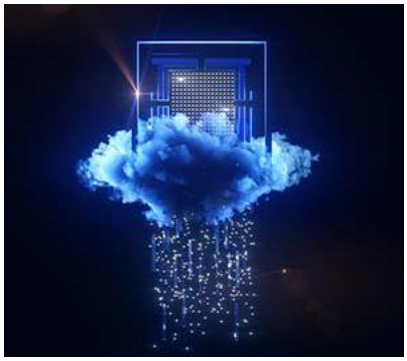
www.pipelinepub.com
Volume 18, Issue 11

Unleashing 5G & 6G with AI-empowered Automation

By: Nurit Sprecher



5G and 6G networks are expected to provide virtually unlimited gigabit and ultra-reliable connections to people and objects, when and where it matters, supporting diverse use cases with an extremely demanding range of requirements in terms of latency, throughput, reliability, coverage and security, cost targets, and more. Building a network that supports a diverse set of new services, however, all of which can be set up, dynamically reconfigured, scaled and torn down at a moment's notice, introduces several challenges.

Unprecedented operational agility is required to allow services to be rapidly deployed, dynamically adapted, and continuously and seamlessly assured—similar to the way in which cloud providers offer on-demand, managed cloud services.

The network's performance, coverage and capacity should be constantly assured to satisfy the requirements of the active services. Any fault or degradation that might adversely impact the services should be resolved.

An exponentially more complex network

Each and every service spans multiple technological domains and is composed of cloud resources, connectivity, virtual and physical network functions, augmenting services and application logic. The network includes hundreds of thousands of network functions and each function has multiple versions. In addition, 5G runs on a virtualized infrastructure and is designed with a fully programmable approach to software and microservices, capable of supporting diverse use-cases. This makes the 5G network exponentially more complex to operate and manage! When we add distributed clouds, heterogenous networks, the 10X densification of RAN sites, meshing and integrated multi-supplier technologies to the mix, we introduce even more complexity, driving

up the timescale and cost. The accelerated worldwide deployment of 5G networks drives a radical change in the way networks and services are created, orchestrated, and managed. Evolution toward zero-touch and full end-to-end network and service automation has become an urgent necessity to manage this complexity and deliver services with agility and speed, while adapting, assuring, and ensuring the economic sustainability of the highly diverse service portfolio.

