International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3324

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Requirements and architectural framework for autonomic management and control of IMT-2020 networks

Recommendation ITU-T Y.3324

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3324

Requirements and architectural framework for autonomic management and control of IMT-2020 networks

Summary

Recommendation ITU-T Y.3324 specifies the high-level and functional requirements and architecture of autonomic management and control (AMC) for IMT-2020 networks. It also specifies interworking reference points between AMC and IMT-2020 management and orchestration architecture, and legacy NMS/OSS. In Appendix I, it describes a use case to realize the AMC architecture through the ETSI GANA reference model.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3324	2018-12-14	13	11.1002/1000/13811

Keywords

Autonomic management and control (AMC), IMT-2020 slice life-cycle management, requirements and architecture.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3324

Requirements and architectural framework for autonomic management and control of IMT-2020 networks

1 Scope

This Recommendation specifies the high-level functional requirements and architecture of autonomic management and control (AMC) for IMT-2020 networks. It also specifies interworking interfaces and mechanisms between AMC and IMT-2020 management and orchestration architecture, and legacy NMS/OSS. AMC architecture and interworking mechanisms include functional entities, reference points and procedures. Appendix I it describes a use case to realize the AMC architecture through the ETSI GANA reference model.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3010] Recommendation M.3010 (2000), *Principles for a telecommunications management network.*

[ITU-T T.50] Recommendation ITU-T T.50 (1992), *International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) – Information technology – 7-bit coded character set for information interchange.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), S*ecurity requirements for NGN release 1.*

[ITU-T Y.3111] Recommendation Y.3111 (2017), *IMT-2020 network management and orchestration framework.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

3.2.1 autonomic management and control (AMC): A behaviour or action that is determined in a reactive or proactive manner based on the external stimuli (environment aspects) as well as the goals they are required to fulfil, principles of operation, capabilities, experience and knowledge.

NOTE – In the case of software-defined networks, this definition means that AMC has the ability to dynamically select the network's configuration, control and manage the network, through its self-management functionality that reaches optimal decisions, taking into account the context of operation (environment requirements and characteristics), goals and policies (corresponding to principles of operation), profiles (corresponding to capabilities i.e., functional features supported), and machine learning (for managing and exploiting knowledge and experience.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADS-FE	Autonomic Decision Support Functional Entity
AI	Artificial Intelligence
AMC	Autonomic Management and Control
ASLMD-FE	Autonomic Slice Life-cycle Management Decision Functional Entity
ASPADS-FE	Application and Service Plane Autonomic Decision Support Functional Entity
ASPM	Application and Service Plane Management
ASPM-S	Application and Service Plane Management Support
CPADS-FE	Control Plane Autonomic Decision Support Functional Entity
CPM	Control Plane Management
CPM-S	Control Plane Management Support
CP-S	Control Plane Support
DE	Decision-making Element
DNS	Domain Name System
DP-S	Data Plane Support
DPADS-FE	Data Plane Autonomic Decision Support Functional Entity
DPM	Data Plane Management
DPM-S	Data Plane Management Support
DoS	Denial of Service
EMES	External Management Entity Support
ERM	External Relationship Management
IASP	IMT-2020 Applications and Service Plane
ICP	IMT-2020 Control Plane
ID	Identifier
IDP	IMT-2020 Data Plane
IoT	Internet of Things
KIER-FE	Knowledge Information Exchange Repository Functional Entity
KP	Knowledge Plane
LTE	Long Term Evolution
MANO	Management and Orchestration
ME	Managed Entity
NE	Network Element
NF	Network Function
NFV	Network Function Virtualization
NMS	Network Management System
ODA	Open Digital Architecture

OFE	Orchestration Functional Entity
ONIX	Overlay Network for Information exchange
OPEX	Operation Expenses
OSS	Operational Support System
PoC	Proof of Concept
QoS	Quality of Service
SDN	Software Defined Network
SI	Slice Instance
SLA	Service Level Agreement
SLM	Slice Life-cycle Management
SON	Self-Organizing Networks
TMF	Tele-management Forum
VPN	Virtual Private Network

5 Conventions

In clause 8, each requirement is indicated mandatory (M), recommended to be mandatory (R) or optional (O).

In clause 10, by default, all information components in an information flow defined in this clause are to be considered "mandatory" unless they are explicitly identified as being "optional".

6 Introduction

As demonstrated by self-organizing networks (SON) in LTE, and many other cases where network automation and autonomic principles of network operation have been devised/experimented, it is now widely agreed that autonomic networking and self-management is a new networking paradigm that brings many benefits to network management and operation, such as operation expenses (OPEX) reduction and enhanced network intelligence through the adaptive control of network resources. The paradigm includes so-called self-management features of network operation such as self-configuration, self-diagnosing, self-healing/self-repair and self-optimization.

Recently, the four emerging networking paradigms that have influenced ICT/telecommunication industries are cloud computing, Internet of things (IoT), software-defined networking (SDN) and network function virtualization (NFV). Fundamental research on these paradigms has quite matured and enough results are available for exploitation. Another network paradigm which is of the same importance is autonomic management and control (AMC) of networks and services. Its fundamental research has also matured. Further developments, however, are needed to take advantage of the benefits of these five paradigms when combined together in future network design. Cloud computing, IoT, SDN and NFV are core enablers of AMC. AMC requires the seamless intelligent decision-making feedback loop of the precise monitoring of status of managed resources, intelligent decision making and necessary policy generation based on the monitored information and open programmable enforcement of generated policies. Cloud computing and IoT provide an abundant resource pool which complex autonomic decision making processes are required for. SDN provides open control capability of enforcing autonomic decision policies. NFV provides a virtual programmable execution environment that autonomic decision entities could run. Due to the relatively static nature of management and control, legacy NMS/OSS and networking infrastructure were not ready for autonomic management and control innovation. These four emerging networking paradigms, however, have become enablers of AMC when they are combined in a standard way. Be

aware that AMC does not replace the legacy NMS/OSS but rather augment self-management capabilities only by interworking with and leveraging SDN, NFV, cloud computing and IoT capabilities as described above.

To support such autonomics and self-management principles and capabilities for IMT-2020 networks including, but not limited to, interconnected large-scale hybrid clouds, SDN-based virtual networks and complex IoT networks, this Recommendation specifies AMC high-level and functional requirements and architecture. It also specifies interworking interfaces and mechanisms with IMT-2020 architecture and legacy NMS/OSS. AMC architecture and interworking mechanisms include AMC and interworking functional entities, reference points and procedures, and a use case scenario.

7 High-level requirements for AMC

Autonomic management and control of IMT-2020 network architecture is required to meet the following high-level requirements:

1) Support of autonomic management capabilities including knowledge plane with cognitive management functionality for IMT-2020 network and services

NOTE 1 – Knowledge plane provides the necessary functionality to support autonomic management of IMT-2020 network and services. One of the main functions of the knowledge plane is a cognitive management process which is a control loop of observe, normalize, compare, learn, plan, decide and act subprocesses. Autonomic management decisions and associated actions are made through this process. It supports three modes of operation: expedited, high-priority and normal, which can be chosen depending on the requirement of the service urgency.

2) Support of scalability of its management functionality

NOTE 2 – Autonomic management functionality should be scalable to be used in complex and large management environments.

