential for sharing this data and enabling data-driven services and use-cases. Data Space [47] provides a data governance framework with access control usage for sovereign, secure and scalable exchange of data within a "trusted ecosystem" involving stakeholders across the commercial, social, and industry verticals dimensions. A Data Space allow data providers remain in control of shared data which could be consumed by decision making element while collaborating securely to develop the autonomous network Fair, Explainable, Accurate and Sustainable (FEAS) compliant with AI Ethics act, Secure, Auditable, Factual and Ethical (SAFE) to be compliant with provider policy. A set of cooperations scenarios and opportunities can then be leveraged by CSPs, allowing them to monetise after unleashing the potential of sovereign data sharing [48].

6.5.2 New PoCs

The TC INT/AFI is working on several Proof of Concept and implementations to then define comprehensive guide for implementing an Autonomous Network:

- Access Control as a Service (ACaaS) based on Zero Trust Architecture (ZTA) within critical infrastructure (CI). It emphasises the transformative impact of ACaaS in enhancing CI (e.g. Telco) security against sophisticated cyber threats. implementations, focusing on interoperability, scalability, and stringent security standards for sharing contextualised data which could be consumed for future digital resilience.
- Implementing GANA Knowledge Plane (KP) within 5G MEC Edge cloud and multi-layer transport networks, focusing on the integration of GANA KP decision elements (DEs) agents with various AI models, (including generative AI) consuming contextualised data from on Overlay Network Information eXchange (ONIX) for AI Journey (development security and operations of AI models) analysing real time or historical contextualised information.

The previous PoCs reports could be retrieved on the following link: [Accepted PoC proposals - INTwiki](#).



6.5.3 Main Achievements

Key accomplishments of TC INT/AFI in the autonomous networks' domain include:

Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet;

Business drivers for autonomic networking

A Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services: Generic Autonomic Network Architecture (GANA) Model.

GANA Model and its instantiations onto various types of network architectures and their associated management and control architectures (BBF, 3GPP, ONAP, NFV, SDN, etc.).

And some new achievements:

- End-to-End Autonomic Security Management and Control Multi-Domain 5G Networks (ETSI TR 103 857 [70]).
- Autonomic 5G Networks, powered by ETSI GANA Multi-Layer Autonomics & AI and IPv6 (ETSI TR 103 858 [71]).
- A joint work with ITU-T Focus Group SG11 on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) ETSI TR 104 164 [82].

6.6 ISG 5th Generation Fixed Network (ISG F5G)

6.6.1 Overview of F5G Advanced and its relation to Autonomous Networks and AI

ETSI ISG F5G is currently focusing on the development of standards for F5G Advanced and fostering the evolution to a "fibre to everywhere and everything" ecosystem. The business and technology characteristics of F5G Advanced is shown in the following figure visualised by 6 dimensions and the dimensional progress over F5G. To note is the dimension on GRE (Guaranteed Reliable Experience), which enhanced the autonomous network level.

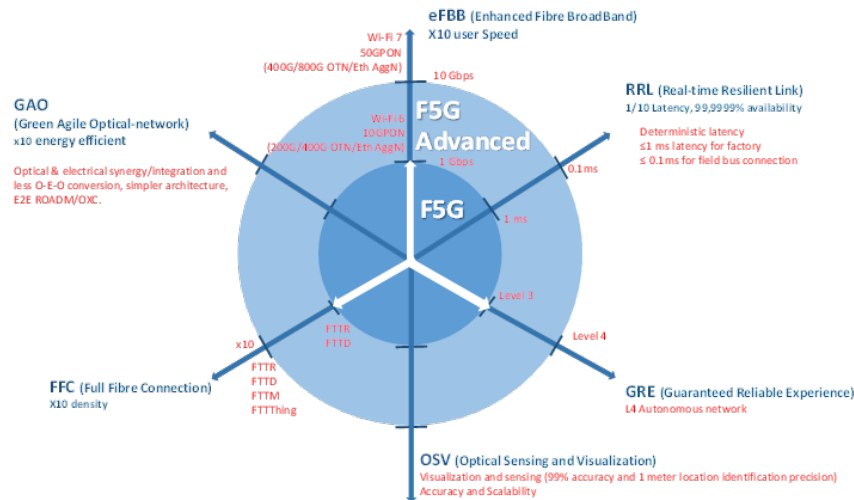


Figure 14: Overview of the 6 F5G Advanced Dimensions (from ETSI GR F5G 021 [51])

The F5G Advanced proposes 17 use cases [52] across various dimensions, market segments and technology focus. Of relevance with regards to AN are the following:

- F5G-A Use Case #3: "Computing Collaboration in PON networks".
- F5G-A Use Case #7: "Unified access and on-premises networks".
- F5G-A Use Case #8: "OTN intelligent fault management".
- F5G-A Use Case #9: "Evaluation and assurance of user service experience".
- F5G-A Use Case #11: "Dynamically digitised ODN".
- F5G-A Use Case #16: "Optical Fibre Sensing for Telecom Operators".
- F5G-A Use Case #17: "QoD App-Flow service provisioning".

