China Unicom TMF ANL Evaluaion (Core Network Fault Management)

November 2025

ANL Assessment - Core Network Fault Management Questionnaire (1/2)

Scenarios	Category	Capability or Task	Weight (Optional)	Questions	Option A	Option B	Option C	Option D
Core network fault management - maintenance	**Intent**	Intent	**0%**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**
	Awareness	Data collection Alarm correlation	10%	Does your system automatically collect data? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can automatically collect data (alarms, configuration data, and performance data etc.) and sort alarms. The data should be at the module level, including NF modules, cloud OS (VMs or pods), hardware (hosts and ports), detected KPIs indicating slight service damage (e.g., service KPI deterioration < 5%) and infrastructure-layer hardware data (servers, storage devices, EOR/TOR devices and IP core).	The system can automatically collect data (alarms, configuration data, and performance data), associate alarms, and sort alarms. The data should be at the NE level and cloud OS ((VMs or pods).	No. The system supports manual data collection.	
	Analysis	Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault management supports visualization of the following management capabilities in one view of NEs/NFs and the telecom cloud. 1. NE object (5GC NFs and EPC NEs) status (faulty or normal) visualization 2. NE health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud 4. Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information, vNIC information and rack information	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on alarms or KPIs. The system can identify and filter out redundant alarm notifications and related tickets based on pre-defined rules. Fault management supports visualization of the following management capabilities: 1. NE object (5GC NFs and EPC NEs) status (faulty or normal) visualization 2. NE health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud	No. The system supports manual fault detection based on the alarm notification and KPIs.	
		Risk prediction	10%	Does your system automatically detect and prevent risks of NE faults? Assessment object: management entities Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can use intelligent risk identification to recognize potential faults and automatically prevent faults. It can: 1. Prevent potential risks and analyze the risks involving capacity links, signaling storms, DR, and hardware. 2. Analyze the cause of risks and provide recommended actions automatically.	The system can use automatic risk identification, which requires manual confirmation, to recognize potential faults and prevent faults. It can: 1. Prevent potential risks and analyze the risks involving capacity and links.	The system can use risk identification to recognize potential faults and prevent faults by providing an automatic checklist which requires engineers to periodically confirm the potential risks in this checklist. It can: 1. Prevent potential risks and analyze the risks involving capacity.	No. The system does not support risk prediction.
		Demarcation	15%	Does your system support automatic demarcation of core network faults? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs and IMS NEs)	Yes. The intelligent system supports automatic fault demarcation without manual intervention (e.g., core network NEs and managed objects in telecom cloud) covering 95% or higher of live network faults. The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for NEs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation covering 80% or higher of faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for NEs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation and provides one or multiple analysis results to assist fault demarcation.	No. The system does not support automatic fault demarcation.

ANL Assessment - Core Network Fault Management Questionnaire (2/2)

Scenarios	Category	Capability or Task	Weight (Optional)	Questions	Option A	Option B	Option C	Option D
Core network fault management - maintenance	Analysis	Locating	15%	Does your system support automatic locating related to core network fault management? Assessment object: the core network management function and network function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs)	Yes. Intelligent fault diagnosis is capable of automatically providing precise locating (e.g., detailed causes of identified faults, including minimum units, software modules, and ports) of faults, covering 95% or higher of live network faults without human intervention. The average accuracy per month is above 90%.	Automatic fault diagnosis is capable of providing root causes of faults, and providing precise fault locating, covering 80% or higher faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%.	The system supports automatic fault locating and provides one or multiple analysis results to assist fault locating.	No. The system does not support automatic fault locating.
	Decision	Fault rectification solution generation	10%	Does your system automatically generate the fault rectification solution? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can generate the optimal rectification solution (minimum impact scope and time). Fault rectification can cover but not be limited to the following scenarios: 1. Generating an NF fault rectification solution automatically 2. Generating a solution to recover slight service losses 3. Providing a DR solution in case of accidents or natural disasters 4. System can generate optimization to network for failure (e.g., signaling storm, service outage etc.) automatically.	The system can generate a fault rectification solution (e.g., fault rectification scripts including operation objects and operation sequences). Fault rectification can cover the following scenarios: 1. Providing a DR solution in case of accidents or natural disasters. 2. System can generate optimization to network for failure (e.g., signaling storm, service outage etc.) automatically.	The system can generate fault rectification recommendations based on specialized checklist, to determine the rectification operations and operation objects based on rectification decision rules (configuration). Fault rectification can cover the following scenarios: 1. Providing a DR solution in case of accidents or natural disasters	No. The system supports fault rectification based on manual decisions.
		Solution pre-verification	10%	Does your system support rectification solution evaluation and verification to support decisions in core network? NOTE: Fault rectification solution can be evaluated before implementation by being verified in a simulation or sandbox environment. Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system supports intelligent rectification solution evaluation for the core network to verify the feasibility of rectification solution and provides the visualization results of accuracy effect before implementation. The evaluation tasks can cover but not be limited to the following scenarios: 1. Solution feasibility check and configuration verification 2. Emulation or simulation of rectification solution based on network digital twin The system supports the decision.	The system supports automatic rectification solution evaluation for core network, to verify the feasibility of rectification solution before implementation. The evaluation tasks can cover the following scenarios: 1. Solution feasibility check and configuration verification 2. DR rectification solution evaluation and verification The system supports the simulation results for manual decisions made for rectification solution.	The system provides a checklist for manual evaluation to verify the feasibility of rectification solution before implementation. The checklist includes but is not limited to: 1. NF healthy status check 2. Influence of rectification solution	No. The system verifies the rectification solution based on manual decisions.
	Execution	Solution implementation	10%	Does your system support automatic fault rectification? Assessment object: the core network management function and network element Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs).	Yes. The system can support automatic fault rectification in all fault rectification scenarios.	The system supports fault rectification after manual confirmation.		
		Service verification	10%	Does your system support automatic service verification after faults on core networks are rectified? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g. 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system automatically verifies whether network services are recovered and faults are rectified successfully.	The system automatically verifies that the alarms are cleared and KPI data is successfully recovered	No. The system does not support automatic service verification.	

Self-assessment Results

- The self-assessment score for the ANL evaluation of core network fault management is **3.82**. The intensive platform fault center, core network enhanced network management system, and core network fault handling agent provide four O&M capabilities: service prediction and prevention, event-level identification, automatic fault diagnosis, and intelligent disaster recovery support. The system supports intelligent identification and effective management of cloud-based core network faults, providing effective support for network O&M perception, analysis, decision-making, and execution.
- **Weaknesses and future improvement direction:** Solution pre-verification still depends on manual intervention. Intelligent O&M needs continuous evolution to achieve end-to-end automation.

Category	Capability or Task	Weight (Optional)	Questions	Answer	
				Equipment	Communication and Quality of service
				Infrustructure failure (If case of VNF, it is the failure occurs on the infrastructure harware resource that host the VNF)	Including failures of Transport link, user plane issues and control plane issues
Awareness	Data collection Alarm correlation	10%	Does your system automatically collect data? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A	A
Analysis	Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	A	A
	Risk prediction	10%	Does your system automatically detect and prevent risks of NE faults Assessment object: management entities Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A	A
	Demarcation	15%	Does your system support automatic demarcation of core network faults? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs and IMS NEs)	A	A
	Locating	15%	Does your system support automatic locating related to core network fault management? Assessment object: the core network management function and network function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A	A
Decision	Fault rectification solution generation	10%	Does your system automatically generate the fault rectification solution? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A	A
	Solution pre-verification	10%	Does your system support rectification solution evaluation and verification to support decisions in core network? NOTE: Fault rectification solution can be evaluated before implementation by being verified in a simulation or sandbox environment. Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	B	A
Execution	Solution implementation	10%	Does your system support automatic fault rectification? Assessment object: the core network management function and network element Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs).	A	A
	Service verification	10%	Does your system support automatic service verification after faults on core networks are rectified? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A	A

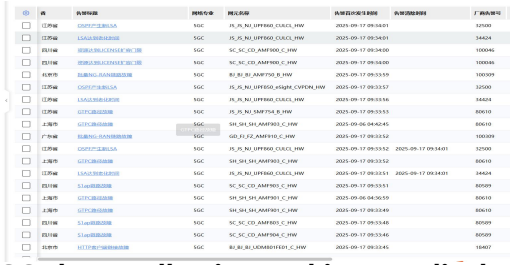
Question 1 Data Collection Alarm Correlation

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Data collection Alarm correlation	10%	Does your system automatically collect data? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can automatically collect data (alarms, configuration data, and performance data etc.) and sort alarms. The data should be at the module level, including NF modules cloud OS (VMs or pods), hardware (hosts and ports), detected KPIs indicating slight service damage (e.g., service KPI deterioration < 5%) and infrastructure-layer hardware data (servers, storage devices, EOR/TOR devices and IP core).	The system can automatically collect data (alarms, configuration data, and performance data), associate alarms, and sort alarms. The data should be at the NE level and cloud OS ((VMs or pods).	No. The system supports manual data collection.	

