Standards Update

Network Transformation

(Orchestration, Network and Service Management Framework)

By Chairmen of ISG ENI, MEC, NFV and ZSM

ETSI addresses the network transformation challenge and highlights the value that core ETSI Technical Bodies provide to the industry.

Executive Summary

The telecommunication industry is in the middle of a significant transformation. Driven by the needs of 5G networks and applications and enabled by transformative technologies, such as NFV and cloud-native deployment practices, this is likely to be the single greatest technological and business transformation of the telecom industry since the consolidation of mobile communication infrastructures.

The telecom networks that will emerge from this transformation are going to be highly distributed and fully software-defined, running primarily on homogeneous cloud resources. The flexibility that these characteristics bring will allow mobile operators to address the heterogeneous and divergent needs of 5G applications in a highly efficient manner (e.g. through the use of techniques such as network slicing) – but only if overall network services can be properly managed.

The issue of management is perhaps the most critical challenge facing the telecom industry as it moves into 5G. Given the scale, heterogeneity and complexity of the emerging 5G networks, management solutions need to be highly automated and extremely "intelligent", in the sense of a "machine intelligence" able to collect large amounts of relevant data as well as process and act on them in an automated fashion. To use an over-simplified example, truck rolls are expensive. When they are "emergency" truck rolls, they are very expensive and if they require a 5G network expert to be on the truck, they are a financial disaster. The challenge is to use automation to completely eliminate the need for network expertise on a truck, minimise emergency rolls by using predictive maintenance and significantly reduce truck rolls through automation.

The purpose of this article is to describe how ETSI addresses the network transformation challenge, as well as highlight the value that core ETSI Technical Bodies provide to the industry.

Specifically, we address the common framework for management of virtualised network environments, as defined by NFV, and extended to the distributed edge with public-cloud aspects by MEC. We discuss how ENI solutions can be deployed within or across network domains to optimise the processing of data, extract knowledge and enable decision-making. Finally, we demonstrate the work of ZSM in bringing all these and other technologies together into a single automated management framework.

The need for network transformation

Network transformation has, at its root, the various *digital transformations* which other industries are facing. For the network case, we are talking about a much deeper change as the process is focused on changing the very nature of the network infrastructure itself. It naturally implies a serious and profound change in network management mechanisms.

Traditional network management was done in a silo-oriented way (fixed, mobile…) with very limited automated interaction between those management silos. The automated management of services was also out of scope. Service has been considered from a commercial perspective, focused on what customers are expected to consume, without incorporating network technical requirements into a holistic network service concept.

The split between hardware, software and the consideration of service management from an exclusive commercial point of view, as discussed above, did not allow the required integral approach to achieve automation. The classical management of networks (what we could call the old OSS) is not able to support network transformation from a management point of view. A transformation from the old world of OSS into a modern, autonomous network management environment is required.

This goal can be achieved if the split between what we could call the "OSS plane" and the network plane disappears. The integration of dynamic, intelligent and close network telemetry, the application of closed-loop control techniques and the use of AI techniques open new ways for management. It is important that the application of these technologies is achieved with the foundation of a common vision and a consistent technology framework.

The network management technologies supported by the OSS approach have recently been augmented by applying concepts originating from cloud-based environments. OSS is conceived as an open-loop system providing FCAPS (Fault Management, Configuration Management, Account Management, Performance Management and Security Management) management capabilities to human (and non-human) users, while closed-loop automation of operational procedures eliminates the need for detailed FCAPS analysis and management. The ultimate goal is to enable a higher degree of management flexibility by enablers such as orchestration and service composition, empowering customers with the capability to manage their own services, and enabling the vision of network slicing, as described in the seminal NGMN 5G White Paper [1].

A flexible and integral approach to business processes is key to achieving the transformation goals in network management. Flexibility is essential in adapting to the different network segments and deployment styles in the highly multi-tenant, multi-provider telecommunications environment and to support consistent service definition, creation and maintainability.

Automation must become an integral part of all the phases of business processes - not only in the execution (or run-time) phase, but also in the service design phase. Each phase has specific requirements, which have an impact on the solution. To achieve the optimum, both processes must influence each other, including feedback of the insights achieved in the run-time to the design phase.

Additionally, a note on the DevOps approach needs to be made. In many cases, the application of DevOps principles for network management has been highlighted as an essential enabler for a complete network transformation. While it is true that those principles are of general interest and well aligned with the goals of network management transformation, a better understanding of how these principles can be translated into the telecommunications environment is required to apply them. Networks have different conditions and must abide by a series of invariants regarding topology, forwarding preservation, full interoperability and even regulatory aspects, which need to be incorporated to assess how to apply shorter cycles between development and operation.