3) Support of availability and reliability of its management functionality

4) Support of real, near-real, and/or non-real time autonomic management decision making and operations

NOTE 3 – The cognition process supports three modes of operation: expedited, high-priority and normal to meet this requirement.

5) Support of interworking with the management functionality of IMT-2020 and legacy OSS to enable autonomic management functionality

NOTE 4 – Autonomic management should coexist with the other management functionality. It is a supporting functionality of the other management functionality.

8 Functional requirements for AMC

Autonomic management and control of IMT-2020 network architecture is required to meet the following functional requirements:

– auto-configuration;
– auto-optimization;
– auto-monitoring;
– auto-diagnose;
– auto-healing;
– auto-protection;
– interworking with the management functionality of emerging complementary networking technologies such as SDN, NFV and cloud.

NOTE –These functional requirements can be applied in one or multiple of the following entities: user devices, access, edge and core network for IMT-2020 network and services.

1) Auto-configuration functional requirements
   - FR-1-1 (M): support of auto-configuration of virtual network functions.

2) Auto-optimization functional requirements
   - FR-2-1 (M): support of network auto-optimization in order to adapt and tune their own performance parameters to make accurate decisions with IMT-2020 network and service contexts.
   - FR-2-2 (R): support of SLA guarantee with regard to auto-provisioning and configuration.

3) Auto-monitoring functional requirements
   - FR-3-1 (M): support of auto-monitoring of network devices including virtual devices of its own traffic load and/or traffic type parameters (e.g., available bandwidth, packet loss, QoS) in order to ensure a reliable and efficient network.

4) Auto-diagnose functional requirements
   - FR-4-1 (M): support of auto-diagnose of the known faults (e.g., traffic affected faults or non-traffic affected faults).

5) Auto-healing functional requirements
   - FR-5-1 (M): support of auto-healing, for example, based on auto-location and auto-correction of the root cause of known failures.

NOTE – Since the target failure in this requirement is known in the past, auto-location and auto-correction of the same types of failure can be supported. Auto-healing is the overall process to remedy such known failures based on these two functionalities (i.e., auto-location and correction).

6) Auto-protection functional requirements
   - FR-6-1 (R): support of auto-protection of IMT-2020 network including virtual ones from malicious attacks and unauthorized access.

7) Interworking with the management functionality of IMT-2020 network requirements
   - FR-7-1 (M): support of interface with the management functionality of IMT-2020 network.
   - FR-7-2 (M): support of information model for the interface with the management functionality of an IMT-2020 network.

9 Architectural framework for AMC

NOTE – A term "functional entity" in this Recommendation is equivalent to a term "functional element" in [ITU-T Y.3111].

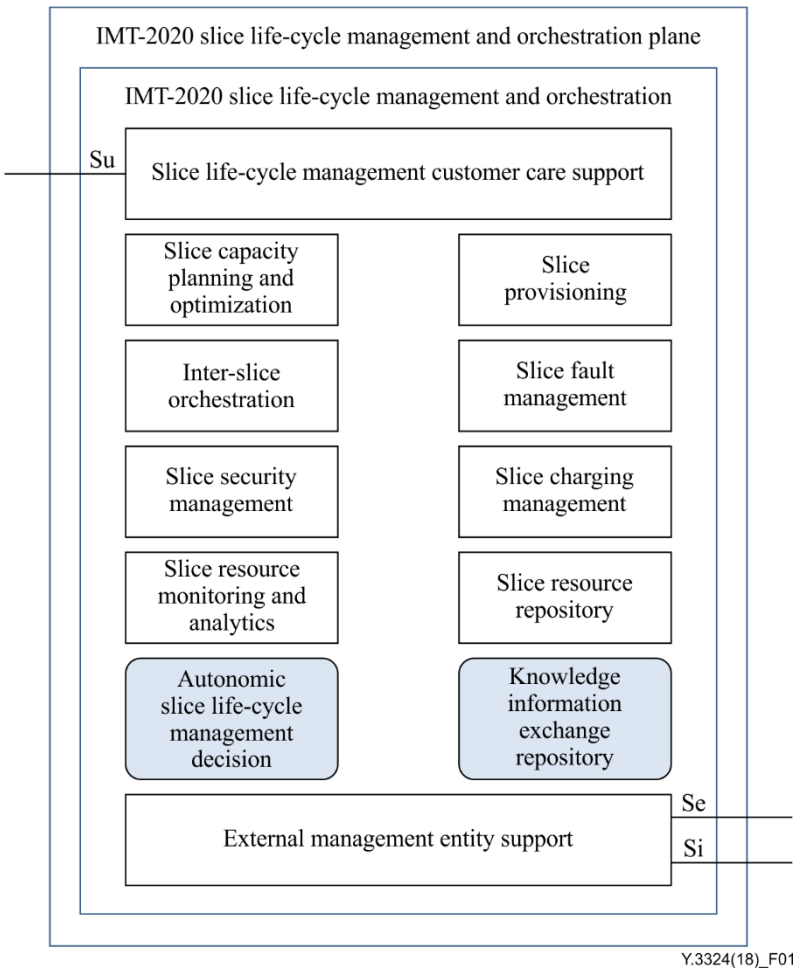

Figure 1 – High-level AMC architecture for IMT-2020 network slice life-cycle management