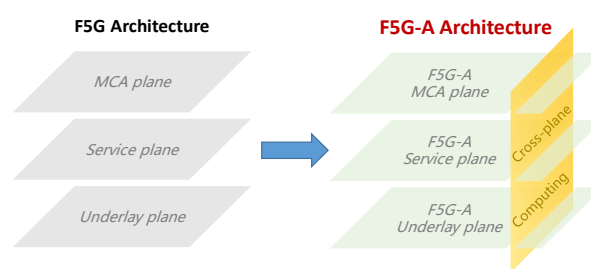


Figure 15: Addition of Cross-plane Computing

The end to end F5G Advanced network architecture includes the Underlay Plane, the Service Plane and the Management, Control, and Analytics (MCA) plane, where the MCA plane has various AN concepts for managing and controlling the F5G-A network. The cross-plane computing feature is added vertically, allowing deploying computing functions at various locations in the F5G-A network architecture. Figure 15 shows the migration from F5G to F5G Advanced adding the cross-plane computing feature.

6.6.2 Innovative perspectives

AN level definition and evaluation for F5G Advanced optical networks [54]

TM Forum IG1252 defines the general workflow of network management, control and operation. The F5G Advanced level definition and evaluation work items use this general workflow as the key evaluation dimensions for the F5G Autonomous Network level classification. It basically applies the general level definition to the end-to-end optical network architecture.

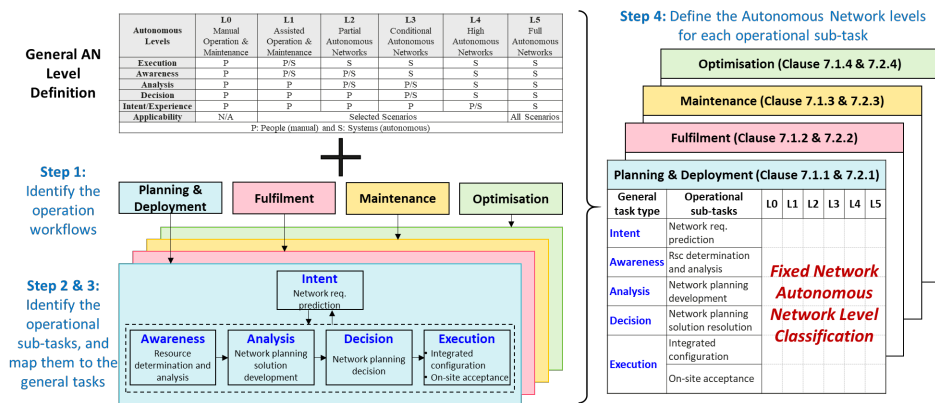


Figure 16: Methodology to define the fixed network Autonomous Network levels

F5G Advanced AI-based Network Management and Control Architecture [55]

TM Forum IG1251 [50] defines the methodology, general principles, and the high-level business and technical architecture of Autonomous Networks. The F5G Advanced E2E management and control architecture [55] applies those concepts to the fixed network and enables self-configuration, self-healing, self-optimising and self-evolving of F5G Advanced resources and services with less human intervention.

6.6.3 F5G Advanced PoCs related to AN

F5G-A end-to-end management and control for Building Cloud AR/VR Service [56]

This PoC demonstrates the feasibility of deploying a F5G Advanced E2E management and control system for transport (access and aggregation) slice management with quality on demand (QoD) service classification and differentiation, service status monitoring and telemetry, and closed-loop automation for service assurance.

Energy Saving based on Traffic Prediction Based on Telemetry [56]

This PoC demonstrates traffic prediction based on telemetry streaming solutions for energy-saving in Passive Optical Network (PON) ports within optical access networks. It is expected to contribute the AI-based prediction and energy-saving (in the future) components of the F5G Advanced architecture.



6.7 TC Securing Artificial Intelligence (TC SAI)

6.7.1 Innovative perspectives

TC SAI has a primary purpose to ensure that any AI capability is provided to the market in a way that preserves the security of its users, its environment and its direct and indirect stakeholders. With respect to the AN environment SAI therefore provides the framework for secure design and market placement of the AN system.

The role of SAI in development of standards is to address the entire lifecycle, thus: Design, Development, Deployment, Maintenance, End-of-Life.