Considering all these points, it was clear that industry specifications would play an important role in addressing the challenges in an interoperable way. In the next section, we will introduce the steps taken in ETSI to develop such specifications in a manner open to all stakeholders.

> **"The issue of management is perhaps the most critical challenge facing the telecom industry as it moves into 5G."**

Steps towards autonomous network management

The telecommunication and IT industry assembled in different industry specification groups within ETSI to address challenges facing the industry at specific intervals. In this section, we introduce these groups, their main goals and their achievements in the order of foundation, reflecting how the industry is reacting to the desire for change.

NFV (Network Functions Virtualisation)

Formed in 2012, the ETSI NFV Industry Specification Group (ISG) has been the spearhead of network transformation activities within ETSI, being at the core of NFV technology, definition and standardisation. In more than seven years, the ISG NFV community has evolved through several phases, moving from defining the initial framework (including the archetypal architecture diagram for anyone dealing with NFV, which is included below for reference and also as a reminder) and pre-standardisation studies to detailed specifications in the close-to-finished Release 3. At the current stage, the NFV community has produced a set of mature specifications, consolidated their applicability in the industry and continues to work on guaranteeing widespread interoperability and addressing new architectural and application challenges. While NFV was originally conceived to help network service providers in the quest for cost reduction and agility, it has proved to be an essential tool in enhancing how these services are requested and consumed by users. It is a necessary ingredient for next-generation networks and, in particular, the emerging 5G.

With NFV, standard IT virtualisation technology is adapted to consolidate the heterogeneous network infrastructure based on disparate, ad-hoc equipment types onto industry-standard high-volume servers, switches and storage. This involves implementing network functions in software which can run on a homogeneous, industry-standard infrastructure. This software can then be moved to, or introduced in, various locations in the network as required. The use of NFV simplifies the roll-out of network services, reduces deployment and operational costs, facilitates network management automation and encourages innovation. The technology has been adopted increasingly for network planning, deployment and evolution and has become an essential element of modern network design. NFV delivers