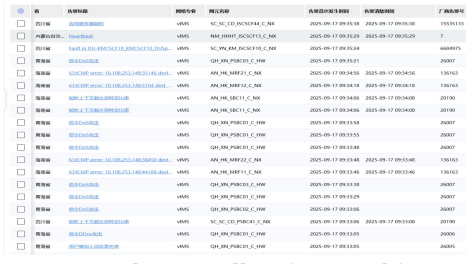
Evidence

Capability Introduction: The intelligent troubleshooting system can automatically collect alarm, performance, and resource configuration data of the core network 5GC and vIMS. The data is differentiated by module at different layers, including VNFs, VMs, hosts, switches, and routers. In addition, the system supports cross-layer alarm correlation analysis.
Self-assessed Capability: Option A

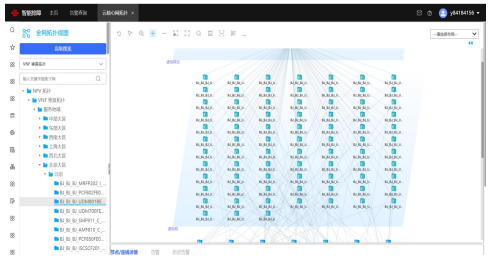
Sub Scenarios 1: Equipment



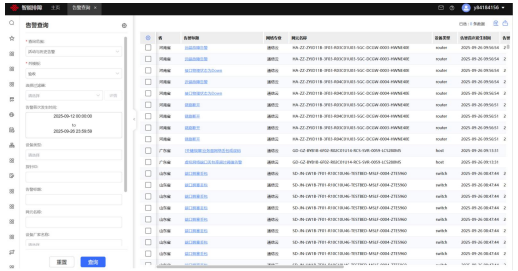
5GC alarm collection and import display



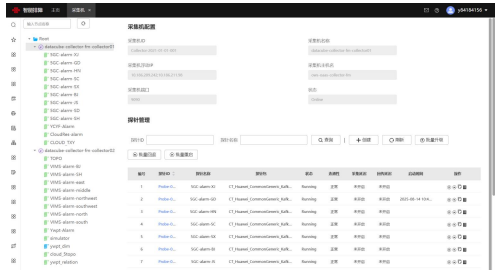
VIMS alarm collection and import



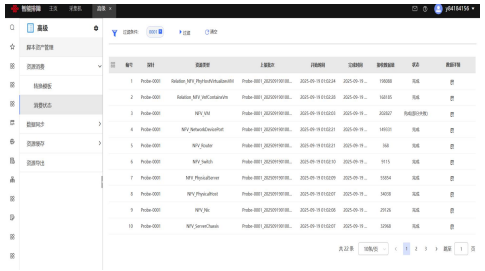
Resource Data



CloudOS data + IaaS hardware data



Data sorting for collector configuration



Importing NE resources to the database

Sub Scenarios 2: Communication and Quality of service

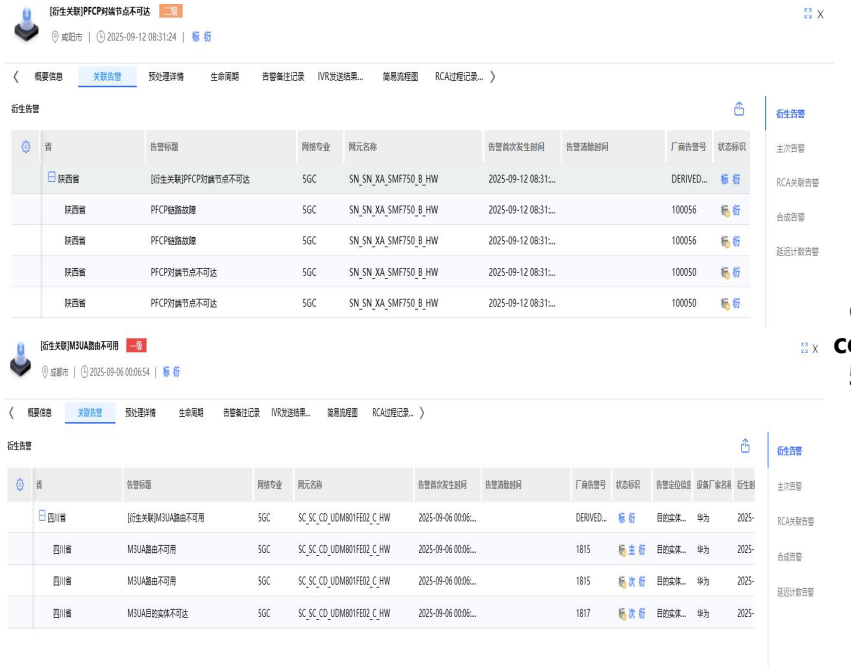
KPI deterioration data

Question 2 Fault Identification (1)

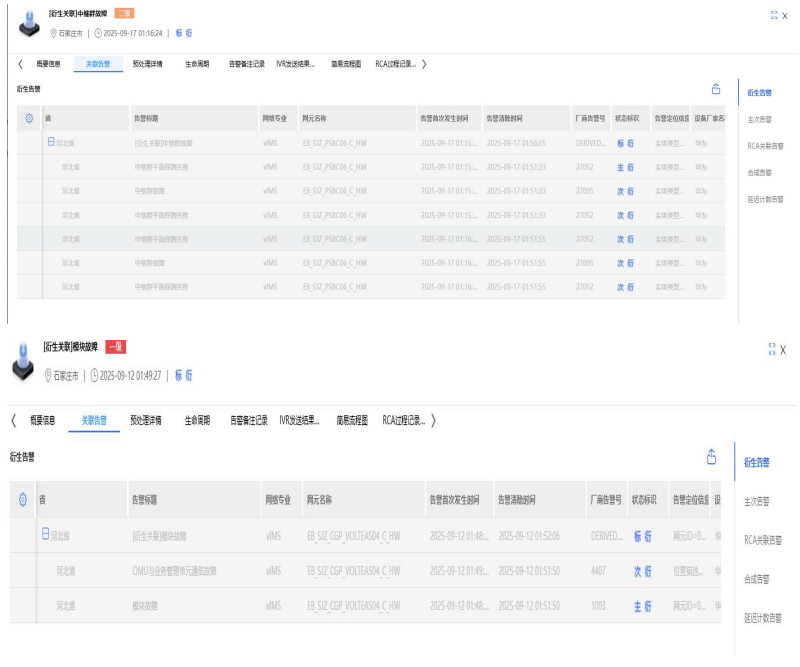
Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault management supports visualization of the following management capabilities in one view of NEs/NFs and the telecom cloud. 1. NE object (5GC NFs and EPC NEs) status (faulty or normal) visualization 2. NE health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud 4. Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information, vNIC information and rack information	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on alarms or KPIs. The system can identify and filter out redundant alarm notifications and related tickets based on pre-defined rules. Fault management supports visualization of the following management capabilities: 1. NE object (5GC NFs and EPC NEs) status (faulty or normal) visualization 2. NE health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud	No. The system supports manual fault detection based on the alarm notification and KPIs.	

