

# Recommendation

## **ITU-T X.1010 (05/2025)**

SERIES X: Data networks, open system communications  
and security

Information and network security – Security orchestration  
and service access

---

**Guidelines for the security orchestration of the  
service access process**



ITU-T X-SERIES RECOMMENDATIONS

**Data networks, open system communications and security**

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
<b>Security orchestration and service access</b>	<b>X.1000-X.1011</b>
Security architecture and capabilities	X.1012-X.1029
Network security	X.1030-X.1049
Security management	X.1050-X.1079
Telebiometrics	X.1080-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

# Recommendation ITU-T X.1010

## Guidelines for the security orchestration of the service access process

### Summary

Security requirements on one service access process need to be met based on security capabilities with the support of network capabilities. The existence of multidomain introduces different security requirements of different domains and interdomain access control security requirements in the service access process, which are variable and diverse. Therefore, the distributed, complex and diverse security protections of the network need to be orchestrated in coordination with network routing in order to protect the service access process.

Network operators need to have the ability to orchestrate security capabilities and network capabilities to provide such a secure network to protect the service access process. This new work item describes the orchestration framework to help all stakeholders build, integrate, interact and manage a secure service access process in a secure and low-cost way.

### History\*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1010	2025-05-29	17	11.1002/1000/16380

### Keywords

Orchestration, security.

---

\* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <https://www.itu.int/ITU-T/ipr/>.

© ITU 2025

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions .....	1
	3.1 Terms defined elsewhere .....	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms .....	1
5	Conventions .....	2
6	Challenges for building service access process .....	2
7	Security requirements of service access process .....	2
8	Functional framework for security orchestration of service access process.....	3
	8.1 Overview of the reference framework.....	3
	8.2 Component capabilities .....	4
9	Procedures for security orchestration of service access process .....	6
	9.1 Registration and operational status monitoring process for functional modules.....	6
	9.2 Process for distributing network and security policies.....	7
	9.3 Process for execution of policies .....	8
10	Stakeholders involved in the functional framework for security orchestration of the service access process.....	11
	10.1 Overview .....	11
	10.2 User.....	11
	10.3 Security function provider .....	11
	10.4 Network function provider .....	11
	10.5 System integrator.....	12
11	The implementation modes of functional framework for security orchestration of the service access process .....	12
	11.1 Implementation mode based on multiple security providers.....	12
	11.2 Multi-network providers based implementation mode.....	12
	11.3 Multiple security and multiple network providers based implementation mode .....	13
Annex A – Extension of functional framework for security orchestration of service access process with other technologies.....		14
	A.1 Advanced user requirements collection framework based on the intent- driven approach .....	14
	A.2 Advanced policy execution framework based on playbook.....	16
	A.3 Advanced policy optimization framework based on data analysis techniques .....	17
	A.4 Mixing multiple advanced frameworks.....	17
Bibliography.....		20



# Recommendation ITU-T X.1010

## Guidelines for the security orchestration of the service access process

### 1 Scope

This Recommendation provides guidelines for the orchestration of security capabilities and network capabilities to provide a secure network and protect the service access process. This Recommendation covers the following:

- Challenges for building service access process mainly due to the mega-trend of multi-domain; and
- Guidelines for an orchestrating system which can be used to provide a secure service access process based on orchestrating security capabilities and network capabilities, including functional framework and procedure.

### 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.

None.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 domain** [b-ITU-T Y.3090]: A collection of physical or functional entities which are owned and operated by a player and can include entities from more than one role. The extent of a domain is defined by a useful context and one player can have more than one domain.

**3.1.2 intent** [b-3GPP 28.312]: Expectations including requirements, goals and constraints given to a 3GPP system, without specifying how to achieve them.

#### 3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

**3.2.1 security and network function processing sequence**: An ordered processing sequence consisting of network function modules and security function modules, with specific function processing sequences consisting of unique identifiers for the network function modules and the security function modules.

### 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CACAO Collaborative Automated Course of Action Operations

CPE Customer Premises Equipment

IDE	Integrated Development Environment
IP	Internet Protocol
PoP	Point of Presence
UI	User Interface

## 5 Conventions

In this Recommendation:

The keyword "shall" indicates a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keyword "should" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

## 6 Challenges for building service access process

Accessing corporate resources from various locations over public or insecure networks exposes the business to security threats and data leakage, highlighting the need for better security measures to protect remote entities and corporate resources.

Furthermore, the trend of hosting and accessing business applications, data and services on cloud platforms has made network traffic flow more complex and diverse, no longer centralized in enterprise data centres but distributed across various locations and cloud services. This trend increases the frequency of connectivity and interaction between internal enterprise networks and external network environments and also complicates network security monitoring and management. Traditional boundary security devices are unable to fully meet the protection requirements, which necessitates more diverse security services and collaborative orchestration of security and networking capabilities. A comprehensive and unified security and network architecture is required to handle the distributed traffic and provide consistent security policies.

Besides, widely distributed physical branches result in high network and security costs. Routing all business traffic through a centralized data centre leads to latency and bottlenecks, while deploying individual security protection devices for each branch incurs high costs in purchasing, configuration, maintenance and personnel. The widespread deployment and maintenance of multiple security devices can introduce inconsistency and conflicts in security services, increasing operational and maintenance costs.

## 7 Security requirements of service access process

To address the aforementioned challenges for the service access process, the following requirements are necessary:

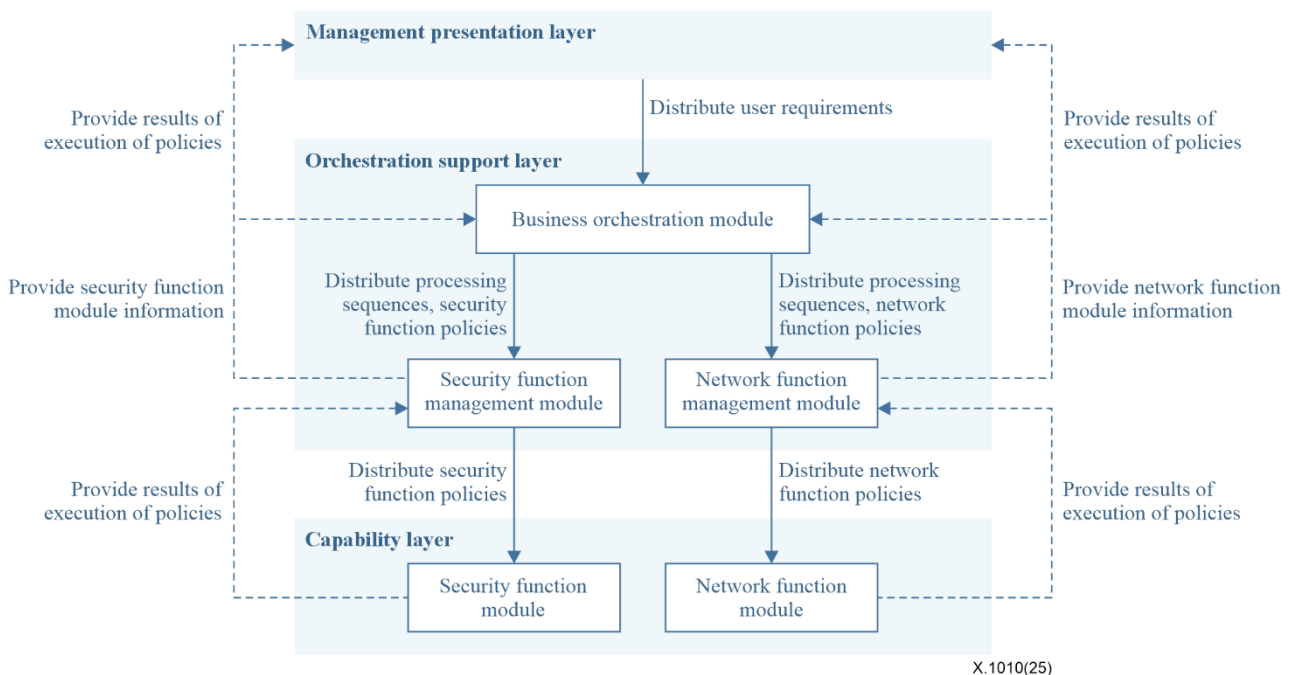
- a) Safeguarding the entire user access process:  
Security measures shall be implemented at every node throughout the entire access process, including user terminals, routing nodes and target resource sites. These security measures should be connected, integrated and programmed to protect every connection during the access process. This would deter any unauthorized entry or attack and ensure that all transmitted data is confidential and maintain its integrity.
- b) Distributed deployment of network and security functions:  
The network and security infrastructure should be deployed across multiple geographical locations, as well as different nodes. Consequently, these distributed components would be flexibly and efficiently composed and synchronized.