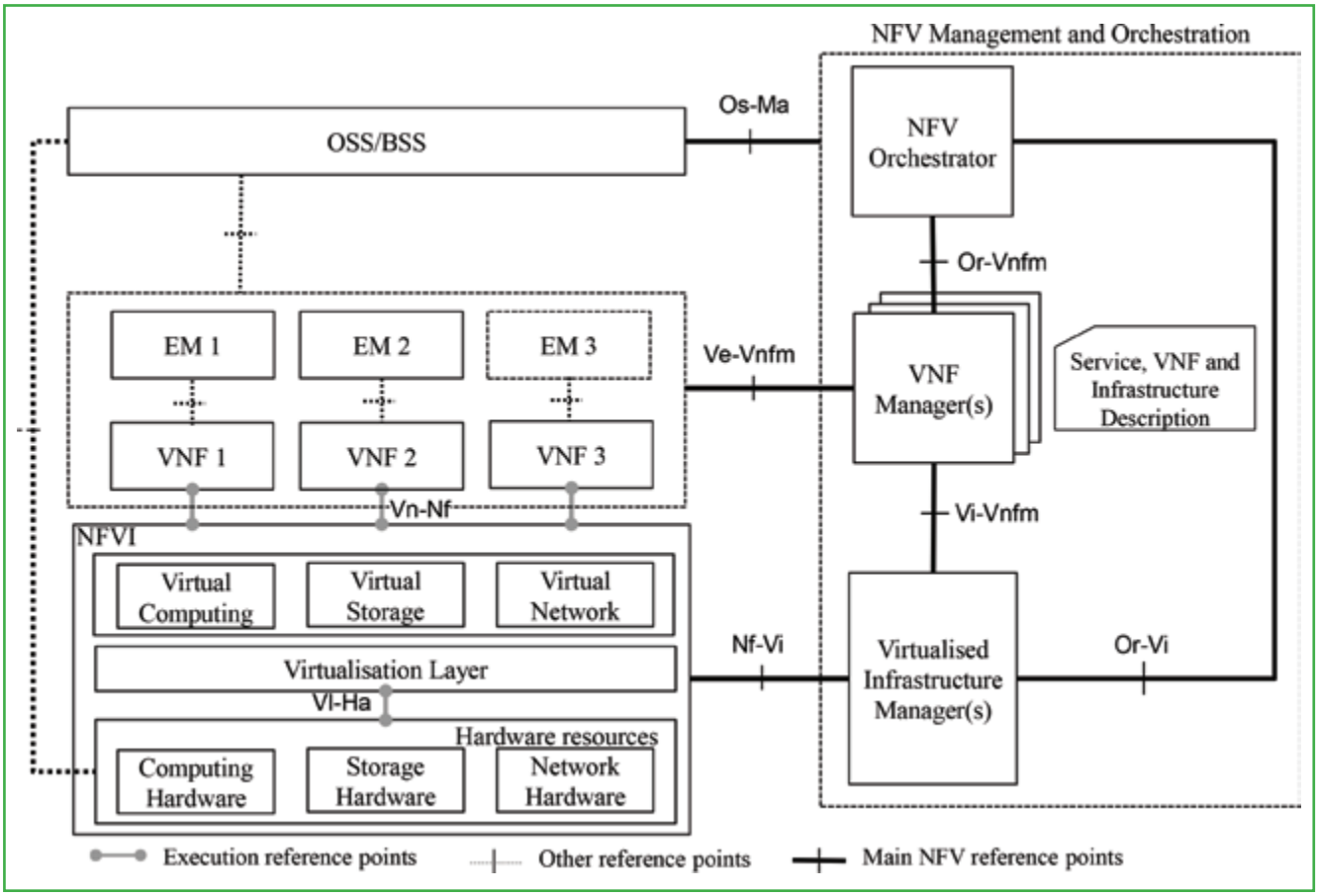

Figure 1: The NFV architecture framework

significant benefits to service users and providers, especially in emerging 5G networks.

ETSI NFV started by building a basic framework to provide a common ground to all involved parties, including the agreement on common terms, essential to address the change that was taking place. This effort to build the fundamental NFV framework happened in parallel with a strong activity to demonstrate the feasibility of NFV concepts and principles, especially relevant for a groundbreaking proposal. This constituted what ETSI NFV called Release 1.

Once the fundamentals were set and proved to be solid, it was time to go into a detailed exploration of network virtualisation, its requirements in terms of orchestration, management, performance, reliability and security, and the necessary interfaces, information and data models. The result of this work was ETSI NFV Release 2, which provides a set of detailed specifications addressing the aspects mentioned, bringing a final consolidation of the essential concepts established by Release 1.

After this set of concrete specifications, an equally important challenge remained: the integration of NFV procedures with operational practice, so that NFV-enabled infrastructures and services could be incorporated into actual industrial processes and provide a clear migration path. This was the main goal of Release 3, which the group is about to complete.

Release 4 considers the following technical areas:

- **Consolidation of the infrastructural aspects**, by a redefinition of the NFV infrastructure (NFVI) abstraction, incorporating enhancements to support lightweight virtualisation technologies (with containers as the key goal), optimising NFVI abstraction for reducing the coupling of functions to infrastructures and easing connectivity for functions and services.
- **The enhancement of NFV automation and capabilities**, by improving lifecycle management and orchestration, simplifying function and service management and incorporating advances in autonomous networking.
- **Evolution of the Management and Orchestration (MANO) framework**, with the goal of optimising internal capability exposure and usage.
- **NFV operationalisation**, focused on the simplification of NFV specification space to ease development and deployment of sustainable NFV-based solutions, the consideration of verification (and certification) procedures and mechanisms and the integration and use of NFV with other management and network frameworks.
- Some specific technical aspects, related to the security hardening of NFV orchestration, functions and services, and the enhancement of models and their mapping onto function and service descriptors.

As illustrated in the (already classical) diagram on the previous page, the NFV scope is essentially focused on the lifecycle of virtualised network functions (VNFs) and the services built by composing VNFs among them, and with other components with a lifecycle not managed by NFV, generally referred to as PNFs (with the "P" standing for "physical"), irrespectively of their nature. Software-enabled function and service lifecycle management constitutes a new dimension to be considered, and it has to be:

- Integrated with other end-to-end management facets of any network system.
- Deemed as an essential enabling technology for scalable network automation.
- Considered as a key target for new operational architectures and techniques.

MEC (Multi-access Edge Computing)

Although all ETSI MEC specifications are defined to enable a self-contained MEC cloud which can exist in different cloud environments, in most telco environments the need is to extend NFV into the MEC realm. To that end, ETSI MEC has defined a MEC-in-NFV reference architecture in GS MEC 003 [2], reproduced in Figure 2 overleaf.

As shown here and discussed in GS MEC 003 [2], this architecture takes full advantage of the NFV MANO architecture and demonstrates how ETSI MEC defined entities integrate with it. Specifically, we note the following key observations:

- The ETSI MEC Platform is an NFV VNF, albeit one that requires special handling. For example, in any ETSI MEC "edge cloud", it must be instantiated before any other ETSI MEC Application.
- All other ETSI MEC Applications can be treated by ETSI NFV entities as VNFs – even if they were not designed as such.