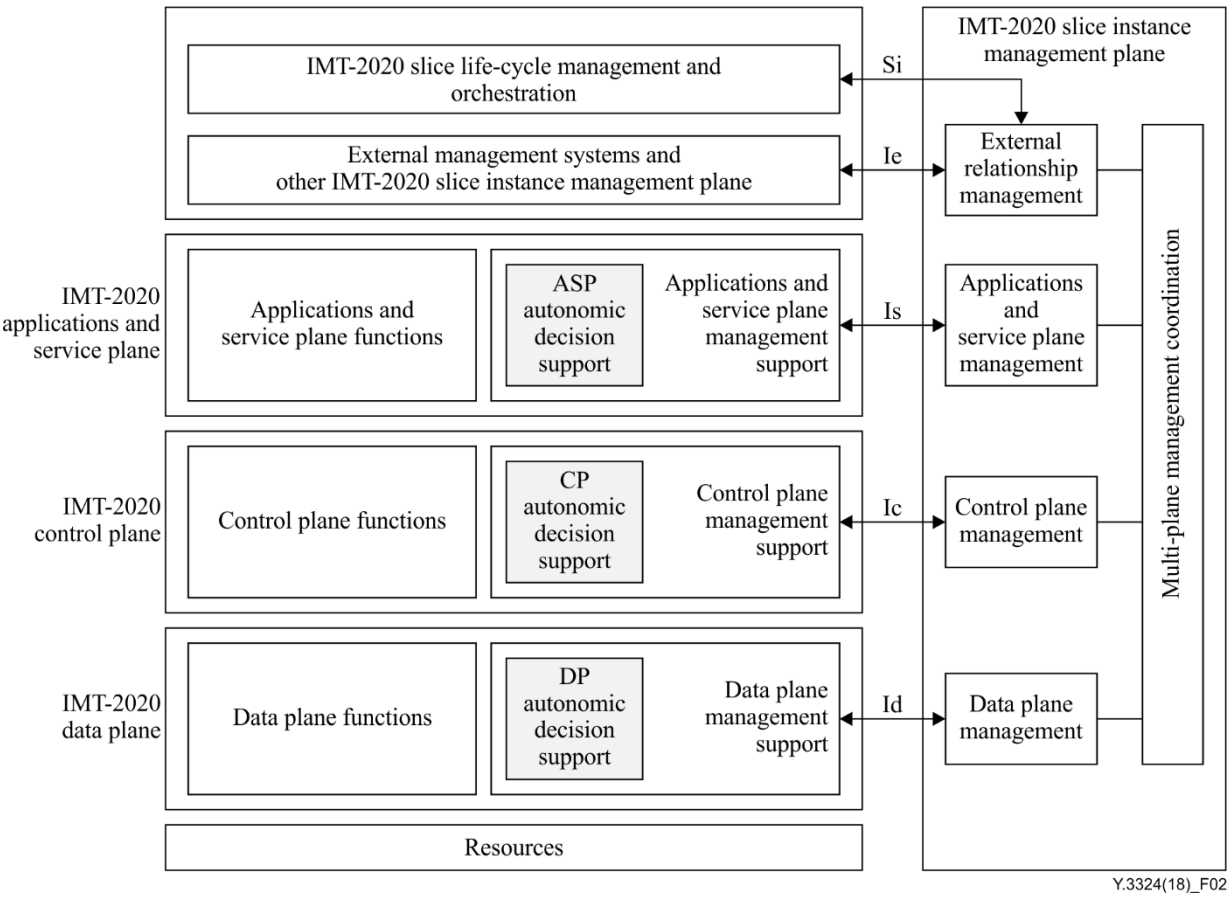

Figure 2 – High-level AMC architecture for IMT-2020 network slice instance management

The high-level architecture described in this Recommendation (see Figures 1 and 2) is augmented based on the high-level architecture of IMT-2020 network management provided in [ITU-T Y.3111]. AMC provides autonomic management and control capabilities for the virtual and physical resources of IMT-2020 networks. Both IMT-2020 network physical and virtual resources are managed and controlled by the IMT-2020 network slice life-cycle management and orchestration plane and IMT-2020 network slice instance management plane. Autonomic management and control capabilities are embedded in physical and virtual resources, control layer and applications and service layer in the form of the autonomic decision support functional entity (ADS-FE). Local AMC policy is stored in each ADS-FE but global AMC policy is stored and managed by AMC capabilities in the slice life-cycle management plane. It consists of the distributed knowledge information exchange repository functional entity and slice life-cycle management level ADS-FEs. ADS-FE has four different levels: protocol, functional, node and network level. The details on the capabilities of ADS-FEs are described in the functional architecture clause below.

9.1 Functional entity overview

The AMC functional entities introduced in this Recommendation are:

– Data plane autonomic decision support functional entity (DPADS-FE)

  DPADS-FE provides autonomic decision support capabilities for both physical and virtual data plane resource as follows:

  The DPADS-FE provides autonomic capabilities within a physical node. It includes self-management capabilities of protocol and function levels. In general, examples of functions can be routing, forwarding and mobility management, etc. However, the functions that the DPADS-FE should autonomically manage (i.e., dynamic and adaptive configuration

of the forwarding function's configurable parameters or managed entities) are forwarding and switching functions of a node (i.e., a network element (NE) or network function (NF)).

It also provides autonomic capabilities within a virtual node or function. It can be similar to the physical node case except that it does not have a physical node associated with it. It also includes the self-management capabilities of protocol and function levels of a virtual node. Examples of functions can be firewall, intrusion detection and virtual EPC, etc.

– Control plane autonomic decision support functional entity (CPADS-FE)

  CPADS-FE provides autonomic capabilities within a control plane. It includes the self-management capabilities of control plane resources and functional entities. Examples of functions can be autonomic control orchestration and autonomic control entities management, etc.

– Application and service plane autonomic decision support functional entity (ASPADS-FE)

  ASPADS-FE provides autonomic capabilities within an application and service plane. It includes the self-management capabilities of application and service plane resources and functional entities. Examples of functions can be autonomic application and service orchestration and autonomic application and service entities management, etc.

– Autonomic slice life-cycle management decision functional entity (ASLMD-FE)

  ASLMD-FE provides autonomic capabilities for an overall network slice life-cycle management perspective, which is highest-level automaticity. It interacts with the DPADS-FE to realize network-wide self-management policy decisions. It conveys network slice life-cycle management level self-management policies into slice instance management planes and orchestrates their local self-management actions. It also interacts with the CPADS-FE to realize its autonomic control actions, the multi-layer management functions to exchange the management information required to make autonomic policy decisions, and the OSS/BSS to exchange management information to deal with the self-management of legacy networks.

– Knowledge information exchange repository functional entity (KIER-FE)

  KIEF-FE provides capabilities to store the network slice life-cycle management-wide self-management policy information in a distributed manner to deal with scalability of large volumes and performance of accessing distributed information repositories.

9.2 Functional entity description

9.2.1 Data plane autonomic decision support functional entity (DPADS-FE)

The DPADS-FE provides autonomic decision and operation capabilities within a physical and virtual node. The functions of the DPADS-FE include:

– monitoring of the status of forwarding, switching and tunnelling related protocols and functions in a physical and virtual node;

– decision making of autonomic behaviours for protocols and functions in a physical and virtual node;

– provisioning of autonomic physical and virtual node-level behaviour such as autonomic routing, forwarding, mobility management, fault management and configuration management in a node;

– sending monitored information and decision-making policies to a local information repository.

9.2.2 Control plane autonomic decision support functional entity (CPADS-FE)

The CPADS-FE provides autonomic capabilities within a control plane. It includes the self-management capabilities of control plane resources and functional entities. The functions of the CPADS-FE include:

– monitoring of the status of functions in a control plane;

– decision-making of autonomic behaviours for functions in a control plane;

– provisioning of autonomic controller behaviour such as autonomic control orchestration, autonomic control entities management agent in a control plane;

– sending monitored information and decision-making policies to a local information repository.

9.2.3 Application and service plane autonomic decision support functional entity (ASPADS-FE)

The ASPADS-FE provides autonomic capabilities within an application and service plane. It includes the self-management capabilities of application and service layer resources and functional entities. The functions of the ASPADS-FE include:

– monitoring of the status of functions in an applications and service plane;

– decision making of autonomic behaviours for functions in an applications and service plane;

– provisioning of autonomic controller behaviour such as autonomic application and service orchestration, autonomic application and service entities management agent in an applications and service plane;

– sending monitored information and decision-making policies to a local information repository.

9.2.4 Autonomic slice life-cycle management decision functional entity (ASLMD-FE)

The ASLMD-FE provides autonomic capabilities for the overall network slice life-cycle management, which is highest-level automaticity. It interacts with DPADS-FEs and CPADS-FEs to realize network-wide self-management policy decisions. It conveys network slice life-cycle management-level self-management policies into distributed repositories and orchestrates their local self-management actions. It also interacts with the control layer to realize its autonomic control actions, the multi-layer management functions to exchange management information required to make autonomic policy decisions, and the OSS/BSS to exchange management information to deal with the self-management of legacy networks. The functions of the ASLMD-FE include:

– monitoring of the status of the DPADS-FE and CPADS-FE;

– decision-making of autonomic behaviour of network slice life cycle management-level management functions:

– provisioning of autonomic network slice life cycle management-level behaviours and policies such as autonomic network slice life cycle configuration management, network slice life cycle fault management, network slice life cycle performance management, network slice life cycle security management and network slice life cycle accounting management;

– sending monitored information and decision-making policies to the KIER-FE.