- c) **Orchestration of network and security in an integrated manner:**  
The network and security operations should be coordinated within an integrated architecture, ensuring consistent and synchronized function. Consequently, this would enhance efficiency, simplify management and guarantee stable and dependable network and security policies.
- d) **Centralized management and enforcement of network policies and security policies:**  
The network and security operations can be managed, configured and distributed centrally.
- e) **Compatibility with networking and security functions from multiple vendors:**  
Network devices, security devices and solutions from multiple vendors are interoperable and compatible with each other. This can improve flexibility, interoperability, minimize expense and simplify management.

## 8 Functional framework for security orchestration of service access process

### 8.1 Overview of the reference framework

This Recommendation proposes a reference framework for the orchestration of security and network capabilities to safeguard the service access process. The reference framework is shown in Figure 1.



**Figure 1 – Reference framework of the service access process**

The framework consists of three components: a management presentation layer, an orchestration support layer and a capability layer. The orchestration support layer includes business orchestration modules, security and network function management modules. The capability layer includes security and network function modules. The overview of each level and the modules it contains are as follows:

- a) **Management presentation layer:** Collect and issue user policies to the orchestration support layer.

- b) **Orchestration support layer:** integrate security and network functions, analyse and transform user policies, and select applicable network and security function modules to construct network and security function processing sequences. This includes three modules:
- Business orchestration module: analyse user policies and formulate security and network function processing sequences, security function policies and network function policies.
  - Security function management module: manage security function modules, negotiate resources, transform and issues security function policies, and provide feedback on module status and policy execution results.
  - Network function management module: manage network function modules, negotiate resources, implements security and network function processing sequences, transform and issue network function policies, and provide feedback on module status and policy execution results.
- c) **Capability layer:** Provide network and security functions. It includes two different types of modules:
- Security function modules: execute security function policies; can be deployed physically, virtually or in the cloud at point of presence (PoP), customer premise equipment (CPE), gateways, user terminals and the cloud.
  - Network function modules: execute network function policies and can be deployed physically, virtually or in the cloud at PoPs, CPE, gateways, user terminals and the cloud.

## 8.2 Component capabilities

### 8.2.1 Management presentation layer

The management presentation layer is responsible for gathering user policies through interfaces or configuration files and then sending them to the orchestration support layer for execution. User policies describe the network and security requirements that users expect to achieve and contain both traffic-based and non-traffic-based policies.

- Traffic-based user policies: contain information such as source and destination addresses, business types, resource negotiation interfaces, network and security service quality requirements and access control conditions. The policy's objective is traffic, and its processing behaviour includes traffic content awareness, filtering, access control, forwarding and acceleration, such as filtering traffic for a specified five-tuple.
- Non-traffic-based user policies: contain information such as target asset addresses, resource negotiation interfaces, security service quality requirements, execution cycle and time. The policy's objective is non-traffic objects such as resources, and its processing behaviour includes scanning, monitoring and authentication recognition of the target asset address device, such as vulnerability scanning for devices in a specific Internet protocol (IP) range.

### 8.2.2 Orchestration support layer

#### 8.2.2.1 Business orchestration module

The business orchestration module analyses user policies to select suitable network function modules and security function modules, develops security and network function processing sequences, security function policies and network function policies, and sends them to the security function management module and network function management module.

- Processing sequence development: Analyse user policies to select and arrange network and security function modules based on the security function module information and network function module information such as functional descriptions, operational status, functional sequence rules and network information such as network topology, network latency, and network traffic load balancing, and functional characteristics (such as proximity to user-side

and resource-side and requirements for computing power), to construct an ordered sequence of security and network function processing.

- Security policy development: According to user policies, develop security policies for security functions in the processing sequence.
- Network policy development: According to user policies, develop network policies for network functions in the processing sequence.

#### **8.2.2.2 Security function management module**

The security function management module manages security function modules, provides information on security function modules, converts and issues security function policies, and reports on the operational status of security function modules.

- Registration module: receive and aggregate registration information from security function modules.
- Monitoring status: monitor the operational status of security function modules.
- Resource negotiation: send resource negotiation requests to security function modules or their management systems, including but not limited to resource application and release.
- Policy issuance: convert security function policies into specific security function module policies recognizable by selected security function modules, and issues policies.
- Information provision: analyse registration information, logs, alarms and operational status of security function modules to provide all managed security function module information to both business orchestration modules and management presentation layers. Security function module information can be retrieved by functional description, unique identifier and name.
- Status reporting: collect information on security function operational status, policy execution results, logs and alarms, and report them to the management presentation layer.

#### **8.2.2.3 Network function management module**

The network function management module manages network function modules, provides information on network function modules, converts and issues network function policies, implements security and network function processing sequences, accesses orchestration and reports on the operational status of network function modules.

- Registration module: receive and aggregate registration information from network function modules.
- Monitoring status: monitor the operational status of network function modules.
- Resource negotiation: send resource negotiation requests to network function modules or their management systems, including but not limited to resource application and release.
- Policy issuance: convert network function policies into specific network function module policies recognizable by selected network function modules, and issue policies.
- Information provision: analyse registration information, logs, alarms, and operational status of network function modules to provide all managed network function module information to both business orchestration modules and management presentation layers. Network function module information can be retrieved by functional description, unique identifier and name.
- Execution of processing sequence: issue the corresponding network forwarding policies to the network function modules, when the execution of the security and network function processing sequence requires network forwarding cooperation.
- Status reporting: collect information on network function operational status, policy execution results, logs and alarms, and report them to the management presentation layer.