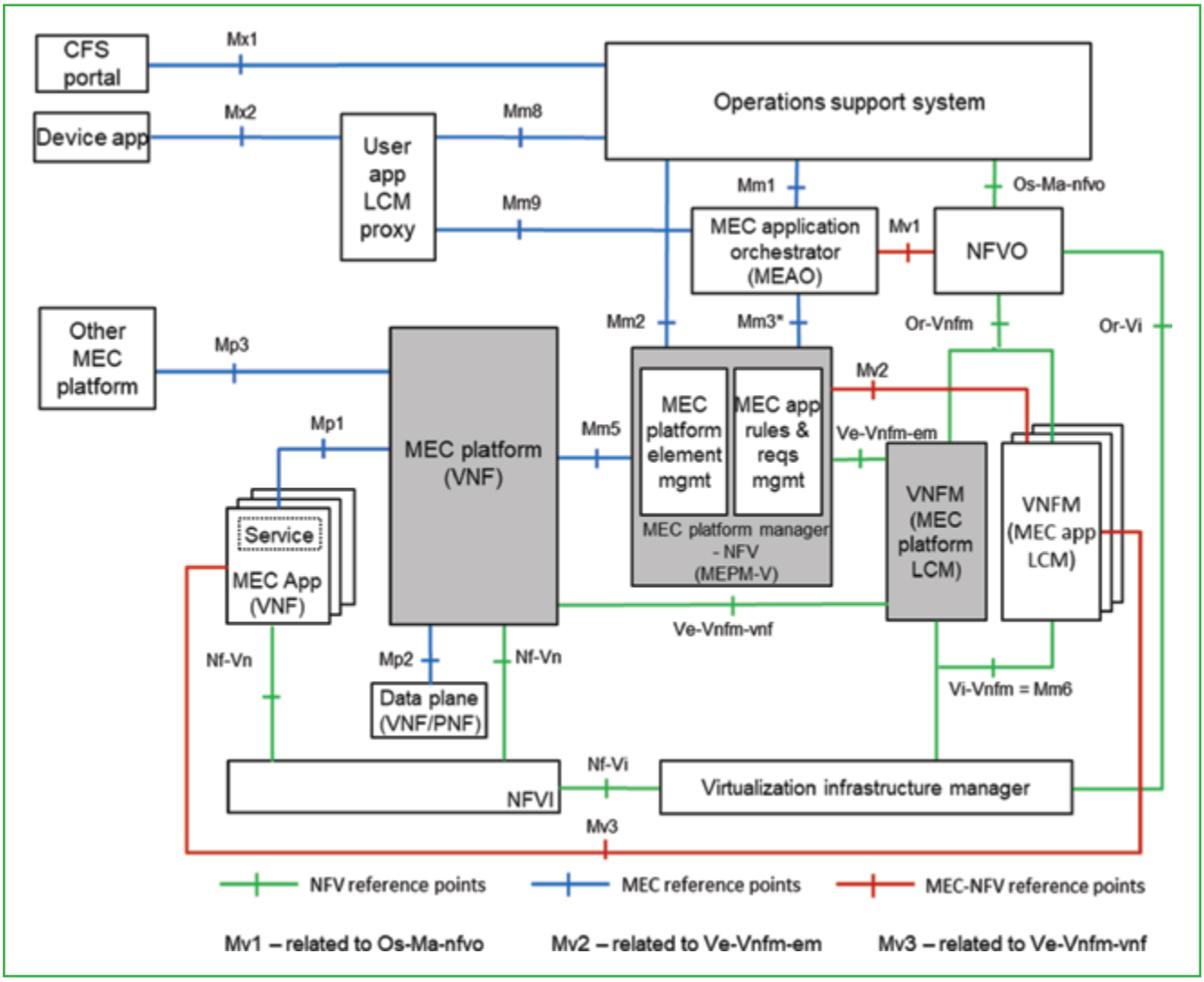

Figure 2: MEC-in-NFV reference architecture (GS MEC 003 [2])

- The ETSI MEC Platform Manager acts as EM for the MEC Platform and all Apps, including interactions with VNFM on behalf of Apps (thus "making" them VNFs). If needed, it can also assume the role of VNFM for these apps.

Figure 2 above also shows a number of interfaces that appear to require coordination and cooperation between ETSI MEC and ETSI NFV, resulting in integration complexities. In fact, the integration is much simpler then the visual perception from this Figure. Specifically:

- Mv3 utilises the same APIs as Ve-Vnfm-vnf.
- Mv2 requires some changes to Release 2 of Ve-Vnfm-em APIs, but ETSI NFV has already implemented these for Release 3.
- Mv1 will require some additional definitions in APIs for Os-Ma-nfvo, with current work planned for ETSI NFV Release 4.