9.2.5 Knowledge information exchange repository functional entity (KIER-FE)

The knowledge information exchange repository functional entity (KIER-FE) provides capabilities to store the network-wide slice life-cycle management self-management policy information in a distributed manner to deal with the scalability of large volumes and performance of accessing distributed repositories. The functions of the KIER-FE include:

– storing the network-wide self-management policy information received from the DPADS-FE and ASLMD-FE in a distributed manner;
– providing API for querying the stored information;
– providing coordination of distributed repositories for consistency and reliability;
– managing the life cycle of the information in the repository.

10 Reference points

NOTE – [ITU-T M.3010] specifies management reference points among various management functional entities such as x, q, g, m, and f depending on the context that they are used. Two of them are applicable in this Recommendation: x and q. x is for an inter-operators system and q is for intra-operator system purposes. Although SG13 uses different naming conventions for reference points, Si and Se reference points may serve in the context of x or q and Is, Ic and Id reference points in the context of q.

10.1 Reference point Si

The Si reference point is required to enable request/response information needed for IMT-2020 network slice instance life-cycle management to be exchanged between the external management entity support functional element (EMES) in the management and orchestration plane of the IMT-2020 network slice life-cycle management (SLM) and the external relationship management functional component (ERM) in the management plane of a network slice instance (SI).

This reference point is extended to support autonomic management of the overall network slice life cycle. The extension is described in this clause.

The Si reference point may operate as an intra-domain and/or inter-domain reference point.

10.1.1 Functional requirements

10.1.1.1 Slice instance life-cycle management functional requirements

The Si reference point provides the ability to make requests/responses between the EMES in the SLM and ERM in SI for:

– network slice provisioning;
– network slice instance monitoring;
– network slice instance fault management;
– network slice instance charging management;
– network slice instance security management;
– inter-network slice instance orchestration;
– autonomic network slice life-cycle instance management;
– a status report of network slice provisioning, network slice instance performance, fault, charging and security events.

10.1.1.2 Slice instance life-cycle management session processing functional requirements

To assure the reliability and performance of slice instance life-cycle management session operations across the Si reference point, the following capabilities are required:

– **Overload control**: The Si reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the EMES and ERM.
– **Synchronization and audit**: The Si reference point is required to support the capability on synchronization and audit of the network slice instance life-cycle management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Si reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

10.1.2 Information exchange requirements

This clause provides brief descriptions of the information exchange requirements for the Si reference point:

– **Request-response transactions**: The reference point is required to allow EMES to request a transaction to be performed by the ERM and get a response (that can be correlated with the request) in return and also vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: EMES and ERM.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting network slice instance life-cycle management functions.

– **Security**: The Si is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: an EMES is required to be able to communicate with multiple ERMs; 2) many-to-one mode: multiple ERM instances are required to be able to make requests to a given EMES.

10.1.3 Information components

The information components exchanged across the Si reference point are categorized as follows:

Table 10-1 – Information components for reference point Si

Information component	Description
Connection ID	Identifies a transport connection or path. A unique value for Connection ID is set by ERM in SI. Two types supported are IPv4 & IPv6 transport connection IDs.
Authentication Information	Authenticates the peers (i.e., EMES and ERM).
Reason Code	Specifies the reason associated with a particular connection ID or service ID.
Identity Identification	Specifies unique identification. It adopts only International Alphabet No.5 string format defined in the [ITU-T T.50]. Generally, it is a static IP address of EMES/ERM. When the ERCM/ERM adopts dynamic IP address, identity identification object can use domain name system (DNS) domain name.
Keep-Alive Timer	Specifies the maximum time interval over which an Si protocol transport channel message is recommended in order to be sent or received.
Data Consistency Information	Verifies the consistency of the Se protocol message.
SLM Service ID	Identifies an SLM service and a unique value should be set for each service by ERCM.
Service Profile	Describes a service profile generated by ERCM for a service request.

Table 10-1 – Information components for reference point Si

Information component	Description
Connection Profile	Describes a connection that can be set up or has already been set up by ERM.
EventNotify	Allows ERM send notification to ERCM for event that may need ERCM take appropriate action.
Service Attribute Object	Describes the attributes associated with the service profile. It is a sub-object of the Service Profile Object.
Constraint Object	Describe the constraint imposed by a service. It is a sub-object of the Service Profile Object.
Connection Attribute Object	Describes the attributes associated with the transport connection. It is a sub-object of the Connection Profile Object.
Autonomic Management Profile	Describes overall network slice life-cycle autonomic management monitoring and provisioning policies.
Autonomic Management Attribute Object	Describes the attributes associated with overall network slice life-cycle autonomic management monitoring and provisioning policies.

10.2 Reference point Se

The Se reference point is required to enable request/response information needed for an IMT-2020 network slice instance communicating with external management entities to be exchanged between the external management entity support functional element (EMES) in the management and orchestration plane of the IMT-2020 network slice life-cycle management (SLM) and external management entities (MANO, OSS/BSS, etc.).

This reference point is extended to support autonomic management of the overall network slice life cycle in relationship with external management entities. The extension is described in this clause.

The Se reference point may operate as an inter-domain reference point.

10.2.1 Functional requirements

10.2.1.1 Communication of a slice life-cycle management and orchestration plane with external management entities functional requirements

The Se reference point provides the ability to make requests/responses between the EMES in the SLM and external management entities for;

– network slice management interworking and orchestration including autonomic management capabilities;

– a status report of interworking and orchestration requests including autonomic management capabilities.

10.2.1.2 Communication of a slice life-cycle management and orchestration plane with external management entities session processing functional requirements

To assure the reliability and performance of communication of a slice life-cycle management and orchestration plane with external management entities session operations across Se reference point, the following capabilities are required:

– **Overload control**: The Se reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the EMES and external management entities.

– **Synchronization and audit**: The Se reference point is required to support the capability on synchronization and audit of the communication of a slice instance with the external management entities session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Se reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

10.2.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Se reference point.

– **Request-response transactions**: The reference point is required to allow the EMES to request a transaction to be performed by the external management entity and get a response (that can be correlated with the request) in return and vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: EMES and external management entities.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting communication of a slice instance with external management entities functions.

– **Security**: The Se is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: an EMES is required to be able to communicate with multiple external management entities; 2) many-to-one mode: multiple EMES are required to be able to make requests to a given external management entity.

10.2.3 Information components

The information components exchanged across the Se reference point are categorized as follows:

Table 10-2 – Information components for reference point Se

Information component	Description
User Identifier	A unique identifier for different instances of the IMT-2020 slice life-cycle management and orchestration plane within the same administrative domain of a single requester
Authentication Information	Authenticates the peers (i.e., IMT-2020 slice life-cycle management and orchestration plane and external management system).

Table 10-2 – Information components for reference point Se

Information component	Description
Management Interworking Profile Identifier	A unique management interworking profile identifier required for an exchange of management information between EMES and external management entity.
Management Interworking Profile	Describes management interworking profile information required for an exchange of management information including autonomic management information between EMES and external management entity.
EventNotify	Allows IMT-20202 management plane to send notification to the external management entities for an event that may need external management entities to take appropriate actions.