Evidence

Capability Introduction: Correlative rules are triggered based on NE alarms. The details about correlative rules are displayed on the page. The system can correlate and compress 5GC/vIMS cross-layer alarms to identify typical cross-layer fault scenarios. In addition, the 5GC/vIMS provides five-layer topology visualization capabilities to display NE status in real time.
Self-assessed Capability: Option A



Cross-layer correlation of 5GC alarms



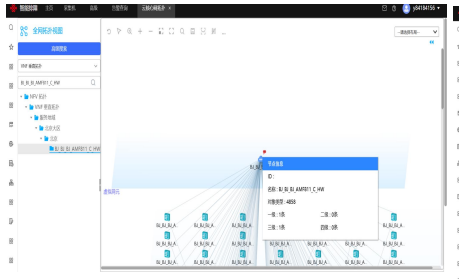
Cross-layer association of VIMS alarms

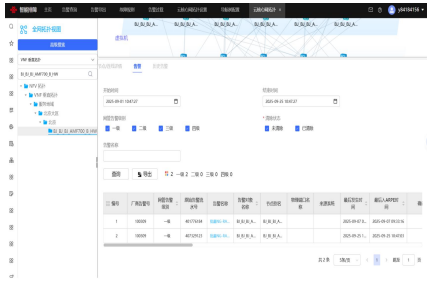
Question 2 Fault Identification (2)

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault management supports visualization of the following management capabilities in one view of NEs/NFs and the telecom cloud. 1. NE object (5GC NFs and EPC NEs) status (faulty or normal) visualization 2. NE health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud 4. Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information, vNIC information and rack information	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on alarms or KPIs. The system can identify and filter out redundant alarm notifications and related tickets based on pre-defined rules. Fault management supports visualization of the following management capabilities: 1. NE object (5GC NFs and EPC NEs) status (faulty or normal) visualization 2. NE health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud	No. The system supports manual fault detection based on the alarm notification and KPIs.	

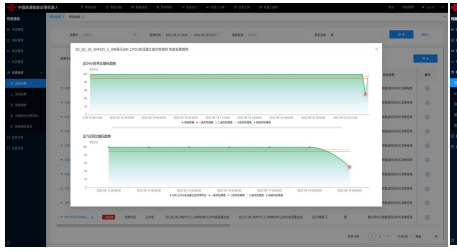
Evidence

Sub Scenarios 1: Equipment

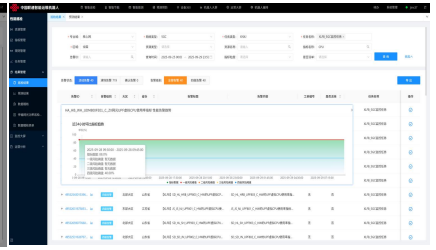




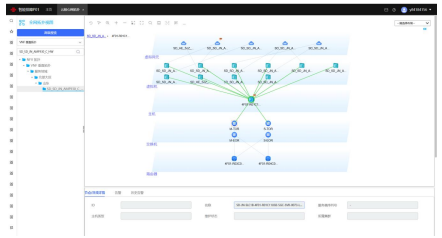
5GC VNF Alarm Status Visualization - Support 1

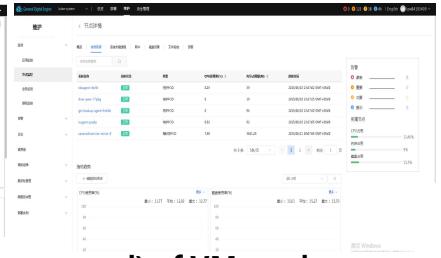


NE health status visualization (degraded) - Support 2

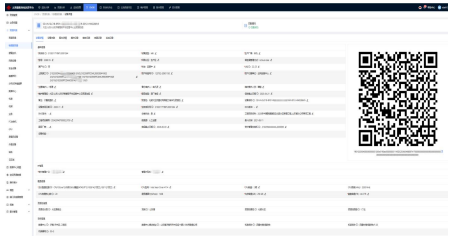


NE health status visualization (overloaded) - Support 2



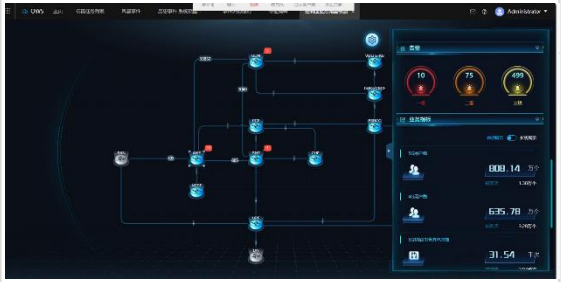


Visualized status (faulty or normal) of VMs and pods in the telecom cloud - Support 3



Visualized Monitoring of Telecom Cloud Infrastructure Configuration Information - Support 4

Sub Scenarios 2: Communication and Quality of service



The system displays link status, alarms, and link indicators.

If a link alarm is generated or a link fault occurs, the link color is displayed in red.

Question 3 Risk Prediction

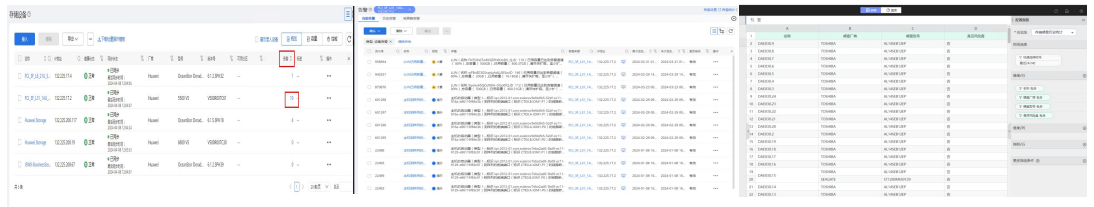
Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Risk prediction	10%	Does your system automatically detect and prevent risks of NE faults? Assessment object: management entities Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can use intelligent risk identification to recognize potential faults and automatically prevent faults. It can: 1. Prevent potential risks and analyze the risks involving capacity, links, signaling storms, DR, and hardware. 2. Analyze the cause of risks and provide recommended actions automatically.	The system can use automatic risk identification, which requires manual confirmation, to recognize potential faults and prevent faults. It can: 1. Prevent potential risks and analyze the risks involving capacity and links.	The system can use risk identification to recognize potential faults and prevent faults by providing an automatic checklist which requires engineers to periodically confirm the potential risks in this checklist. It can: 1. Prevent potential risks and analyze the risks involving capacity.	No. The system does not support risk prediction.

Evidence

Capability Introduction: The system supports risk identification based on golden service KPIs, 5GC/vIMS prediction and prevention, and signaling storm detection. Based on identified risks, the system diagnoses risks based on CHR data and provides risk rectification suggestions.
Self-assessed Capability: Option A

Sub Scenarios 1: Equipment

Potential capacity identification

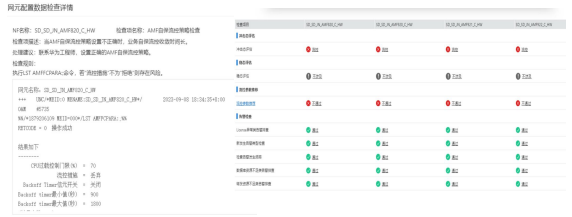


Hardware risk identification (DC disk)

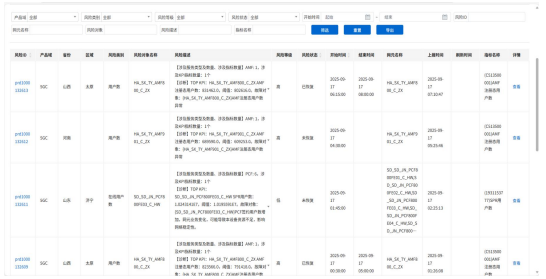
Sub Scenarios 2: Communication and Quality of service

Link risk identification

Signaling storm detection



Disaster recovery risk identification



Prediction and prevention risk identification

Provide handling suggestions

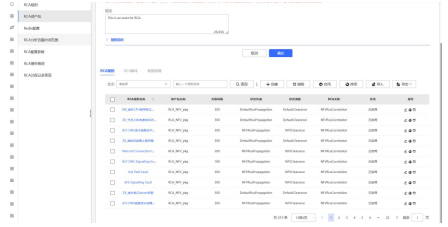
Question 4 Demarcation

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Demarcation	15%	Does your system support automatic demarcation of core network faults? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs and IMS NEs)	Yes. The intelligent system supports automatic fault demarcation without manual intervention (e.g., core network NEs and managed objects in telecom cloud) covering 95% or higher of live network faults. The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for NEs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation covering 80% or higher of faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for NEs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation and provides one or multiple analysis results to assist fault demarcation.	No. The system does not support automatic fault demarcation.