For each phase TC SAI has defined, in ETSI TS 104 223 [12], a set of principles to be followed. These are summarised below:

Principle 1: Raise awareness of AI security threats and risks: This is fundamental and requires significant investment in time and resources. It does presume that a design group is cyber-security aware and understands the principles of designing a functionally secure system

Principle 2: Design the AI system for security as well as functionality and performance: A large part of this is making sure the use of AI is appropriate

Principle 3: Evaluate the threats and manage the risks to the AI system

Principle 4: Enable human responsibility for AI systems

Principle 5: Identify, track and protect the assets

Principle 6: Secure the infrastructure

Principle 7: Secure the supply chain

Principle 8: Document data, models and prompts

Principle 9: Conduct appropriate testing and evaluation

Principle 10: Communication and processes associated with End-users and Affected Entities

Principle 11: Maintain regular security updates, patches and mitigations

Principle 12: Monitor the system's behaviour

Principle 13: Ensure proper data and model disposal

From a very simple standpoint ANs are just another AI application and the principles listed above apply to AN as to any other. In addition one of the key requirements to AI that is addressed by TC SAI is the necessary provision of transparency and explicability of what the AI, the AN, is doing. This is considered across, again, the entire lifecycle and addresses both static and run-time operation of the AI/AN and defined in ETSI TS 104 224 [65].

6.7.2 PoC related to AN

Not applicable for TC SAI.

6.7.3 Main achievements

The main achievements are reported in ETSI TS 104 224 [65] and ETSI TS 104 223 [12].



6.8 SDG TeraFlowSDN (SDG TFS)

6.8.1 Innovative perspectives

Intent-based Networking with Large Language Models

One of the most promising innovative perspectives revolves around the use of LLMs for intent-based networking. TeraFlowSDN enables operators to input high-level service requests in natural language, allowing AI-driven engines (e.g., IntentLLM) to interpret, classify, and translate these requests into actionable configurations [TFS24a]. By automating the intent-lifecycle—from creation and validation to explanation and deployment—LLMs reduce manual interventions, accelerate service instantiation, and minimise human errors. This advancement embodies an evolutionary step for SDN controllers, aligning with the ETSI ambition to simplify and optimise multi-layer network management.

Digital Twins for Predictive Orchestration

A second significant perspective is the integration of Network Digital Twins (NDT) [TFS23]. These virtual replicas of physical networks leverage real-time data analytics and AI algorithms to mirror and predict network behaviour under diverse scenarios. In TeraFlowSDN, the digital twin operates in tandem with the cloud-native SDN controller, enabling pre-deployment testing, early fault detection, and performance optimisation before changes are applied to the live network. This proactive approach reduces risks, shortens troubleshooting times, and further automates network operations, thus advancing the concept of self-adaptive and self-healing infrastructures.

6.8.2 PoC related to AN

TeraFlowSDN's PoC on autonomous networks demonstrates a multi-layer AI-driven architecture to provide Traffic Forecasting and Anomaly Detection. It leverages containerised ML modules for real-time demand prediction, the PoC dynamically allocates network resources to address changing traffic patterns. Simultaneously, advanced anomaly detection (e.g., SmartNIC-based profiling) identifies suspicious traffic flows or hardware malfunctions before they degrade service quality [TFS24b], [TFS24c], [TFS24d].

6.8.3 Main achievements

Unified SDN Controller with Embedded AI: TeraFlowSDN achieves an unprecedented level of AI integration within a cloud-native SDN framework. By embedding microservices for forecasting, anomaly detection, and LLM-based intent parsing, it paves the way for more sophisticated, policy-driven network automation.

End-to-End Network Automation: The synergy of IP and optical orchestration layers under a single control plane highlights TeraFlowSDN's comprehensive approach. This holistic view ensures minimal latency for operational tasks, real-time resource allocation, and a more robust end-user experience.

Proactive Resource Management: With accurate traffic forecasting and anomaly detection modules, TeraFlowSDN reduces reaction times to traffic surges, planned maintenance, or unforeseen failures. Operators benefit from optimised capacity planning and proactive fault mitigation, achieving higher service reliability at lower operational costs.

Enhanced Network Security: Through LLM-driven policy generation, TeraFlowSDN automates security policy enforcement across multiple network domains. Automatically generated ACLs and other context-specific rules offer heightened levels of threat prevention and system hardening without manual overhead.

Faster Innovation and Experimentation: The integrated Network Digital Twin capability accelerates testing of new features—such as advanced QoS policies, slicing scenarios, or hardware upgrades—before bringing them into production. This not only expedites innovation cycles but also reduces the risk of network misconfigurations.

6.9 SDG OpenSlice (SDG OSL)

SDG for OpenSlice is developing an open-source, service-based Operations Support System (OSS) to deliver Network-as-a-Service (NaaS), following specifications from main SDOs, including ETSI, TM Forum and GSMA. It provides a platform for early experimentation and regular feedback to standardisation groups aiming to contribute towards higher quality standards and faster time to market.

OpenSlice supports a layered architecture pattern, namely the business, service, and resource operation layers by implementing the respective TM Forum APIs, thus potentially supporting an AN platform. Towards this, its streamlined Business Process Management (BPM), supervised by the inherent orchestrator, along with the capability to introduce dynamic business logic throughout the service lifecycle, can be leveraged to deliver and maintain a partially AN, at least in terms of execution tasks. Also, OpenSlice offers an inbuilt mechanism to integrate real-time monitoring solutions within the aforementioned lifecycle, enabling efficient closed-loop management.