10.3 Reference point Is

The Is reference point is required to enable request/response information needed for an IMT-2020 network slice application and service plane management to be exchanged between the ASP-S of the application and service plane management (ASPM) in the SI and application and service plane management support (ASPM-S) of the IMT-2020 applications and service plane (IASP) in the SI.

This reference point is extended to support autonomic management of the network slice instance application and service plane. The extension is described in this clause.

The Is reference point may operate as an intra-domain and/or inter-domain reference point.

10.3.1 Functional requirements

10.3.1.1 Network slice application and service plane management functional requirements

The Is reference point provides the ability to make requests/responses between the ASP-S in the ASPM and the ASPM-S in the IASP for;

– network slice application and service plane management including autonomic management capabilities;

– a status report of slice application and service plane management actions including autonomic management actions.

10.3.1.2 Network slice application and service plane management session processing functional requirements

To assure the reliability and performance of network slice application and service plane management session operations across the Is reference point, the following capabilities are required:

– **Overload control**: The Is reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the ASP-S in the ASPM and the ASPM-S in the IASP.

– **Synchronization and audit**: The Is reference point is required to support the on synchronization and audit of the network slice application and service plane management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Is reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

10.3.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Is reference point.

– **Request-response transactions**: The reference point is required to allow the ASP-S in the ASPM to request a transaction to be performed by the ASPM-S in the IASP and get a response (that can be correlated with the request) in return and vice versa.
– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: ASP-S and ASPM-S.
– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.
– **Capabilities**: Each entity is required to be able to determine the capabilities of the appropriate corresponding instance when requesting network slice application and service plane management functions.
– **Security**: The Is is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.
– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: an ASP-S is required to be able to communicate with multiple ASPM-S; 2) many-to-one mode: multiple ASP-S are required to be able to make requests to a given ASPM-S in the IASP.

10.3.3 Information components

The information components exchanged across the Is reference point are categorized as follows:

Table 10-3 – Information components for reference point Is

Information component	Description
User Identifier	A unique identifier for different instances of the application and service plane management (ASPM) within the same administrative domain of a single requester
Management Operation Request Session Identifier	An identifier for the session for which the management operation requests are sent to the application and service plane. The identifier has to be unique within the same application and service plane instance.
Globally Unique IP Address Information (Optional)	A set of IP address information used for locating the network in which the ASP-S is requesting the management operations.
Unique IP address	The IP address for identifying ASP-S
Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID)
Management Operation Requester Identifier	An identifier for the requester (i.e., the owner of ASP-S in ASPM) of application and service plane management service. It is unique over the requesters sending requests for the ASPM.
Management Operation Request Priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by application and service plane management based on the priority level.
ASP Autonomic Management Operation Profile	Describes the policies related to autonomic management monitoring and provisioning of network slice instance application and service plane.
ASP Autonomic Management Operation Attribute Object	Describes attributes associated with the policies of the autonomic management monitoring and provisioning of the network slice instance application and service plane.

Table 10-3 – Information components for reference point Is

Information component	Description
Management Operation Request Result	Indication of the result for a management operation request (includes both synchronous and scheduled request result)
EventNotify	Allows application and service plane to send notifications to ASP-S for events that may need to take appropriate action for requested management operations.

10.4 Reference point Ic

The Ic reference point is required to enable request/response information needed for an IMT-2020 network slice control plane management to be exchanged between the CP-S of Control Plane Management (CPM) in the SI and Control Plane Management Support (CPM-S) of the IMT-2020 Control Plane (ICP) in the SI.

This reference point is extended to support autonomic management of the network slice instance control plane. The extension is described in this clause.

The Ic reference point may operate as an intra-domain and/or inter-domain reference point.

10.4.1 Functional requirements

10.4.1.1 Network slice control plane management functional requirements

The Ic reference point provides the ability to make requests/responses between the CP-S in the CPM and the control plane management support (CPM-S) in the ICP for:

– network slice control plane management including autonomic management capabilities;

– a status report of slice control plane management actions including autonomic management actions.

10.4.1.2 Network slice control plane management session processing functional requirements

To assure the reliability and performance of network slice control plane management session operations across the Ic reference point, the following capabilities are required:

– **Overload control**: The Ic reference point is required to support the on overload control for preventing the overflow of information messages exchanged between the CP-S and the CPM-S in the ICP.

– **Synchronization and audit**: The Is reference point is required to support the capability on synchronization and audit of the network slice control plane management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Ic reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

10.4.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Ic reference point.

– **Request-response transactions**: The reference point is required to allow the CP-S to request a transaction to be performed by the CPM-S in the ICP and get a response (that can be correlated with the request) in return and vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: CP-S and CPM-S.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting network slice control plane management functions.

– **Security**: The Ic is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: a CP-S is required to be able to communicate with multiple CPM-S in the ICP; 2) many-to-one mode: multiple CP-S are required to be able to make requests to a given CPM-S in the ICP.

10.4.3 Information components

The information components exchanged across the Ic reference point are categorized as follows:

Table 10-4 – Information components for reference point Ic

Information component	Description
User Identifier	A unique identifier for different instances of the control plane management (CPM) within the same administrative domain of a single requester
Management Operation Request Session Identifier	An identifier for the session for which the management operation requests are sent to the control plane. The identifier has to be unique within the same control plane instance.
Globally Unique IP Address Information (Optional)	A set of IP address information used for locating the network in which the CP-S is requesting the management operations
Unique IP address	The IP address for identifying CP-S
Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID)
Management Operation Requester Identifier	An identifier for the requester (i.e., the owner of CP-S in CPM) of control plane management service. It is unique over the requesters sending requests for the CPM.
Management Operation Request Priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by control plane management based on the priority level.
CP Autonomic Management Operation Profile	Describes the policies related to autonomic management monitoring and provisioning of network slice instance control plane.
CP Autonomic Management Operation Attribute Object	Describes attributes associated with the policies of the autonomic management monitoring and provisioning of the network slice instance control plane.
Management Operation Request Result	Indication of the result for a management operation request (includes both synchronous and scheduled request result)
EventNotify	Allows control plane to send notifications to the CP-S for events that may need to take appropriate action for requested management operations.

10.5 Reference point Id

The Id reference point is required to enable request/response information needed for an IMT-2020 network slice physical and virtual data plane management to be exchanged between the DP-S of the

data plane management (DPM) in the SI and data plane management support (DPM-S) of the IMT-2020 data plane (IDP) in the SI.

This reference point is extended to support autonomic management of the network slice instance physical and virtual data planes. The extension is described in this clause.

The Id reference point may operate as an intra-domain and/or inter-domain reference point.

10.5.1 Functional requirements

10.5.1.1 Network slice data plane management functional requirements

The Id reference point provides the ability to make requests/responses between the DP-S in the DPM and the DPM-S for a status report of slice data plane management actions including autonomic management actions.

10.5.1.2 Network slice data plane management session processing functional requirements

To assure the reliability and performance of network slice data plane management session operations across the Id reference point, the following capabilities are required:

– **Overload control**: The Id reference point is required to support the capability on overload control for preventing the overflow of information messages exchanged between the DP-S and DPM-S of the IDP in the SI.

– **Synchronization and audit**: The Id reference point is required to support the capability on synchronization and audit of the network slice data plane management session status in support of recovery and operational information statistics and auditing.

– **Session state maintenance**: The Id reference point is required to support the capability on maintaining the session state using either soft-state or hard-state approaches.

10.5.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Id reference point.