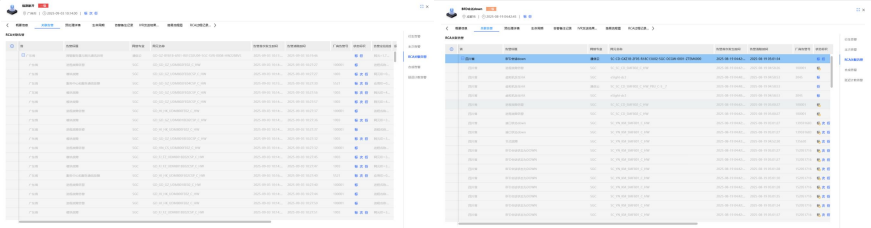
Evidence

Capability Introduction: When a fault is detected, the core network troubleshooting agent starts fault demarcation and provides fault demarcation results through task action analysis such as fault authenticity check, fault impact evaluation, fault demarcation, and fault location. Currently, more than 95% of live network faults are covered, and the average accuracy exceeds 90%. Cross-layer alarm correlation implements multi-dimensional alarm correlation. Alarms are correlated from the time, space resource, and alarm feature dimensions. The time dimension and alarm feature dimension are basically the same as the traditional single-domain fault correlation dimension. Cross-layer fault locating mainly enhances the spatial resource correlation dimension.

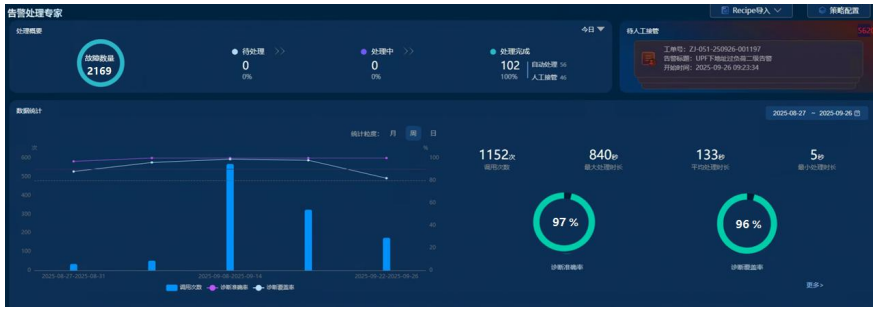
Self-assessed Capability: Option A

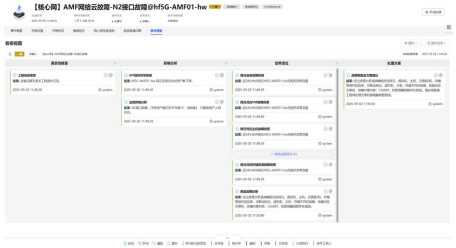


Diagnosis rule configuration



Diagnose fault correlation



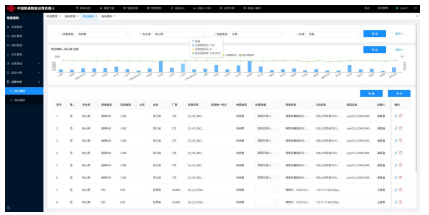


The system identifies faults, starts the fault diagnosis process, performs authenticity check, fault impact analysis, and fault demarcation, and provides comprehensive demarcation results. - Support 1

Sub Scenarios 1: Equipment

Sub Scenarios 2: Communication and Quality of service

The system supports horizontal VNF demarcation, link fault demarcation between VNFs, and cross-layer vertical demarcation. - Support 2



More than 95% of live-network faults have been covered, and the average accuracy exceeds 90%.

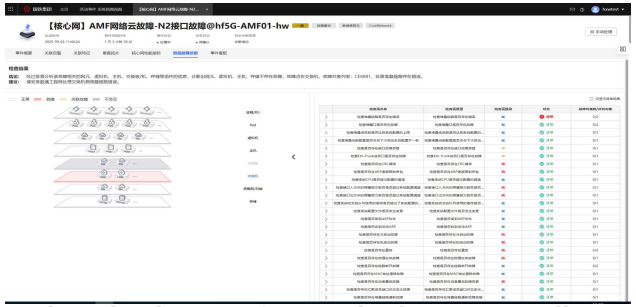
Question 5 Locating

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Locating	15%	Does your system support automatic locating related to core network fault management? Assessment object: the core network management function and network function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. Intelligent fault diagnosis is capable of automatically providing precise locating (e.g., detailed causes of identified faults, including minimum units, software modules, and ports) of faults, covering 95% or higher of live network faults without human intervention. The average accuracy per month is above 90%.	Automatic fault diagnosis is capable of providing root causes of faults, and providing precise fault locating, covering 80% or higher faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%.	The system supports automatic fault locating and provides one or multiple analysis results to assist fault locating.	No. The system does not support automatic fault locating.

Evidence

Capability Introduction: After the fault is demarcated, the core network troubleshooting agent starts fault locating and collects detailed information about faulty NEs, including operation logs, CHRs, running logs, and operation status, to provide detailed fault causes, such as configurations, modules, and ports. Currently, more than 95% of live-network faults are covered, and the average accuracy exceeds 90%.
Self-assessed Capability: Option A

Sub Scenarios 1：Equipment

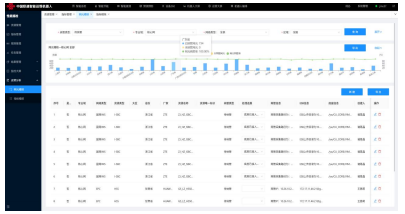


Based on the demarcation result, the system collects detailed NFVI information and locates the fault. It is determined that the upper-layer VNF fault is caused by a hardware port or hardware fault at the NFVI layer.

Locate the smallest unit POD

Sub Scenarios 2：Communication and Quality of service

Based on the demarcation result, the system collects and analyzes NE CHRs, operation logs, and run logs, and provides a fault locating conclusion.



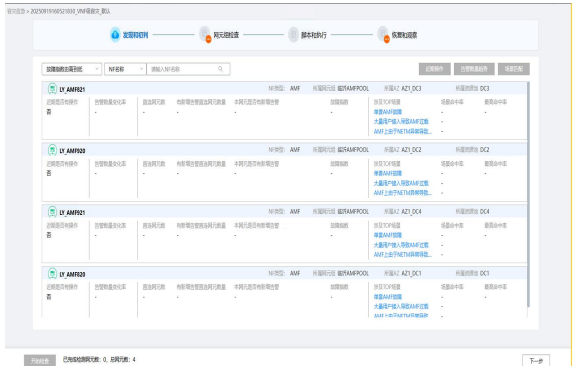
More than 95% of live network faults have been covered, and the average accuracy exceeds 90%.

Question 6 Fault Rectification Solution Generation

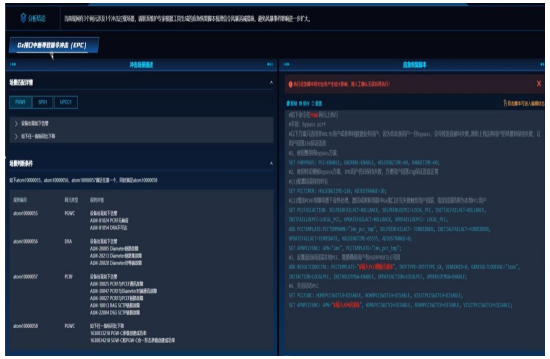
Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Fault rectification solution generation	10%	Does your system automatically generate the fault rectification solution? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can generate the optimal rectification solution (minimum impact scope and time). Fault rectification can cover but not be limited to the following scenarios: 1. Generating an NF fault rectification solution automatically 2. Generating a solution to recover slight service losses 3. Providing a DR solution in case of accidents or natural disasters 4. System can generate optimization to network for failure (e.g., signaling storm, service outage etc.) automatically.	The system can generate a fault rectification solution (e.g., fault rectification scripts including operation objects and operation sequences). Fault rectification can cover the following scenarios: 1. Providing a DR solution in case of accidents or natural disasters. 2. System can generate optimization to network for failure (e.g., signaling storm, service outage etc.) automatically.	The system can generate fault rectification recommendations based on specialized checklist, to determine the rectification operations and operation objects based on rectification decision rules (configuration). Fault rectification can cover the following scenarios: 1. Providing a DR solution in case of accidents or natural disasters	No. The system supports fault rectification based on manual decisions.