In an attempt to achieve higher levels of autonomy, this section outlines the employment of GenAI in the process of tailoring the deployment and reconfiguration of a network to the respective stakeholder's high-level Intent.

6.9.1 Innovative perspectives

As already introduced, the AN framework dictates the decoupling of the operating domains, each determined by independent inputs. The precision of these inputs can be enhanced by the employment of GenAI and LLMs, which facilitate the expression of requirements and constraints in a declarative manner, through high-level Intents. The context distillation is consecutively translated into machine-consumable standardised interfaces, namely TMF Forum APIs, which can be natively consumed by OpenSlice. This process streamlines the overall deployment while alleviating the need for error-prone user interventions.



6.9.2 PoC related to AN

The presented innovative perspective has been materialised through a PoC [57], which trains an LLM to serve as a network slice co-designer and assistant, within the context of a network provider's domain. Specifically, it receives high-level Intents from a candidate user, matches it with the corresponding choice from a pool of available network slices, allowing for further customisation if prompted, and eventually formulates a TMF-based request towards OpenSlice. The latter is in the native OSS context, which is directly comprehended and fulfilled.

Building on this foundation, a subsequent PoC [58] explores the same co-design paradigm using a local LLM deployment, aimed at reducing dependency on cloud-based inference and promoting sustainability and data sovereignty. This version retains the core workflow but leverages a resource-efficient, on-premise model to perform inference and intent processing, while maintaining full compatibility with OpenSlice and the TMF-based orchestration logic.

6.9.3 Main achievements

Key accomplishments of SDG OSL in the autonomous networks' domain comprise:

End-to-End Network Orchestration and Automation: OpenSlice incorporates business processes that employ several controllers across the network continuum to deliver NaaS. Furthermore, the comprehensive orchestration flows can be augmented with tailored logic that can be dynamically introduced.

Closed-Loop Management: The capability to integrate external monitoring sources within the service lifecycle enables rule-based actuation of designed policies and procedures.

AI-enabled NaaS delivery: The network provision is enhanced by the adoption of GenAI, serving as a key enabler to facilitate the seamless translation of the high-level description of desired business requirements into network consumable information.

7 ISG/TC/ SDG progress table

In order to present the reader a map of ETSI activities and work progress the following table shows the current ongoing work in the several groups of ETSI, on topics related to Autonomous Networks. The table represents the update of the Table presented in [23], and is available on the OCG AN repository. In particular in blue rows at the end we reported the progress of the new enablers based on AI capabilities.



The table legend (an empty table entry shows the AN aspect is not considered by the ISG/TC):

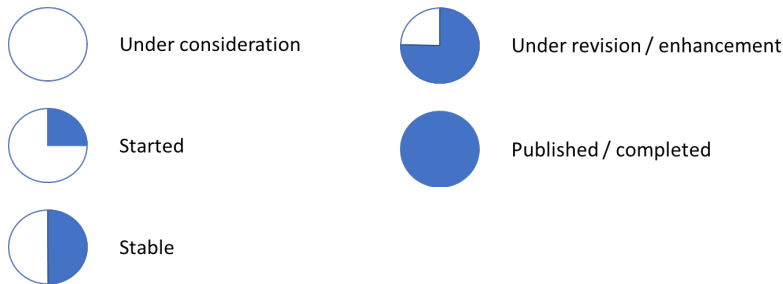










































































































































Table 2: ISG/TC/SDG activities progress Table

	AN topics / ETSI Groups	TC INT AFI WG	ISG ENI	ISG ZSM	ISG F5G	ISG NFV	TC SAI	TC MTS	SDG TFS	SDG OSL
1	Terms & definitions									
2	Use cases & requirements									
3	Architecture / framework									
4	Levels of autonomy/ autonomicity									
5	Cognition									
6	Self-X properties									



	AN topics / ETSI Groups	TC INT AFI WG	ISG ENI	ISG ZSM	ISG F5G	ISG NFV	TC SAI	TC MTS	SDG TFS	SDG OSL
7	Governance interface									
8	Intent-driven management ¹									
9	Policy Control Management Framework(s)									
10	AN services, functions and resources Life-cycle management									
11	Closed control loop automation									
12	Analytics and intelligence (including AI topics)									
13	Knowledge representation (e.g. information models & Ontologies) & management									
14	ANs federation and Inter-AN coordination									
15	Data Model									



	AN topics / ETSI Groups	TC INT AFI WG	ISG ENI	ISG ZSM	ISG F5G	ISG NFV	TC SAI	TC MTS	SDG TFS	SDG OSL
16	Robustness, trustworthiness, traceability									
17	Security/privacy									
18	Testing framework and methodology									
19	Metrics and KPIs									
20	PoCs									
21	Network Digital Twin/ NDT for AN									
22	GenAI for AN									
23	AI agent for AN									
24	AN API									