Additionally, the MEC descriptor (AppD), to be defined in the forthcoming release of the ETSI GS MEC 010-2 specification, must be linked to NFV descriptor (VNFD). This has been enabled as part of ETSI NFV Release 3 work using the Non-MANO artifact capability as defined in Annex B of GS NFV-SOL 004 v. 2.6.1 [3] and higher. With this capability, ETSI MEC defined AppD will be registered as a Non-MANO artifact, once it is officially defined by the ISG (something expected within about a year).

Of particular note to the subject of this article is the presence of the operations support system (OSS) in the MEC reference architecture, as shown in Figure 2. This traditional management node is included for completeness of the reference architecture – ETSI MEC does not specify anything about it. However, as a service-based approach to management is developed by ETSI ZSM and other organisations, ETSI MEC expects to align with

the emerging zero-touch management entities, such as those in the ETSI ZSM End-to-End Service Management Domain, and update the reference architecture accordingly. Moreover, given the critical importance of automation for actual MEC deployments, we expect telcos to increasingly look to such modern evolutions of OSS for their deployments.

ENI (Experiential Networked Intelligence)

ENI specifies an architecture to enable closed-loop network operations and management-leveraging AI. The need for close-loop operations at any domain of the network and cross-domains requires ENI to be deployed and operate at, for example, one domain of the network and/or cooperatively across different domains.

ENI can be deployed as an external AI/ML entity, outside an existing "Assisted System". ENI can be configured to operate in two modes – Recommendation and/or Direct Control Management mode. In the former, it provides insights and advice for the operator or Assisted System. In the latter, it is coupled to the Assisted System control loop to participate in its management, based on gathered data, Knowledge, policies and Context and Situational awareness.

Shown below, four classes of Assisted Systems are anticipated – from those capable of communicating with the operator only, to those where some information can be shared directly with ENI while the other has to go through the operator or other existing management tools.

While in more sophisticated cases, shown below, the Assisted System may already have Closed Control Loop (or is a hybrid system where some modules enjoy the benefits of a closed control loop while others do not), ENI can be directly coupled to influence the overall closed control loop of the combined system.

A brief overview of the architecture is provided here. A high-level Functional Block diagram that includes the use of an API Broker is shown in Figure 3 below. This is a simplified view of the main processing components of an ENI System. It is important that a linear flow from input to output may not actually occur. This is explained in the following sections. The arrows in Figure 3 represent the directionality of data and information using any of the twelve External Reference Points.

ENI is a closed loop policy-driven AI/ML designed to employ existing and emerging technologies, such as Big Data