Evidence

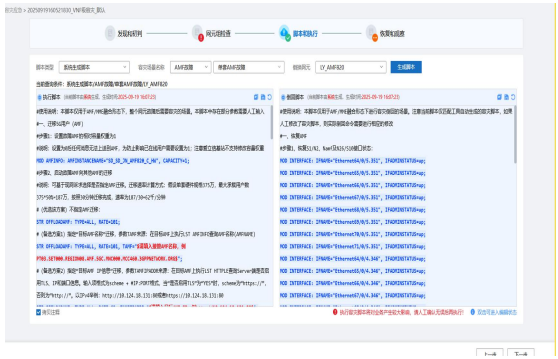
Capability Introduction: After a fault is identified and located, the core network troubleshooting agent and MDAF automatically generate a fault recovery solution based on the root cause of the fault. The solution includes the NE fault recovery solution, NE fault and accident recovery script, and emergency recovery script. The solution can be used as a reference for O&M personnel. In addition, the system automatically provides a signaling procedure parameter adjustment optimization solution in signaling storm scenarios.
Self-assessed Capability: Option A (cover two sub-scenarios: Device & Communication and Quality of service)



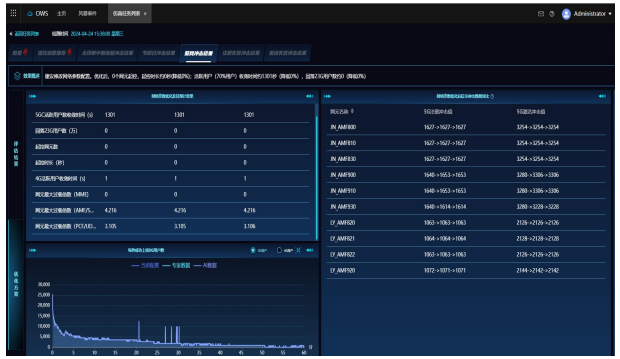
After a fault is identified and diagnosed, the system can automatically generate a troubleshooting solution based on the root cause of the fault and the built-in solution example. -Support 1



Gx interface interruption causes signaling impact. The system automatically generates emergency recovery scripts for O&M personnel to refer to and execute, thereby restoring minor service losses. -Support 2



Based on the fault handling solution, the system automatically generates disaster recovery switchover scripts and handling scripts according to the network element information for reference and execution by O&M personnel. -Support 3



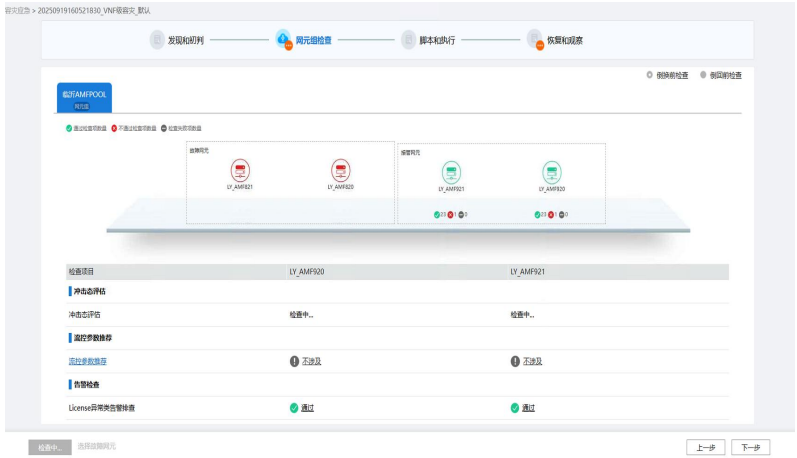
In signaling storm scenarios, the system automatically generates signaling flow control suggestions for each interface based on signaling storm conditions for O&M personnel. –Support 4

Question 7 Solution Pre-verification

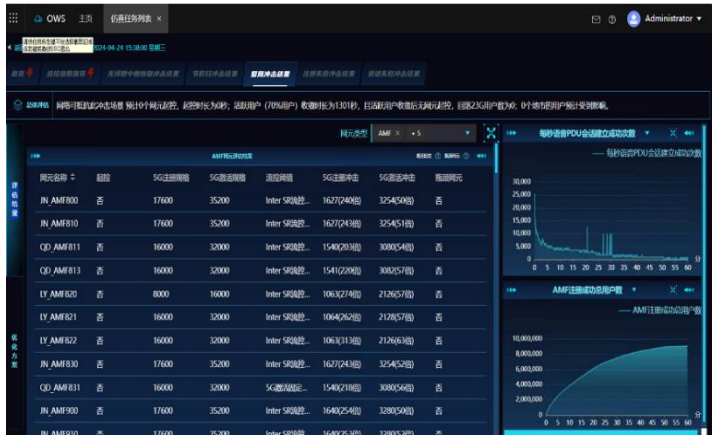
Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Solution pre-verification	10%	Does your system support rectification solution evaluation and verification to support decisions in core network? NOTE: Fault rectification solution can be evaluated before implementation by being verified in a simulation or sandbox environment. Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system supports intelligent rectification solution evaluation for the core network to verify the feasibility of rectification solution and provides the visualization results of accuracy effect before implementation. The evaluation tasks can cover but not be limited to the following scenarios: 1. Solution feasibility check and configuration verification 2. Emulation or simulation of rectification solution based on network digital twin The system supports the decision.	The system supports automatic rectification solution evaluation for core network, to verify the feasibility of rectification solution before implementation. The evaluation tasks can cover the following scenarios: 1. Solution feasibility check and configuration verification 2. DR rectification solution evaluation and verification The system supports the simulation results for manual decisions made for rectification solution.	The system provides a checklist for manual evaluation to verify the feasibility of rectification solution before implementation. The checklist includes but is not limited to: 1. NF healthy status check 2. Influence of rectification solution	No. The system verifies the rectification solution based on manual decisions.

Evidence

Capability Introduction: Core network troubleshooting agents work with the MDAF to evaluate and verify the recovery solution in the DR switchover scenario. Dynamic and static evaluation ensures the feasibility and accuracy of the DR switchover solution.
Self-assessed Capability: Option B (cover two sub-scenarios: Device & Communication and Quality of service)



After the DR switchover evaluation is started, the system automatically collects and analyzes the information about the switched NEs and provides static evaluation based on alarms, indicators, configurations, and resources. - Support 1



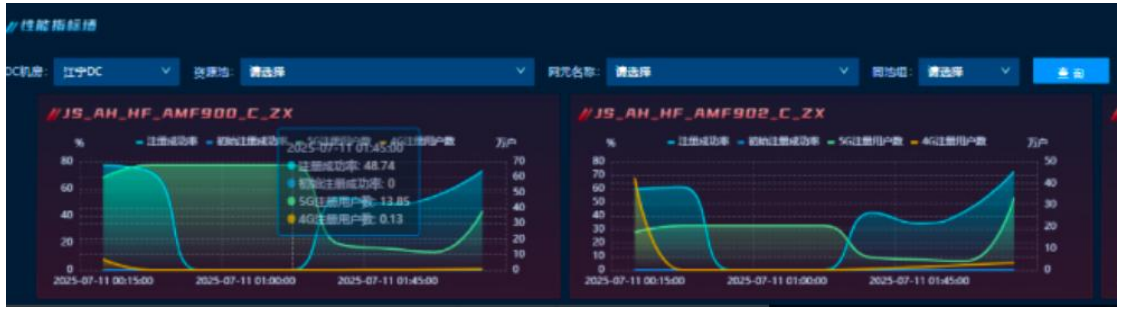
The system collects dynamic information for simulation evaluation, determines whether signaling storms and signaling storms may occur after a switchover, and collects dynamic and static evaluation results to support manual decision-making. - Support 2

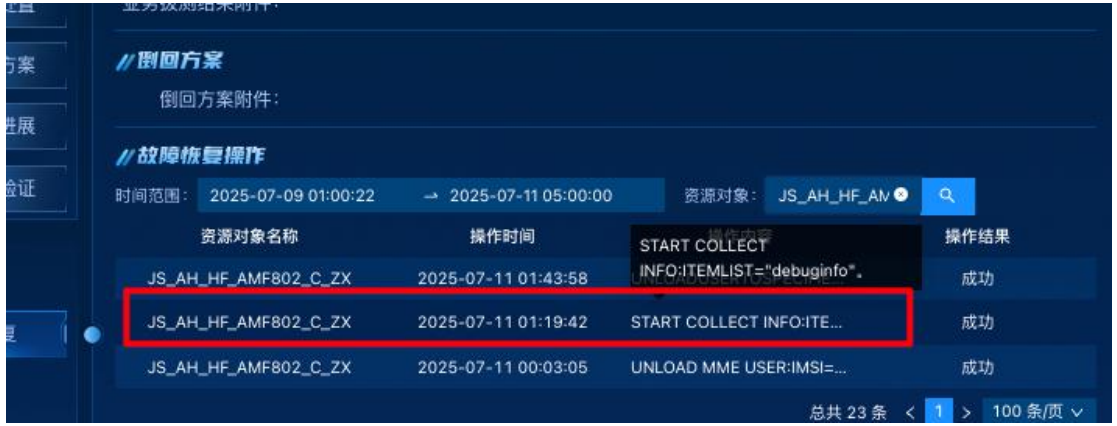
Question 8 Solution Implementation

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Solution implementation	10%	Does your system support automatic fault rectification? Assessment object: the core network management function and network element Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs).	Yes. The system can support automatic fault rectification in all fault rectification scenarios.	The system supports fault rectification after manual confirmation.		