## **8.2.3 Capability layer**

### **8.2.3.1 Security function modules**

The security function module registers with the security function management module, executes security function module policies, provides feedback on policy execution results, logs and alarms, and reports operational status information. The security function modules are divided into traffic-based security function modules (to process user traffic) and non-traffic-based security function modules (to process non-traffic objects such as assets) based on their processing objects.

- Registration: register descriptive information about its function, unique identifier, name, address, calling interface, resource negotiation interface, deployment type, etc. to the security function management module.
- Execution of policies: receive and execute security function module policies.
- Feedback on results, logs and alarms: provide feedback on the execution results, logs and alarms of security function module policies in a unified format.
- Status reporting: report operational status to the security function management module through a unified interface.

### **8.2.3.2 Network function modules**

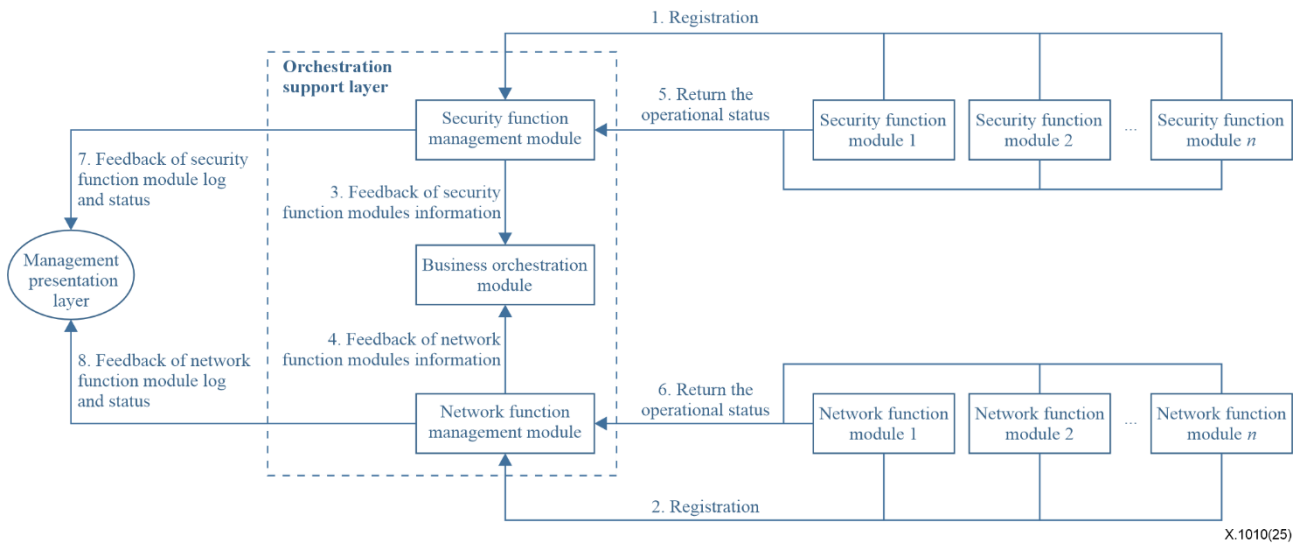
The network function module executes the network function module policies, provides feedback on execution results, logs and alarms, registers modules and regularly reports operational status.

- Registration: register descriptive information about its function, unique identifier, name, address, calling interface, resource negotiation interface, deployment type, etc. to the network function management module.
- Execution policy: receive and execute network function module policies.
- Feedback on results, logs and alarms: provide feedback on the execution results, logs and alarms of the network function module policies in a unified format.
- Status reporting: report operational status to the network function management module through a unified interface.

## **9 Procedures for security orchestration of service access process**

### **9.1 Registration and operational status monitoring process for functional modules**

The registration and operational status monitoring process for network and security function modules is shown in Figure 2.



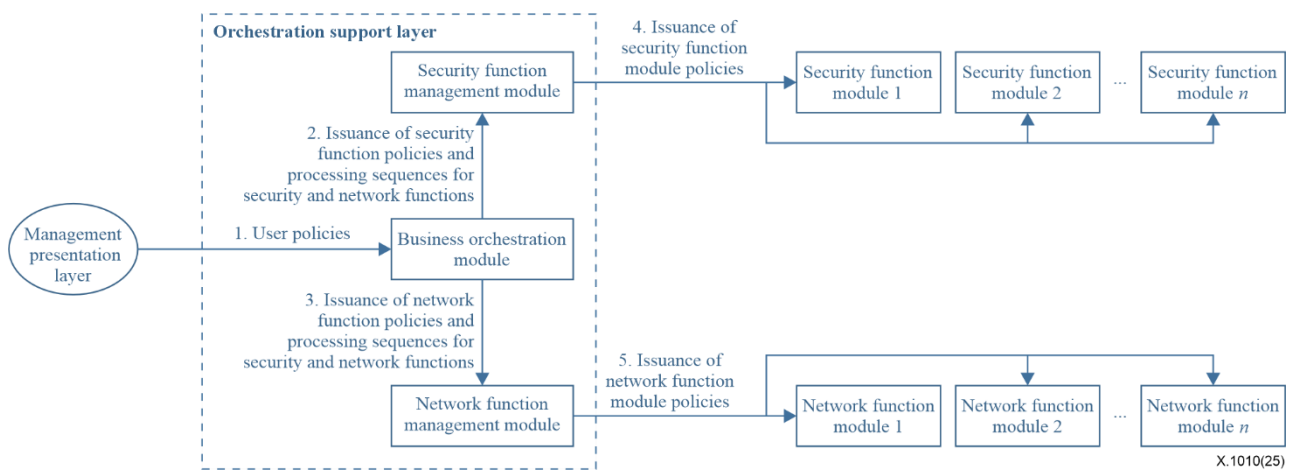
**Figure 2 – Registration and operational status monitoring process for network and security function modules**

The registration and operational status monitoring process for network and security function modules is as follows:

- 1) The security function modules submit the registration information and registers with the security function management module.
- 2) The network function modules submit the registration information and register with the network function management module.
- 3) The security function management module processes and stores the registration information of the security function modules and provides security function module information to the business orchestration module.
- 4) The network function management module processes and stores the registration information of the network function modules and provides network function module information to the business orchestration module.
- 5) The security function module returns the operational status, logs and alarms.
- 6) The network function module returns the operational status, logs and alarms.
- 7) The security function management module monitors the operational status of the security function module, aggregates logs and alarms, updates and provides the security function module information to the management presentation layer.
- 8) The network function management module monitors the operational status of the network function module, aggregates logs and alarms, updates and provides the security function module information to the management presentation layer.

## 9.2 Process for distributing network and security policies

The process of distributing network and security policies is shown in Figure 3.