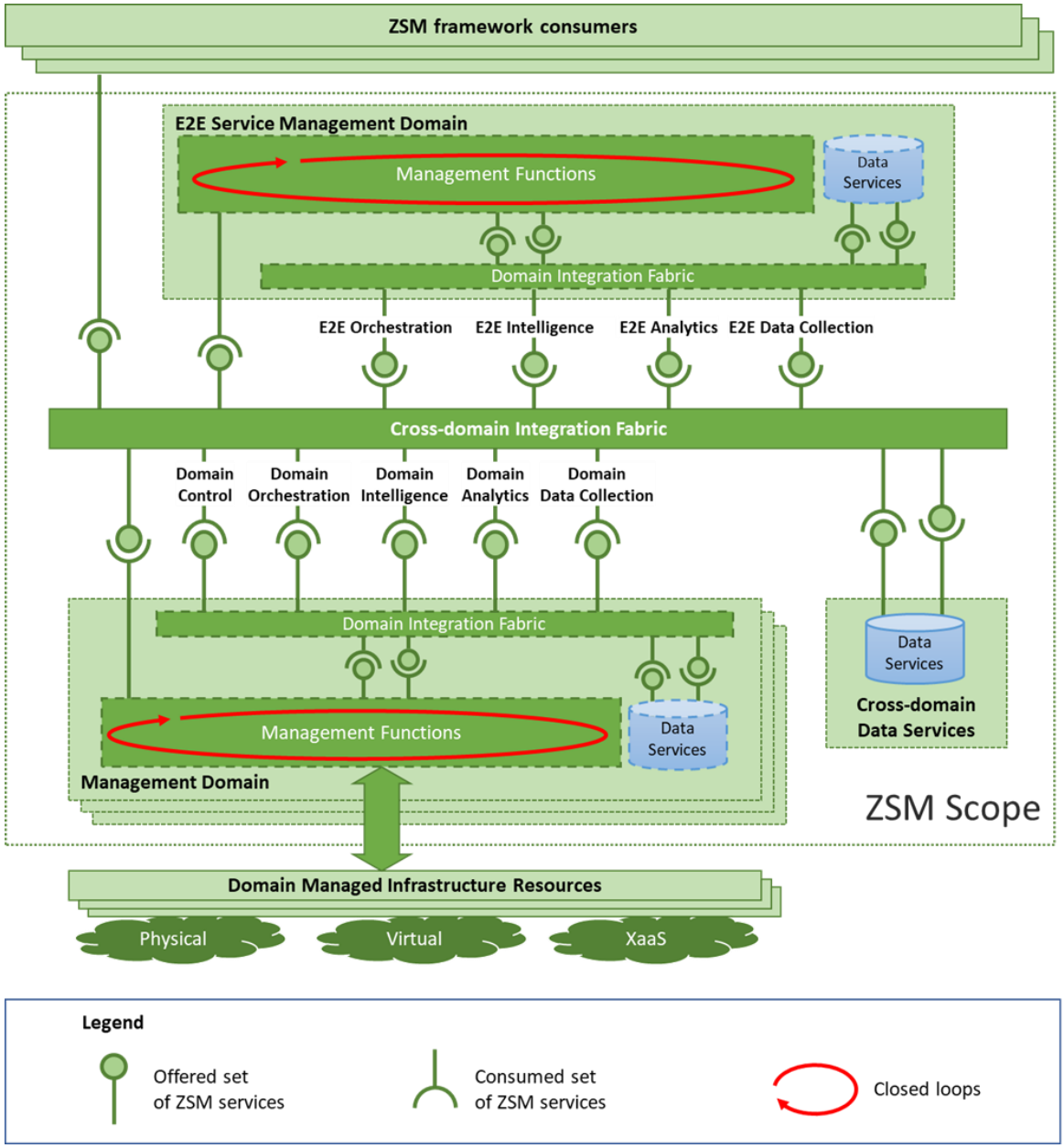


Figure1: ZSM framework

The ultimate target is to achieve the highest degree of automation, ideally 100 percent, while enabling fully autonomous operation driven by high-level business goals and policies. The autonomous networks will be able to self-manage and self-organize (configuration, healing, assurance, optimization, and so on) without human intervention beyond the initial transition of the business intents.