Evidence

Capability Introduction: After a fault occurs, the core network automatically switches services from the faulty DC to the redundancy DC. Services on the redundancy NE increase. After the fault is rectified, services are automatically switched back to the original NE.
Self-assessed Capability: Option A (cover two sub-scenarios: Device & Communication and Quality of service)





Configuration commands and actions during switchover and restoration can be automatically executed. Based on the network operation logs generated during the fault recovery process, the system can detect the configuration commands executed during the automatic handling process.

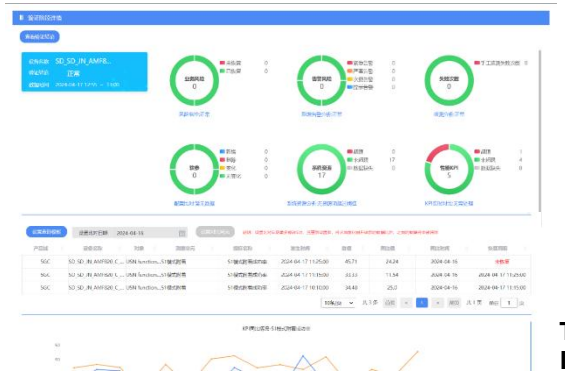
Question 9 Service Verification

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Service verification	10%	Does your system support automatic service verification after faults on core networks are rectified? Assessment object: the core network management function Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system automatically verifies whether network services are recovered and faults are rectified successfully.	The system automatically verifies that the alarms are cleared and KPI data is successfully recovered.	No. The system does not support automatic service verification.	

Evidence

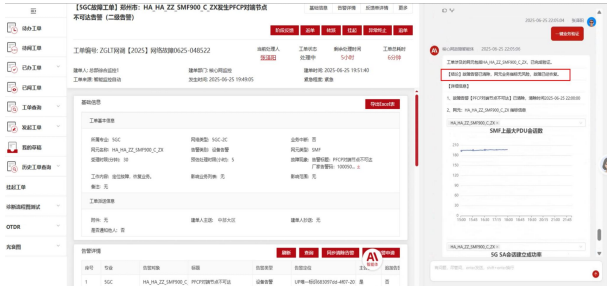
Capability Introduction: The fault center and core network troubleshooting intelligent twin jointly provide automatic service verification capabilities after core network faults are rectified. Through multi-dimensional data analysis and comparison, O&M personnel can confirm that services are restored or report other exceptions for reference.
Self-assessed Capability: Option A (cover two sub-scenarios: Device & Communication and Quality of service)

After the fault is rectified, the service fault recovery verification function is automatically invoked to verify the service recovery from multiple dimensions, such as service risks, alarm risks, dialing test risks, configuration comparison, system resources, and performance KPIs. After confirming that no exception is found, the verification conclusion is returned.



If an exception is detected during the verification, the system prompts O&M personnel to analyze the exception and confirm the verification result.

Take an abnormal indicator as an example. If the system finds that the recovery status of a key service indicator is not as expected when comparing multiple key indicators, Take an abnormal indicator as an example. If the system finds that the recovery status of a key service indicator is not as expected when comparing multiple key indicators.



The core network troubleshooting agent can trigger service verification by one click. The agent invokes the small model tool to check alarms and real-time service status, intelligently generates verification results, and provides detailed indicator trend charts and exception detection results based on AI dynamic thresholds.

China Unicom TMF ANL Evaluaion

(Core Network Architecture Stability)

November 2025

ANL Assessment - Core Network Architecture Stability Assessment Criteria (1/2)

中国联通 China unicom

Scenario	Category	Capability or Task	Weight (Optional)	Question	Option A	Option B	Option C	Option D
Core network architecture stability - planning	Basic stability	Stable deployment architecture	10%	Does the core network deployment architecture have a capability for redundancy modules to take over the services carried by faulty modules? NOTE 1: There are service processing modules, LB load sharing modules, and service data modules. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, IMS NEs)	Yes. The system can deal with multiple-module faults within a VNF, which uses multiple types of module resources within this VNF. If M module experiences an abnormal situation, N backup module can take over all service loads, preventing a decrease in the VNF overall processing capacity. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service connection context remains uninterrupted. 2. Service access can recover within minutes.	The system can deal with multiple-module faults within a VNF, which uses multiple types of module resources within this VNF. If M module experiences an abnormal situation, N backup module can take over all service loads, preventing a decrease in the overall processing capacity. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service access can recover within minutes.	The system can deal with a single module fault and restore service loads. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service access can recover within minutes.	Not supported
		Control-plane disaster recovery (DR)	15%	Does your system support automatic control-plane DR for DR NEs to take over communication services without service interruption? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC Control-plane NFs (AMF, SMF, PCF, UDM, NRF, SCP etc.), EPC NEs (SGW, MME, etc.), IMS NEs)	Yes. The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios in minutes and UEs remain connected. 1. When an accident or natural disaster occurs, core network NEs can switch over services across DCs and the backup NEs can take over all services successfully. 2. When control-plane NEs are faulty, backup NEs can take over the services carried by faulty NEs and UEs remain connected. 3. In the case of control-plane NE (UDM/HSS, PCF/PCRF, OCS/CHF, NRF, ENUM etc.) faults, control-plane NEs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). 4. In the case of a management entity fault, control-plane NEs can maintain subscribers' communication active for a period of time (hours or above). During control-plane DR, control-plane NEs are required to maintain data connections.	The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios in minutes. 1. When an accident or natural disaster occurs, core network NEs can switch over services across DCs and the backup NEs can take over all services successfully. 2. When control-plane NEs are faulty, backup NEs can take over the services carried by faulty NEs. 3. In the case of critical control-plane NE (UDM/HSS and PCF/PCRF and OCS/CHF) faults, control-plane NEs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). 4. In the case of a management entity fault, control-plane NEs can maintain subscribers' communication active for a period of time (hours or above).	The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios: 1. When an accident or natural disaster occurs, backup DCs can restore all service data and subscribers' data. 2. When control-plane NEs are faulty, backup NEs can take over the services carried by faulty NEs. During control-plane DR, the control-plane NEs can restore subscribers' data.	No. The service switchover can be triggered manually.
		User-plane disaster recovery	15%	Does your system support automatic user-plane DR to take over all services without service interruption? NOTE 1: The user-plane DR scenario indicates that the backup UP NE (UPF) can take over the services in the fault scenario. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs (UPF), EPC NEs (PGW), IMS NEs (SBC))	Yes. The user-plane DR NEs and DR DCs can take over all services without service interruption: 1. When an accident or natural disaster occurs, user-plane NE's pool-based deployment supports the switching of traffic among user-plane NEs in minutes. 2. In the case of a management entity fault, user-plane NEs can maintain communication services for a period of time (hours or above). 3. The data connection remains active.	The user-plane DR NEs and DR DCs can take over all services in a short period of time: 1. User-plane NEs can take over all traffic in minutes. 2. The data connection can recover in minutes.	The user-plane DR NEs and DR DCs can take over traffic of faulty user-plane NEs 1. User-plane NEs can take over all traffic.	Not supported
		Infrastructure disaster recovery	15%	Does your system support automatic disaster recovery on telecom cloud infrastructure to ensure uninterrupted communication services? NOTE: Telecom cloud infrastructure is considered to include the following elements: Cloud OS and hardware (server, storage, and IP Core). The faults may result from the IP backbone router, transmission faults, or the overall telecom cloud faults. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When DC transmission is faulty, the core network can provide local area (e.g., within a region) communication normally. 2. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the NEs in running status for a period of time, or trigger DR switchover to maintain the communication without interruption. 3. In case of whole core network outage, at least VIP calls and emergency calls can proceed through the backup core network. 4. Distributed user-plane NE deployment can reduce the impacts of user-plane NEs faults, and user-plane NE switchover can minimize the affected region. 5. When the core network subdomain or subsystem experiences faults, network can fallback without affecting other communication services (e.g., IMS fallback should not affect data connection). 6. When the core network subdomain becomes faulty, network in the subdomain can fall back, keeping normal UE connection. (e.g., 5GC data connectivity can fall back to EPC network and EPC data connectivity can fall back to 3G PS services.) 7. When a natural disaster occurs and affects two active DCs, additional third DC can take over service loads from the two active DCs and remain data connection alive.	The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When DC transmission is faulty, the core network can provide local area (e.g., within a region) communication for a period of time. 2. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the NEs in running status for a period of time. 3. Distributed user-plane NE deployment can reduce the impacts of user-plane NEs faults, and user-plane NE switchover can minimize the affected region. 4. When the core network subdomain experiences faults, network in the subdomain can fall back, keeping normal UE connection. (e.g., 5GC data connectivity can fall back to EPC network and EPC data connectivity can fall back to 3G PS services.)	The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the NEs in running status for a period of time.	Not supported