8 AN Ecosystem

Significant effort and relevant initiatives are active across the Industry Ecosystem on Network Automation. This outlines the business interest and technological value of Autonomous Networks across the Industry. Major Standard and Industry Fora (e.g. ETSI, IETF, ITU-T, TM Forum, GSMA, NGMN etc.), Multi-partnership Project for interoperable standards (3GPP) and open-source communities (eg. Linux Foundation etc.) are delivering recommendations, preliminary standards, deliverables and APIs. Industry cooperation and coordination are essential for harmonisation, widespread interoperability, and consistent behaviours, across a multi-vendor ecosystem. This cooperation brought to creation of the **Autonomous Networks (AN) M-SDO Table**, managed and facilitated by TM Forum.

This AN M-SDO Table that includes the main projects on AN across the mentioned Fora and Open Source Communities (ETSI, ITU-T, IETF, GSMA, 3GPP, NGMN, Linux Foundation...) organises on-line workshops to share results and present ideas, architectures, solutions. Initiatives like allowed to improve a stronger cooperation among experts in the field. ETSI plays a significant role in the AN MSDO Table presenting results, architecture evolutions and significative PoCs in several vertical application of AN. This successful initiative shows the committed interest of the Industry on Autonomous Networks, with great emphasis on the use of AI for Network evolution.

3GPP: Particular attention for its role in the evolution of Mobile Network and Operations, ETSI is a key partner of the Project, is playing 3GPP on Autonomous Networks, in particular SA5. 3GPP has significantly expanded its standardisation efforts around Autonomous Networks, with increasing focus on incorporating AI capabilities across multiple technical specifications and study items.

Core Specifications: 3GPP TS 23.288 [73] Architecture Enhancements: AI/ML capabilities for 5G System, Model distribution and transfer frameworks, Training mechanisms for AI capabilities, Integration patterns for foundation models, Support for distributed AI processing.

Network Intelligence: 3GPP TS 28.100 [74] "Levels of Autonomous Network": Defined autonomy levels incorporating GenAI, Classification of AI-enabled functions, Requirements for each autonomy level, Integration guidelines for language models, Cognitive capabilities framework.

Enhancement Studies:

3GPP TR 28.910 [75] Network Optimisation: GenAI for RAN energy optimisation, Autonomous configuration management, AI-driven performance optimisation, Predictive maintenance capabilities, Natural language interfaces for management.

3GPP TR 28.909 [76] Autonomous Network Evaluation: Assessment frameworks for AI functions, Performance metrics for autonomous operations, Testing methodologies for AI components, Validation of GenAI implementations.

Intent- Driven Management: 3GPP TS 28.312 [39] Intent Management: Natural language processing for intents, LLM-based intent translation, Semantic understanding of requirements, Intent validation and verification, Autonomous intent execution.



Network Data Analytics: Integration with GenAI models, Advanced analytics capabilities, Real-time processing support, Federated learning framework, Model sharing and collaboration.

Evolution towards 6G: Native AI integration, Cognitive network management, Advanced automation capabilities, Zero-touch operations, End-to-end network intelligence.

Security and Privacy: Enhanced Framework: AI model protection, Data privacy in training, Secure model deployment, Trustworthy AI operations, Compliance monitoring.

ITU-T, particularly through Study Group 13 (Future Networks), has been actively developing standards and recommendations for Autonomous Networks (AN), with increasing focus on integrating Generative AI capabilities. Their work encompasses the following areas: Architecture and Framework, Trustworthiness and Evaluation, Gen AI applications and standardisation efforts on data format and protocols and security requirements.

IETF and IRTF have significantly expanded their work on automated network management to incorporate Generative AI capabilities, particularly through several key working groups in particular Network Management (NETCONF, NETMOD, OPSAWG) and research initiative (NMRG).

TMForum has been at the forefront of Autonomous Networks (AN) development, with particular emphasis on leveraging Generative AI to enhance network automation and digital transformation. Their comprehensive approach encompasses: Autonomous Networks Technical Architecture and Framework, Open APIs, Industry Collaboration (AN MSDO), Autonomous Operation, Data Governance, GenAI for AN, Catalysts projects, AN business impact and value creation.

NGMN (Next Generation Mobile Networks) Alliance has significantly expanded its focus on Autonomous Networks, particularly through its dedicated initiative on Network Automation and Autonomy based on AI. Their work has evolved to incorporate Generative AI as a transformative technology. They released a Network Operators Survey on AN and 2 White Papers. The Alliance continues to represent the Telco Operators perspective on network evolution, including the AN role in 6G, with a strong focus on integrating emerging AI technologies in operational networks.

9 Future perspectives and recommendations

Looking forward, the integration of AI in network evolution points toward increasingly sophisticated autonomous systems. The development of 6G networks will likely rely heavily on AI for managing complex network slicing, massive MIMO configurations, and intelligent spectrum utilisation. These networks will not only be self-managing but also self-evolving, capable of learning from experience and adapting to new requirements without human intervention.