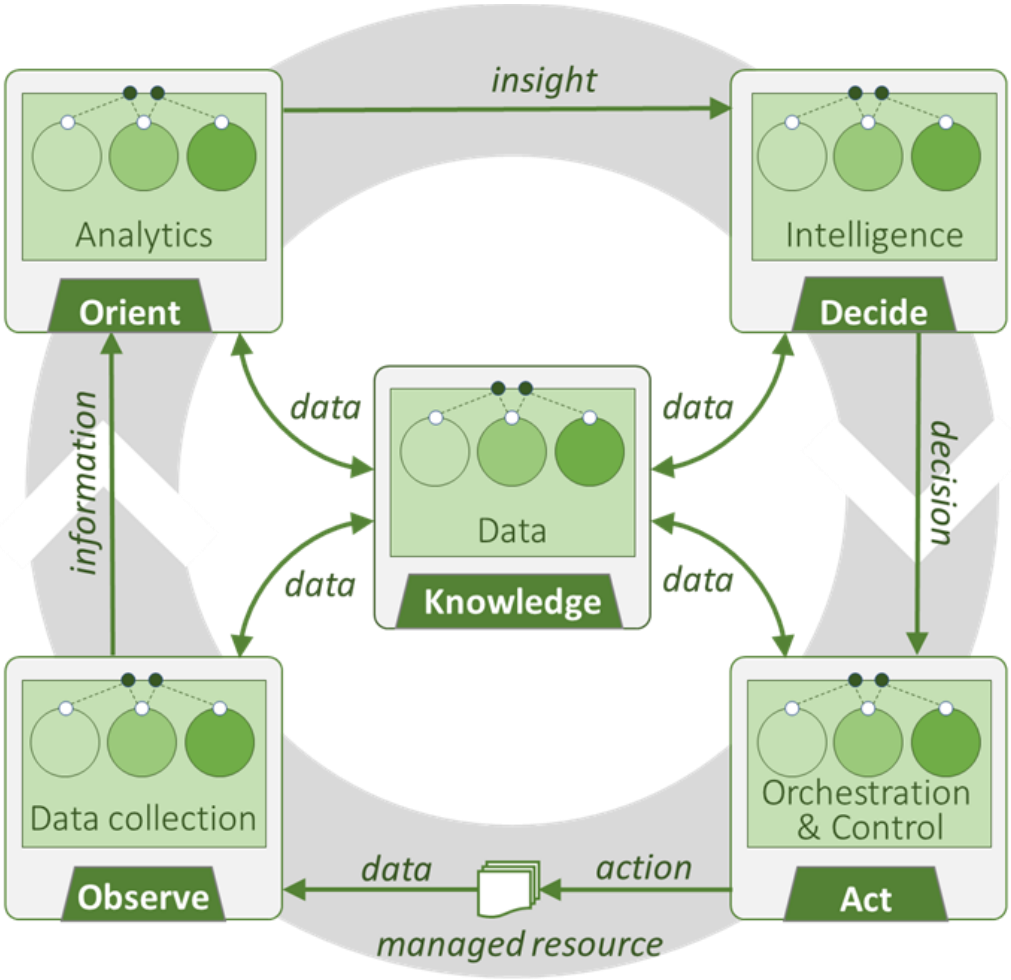


Figure 2: Closed loop example

Realizing this vision requires a novel end-to-end architecture framework and enablers designed for self-management, near-real-time closed-loop automation and optimized for data-driven analytics. Advanced machine-learning algorithms and artificial intelligence (AI) will be essential tools to deal with the complexity and the diverse services.

ETSI ZSM and new specifications

The ETSI ZSM (Zero-touch network and Service Management) group was formed in December 2017 with the goal to define a future-proof, end-to-end operable framework and solutions and key automation technologies to enable agile, efficient, andqualitative management of emerging and future networks and services.

The ZSM framework (depicted in Figure 1 on previous page, and specified in ETSI ZSM 002) is versatile and built on service-based principles offering scalability, modularity, extensibility, and flexibility. It supports the transfer of autonomy from the operator to the network using intent-based interfaces. The framework provides capabilities to integrate AI-based functionalities and enable closed-loop automation.

The framework supports the separation of management and automation into areas of concern, or management domains (where the scope is delineated, for example, by an administrative or

technological boundary, such as Radio Access) and end-to-end cross-domain service management domains. Each management domain is responsible for the fulfillment and assurance processes within its scope. The separation of concerns allows the abstraction of the complexity of the management domains.

The ZSM framework supports open interfaces as well as model-driven service and resource abstraction. The management services, which are exposed by the management domains, are described and specified. The architecture allows operational data to be kept separately from the management applications, enabling rapid and efficient access to current, real-time management data within and across the management domains to support the automation processes.

The framework is designed to enable adaptive, closed-loop automation—providing a feedback loop (depicted in Figure 2 on previous page) between data monitoring, data analytics, decision-making and adaptive actions that aims to reach and preserve a set of objectives without external intervention.

A closed loop enables the continuous optimization and adaption of network and resource utilization and automated service assurance and fulfillment. The automated decision-making mechanisms can be bounded by rules and policies. Advanced machine learning and artificial intelligence can empower the closed-loop operation.