**Figure 3 – Network and security policies distributing process**

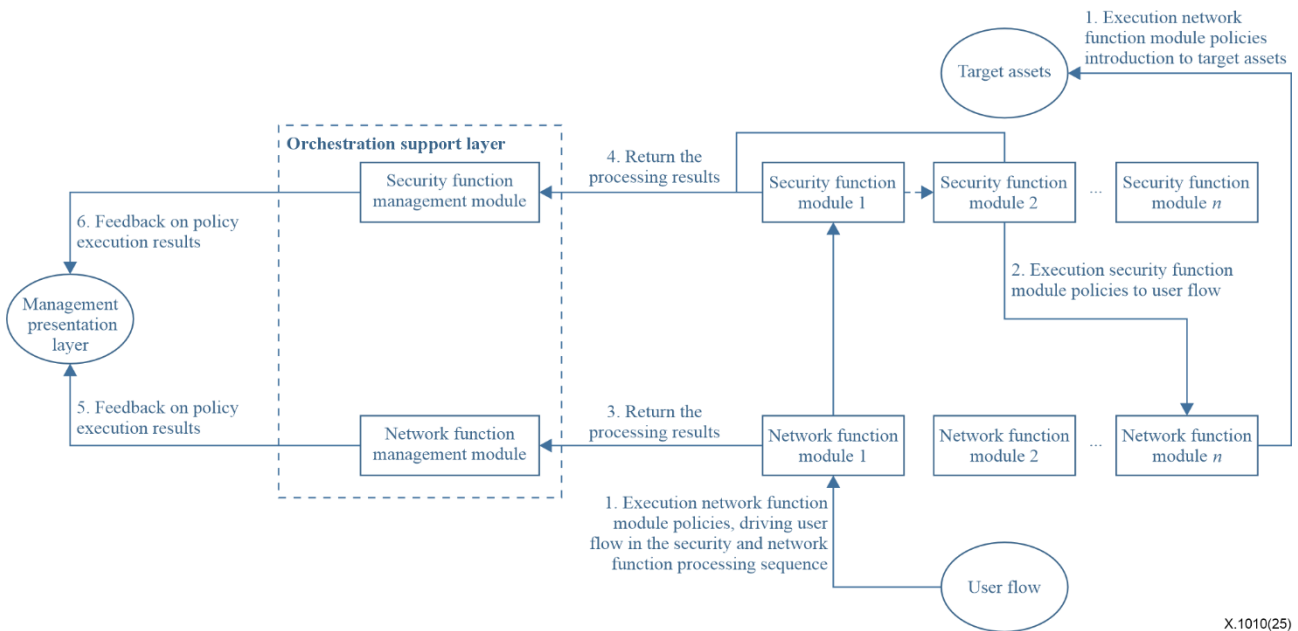
The process of distributing network and security policies is as follows:

- 1) The business orchestration module receives user policies from the management presentation layer. The business orchestration module filters the appropriate security function modules and network function modules by analysing the user policies and security function module information and network function module information such as functional descriptions, functional characteristics, functional sequence rules, operational status and network information such as network topology, network latency and network traffic load balancing. The business orchestration module sends resource negotiation requests to the security function modules and network function modules to be selected. Business orchestration selects the security function modules and network function modules based on the resource negotiation results to construct security and network function processing sequences.
- 2) The business orchestration module distributes the security and network function processing sequences and security function policies.
- 3) The business orchestration module distributes the security and network function processing sequences and network function policies.
- 4) The security function management module receives the security and network function processing sequences and security function policies, issues policies to the corresponding security function modules and implements user traffic secure processing.
- 5) The network function management module receives the security and network function processing sequences and network function policies, issues policies to the corresponding network function modules, implements user traffic forwarding scheduling and network optimization processing, and assists in implementing the security and network function processing sequence through traffic forwarding.

### 9.3 Process for execution of policies

#### 9.3.1 Process of the traffic-based security function module execution of policies

The execution process of the traffic-based security function module policies is shown in Figure 4.



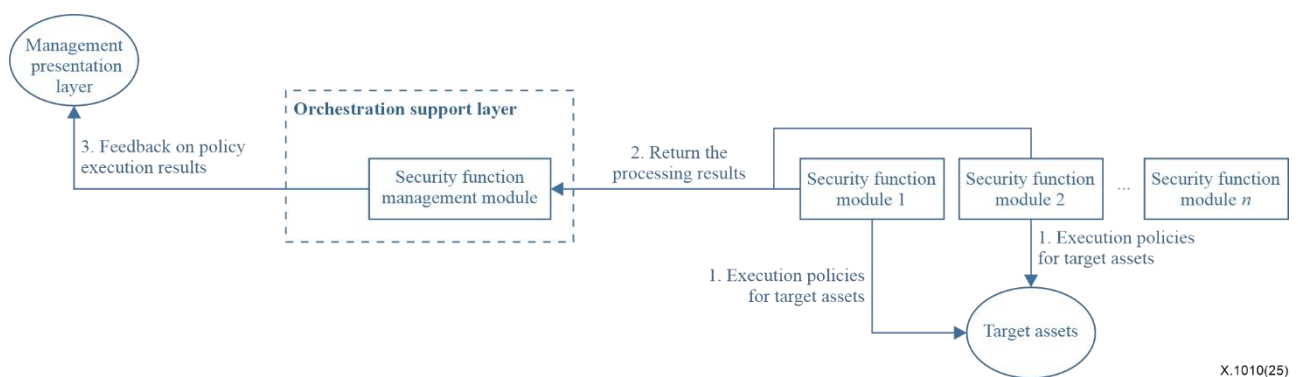
**Figure 4 – Process of the traffic-based security function module execution of policies**

The process of the traffic-based security function module execution of policies is as follows:

- 1) The network function modules execute the network function module policies, direct user traffic to the security and network function processing sequence and finally direct it to the target resource.
- 2) The security function modules execute the security function module policies, process the user traffic and forward the user traffic to the next function module in the security and network function processing sequence.
- 3) The network function modules return the processing result to the network function management module.
- 4) The security function modules return the processing result to the security function management module.
- 5) The network function management module aggregates the processing results and feeds back to the management presentation layer.
- 6) The security function management module aggregates the processing results and feeds back to the management presentation layer.

### 9.3.2 Process of the non-traffic-based security function module execution of policies

The execution process of the non-traffic-based security function module policies is shown in Figure 5.