– **Request-response transactions**: The reference point is required to allow the DP-S to request a transaction to be performed by the DPM-S in the IDP and get a response (that can be correlated with the request) in return and also vice versa.

– **Notifications**: The reference point is required to support the notification of asynchronous events between two entities: DP-S and DPM-S.

– **Reliable delivery**: The reference point is required to provide reliable delivery of messages.

– **Capabilities**: Each entity is required to be able to determine the capabilities of an appropriate corresponding instance when requesting network slice data plane management functions.

– **Security**: The Id is required to support the authentication between two entities so that requests from unauthenticated sources will not be performed and each entity can verify the source of notifications sent.

– **One-to-many/many-to-one**: Two modes are required to be supported: 1) one-to-many mode: a DP-S is required to be able to communicate with multiple DPM-S in the IDP; 2) many-to-one mode: multiple DP-S are required to be able to make requests to a given DPM-S in the IDP.

10.5.3 Information components

The information components exchanged across the Id reference point are categorized as follows:

Table 10-5 – Information components for reference point Id

Information component	Description
User Identifier	A unique identifier for different instances of the data plane management (DPM) within the same administrative domain of a single requester
Management Operation Request Session Identifier	An identifier for the session for which the management operation requests are sent to the data plane. The identifier has to be unique within the same data plane instance.
Globally Unique IP Address Information (Optional)	A set of IP address information used for locating the network in which the DP-S is requesting the management operations
Unique IP address	The IP address for identifying DP-S
Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID)
Management Operation Requester Identifier	An identifier for the requester (i.e., the owner of DP-S in DPM) of data plane management service. It is unique over the requesters sending requests for the DPM.
Management Operation Request Priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by data plane management based on the priority level.
DP Autonomic Management Operation Profile	Describes the policies related to autonomic management monitoring and provisioning of network slice instance data plane.
DP Autonomic Management Operation Attribute Object	Describes attributes associated with the policies of the autonomic management monitoring and provisioning of the network slice instance data plane.
Management Operation Request Result	Indication of the result for a management operation request (includes both synchronous and scheduled request result)
EventNotify	Allows data plane to send notifications to DP-S for events that may need to take appropriate action for requested management operations.

11 Security consideration

This clause describes security threats and potential attacks and defines security requirements for autonomic management and control of IMT-2020 networks (AMC). The security requirements are based on [ITU-T Y.2701]. These considerations are relevant only insofar as the reference points in AMC are concerned.

The type of generic threats and their applicability to AMC are as follows:

– **Destruction of information**: This threat refers to the deletion of information pertaining to AMC operations, such as transaction state information, resource usage information, accounting information, topology information or policy rules. An example of potential consequences is that when the information about the existence (or availability) of a particular resource has been destroyed, the resource effectively becomes unavailable.

– **Corruption or modification of information**: This threat has three aspects:

1) corruption of the recorded resource information (or policy rules) so that such data is rendered meaningless or unusable;
2) undetected modification of the recorded resource information or policy rules so that such data appears to be meaningful. This can result in theft of service, degradation of service, loss of service, or fraudulent accounting, or any combination of the above;
3) corruption or modification of a signalling message, with the same results as the above.

– **Theft, removal or loss of information**: This threat refers to the theft or loss of recorded resource information. It may result in 1) violation of a subscriber's privacy (in case of theft of subscriber information), 2) theft of service and 3) degradation, interruption and, ultimately, unavailability of service (in case of the loss of information).
– **Disclosure of information**: This can take place because of the interception of the signalling messages or because of granting access to an illegitimate user. The consequence is the same as in the case of theft, removal or loss of information.
– **Interruption of services**: This threat is typically realized through a denial of service (DoS) attack. Such attacks can make the AMC partially or totally unavailable.

The major security requirements for AMC are:

1) taking the above security threats into account and supporting measures to counter relevant attacks;
2) protection of the signalling exchange in support of resource requests and responses;
3) protection of the information contained in all AMC entities involved in this exchange;
4) ensuring the availability and overall expected performance of the AMC;
5) prevention of illegitimate access to the AMC.

Appendix I

Use case of realizing IMT-2020 AMC architecture through GANA reference model

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

This appendix describes a realization use case of IMT-2020 AMC architecture through the ETSI Generic Autonomic Network Architecture (GANA) reference model.

Figure I.1 below is a snapshot of the ETSI GANA model. In the ETSI GANA model, the component (software logic) that drives autonomics at a particular level of abstraction for self-management functionality is called a decision-making element (DE) and is described in depth in [b-ETSI TS 103 195-2]. The question of what types of DEs should be introduced in certain network elements (NEs), depending on the managed entities (MEs) that the NEs support and also points of their attachment to the network topology, and in the outer area of management and control systems, is answered by a process called GANA instantiation onto target implementation-oriented reference network architectures and their associated management and control architectures (e.g., architecture scenarios in which the GANA model has been instantiated including [b-ETSI TR 103 404] and [b-ETSI TR 103 473]). [b-ETSI WP 16] and [b- ETSI TS 103 195-2] provide an implementation guide for making GANA instantiation onto particular target implementation-oriented reference network architectures and their associated management and control architectures.