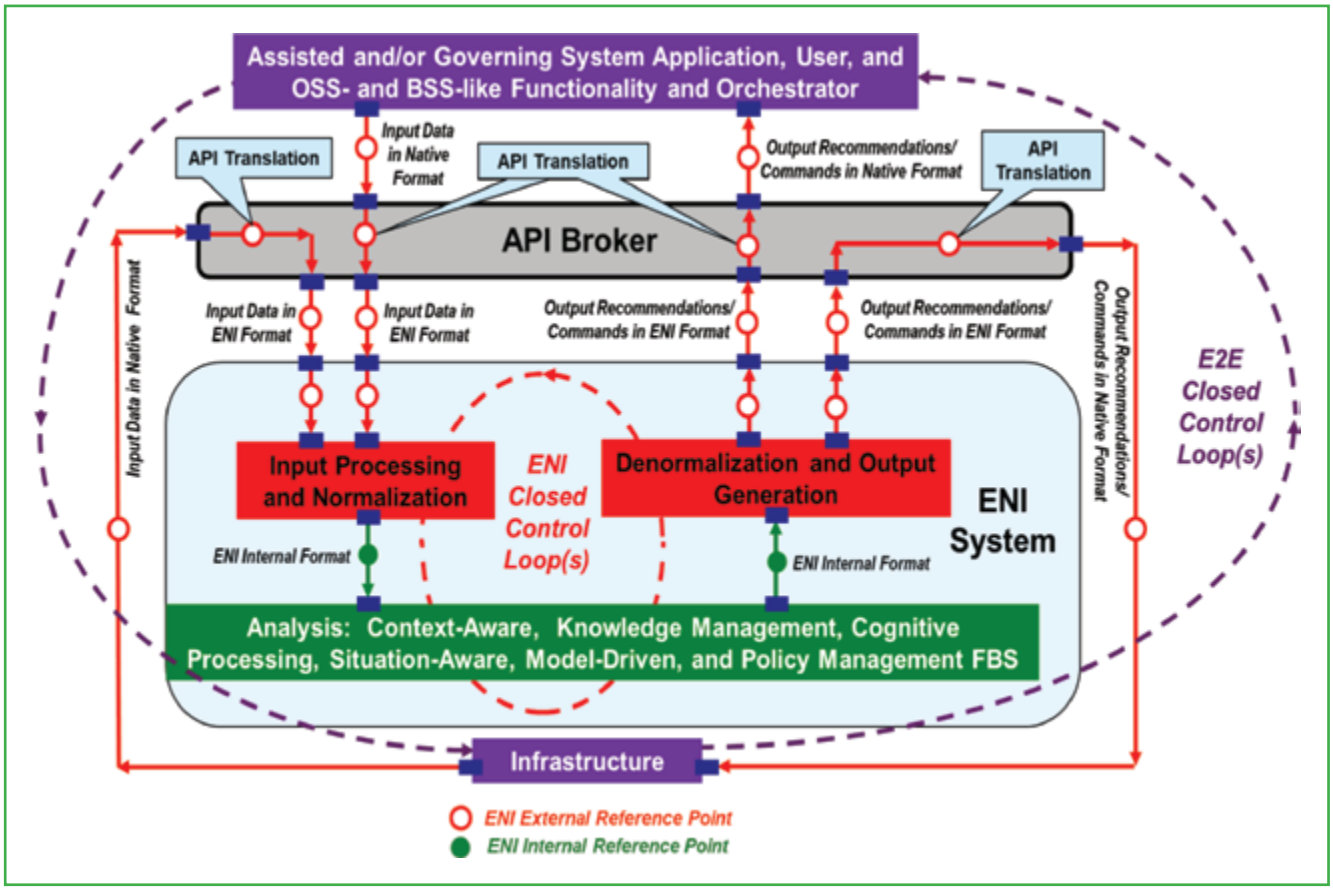

Figure 3: High-level functional architecture of ENI when an API Broker is used

A transformation from the old world of OSS into a modern, autonomous network management environment is required.

analysis, analytics and artificial intelligence mechanisms. An Assisted System, depicted in purple (in Figure 3), may use its own native data format for conveying State or Policy. ENI will offer, in its forthcoming release 2, an Information Model and internal representation of the data/state gathered and manipulated. For systems that use other formats, an API Broker may need to be deployed outside the ENI system to provide a true translation of its formats/models/data to those supported by ENI. A complete functional block description is to be found in the Group Specification GS ENI 005 [4] that specifies the internal interaction and functionality of ENI's Functional Blocks.

ENI is therefore capable of adjusting the configuration and monitoring of networks and networked applications. It dynamically updates its acquired knowledge to understand the environment. It can also help to determine which services should be offered and which services are in danger of not meeting their Service-Level Agreement (SLA), as a function of changing context.

To enable industry momentum and convergence towards an AI/ML enlightened network, given the huge diversity of existing and emerging networks, ENI has published a set of External Reference Points. These External Reference Points are useful to 'canonise' the high-level semantics of ENI interactions with various types of Assisted Systems. ENI has also published Use Cases in GS ENI 001 [5] and requirements in GS ENI 002 [6] that are supported by the ENI System Architecture.

ZSM (Zero-touch Network and Service Management)

The overarching design goal of ZSM is to provide a framework that enables zero-touch automated network and service management in a multi-vendor environment.

The work of the organisations described previously solves dedicated aspects of network and service management. NFV, MEC and ENI have defined management capabilities for their respective focus areas. On top of this, ETSI ZSM aims to provide a holistic end-to-end network and service management concept which, among others, enables the integration of ENI, NFV and MEC management demands. ZSM is building a flexible service-based network and service management framework which supports cross-domain end-to-end management and provides enablers for closed loop automation and for data-driven management algorithms that can be based on machine learning and artificial intelligence.

ZSM scenarios and resulting requirements have been studied and documented first in GS ZSM 001 [7]. To enable deployments that fulfil these requirements, the ZSM framework reference architecture has been defined in GS ZSM 002 [8]. A framework for proofs of concept (PoC) has also been put in place to allow validation of the specifications by the latest implementations, bringing multiple ecosystem partners together. A terminology document GS ZSM 007 [9] defines terms which are commonly used in ZSM documents to avoid misinterpretation.

The ZSM framework reference architecture defines a set of architectural building blocks which collectively enable construction of more complex management services and management functions using a consistent set of composition and interoperation patterns. Management domains provide the means to separate management concerns, taking into account boundaries of different natures (technological, administrative, organisational, geographical etc.). Every management domain provides a set of ZSM management services, featuring management functions that expose and/or consume a set of service end-points. An end-to-end service management domain is a special management domain responsible for cross-domain management and coordination.