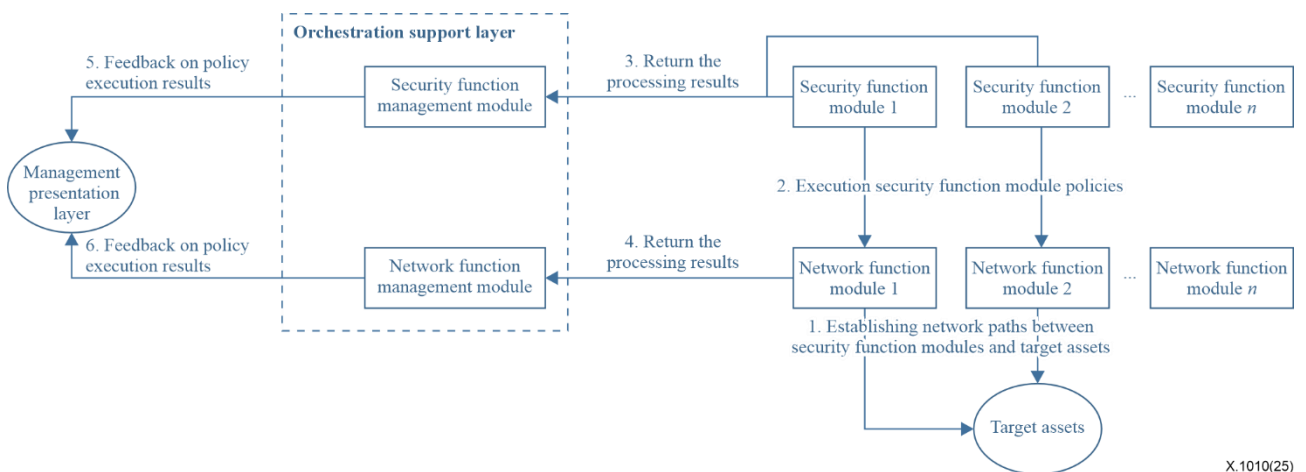


**Figure 5 – Process of the non-traffic-based security function module execution of policies**

When the non-traffic-based security function module is accessible from the target assets network, the process of the non-traffic-based security function module execution of policies is as follows:

- 1) The security function modules execute the security function module policies towards the target asset.
- 2) The security function modules return the policy processing results to the security function management module.
- 3) The security function management module aggregates the policy processing results and feeds back to the management presentation layer.

When the non-traffic-based security function module is not accessible from the target assets network, a network path can be established between the non-traffic-based security function module and the target assets through the network function module. The execution of policies process is shown in Figure 6.



X.1010(25)

**Figure 6 – Process of the non-traffic-based security function module execution of policies**

When the non-traffic-based security function module is not accessible from the target assets network, the process of the non-traffic-based security function module execution of policies is as follows:

- 1) The network function modules execute the policies to establish a network path between the security function module and the target assets.
- 2) The security function modules execute the policies on the target asset via the network path established by the network function module.
- 3) The network function modules return the results to the network function management module.
- 4) The security function modules return the results to the security function management module.
- 5) The network function management module aggregates the policy processing results and feeds back to the management presentation layer.
- 6) The security function management module aggregates the policy processing results and feeds back to the management presentation layer.

### 9.3.3 Process of the network function module execution of policies

The execution process of the network function policies is the same as the process of the network function module described in clause 9.3.1.

## **10 Stakeholders involved in the functional framework for security orchestration of the service access process**

### **10.1 Overview**

The functional framework for security orchestration of the service access process mainly involves the following stakeholders: Users, security function providers, network function providers and system integrators.

- 1) User: The user or operator of the functional framework for the security orchestration of the service access process who defines the user policies.
- 2) Security function provider: The vendor providing security functions, responsible for meeting specific security requirements.
- 3) Network function providers: The vendor providing network functions, responsible for meeting specific network requirements.
- 4) System integrator: The vendor that integrates network and security functions to build the functional framework for the security orchestration of the service access process.

### **10.2 User**

The user should formulate network and security policies through the management presentation layer, understand the results of the implementation of the network and security policies, and adjust subsequent policies based on the results.

### **10.3 Security function provider**

The security function provider should provide security function modules that implement the registration, resource negotiation, function invocation, result feedback and operation status feedback interfaces, and should also provide a security function management module that implements the module registration, status monitoring and reporting, policy issuance, resource negotiation and policy transformation interfaces.

### **10.4 Network function provider**

A network function provider should provide network function modules that implement the registration, resource negotiation, function invocation, result feedback and operation status feedback interfaces, and be compatible with the commonly used network policy format, and should also provide a network function management module that implement module registration, status monitoring and reporting, policy issuance, resource negotiation, execution processing sequence and policy transformation interfaces.

### **10.5 System integrator**

The system integrator should build the management presentation payer and the business orchestration module in the orchestration support layer to enforce user policies by managing and invoking network and security functions. Specifically, the system integrator should collect user policies via interfaces or configuration files and then send them to the orchestration support layer for execution, and connect network and security management modules from multiple vendors, analyse the required network and security functions according to user policies, retrieve security function module information and network function module information, select applicable network and security function modules, and construct security and network function processing sequences, security function policies and network function policies.

## 11 The implementation modes of functional framework for security orchestration of the service access process

### 11.1 Implementation mode based on multiple security providers

When the security function modules under the functional framework for security orchestration of service access process come from multiple security providers, the orchestration support layer should support multiple security function management modules from multiple security providers. The multiple security function management modules should aggregate the security function modules' information from their respective providers to the business orchestration module. The implementation framework is illustrated in Figure 7.

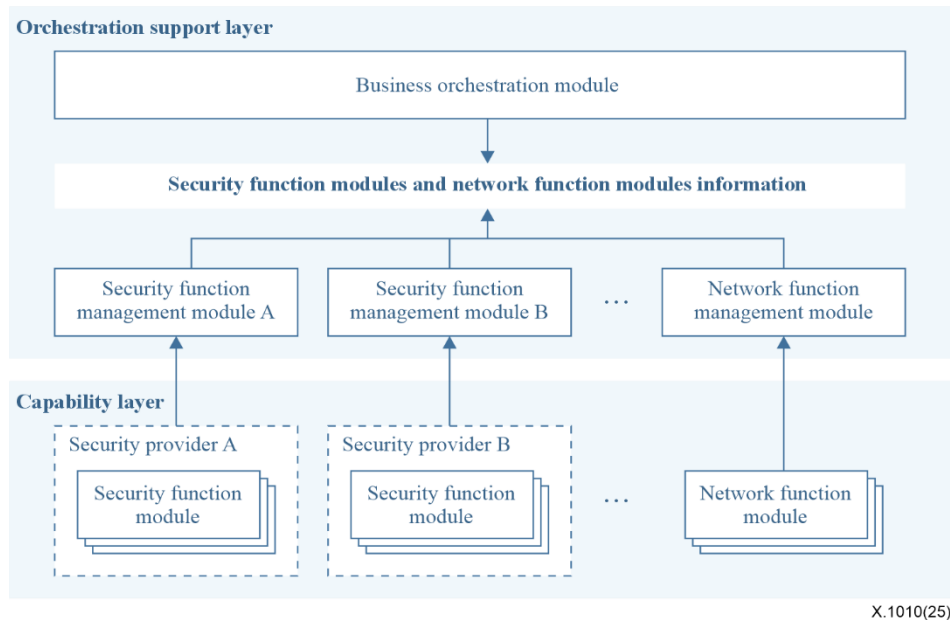
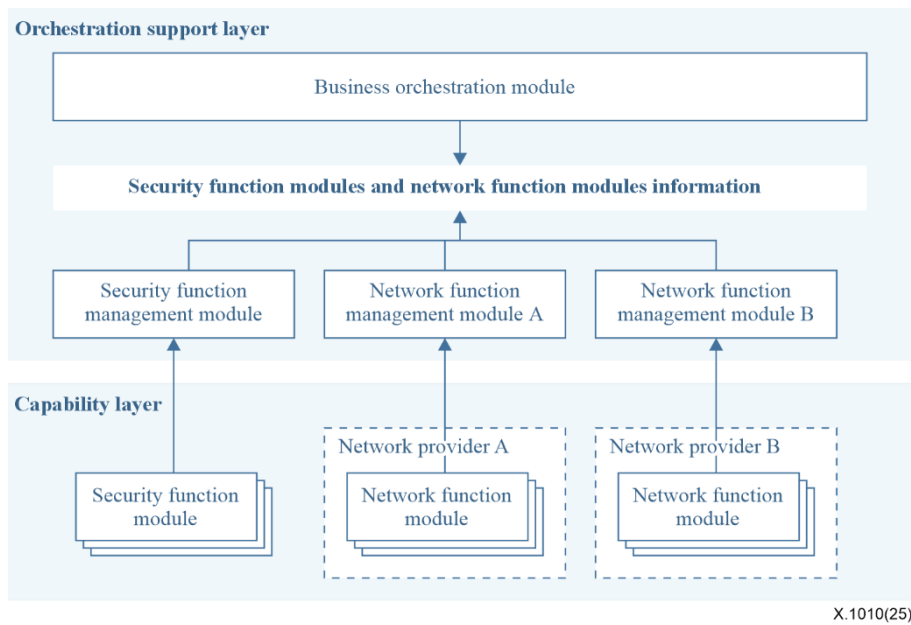