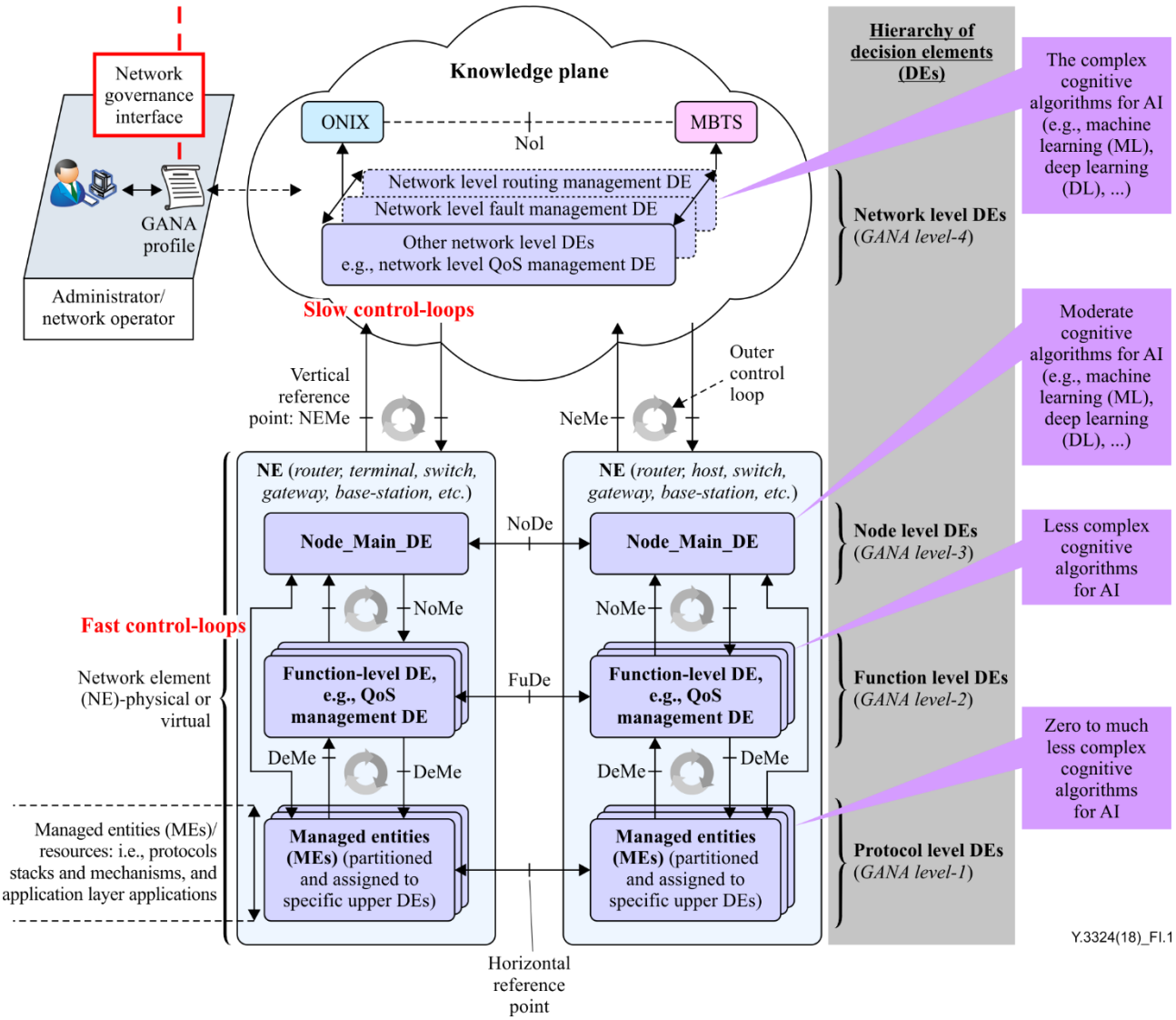

Figure I.1 – Snapshot of the GANA reference model and autonomics cognitive algorithms for artificial intelligence (AI) (Source [b-ETSI PoC Demo-2])

As part of the network automation trend, AMC is now being addressed by a number of standards development organizations and fora. For example, the AMC concepts for autonomic service assurance and use cases presented in the recently published TeleManagement Forum (TMF)' ODA Functional Architecture Functional Architecture Framework (Intelligence Management Function Block) [b-TM Forum ODA] are also aligned to the ETSI GANA model's principles. Within the content of 5G, ETSI TC INT/AFI WG is now running a 5G PoC (Proof-of-Concept) on *"5G Network Slices Creation, Autonomic & Cognitive Management and E2E Orchestration; with Closed-Loop (Autonomic) Service Assurance for Network Slices; using the Smart Insurance IoT Use Case"* [b-ETSI PoC Demo-2], [b-ETSI PoC Smart insurance], with the aim of operationalizing the GANA framework towards industrial deployments, as the 5G PoC is centred on the role of the GANA components in autonomic management and control (AMC) operations in 5G. Readers are encouraged to follow the developments, progression and the results (demo reports (e.g., Demo-2 Report) and more detailed material in form of slides) of the ETSI 5G PoC that are accessible at [b-ETSI PoC Smart insurance], and there are plans for more demos as part of Demo series planned for the overall PoC in the timeframe 2018/2019 and beyond).

I.2 Realization use case of IMT-2020 AMC through ETSI GANA reference model

Figure I.2 serves to illustrate how the high-level AMC architecture for IMT-2020 network slice life-cycle management can be integrated with the GANA functional blocks for AMC.

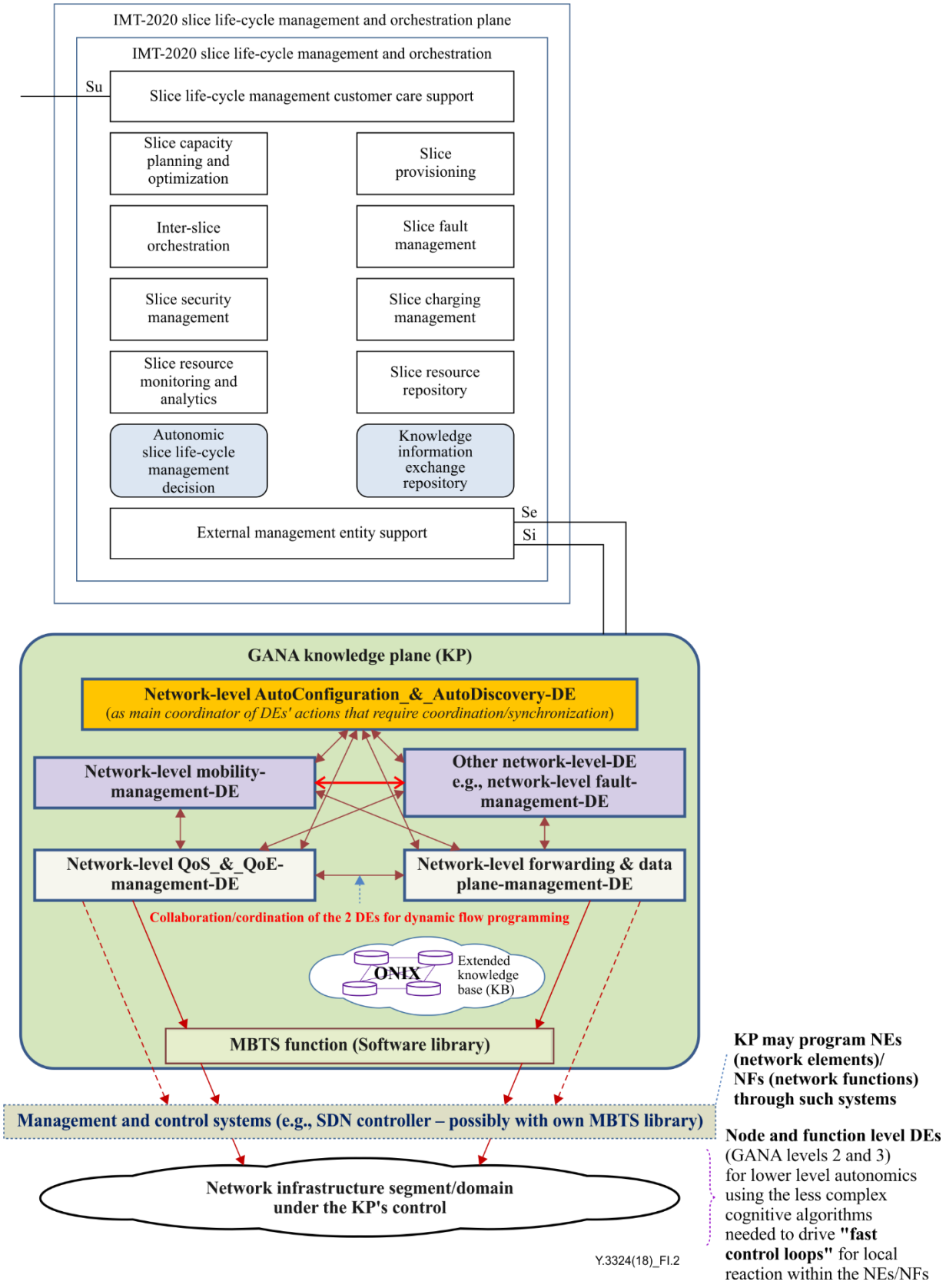

Figure I.2 – Illustration of how high-level AMC architecture for IMT-2020 network slice life-cycle management can be integrated with GANA functional blocks

The key GANA functional blocks of focus in these mappings are the GANA knowledge plane (KP) so-called network-level-DEs, the overlay network for information exchange (ONIX) is a distributed scalable overlay system of federated information servers), and model-based translation service (MBTS) software library, which is an intermediation layer between the GANA KP DEs and the NEs (physical or virtual). [b-ETSI WP 16] and [b- ETSI TS 103 195-2] define and describe the roles of these GANA functional blocks. [b-ETSI TS 103 195-2] defines various types of KP DEs and other lower level DEs that can be implemented at specific GANA abstraction levels for self-management functionality, accordingly.