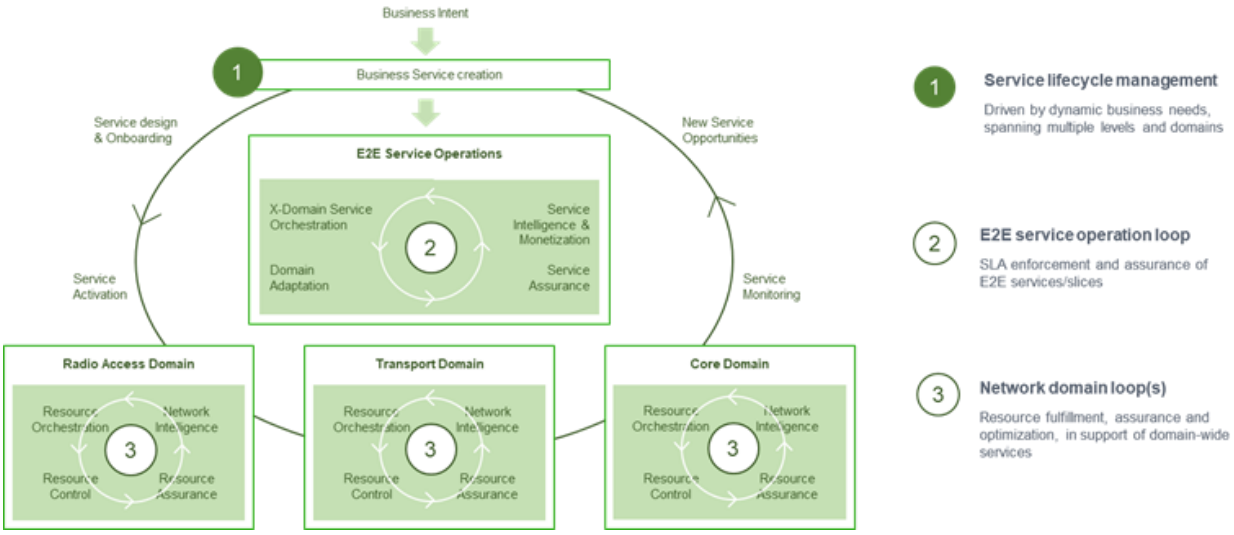


Figure 3: Intelligent, coherent and interconnected loops across business, service and network management domains

ETSI ZSM 009-1 on closed-loop automation enablers specifies "Governance" services that allow for the creation, execution, and lifecycle management of a closed loop as well as the configuration of related policies and rules to steer the behavior. The "Governance" services also support interaction between closed loops and external entities, such as human operators, allowing them to supervise the operation and performance of closed loops. As more automation and closed loops are deployed and start to operate safely and efficiently, human trust will increase and the requirement for a level of supervision and visibility will diminish.

As depicted in Figure 3 on pervious page, closed-loop operation can be implemented at the management-domain level. Closed-loop operation can also occur at the end-to-endservice-management domain level and can span multiple management domains. Multiple closed loops can run simultaneously.

ETSI ZSM 009-1 provides capabilities to support coordination, delegation and escalation between closed loops while ensuring intelligent, consistent, and coherent service delivery.

Coordination between loops is essential when there is dependency between their operations or when they can adversely interfere with each other. It can also help to improve their operations and fulfill their goals, for example by sharing information produced by the different closed-loop stages.

This specification also enables the delegation and escalation of respective goals between superior and subordinate closed loops. A superior closed loop can delegate respective goals to the subordinate closed loop(s), for example by setting the policies and/or the intents that allow the subordinate closed loop to act autonomously. A subordinate closed loop can escalate goals to the superior closed loop in a situation, for example, where it is not able to achieve the goal assigned to it. Escalation and delegation support the separation of management and automation into different autonomous areas of concern (end-to-end cross-domain service operations, management domains), where each is responsible for assurance and intelligent automation within its scope.