ANL Assessment - Core Network Architecture Stability Assessment Criteria (2/2)

Scenario	Category	Capability or Task	Weight (Optional)	Question	Option A	Option B	Option C	Option D
Core network architecture stability - planning	Basic stability	Anti-signaling surge capability	15%	Does your system support automatic signaling overload control to avoid core network service outage? NOTE: The terminal behaviors are affected by the software logic or server design. Since the terminal behaviors are highly consistent, wide-range signaling impact can occur. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, NEs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end NEs can evaluate and adaptively adjust subscribers' service requests delivered to back-end network elements, so the back-end elements can remain at the optimized workload without service congestion. 3. When signaling storm occurs, core network NEs are capable to evaluate and adjust traffic to avoid impact to other domains when services fall back. The system can converge signaling storm in minutes.	The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, NEs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end NEs can reduce the service requests delivered to back-end network elements, so the back-end NE faults can be avoided. The system can converge signaling storm within 1 hour.	NEs are capable to protect its processing capability.	Not supported
	Intelligent stability	Risk prediction	15%	Does your system automatically detect and prevent the risks of network NE faults to ensure the service continuity? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can use intelligent risk identification to recognize the potential faults and automatically prevent faults, and it can do the following: 1. Prevent potential risks and analyze the specification-related risks including capacity, links, signaling storm, and DR. 2. Analyze the cause of risk and provide the recommended measures automatically.	The system can perform automatic risk identification, which requires manual confirmation, to recognize the potential faults and prevent faults, and it can do the following: 1. Prevent potential risk and analyze the specification-related risks, including capacity and links.	The system can use risk identification, which provides an automatic check list and requires periodically manual confirmation about the potential risks in this check list, to recognize the potential faults and prevent faults, and it can do the following: 1. Prevent potential risk and analyze the specification-related risks including capacity.	Not supported
		Service degradation recovery	15%	Does your system support automatic detection and recovery from service degradation related to core network NEs/NFs? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. When abnormal situations (for example, CPU overload, interconnection issues, and slight service damage) occur without any fault alarms generated (for example, the heartbeat is normal), the system supports automatic detection and diagnosis of service degradation, provides recovery recommendations, and enables autonomous execution without human intervention.	When abnormal situations (for example, CPU overload, interconnection issues, and slight service damage) occur without any fault alarms generated (for example, the heartbeat is normal), the system supports automatic detection and diagnosis of service degradation, provides recovery recommendations, and supports manual recovery.	When abnormal situations (for example, CPU overload, interconnection issues, and slight service damage) occur without any fault alarms generated (for example, the heartbeat is normal), the system supports automatic detection of service degradation.	Not supported.

Self-assessment Results

- The self-assessment score for the ANL evaluation of core network architecture stability is **3.60**. China Unicom's core network employs a layered, decoupled, and cloud-based architecture, achieving high service availability and intelligent elastic recovery through control/user plane separation, redundant deployment, and automated failover mechanisms.

Category	Capability or Task	Weight (Optional)	Question	Answer
Basic stability	Stable deployment architecture	10%	Does the core network deployment architecture have a capability for redundancy modules to take over the services carried by faulty modules? NOTE 1: There are service processing modules, LB load sharing modules, and service data modules. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, IMS NEs)	B
	Control-plane disaster recovery (DR)	15%	Does your system support automatic control-plane DR for DR NEs to take over communication services without service interruption? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC Control-plane NFs (AMF, SMF, PCF, UDM, NRF, SCP etc.), EPC NEs (SGW, MME, etc.), IMS NEs)	A
	User-plane disaster recovery	15%	Does your system support automatic user-plane DR to take over all services without service interruption? NOTE 1: The user-plane DR scenario indicates that the backup UP NE (UPF) can take over the services in the fault scenario. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs (UPF), EPC NEs (PGW), IMS NEs (SBC))	A
	Infrastructure disaster recovery	15%	Does your system support automatic disaster recovery on telecom cloud infrastructure to ensure uninterrupted communication services? NOTE: Telecom cloud infrastructure is considered to include the following elements: Cloud OS and hardware (server, storage, and IP Core). The faults may result from the IP backbone router, transmission faults, or the overall telecom cloud faults. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	B
	Anti-signaling surge capability	15%	Does your system support automatic signaling overload control to avoid core network service outage? NOTE: The terminal behaviors are affected by the software logic or server design. Since the terminal behaviors are highly consistent, wide-range signaling impact can occur. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A
Intelligent stability	Risk prediction	15%	Does your system automatically detect and prevent the risks of network NE faults to ensure the service continuity? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	A
	Service degradation recovery	15%	Does your system support automatic detection and recovery from service degradation related to core network NEs/NFs? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	B

Question 1 Stable Deployment Architecture

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Stable deployment architecture	10%	Does the core network deployment architecture have a capability for redundancy modules to take over the services carried by faulty modules? NOTE 1: There are service processing modules, LB load sharing modules, and service data modules. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, IMS NEs)	Yes. The system can deal with multiple-module faults within a VNF, which uses multiple types of module resources within this VNF. If M module experiences an abnormal situation, N backup module can take over all service loads, preventing a decrease in the VNF overall processing capacity The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service connection context remains uninterrupted. 2. Service access can recover within minutes.	The system can deal with multiple-module faults within a VNF, which uses multiple types of module resources within this VNF. If M module experiences an abnormal situation, N backup module can take over all service loads, preventing a decrease in the overall processing capacity. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service access can recover within minutes.	The system can deal with a single module fault and restore service loads. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service access can recover within minutes.	Not supported

Evidence

Capability Introduction: China Unicom's core network equipment adopts a cloud-native microservices architecture, capable of handling multi-module failures within VNFs. It utilizes diverse module resources within VNFs, ensuring that when M modules encounter anomalies, N backup modules can seamlessly take over the entire service load, thereby preventing any degradation in overall processing capacity.
Self-assessed Capability: Option B

Evidence Samples for Option B:

Evidence of High-Availability Deployment Architecture:

Evidence of Availability Deplo

The service modules of production network elements are deployed in an N-Way mode (specifically an N+M redundancy architecture with M>1). This design ensures that in the event of failures in M modules, the N backup modules can assume the entire service load, thereby preventing any degradation in the overall processing capacity of the VNF.

The databases of production network elements are deployed with a distributed multi-replica scheme, ensuring minimal service impact during module failures.

The service processing modules of network elements employ a stateless design. While this cannot guarantee uninterrupted context persistence for all service sessions, it enables service access to be restored at a minute-level timescale.

NEs on the live network include the UNC, UDG, UDM, PCF, and SBC.

Question 2 Control-plane Disaster Recovery (DR)

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Control-plane disaster recovery (DR)	15%	Does your system support automatic control-plane DR for DR NEs to take over communication services without service interruption? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC Control-plane NFs (AMF, SMF, PCF, UDM, NRF, SCP etc.), EPC NEs (SGW, MME, etc.), IMS NEs)	Yes. The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios in minutes and UEs remain connected. 1. When an accident or natural disaster occurs, core network NEs can switch over services across DCs and the backup NEs can take over all services successfully. 2. When control-plane NEs are faulty, backup NEs can take over the services carried by faulty NEs and UEs remain connected. 3. In the case of control-plane NE (UDM/HSS, PCF/PCRF, OCS/CHF, NRF, ENUM etc.) faults, control-plane NEs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). 4. In the case of a management entity fault, control-plane NEs can maintain subscribers' communication active for a period of time (hours or above). During control-plane DR, control-plane NEs are required to maintain data connections.	The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios in minutes. 1. When an accident or natural disaster occurs, core network NEs can switch over services across DCs and the backup NEs can take over all services successfully. 2. When control-plane NEs are faulty, backup NEs can take over the services carried by faulty NEs. 3. In the case of critical control-plane NE (UDM/HSS and PCF/PCRF and OCS/CHF) faults, control-plane NEs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). 4. In the case of a management entity fault, control-plane NEs can maintain subscribers' communication active for a period of time (hours or above).	The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios: 1. When an accident or natural disaster occurs, backup DCs can restore all service data and subscribers' data. 2. When control-plane NEs are faulty, backup NEs can take over the services carried by faulty NEs. During control-plane DR, the control-plane NEs can restore subscribers' data.	No. The service switchover can be triggered manually.