NOTE – A knowledge plane instance's scope of responsibility can be a network segment such as an access network or fronthaul/backhaul or a domain.

The "Autonomic Slice Lifecycle Management Decision" block in the high-level AMC architecture for IMT-2020 network slice life-cycle management may need to interface with the GANA knowledge plane (KP) or be part of the KP's processes, in cases where the KP is required to participate in such "Autonomic Slice Lifecycle Management Decision". The "Knowledge Information Exchange Repository" can be viewed as one of ONIX's federated information servers.

The slice life-cycle management blocks in the high-level AMC architecture for IMT-2020 network slice life-cycle management, e.g., the slice security management, slice fault-management, can be implemented as integral management and control intelligence of a GANA knowledge plane and the federation of multiple knowledge planes to cover multiple network segments/domains. This is because, as being demonstrated in the ETSI 5G PoC on "*5G Network Slices Creation, Autonomic & Cognitive Management and E2E Orchestration; with Closed-Loop (Autonomic) Service Assurance for Network Slices; using the Smart Insurance IoT Use Case*"][b-ETSI PoC Demo-2], [b-ETSI PoC Smart insurance], GANA knowledge planes for specific network segments/domains and also the end-to-end federations of multiple GANA knowledge planes for various network segments/domains, should play roles in autonomic and cognitive management and E2E orchestration of slices and in E2E autonomic service assurance for network slices.

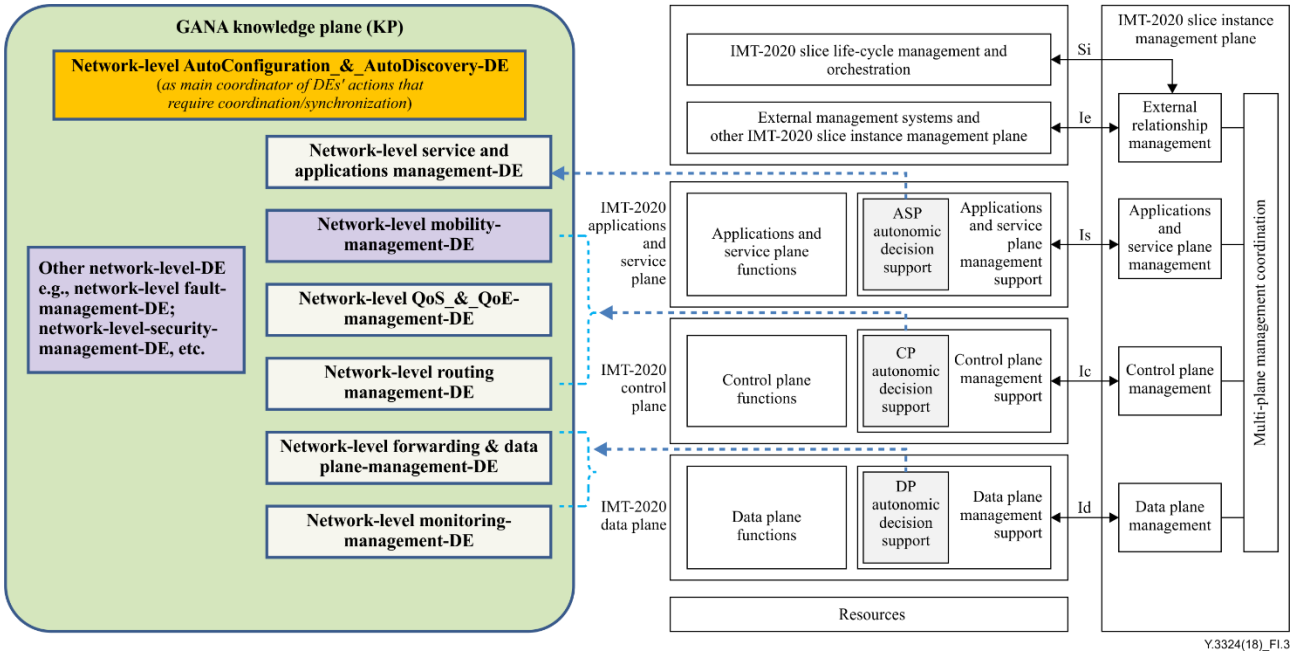

Figure I.3 – Illustrating the types of GANA DEs that can provide for autonomic decision support in applications and service plane management, control plane management and data plane management

Figure I.3 serves to point to examples of DEs that can provide for decision support required for each of the planes indicated. ThoseKP DEs are complemented by their "mirror-DEs" implemented at lower level autonomics layer (i.e., within NEs or NFs and the KP DEs shall policy-control their lower level "mirror-DEs" introduced in NEs/NFs. For example, a Network-Level-Security-Management-DE is "mirrored" by a Node-Level Security Management-DE.

NOTE – External management systems (in the AMC architecture for IMT-2020) include knowledge planes for each network segment or domain and their interworking with other management and control systems such as OSS/BSS, SDN controllers, orchestrators, etc.

A complete mapping of which DEs could provide for decision support can be derived from ETS [b-ETSI TS 103 195-2] and this applies to both cases of logically centralized control planes, as well as for distributed control planes implemented within NEs i.e., the traditional case of control planes that are coupled with the data plane within the NEs.

Bibliography

[b-ETSI PoC Demo-2] ETSI (2018), *5G Network Slicing PoC Demo-2 Datasheet of the ETSI 5G PoC on 5G Network Slices Creation, Autonomic & Cognitive Management & E2E Orchestration with Closed-Loop (Autonomic) Service Assurance for the IoT (Smart Insurance). Use Case:* <https://intwiki.etsi.org/images/ETSI_5G_PoC_Implementation_Case_for_GANA_Conformant_Autonomic_Service_Assurance_Demo-2_Paris_February2018_V0.06_datasheet.pdf>

[b-ETSI PoC Smart insurance] *ETSI 5G PoC on 5G Network Slices Creation, Autonomic & Cognitive Management & E2E Orchestration with Closed-Loop (Autonomic) Service Assurance for the IoT (Smart Insurance). Use Case:* <https://ntechwiki.etsi.org/index.php?title=Accepted_PoC_proposals>

[b-ETSI TR 103 404] ETSI TR 103 404 v.1.1.1 (2016), *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.*

[b-ETSI TR 103 473] ETSI TR 103 473 V1.1.2 (2018), *Evolution of management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures.*

[b-ETSI TS 103 195-2] ETSI TS 103 195-2 (2018), *Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management*. <https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=50970>

[b-ETSI WP 16] ETSI White Paper no. 16 (2016), The *Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services.* <http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp16_gana_Ed1_20161011.pdf >

[b-TM Forum ODA] TM Forum's Open Digital Architecture (ODA): *IG1167 ODA Functional Architecture Vision R18.0.0 (Intelligence Management Function Block).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019