However, challenges remain in achieving fully autonomous networks. These include ensuring the reliability of AI decisions, maintaining transparency in automated processes, and addressing interoperability between different AI-driven systems. The human element remains crucial in overseeing these systems and setting strategic direction, even as routine operations become increasingly autonomous.

The successful implementation of AI in network evolution requires a balanced approach that leverages technological capabilities while maintaining appropriate human oversight. As networks continue to evolve, the role of AI will likely expand, leading to more efficient, reliable, and adaptive network infrastructure that can meet the growing demands of our connected world.

The widespread development of standards, frameworks, and technical specifications for Autonomous Networks (AN) across multiple organisations demonstrates the critical role of network autonomy in driving digital transformation. The momentum behind AN reflects both its technological maturity and strong business value proposition across the telecommunications ecosystem.

However, this rapid proliferation of AN initiatives presents significant challenges. The parallel development of standards and recommendations by different organisations risks creating:

- Fragmented and potentially incompatible approaches to AN
- Overlapping or conflicting technical specifications
- Inefficient use of industry resources and expertise
- Barriers to interoperability across vendor solutions
- Confusion in the marketplace about which standards to adopt

To address these challenges and ensure the successful evolution of AN we reported 2 successful initiatives that were launched:

- **In ETSI:** *the creation of OCG AN - it is open to all ETSI members experts in AN with the scope of: facilitating the exchange of results and deliverables in TBs, ISGs and SDGs working on Autonomous Networks; identifying synergies, best practices and common requirements; coordinating exchange of information on AN with other SDOs and Fora.*

This White Paper and [23] are coordinated and edited by OCG AN.

- **Cross Industry:** *the AN Multi-SDO Table with the scope of - Promote a better understanding of shared challenges and requirements for Autonomous Networks, Encourage the collaboration among SDOs to align on priorities and progress, Facilitate the regular engagement and information exchange to drive industry-wide alignment. The MSDO was created and managed by TM Forum, Multi-SDO participants: 3GPP, BBF, CCSA, ETSI, GSMA, IEEE, IETF, ITU-T, NGNM, ONAP, TM Forum (acting as meeting convener).*

The activity consists mainly in workshops (organised regularly) on key topics (eg. share the latest developments in AN, provide updates on CSP AN journey progress, explore topics of mutual interest: high-value scenarios, AN PoCs, intent-driven processes, AI/GenAI role in AN).

ETSI and 3GPP play a leading role in the AN Multi-SDO community thanks to the excellent results achieved in AN, supported by the wish to share information and to open collaboration opportunities.

Through enhanced coordination both within ETSI and across the broader standards ecosystem, the industry can work toward cohesive, interoperable approaches to autonomous networks while maximising the efficient use of resources and expertise.

Being proactive in these initiatives is a way to promote ETSI results on AN, to contribute to the success of Autonomous Networks and to facilitate recommendations and standards convergence.

10 Conclusions

Cognitive Autonomous Networks can unlock the CSP business and open the era of the Digital Transformation of the Industry, facilitating the transaction from pure CSP to Digital Service Provider. AN Level 4 and beyond can enable service delivery with agility and speed and ensure the economic sustainability of an innovative set of services offered by Digital Service Providers. AI is a key enabler to accelerate and enrich Autonomous Networks, considering seriously the compliance with CSA and AI act. Nevertheless all the ICT Community should avoid too many concerns and delays in investing in AI and GenAI for Networks in order to allow innovation to exploit its role for Digital Transformation.

11 References

- [1] [Nokia - Harnessing the power of AI in autonomous RAN operations.](#)
- [2] [NAE - The path to AI-driven autonomous telecoms networks.](#)
- [3] [Innovile® - AI-Driven Decision Making: How Autonomous Networks are Changing the Game in Telecom.](#)
- [4] [Case Western Reserve University - Advancements in Artificial Intelligence and Machine Learning.](#)
- [5] [NGMN - The outline of a framework for autonomous networks based on AI.](#)
- [6] [The Evolution of AI in Autonomous Systems: Innovations, Challenges, and Future Prospect.](#)
- [7] [IKTARA - Generative AI Background.](#)
- [8] [XENONSTACK - Generative AI for Network Operations.](#)
- [9] Master of Code - Generative AI in Telecom: Success Stories and Potential Use Cases for Improving CX <https://masterofcode.com/blog/generative-ai-chatbot-in-telecom-success-stories-and-potential-use-cases>.
- [10] NGMN Alliance (V1.0): "6G Use Cases and Analysis".
- [11] Recommendation ITU-R M.2160-0 (V1.0): "Framework and overall objectives of the future development of IMT for 2030 and beyond".
- [12] [ETSI TS 104 223 V1.1.1 \(2025-04\)](#): "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".
- [13] TM Forum TMF921 (V5.0.0): "Intent Management".
- [14] [Whitepaper No.62-Vision for Telecommunications 6G.](#)