The cross-domain integration fabric facilitates the provision of services and the accessing of endpoints cross-domain. This also includes services for communication between management functions, which facilitates the provisioning of "live" management data to consumers who require them. Complementing this, cross-domain data services provide services to persist data and to access these. Logical groups of management services contain services with related functionality (such as data collection, analytics, intelligence, orchestration/control) without implying a particular implementation.

Figure 4 (on the next page) depicts the ZSM framework reference architecture.

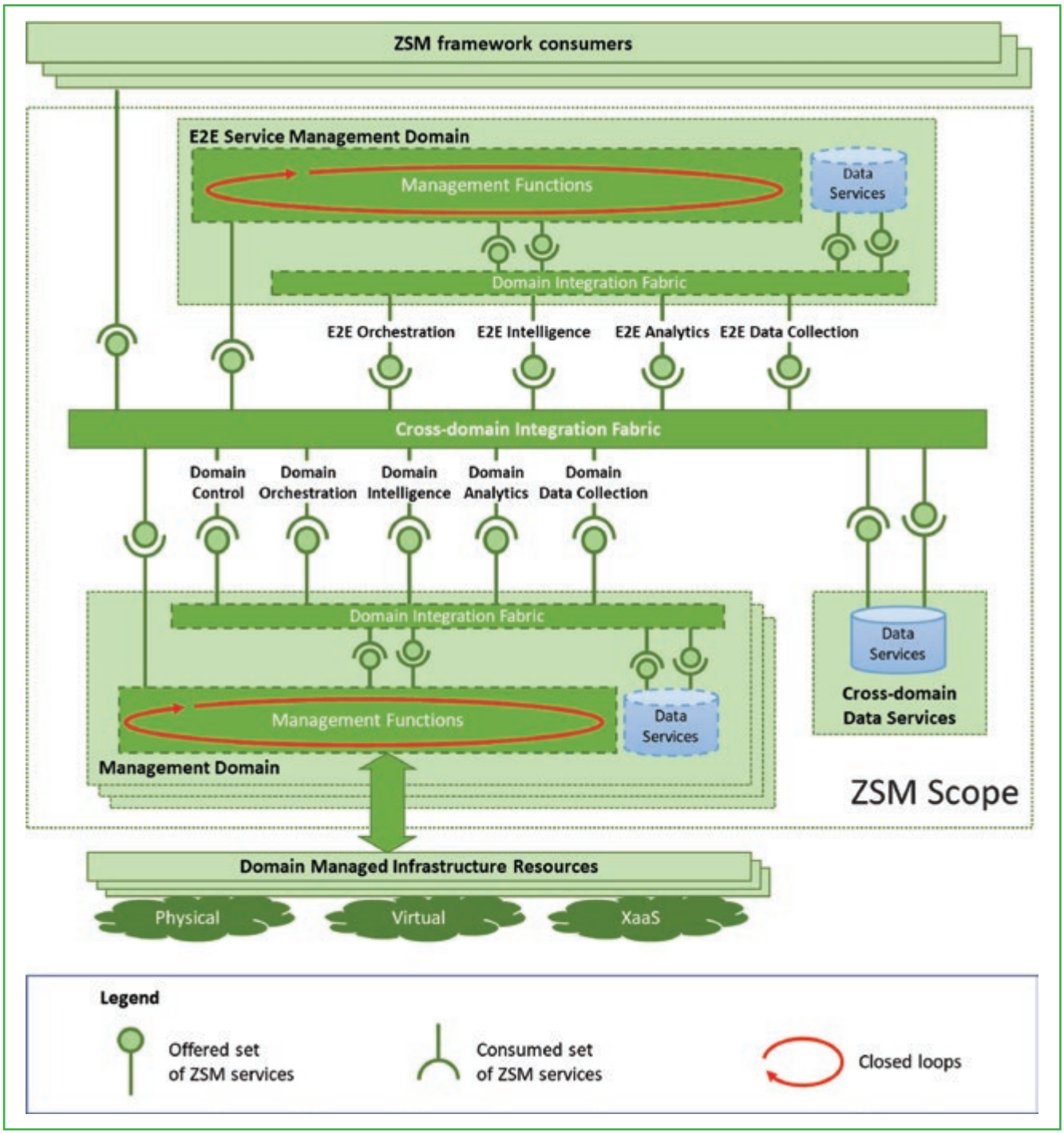

Figure 4: The ETSI ZSM framework reference architecture (from GS ZSM 001 [7])

Because of its flexibility, the ZSM framework reference architecture is able to incorporate management services arising from Open Source implementations or other SDOs. Examples include APIs from the TMForum ODA, management services as defined by 3GPP or, based on work that has just started, from ETSI NFV. The possibility to flexibly compose management services, together with the provisioning of "live" and persisted management data, provide the foundation for closed loop automation. Based on the architecture, the ETSI ZSM group defines enablers and solutions for closed-loop automation as the next step.