Figure 7 – Multi-security providers-based implementation framework

### 11.2 Multi-network providers based implementation mode

When the network function modules under the functional framework for security orchestration of service access process come from multiple network providers, the orchestration support layer should support multiple network function management modules from multiple network providers. The multiple network function management modules will aggregate the network function modules' information from their respective network providers to the business orchestration module. The implementation framework is illustrated in Figure 8.



X.1010(25)

**Figure 8 – Multinetwork providers-based implementation framework**

### 11.3 Multiple security and multiple network providers-based implementation mode

When the security function modules and network function modules under the functional framework for security orchestration of service access process come from multiple providers, the orchestration support layer should support multiple network function management modules and multiple security function management modules from multiple providers. Multiple security function management modules and network function management modules consolidate the network function module information and security function module information from their respective providers to the business orchestration module. The implementation framework is a combination of Figure 7 and Figure 8.

## **Annex A**

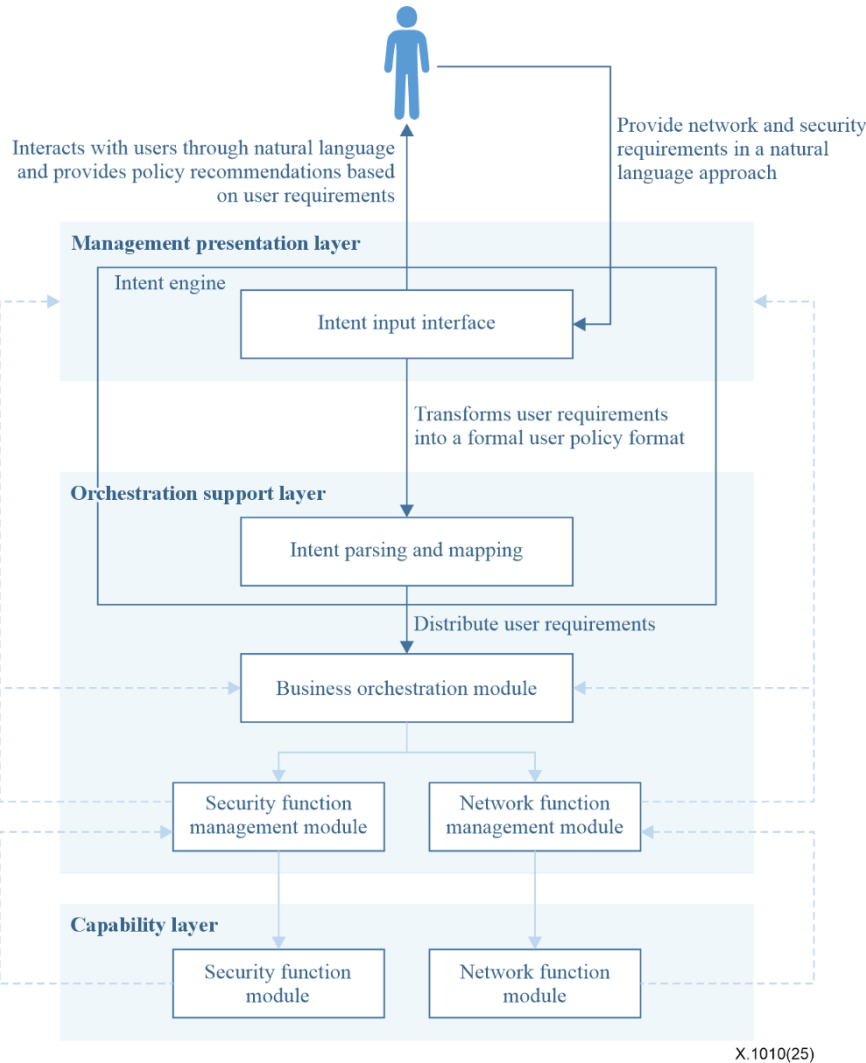
### **Extension of functional framework for security orchestration of service access process with other technologies**

(This annex forms an integral part of this Recommendation.)

This Recommendation builds a basic orchestration framework with extensibility. This framework can be integrated with other technologies to solve more complex security orchestration problems by adding additional functional modules from three aspects, user requirements collection, policy execution and policy optimization, to form an advanced framework.

#### **A.1 Advanced user requirements collection framework based on the intent-driven approach**

In the basic reference framework in the main text, users need to have a certain level of operational technical knowledge and experience in order to enter accurate user policies according to their own requirements and adapt subsequent policies according to the results of the policies. In order to reduce the cost of human interaction with the system, an intent engine can be added to the basic reference framework to acquire user requirements using natural language dialogue. The framework that combines the intent engine is shown in the following figure.