- [15] [Whitepaper No.55-MEC support towards Edge Native Design.](#)
- [16] [Cybersecurity of AI Standardisation.](#)
- [17] [ENISA Threat Landscape, Gartner, 2023.](#)
- [18] [Papernot et al., 2017.](#)
- [19] [Trusting Artificial Intelligence in Cybersecurity, a Double-Edged Sword.](#)
- [20] [Gartner, 2023.](#)
- [21] [NCSC - Digital twins: secure design and development.](#)
- [22] [OWASP API Security Top 10, 2023.](#)
- [23] [Whitepaper No. 56: "Unlocking Digital Transformation with Autonomous Networks".](#)
- [TFS23] R. Vilalta, et al., "Applying digital twins to optical networks with cloud-native sdn controllers", IEEE Communications Magazine, 61, 12, 128-134, 2023.
- [24] [Whitepaper No. 46: "MEC security; Status of standards support and future evolutions".](#)
- [TFS24a] D. Adanza, et al., "IntentLLM: An AI Chatbot to Create, Find, and Explain Slice Intents in TeraFlowSDN", in IEEE 10th International Conference on Network Softwarization (NetSoft), 2024.
- [TFS24b] D. Adanza, et al., "Enabling traffic forecasting with cloud-native SDN controller in transport networks", Elsevier Computer Networks, 2024.
- [TFS24c] D. Adanza, et al., "A Hybrid Method to Predict Network Traffic Demands for Each Link", IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2024.
- [TFS24d] R. Vilalta, et al., "Providing Anomalous Behaviour Profiling by extending SmartNIC Transceiver support in Packet-Optical Networks", Optical Fiber Communications Conference and Exhibition (OFC), 2024.
- [25] [NIST Zero Trust Framework, 2020.](#)
- [26] [Privacy-Preserving Network for Autonomous & Sovereign AI Agents.](#)
- [27] [Privacy-Preserving AI: Securing Data Protection Through Differential Privacy and Federated Learning.](#)
- [28] [EU AI Act, 2024.](#)
- [29] [Security of and by Generative AI platforms.](#)
- [30] [MITRE ATT&CK for Network Security, 2023.](#)
- [31] ETSI ENI White Paper 44 ENI vision for Autonomous operations
https://www.etsi.org/images/files/ETSIWhitePapers/etsi-wp44_ENI_Vision.pdf.
- [32] [ETSI GS ENI 005 \(V3.1.1\)](#): "Experiential Networked Intelligence (ENI); System Architecture".
- [33] [ETSI GR ENI 051 \(V4.1.1\)](#): "Experiential Networked Intelligence (ENI); Study on AI Agents based Next-generation Network Slicing".
- [34] [ETSI ENI: White Paper 64](#), covering AI technologies for Autonomous operations.
- [35] [ETSI GR ENI 007](#): "Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks".
- [36] [ETSI GR ENI 010](#): "Experiential Networked Intelligence (ENI); Evaluation of categories for AI application to Networks".
- [37] [ETSI GR ENI 035](#): "Experiential Networked Intelligence (ENI); Definition of IP networks autonomicity level".