A common way forward

Let us recapitulate the implications which successive transformation initiatives have brought to network operation and management.

> **The ZSM framework reference architecture is able to incorporate management services arising from Open Source implementations or other SDOs.**

With NFV, the decoupling of capacity (hardware) from functionality (software) became feasible. The old, OSS-based approach to network management, that assumed specific functional components associated to concrete capacity supports controlled via dedicated management elements, was no longer the only way. End-to-end, uniform operation and management became possible.

MEC took into account the deployment of functions at the edge of the network, including third-party ones, to enable essential, homogeneous, end-to-end, holistic operation and management mechanisms. A number of interfaces used by MEC and NFV are already jointly specified and implemented. More joint interface specifications will come soon.

ENI is committed to support end-to-end automation enabled by AI solutions. The normalisation and pre-processing of data (facilitating their consumption by AI modules able to generate the appropriate action, informed by high-level policies), is required functionality to close the gap between already available data analytics and policy-based management systems.

ZSM addresses the challenge that a mix of standards bodies, open source initiatives and customer projects are tackling on various parts of the automation challenge, and an overarching framework is missing. ZSM is focused on defining a homogeneous service-based approach, supporting automation across management domains, able to incorporate existing and future solutions in a common automation framework and providing an overarching integration framework towards full end-to-end network service automation.

The ZSM architecture has been designed as a framework which provides flexibility to cover different management architecture deployments and enables closed-loop automation and data-driven procedures for management, machine learning and artificial intelligence. Based on the architecture framework, ZSM is now moving forward to specify solutions for end-to-end network slicing and end-to-end service orchestration, as well as enablers and solutions for closed-loop automation.

Work done inside ETSI (NFV, MEC, ENI, OSM) and in standards and open source organisations outside ETSI (3GPP, IETF, BBF, MEF, ONAP, TMF and others) fits nicely into

the ZSM architecture and can help to enable the orchestration and automation of end-to-end services. The ZSM architecture provides a common foundation which allows a diverse ecosystem of open-source groups to produce interoperable solutions.

NFV, MEC, ENI and ZSM have made, and are still making, significant steps towards the specification of new technologies able to take advantage of the network transformation trends towards virtualisation, softwarisation end-to-end abstractions and network management automation. The work of other standards and open source organisations within and outside ETSI is considered in the developments in all these ISGs.

ETSI started the network transformation journey some time ago, addressing the different stages as they were reached by creating the required communities to achieve open collaboration within the appropriate focus. These communities share a vision and a common way forward, and actively collaborate through it.

In conclusion, ETSI is responsive and rapid, cooperating with bodies inside ETSI and other SDOs outside ETSI.

References

[1] A deliverable by the NGMN Alliance, NGMN 5G White Paper, https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[2] GS MEC 003, V2.1.1 (01/2019): “Multi-access Edge Computing (MEC); Framework and Reference Architecture”. https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.01.01_60/gs_MEC003v020101p.pdf

[3] GS NFV-SOL 004, V2.6.1 (04/2019): “Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; VNF package specification”. https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/004/02.06.01_60/gs_NFV-SOL004v020601p.pdf

[4] ETSI GS ENI 005, V1.1.1 (09/2019): “Experiential Networked Intelligence (ENI); System Architecture”, https://www.etsi.org/deliver/etsi_gs/ENI/001_099/005/01.01.01_60/gs_ENI005v010101p.pdf

[5] ETSI GS ENI 001, V2.1.1 (09/2019): “Experiential Networked Intelligence (ENI); Use Cases”, https://www.etsi.org/deliver/etsi_gs/ENI/001_099/001/02.01.01_60/gs_ENI001v020101p.pdf

[6] ETSI GS ENI 002, V2.1.1 (09/2019): “Experiential Networked Intelligence (ENI); ENI Requirements”, https://www.etsi.org/deliver/etsi_gs/ENI/001_099/002/02.01.01_60/gs_ENI002v020101p.pdf

[7] ETSI GS ZSM 001, V1.1.1 (10/2019): "Zero-touch Network and Service Management (ZSM); Requirements based on documented scenarios", https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM001v010101p.pdf

[8] ETSI GS ZSM 002, V1.1.1 (08/2019): "Zero-touch Network and Service Management (ZSM); Reference Architecture", https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[9] GS ZSM 007, V1.1.1 (08/2019): “Zero-touch Network and Service Management (ZSM); Terminology concepts in ZSM”. https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/007/01.01.01_60/gs_ZSM007v010101p.pdf

Contact

ETSI, 06921 Sophia Antipolis CEDEX, France **T:** +33 4 92 94 42 00 **E:** info@etsi.org **W:** www.etsi.org