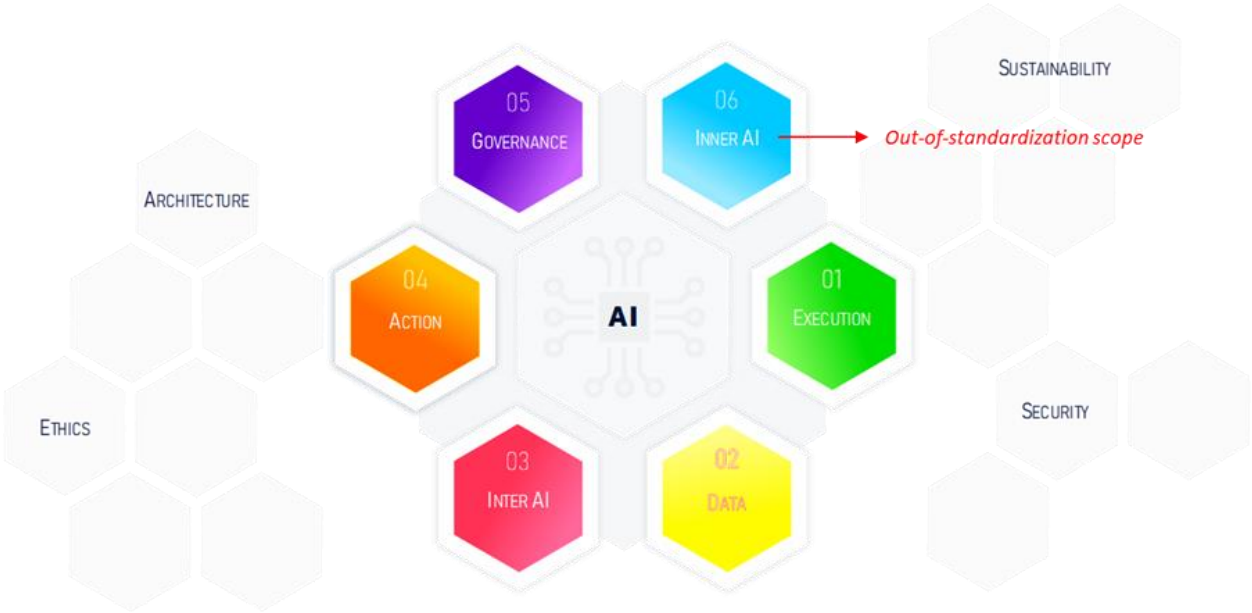


Figure 4: AI enablers

The ZSM group is currently progressing with its report on intent (ETSI ZSM 011). Intents express declaratively all the operational expectations an autonomous management domain needs to fulfill and assure, including requirements, goals, and constraints. The report will propose additional management capabilities and services to support intents and their lifecycle management, and recommend whether existing intent models and semantics can be leveraged. It will also suggest how conflicting intents can be handled. The results from the study will provide the basis for a new normative specification.

The group is also working on the specification of additional management capabilities to enable full AI operations within the ZSM framework (ETSI ZSM 012), ensuring support for deployment diversity. Figure 4 on previous page introduces key AI enablers.

These enablers include capabilities to:

- Access the right data, at the right place and at the right time, while ensuring data integrity and trustworthiness.
- Support coordination between multiple, distributed AI applications, ensuring a consistent and holistic operational view and the means to act on it. AI applications can collaborate in learning different tasks or contribute collectively to solve a common problem.
- Trigger an action based on the AI output to support closed-loop automation while understanding the output is important for correctly applying the decisions or recommendations.
- Govern and supervise the AI-empowered operations. AI results must be reliable, measurable, interpretable and accountable. The AI applications should adhere to applicable laws, regulations, ethical principles and values, and be robust against adversarial threats and missing or erroneous data.
- Express requirements and constraints for the deployment of the AI applications.

ETSI ZSM 008 defines how to manage the lifecycle of cross-domain, end-to-end (E2E) services. It describes the management processes during the lifecycle of E2E services (service onboarding, fulfillment and assurance) and describes the interactions between E2E service management domain and management domains. ETSI ZSM 003 focuses on the E2E aspects of network slice management, supporting vertical use cases and related SLAs (service-level agreements).

The ZSM framework

Automation is not only about technology; it also requires changes in our mindset. Trust is a major barrier to adoption and striving to build it requires a continuous learning process. As more automation processes are deployed and operate safely and efficiently, human trust will increase and the requirement for a level of supervision and intervention will diminish. Having native security (as in an adaptive secured framework, access control, trustworthiness, and data protection) can help to establish confidence and instill trust as the automated processes deliver the intended business outcomes.

The threat surface in the ZSM environment is extensive because of the openness of the framework. Protecting the interfaces and the management services within and across the domains is essential to ensure the trustworthiness of the framework.

In addition, the ZSM services can be produced and consumed by new players coming from diverse industries, including government, vehicle manufacturing, energy, transportation, and more. Each player may require different trust levels according to its own deployment and execution

environments, security policies and regulations. This variety demands flexible and adaptive security control.

Furthermore, the ZSM framework leverages emerging technologies, such as AI/ML, data lake, cloud, and more, which introduce new vulnerability to attacks and impose additional security requirements. For example, it is necessary to ensure trustworthiness and shield the AI/ML algorithms from highly sophisticated, creative, and malicious attacks, including abuse, trolls, data poisoning, and model rescue. Moreover, it is critical to protect data, ensuring its integrity, confidentiality, and availability, and to preserve privacy to comply with security laws and regulations. At the same time, the ZSM framework can take advantage of these emerging technologies to increase security management efficiency. For example, using AI/ML-empowered analytics to trigger actions can help to automate security monitoring and a real-time response to incidents.

ETSI ZSM 010 presents a comprehensive security study identifying and analyzing potential security threats and assessing the related risk scores and priorities. The report proposes mitigation options, countermeasures, and security controls to address the threats and risks to the ZSM framework and solutions. The ZSM group is working to specify requirements and security capabilities (ETSI ZSM 014) to support the automatic security assurance of the ZSM framework, management application and services.

End-to-end automation is a “big deal” and represents the industry’s ongoing journey. The use of AI/ML will evolve incrementally and learnings from real deployments need to be fed into the standardization work. Intent-driven network and service and slice automation will be key elements to provide a zero-touch, zero-problem experience and to simplify automation by hiding the complexity of the federated telco capabilities.

Experimental and showcase ZSM solutions are essential to demonstrate the viability of the technology. View a list of current ZSM Proofs of Concepts (PoCs). The different players in the value chain are welcome to demonstrate PoCs and contribute to the automation journey.