- [38] [ETSI GR ENI 049](#): "Experiential Networked Intelligence (ENI); Definition of Data Centre Networks autonomic level".
- [39] [ETSI TS 128 312](#) Ver. 18.8.0: "Management and orchestration; Intent driven management services for mobile networks".
- [40] [ETSI GS ZSM 002](#): "Zero-touch network and Service Management (ZSM); Reference Architecture".
- [41] [ETSI GS ZSM 008](#): "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management".
- [42] [ETSI GS ZSM 009 series](#): "Zero-touch network and Service Management (ZSM); Closed-Loop Automation".
- [43] [ETSI GR ZSM 016](#): "Zero-touch network and Service Management (ZSM); Intent-driven autonomous networks; Generic aspects".
- [44] [ETSI GS ZSM 012](#): "Zero-touch network and Service Management (ZSM); Enablers for Artificial Intelligence-based Network and Service Automation".
- [45] [ETSI GS ZSM 018](#).
- [46] [ETSI White Paper No. 51](#): "ENI Vision: Understanding the Operator Experience Using Cognitive Management", First edition – January 2023. Not listed in doc.
- [47] TM FORUM: "[Promoting a trusted telco data space to drive new opportunities](#)".
- [48] [The RoadtoEuropeanDigital Sovereignty withGAIA-X andIDSA](#).
- [49] TM Forum IG1230 (V1.1.1): "Autonomous Networks Technical Architecture".
- [50] TM Forum IG1251 (V1.0.1): "Autonomous Networks - Reference Architecture".
- [51] [ETSI GR F5G 021 \(V1.1.1\)](#): "Fifth Generation Fixed Network (F5G); F5G Advanced Generation Definition".
- [52] [ETSI GR F5G 020 \(V1.1.1\)](#): "Fifth Generation Fixed Network (F5G); F5G Advanced Use Cases Release 3".
- [53] [ETSI GS F5G 024 \(V1.1.1\)](#): "Fifth Generation Fixed Network (F5G); F5G Advanced Architecture Release 3".
- [54] [ETSI GR F5G 019 \(V1.1.1\)](#): "Fifth Generation Fixed Network (F5G); Fixed Network Autonomous Network level definition and evaluation".
- [55] [ETSI GS F5G 027 \(V1.1.1\)](#): "Fifth Generation Fixed Network (F5G); F5G Advanced End-to-End Management and Control".
- [56] [List of F5G Advanced PoCs](#).
- [57] [D. Brodimas et al.: "Towards Intent-based Network Management for the 6G System adopting Multimodal Generative AI," 2024 Joint European Conference on Networks and Communications & 6G Summit \(EuCNC/6G Summit\), Antwerp, Belgium, 2024, pp. 848-853, doi: 10.1109/EuCNC/6GSummit60053.2024.10597022](#).
- [58] K. Trantzas et al.: "Intent-driven network automation through sustainable multimodal generative AI," *J Wireless Com Network* 2025, 42 (2025). <https://doi.org/10.1186/s13638-025-02472-x>.
- [59] [ETSI GR NFV-IFA 054](#): "Network Functions Virtualisation (NFV) Release 6; Architecture; Report on architectural support for NFV evolution".
- [60] [ETSI GR NFV-EVE 023](#): "Network Functions Virtualisation (NFV) Release 6; Evolution and Ecosystem; Report on new infrastructure resources for NFV".

- [61] ETSI TR 103 910: "Methods for Testing and Specification (MTS); AI Testing; Test Methodology and Test Specification for ML-based Systems".
- [62] ETSI TS 103 194: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet".
- [63] ETSI EG 203 341 "Core Network and Interoperability Testing (INT); Approaches for Testing Adaptive Networks".
- [64] ETSI TS 103 195-1: "Core Network and Interoperability Testing (INT/ WG AFI) Generic Autonomic Network Architecture; Part 1: Business drivers for autonomic networking".
- [65] [ETSI TS 104 224 V1.1.1 \(2025-03\)](#): "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".
- [66] ETSI TR 103 473: "Evolution of Management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures".
- [67] ETSI TR 103 404: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Backhaul and Core network parts of the 3GPP Architecture".
- [68] ETSI TR 103 495: "Network Technologies (NTECH); Automatic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in Wireless Ad-hoc/Mesh Networks: Autonomicity-enabled Ad-hoc and Mesh Network Architectures".
- [69] [ETSI White Paper no. 16](#) - GANA - Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services First edition – October 2016.
- [70] ETSI TR 103 857: "ETSI TC INT; Autonomic Management and Control (AMC) Intelligence for Self-Managed Fixed & Mobile Integrated Networks (AFI); End-to-End Autonomic Security Management and Control Multi-Domain 5G Networks".
- [71] ETSI TR 103 858: "ETSI TC INT; Autonomic Management and Control (AMC) Intelligence for Self-Managed Fixed & Mobile Integrated Networks (AFI)".
- [72] ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG).
- [73] 3GPP TS 23.288.
- [74] 3GPP TS 28.100.
- [75] 3GPP TR 28.910.
- [76] 3GPP TR 28.909.
- [77] [ETSI GS ENI 006](#) (V2.1.1): "Experiential Networked Intelligence (ENI); Proof of Concepts Framework".
- [78] [ETSI GS ENI 019](#) (V4.1.1): "Experiential Networked Intelligence (ENI); Representing, Inferring, and Proving Knowledge in ENI".
- [79] TM Forum IG1252 (V1.2.0): "Autonomous Networks Level Evaluation Methodology".
- [80] TM Forum IG1339 (V2.1.0): "Autonomous Networks L4 High Value Scenarios".
- [81] TM Forum GB1059A (V2.1.0): "RAN Fault Management Questionnaire".
- [82] ETSI TR 104 164.



The Standards People

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

This White Paper is issued for information only. It does not constitute an official or agreed position of ETSI, nor of its Members. The views expressed are entirely those of the author(s).

ETSI declines all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper.

ETSI also declines responsibility for any infringement of any third party's Intellectual Property Rights (IPR), but will be pleased to acknowledge any IPR and correct any infringement of which it is advised.

Copyright Notification

Copying or reproduction in whole is permitted if the copy is complete and unchanged (including this copyright statement).

© ETSI 2025. All rights reserved.

DECT™, PLUGTESTS™, UMTS™, TIPHON™, IMS™, INTEROPOLIS™, FORAPOLIS™, and the TIPHON and ETSI logos are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM™, the Global System for Mobile communication, is a registered Trade Mark of the GSM Association.