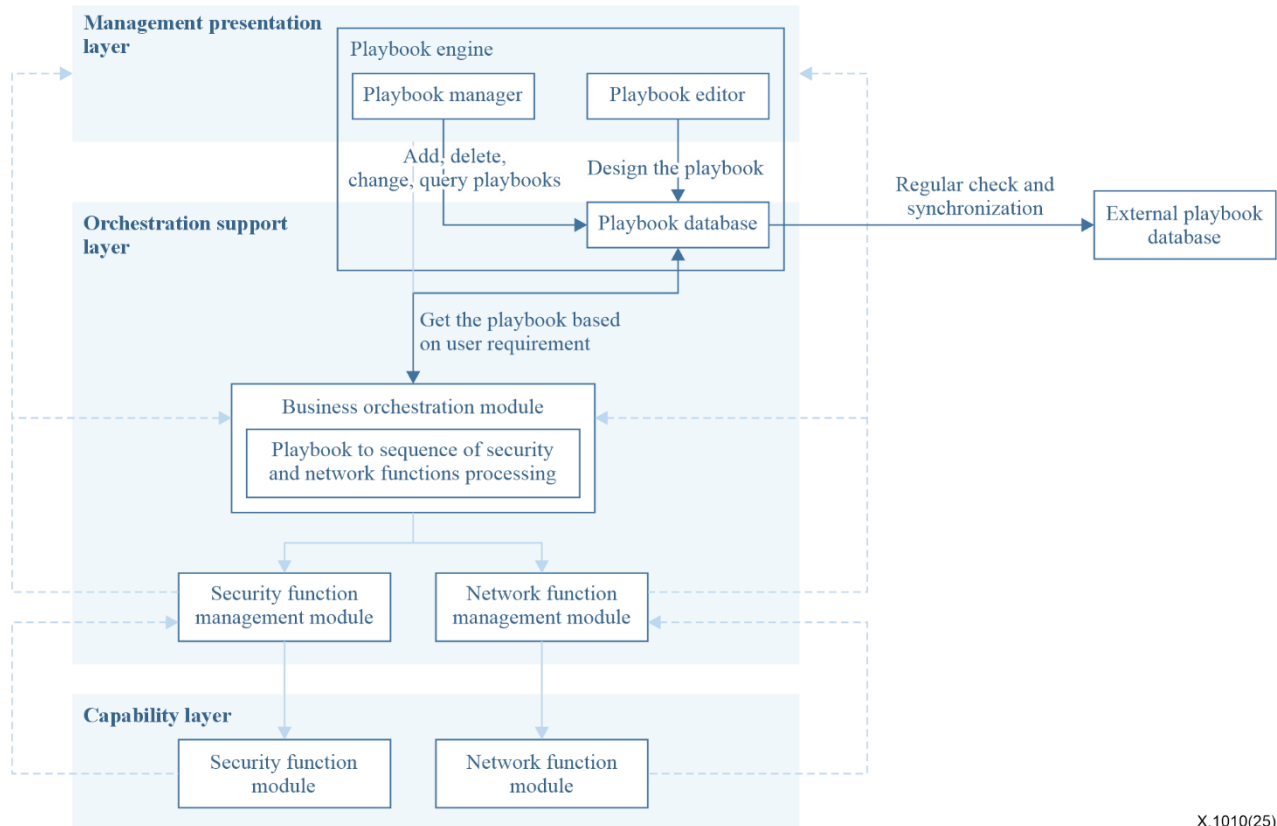


**Figure A.1 – Advanced user requirements collection framework based on the intent-driven approach**

- a) **Intent input interface:** Users enter their business intent using natural language (text or speech) or a graphical interface. Intents can be either simple commands or complex representations of business policies.
- b) **Intent parsing and mapping:**
  - Processes natural language input to extract keywords and phrases to understand the specific requirements of user intent. The structure and meaning of the input is decoded through syntactic analysis and semantic understanding.
  - Map parses user speech intent to a set of pre-defined security and network functions and policies. A domain knowledge base is used to map user intent to specific operations that the system can perform.
  - Check whether the parsed intent policies match the security and network business logic and present the parsed security and network policies to the user for final confirmation.
  - Send the mapped user policies to the orchestration support layer after user confirmation.

## A.2 Advanced policy execution framework based on playbook

In the basic reference framework in the main text, users have to re-execute their user policies each time, whereas there are usually fixed patterns in their business requirements. The security and network function processing sequences and functional policies generated based on the user requirements can be abstracted into pre-generated, tested and ready-to-use workflow templates, i.e., playbooks. To reduce the cost of use and orchestration, a playbook engine can be added to the base reference framework to automate policy enforcement.



X.1010(25)

**Figure A.2 – Advanced policy execution framework based on playbook**

- **Playbook editor:** A business-oriented, graphical integrated development environment (IDE) that provides users with a user interface (UI) to pre-program network and security features without programming and that can abstract the security and network function processing sequences according to the user requirements into playbooks.
- **Playbook manager:** Unified management of playbooks, including but not limited to basic operations such as adding, deleting, exiting and querying playbooks.
- **Playbook database:** A database that stores playbooks and their associated user requirements, and can periodically synchronize, certify and check subscribed third-party playbook content.
- **Business orchestration module:** Send user requirements to the playbook database to retrieve the playbooks that match the requirements, transform the playbooks into appropriate security and network function processing sequences, and issue network and security function policies.
- **External playbook database:** Based on the public playbook definition standards (collaborative automated course of action operations (CACAO), etc.), it stores the playbooks and the corresponding security and network requirements and threat descriptions. Playbooks can then be subscribed for specific tags on demand, and periodic updates are pushed to playbooks under the subscribed tags.

### A.3 Advanced policy optimization framework based on data analysis techniques

In the basic reference framework in the main text, data analysis of the business orchestration module aggregated policy execution results, logs, alarms and functional module operation status information can obtain the current operation status of the service access process and the possible threats.

To the basic reference framework, a security and network analysis module can be added to analyse potential network and security threats, provide threat alerts and processing recommendations to the management presentation layer, map urgent threats with deterministic solutions to appropriate network and security policies and send them to the business orchestration module for autonomous optimization of network security policies and automated threat processing.

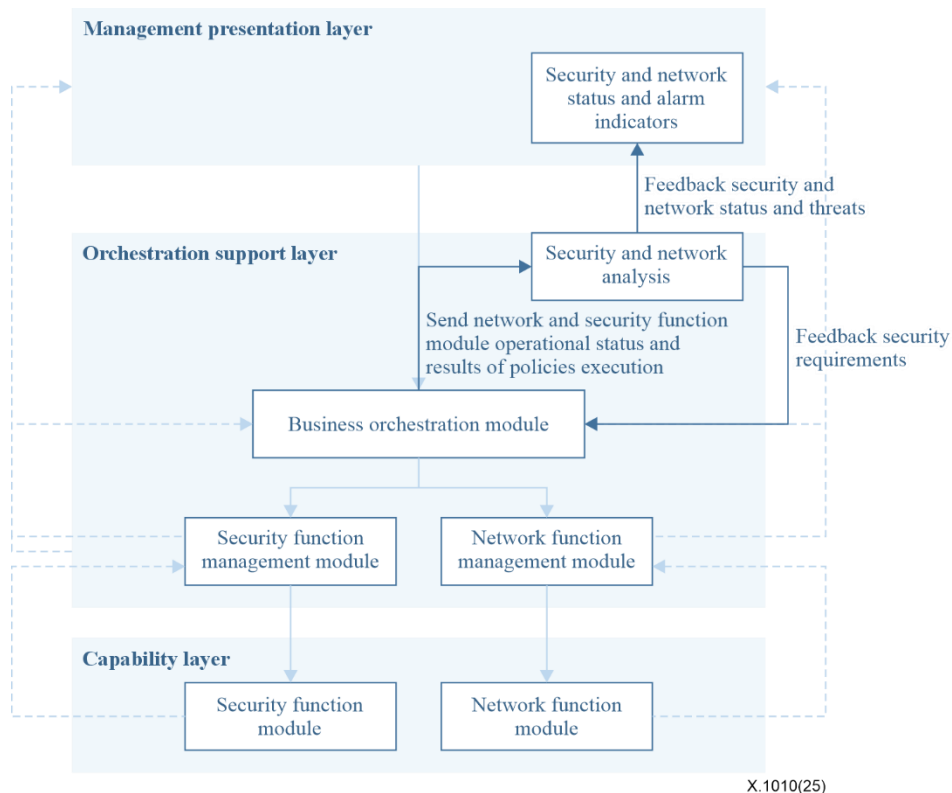
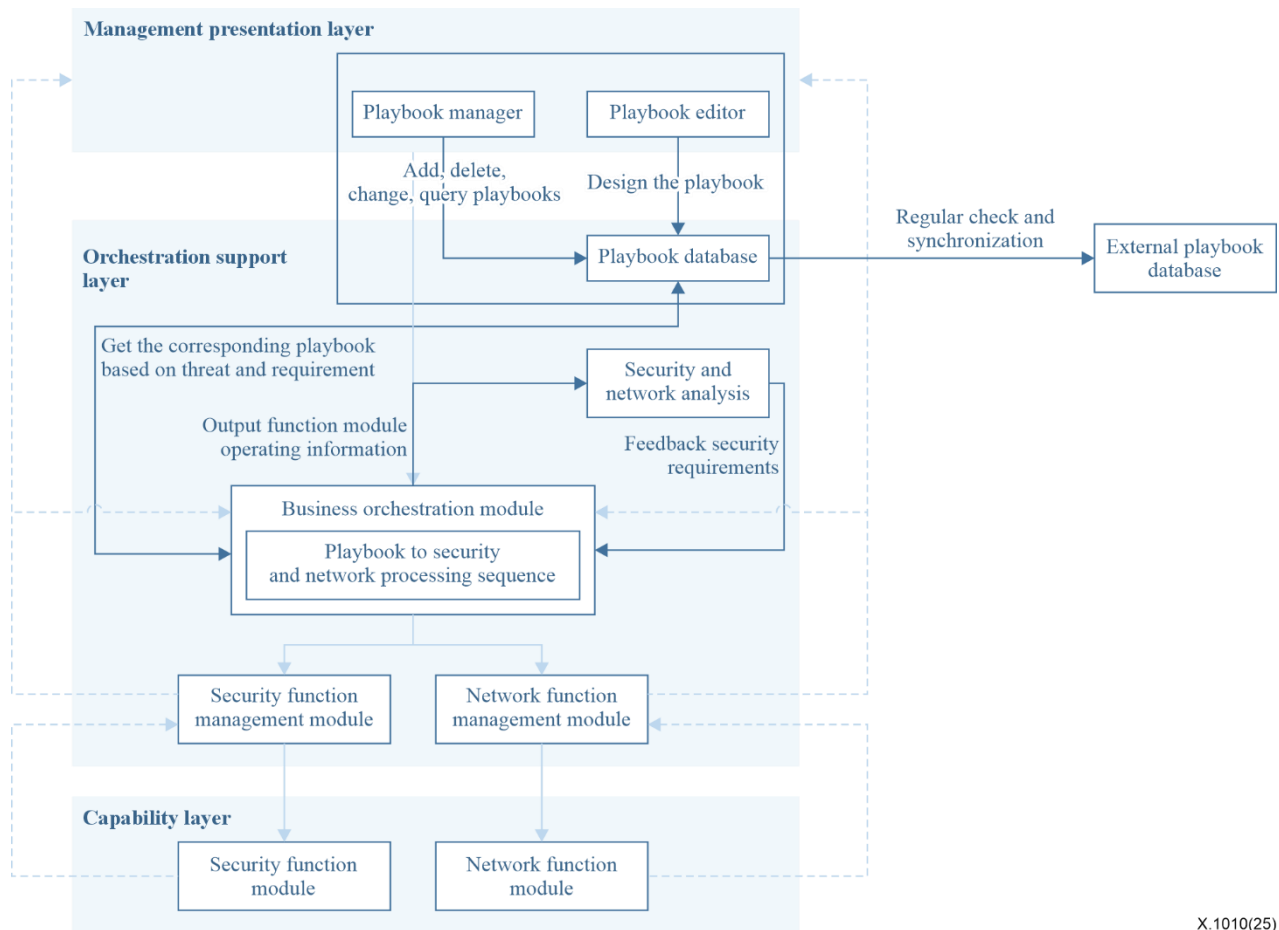


Figure A.3 – Advanced policy optimization framework based on data analysis techniques

- **Security and network analysis:** Based on information input from the business orchestration module, such as policy execution results, logs, alarms and function module operational status, analyse potential security threats, transform the security threats into security requirements and feed the security requirements back to the business orchestration module.
- **Security and network status and alert indicators:** Provide feedback to users on security and network posture and threat alerts.
- **Business orchestration module:** Aggregate policy enforcement results, logs, alerts and functional module status, feed them into security and network analysis and receive feedback on security requirements, and for those that are urgent and with definite measures, convert the requirements into and security and network function processing sequences, and issue the appropriate remediation policies.

### A.4 Mixing multiple advanced frameworks

Combining the playbook engine with data analytics enables a higher level of automated orchestration. The framework is shown in the following figure.



X.1010(25)

**Figure A.4 – Mixing multiple advanced frameworks**

- a) **Playbook editor:** The playbook editor has a business-oriented graphical IDE that provides users with a UI to pre-schedule network and security functions and trigger conditions without programming and can abstract the security and network function processing sequences according to user requirements or security threats into playbooks.
- b) **Playbook manager:** Same as that detailed in clause A.2, i.e., an advanced framework based on the playbook policy enforcement.
- c) **Playbook database:** A database that stores playbooks and the user requirements or security threats associated with them, and can periodically synchronize, certify and check subscribed third-party playbook content.
- d) **Security and network analysis:** Analyse possible security threats based on information such as policy execution results, logs, alarms and function module operating status received from the business orchestration module, and analyse possible attack behaviours and security risks, and transform security threats into security requirements and feed security requirements back to the business orchestration module.
- e) **Business orchestration module:**
  - Aggregate the policy execution results, logs, alarms and function module operating status and feed them into the security and network analysis. If a security threat exists, it receives its feedback on security requirements.
  - Send user requirements to the playbook database to retrieve the playbooks that match the requirements, convert the playbook into the appropriate security and network function processing sequence, and issue a network and security function policy.

- f) **External playbook database:** Based on the public playbook definition standards (CACAO, etc.), it stores the playbooks and the corresponding security and network requirements and threat descriptions. Playbooks can then be subscribed for specific tags on demand, and periodic updates are pushed to playbooks under the subscribed tags.

## Bibliography

- [[b-ITU-T Y.3090](#)] Recommendation ITU-T Y.3090 (2022), *Digital twin network – Requirements and architecture*.
- [b-3GPP 28.312] 3GPP TR (2022), *Management and orchestration; Intent driven management services for mobile networks (Release 18)*.  
<<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554>>



## 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
<b>Series X</b>	<b>Data networks, open system communications and security</b>
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