Evidence

Capability Introduction: China Unicom's core network control plane elements are universally deployed with element-level disaster recovery mechanisms. These resilience schemes, including resource pool groups, 1+1 redundancy, and N+1 redundancy, are implemented to ensure high availability. A representative implementation can be observed in the HeNan provincial network, where multiple AMF (Access and Mobility Management Function) sets are distributed across two physically separate data centers. These AMFs operate within a pool-based redundancy architecture, thereby achieving robust, element-level fault tolerance.
Self-assessed Capability: Option A

The schematic depicts the core network architecture within China Unicom's Central Region:

- Deployed control plane network elements implement robust redundancy mechanisms—including resource pooling, 1+1 active/standby, and N+1 backup configurations. This enables seamless cross-data center service failover during incident scenarios or natural disasters, with redundant elements capable of assuming full operational loads without service degradation. (Supports 1 & 2)
- Operational control plane infrastructure incorporates Bypass disaster recovery capabilities. For critical control plane elements (UDM, PCF/PCRF, NRF, CHF), locally persisted data ensures continuity of voice services for extended durations (exceeding one hour) during element failures. (Supports 3)
- Management plane elements are configured with 1+1 active/standby redundancy. Crucially, complete failure of both primary and standby management nodes does not impair the operational integrity of service plane elements. (Supports 4)

Disaster Recovery Methods for China Unicom's 5GC and IMS Network Elements

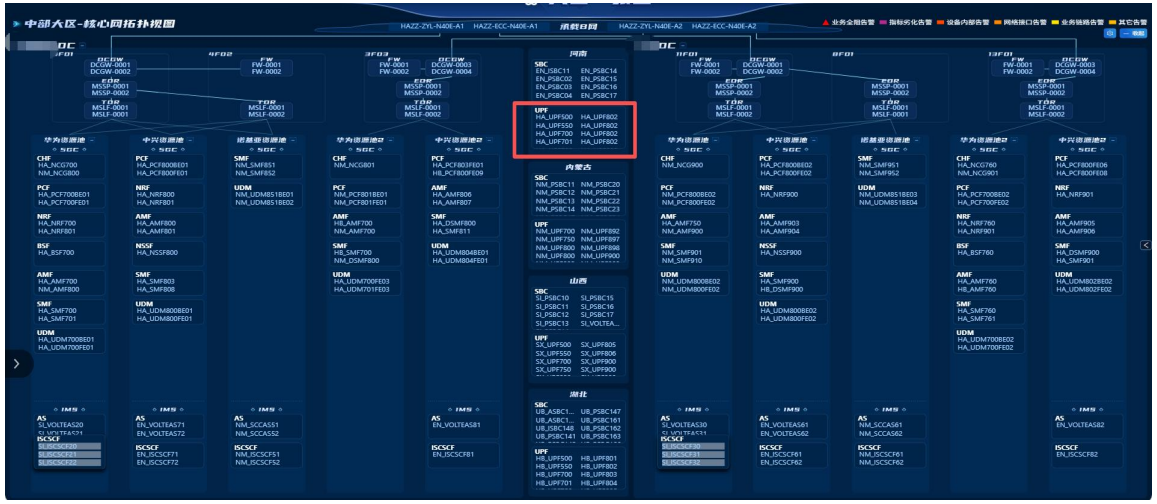
Disaster
Methods for Ch

Question 3 User-plane Disaster Recovery

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
User-plane disaster recovery	15%	Does your system support automatic user-plane DR to take over all services without service interruption? NOTE 1: The user-plane DR scenario indicates that the backup UP NE (UPF) can take over the services in the fault scenario. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs (UPF), EPC NEs (PGW), IMS NEs (SBC))	Yes. The user-plane DR NEs and DR DCs can take over all services without service interruption: 1. When an accident or natural disaster occurs, user-plane NE's pool-based deployment supports the switching of traffic among user-plane NEs in minutes. 2. In the case of a management entity fault, user-plane NEs can maintain communication services for a period of time (hours or above). 3. The data connection remains active.	The user-plane DR NEs and DR DCs can take over all services in a short period of time: 1. User-plane NEs can take over all traffic in minutes. 2. The data connection can recover in minutes.	The user-plane DR NEs and DR DCs can take over traffic of faulty user-plane NEs. 1. User-plane NEs can take over all traffic.	Not supported

Evidence

Capability Introduction: China Unicom's core network user plane has implemented comprehensive network element-level disaster recovery mechanisms utilizing a resource pool architecture. For instance, in the operational network of Henan Province, multiple UPF (User Plane Function) sets are deployed across geographically dispersed equipment rooms. These network elements operate through a pool-based disaster recovery mechanism, achieving complete network element-level service redundancy.
Self-assessed Capability: Option A



The diagram illustrates the core network deployment architecture of China Unicom's Central Region:

The operational User Plane Function (UPF) network elements employ a Pool Groups based disaster recovery mechanism. During incidents or natural disasters, UPFs within the Pool support minute-level traffic switching. (Supports 1 & 3)

The management plane network elements are configured with a 1+1 active-standby redundancy scheme. Crucially, service network elements maintain normal operation even during complete failure of both primary and standby management elements. (Supports 2)

Disaster Recovery Methods for China Unicom's 5GC and IMS Network Elements

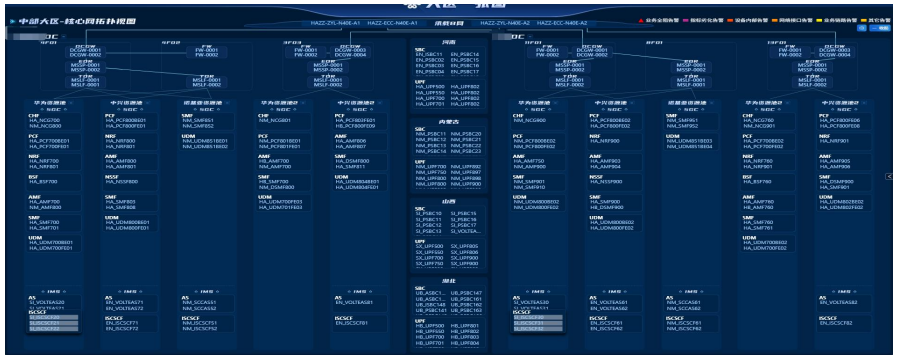
Disaster
y Methods for Ch

Question 4 Infrastructure Disaster Recovery

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Infrastructure disaster recovery	15%	Does your system support automatic disaster recovery on telecom cloud infrastructure to ensure uninterrupted communication services? NOTE: Telecom cloud infrastructure is considered to include the following elements: Cloud OS and hardware (server, storage, and IP Core). The faults may result from the IP backbone router, transmission faults, or the overall telecom cloud faults. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When DC transmission is faulty, the core network can provide local area (e.g., within a region) communication normally. 2. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the NEs in running status for a period of time, or trigger DR switchover to maintain the communication without interruption. 3. In case of whole core network outage, at least VIP calls and emergency calls can proceed through the backup core network. 4. Distributed user-plane NE deployment can reduce the impacts of user-plane NEs faults, and user-plane NE switchover can minimize the affected region. 5. When the core network subdomain or subsystem experiences faults, network can fallback without affecting other communication services (e.g., IMS fallback should not affect data connection). 6. When the core network subdomain becomes faulty, network in the subdomain can fall back, keeping normal UE connection. (e.g., 5GC data connectivity can fall back to EPC network and EPC data connectivity can fall back to 3G PS services.) 7. When a natural disaster occurs and affects two active DCs, additional third DC can take over service loads from the two active DCs and remain data connection alive.	The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When DC transmission is faulty, the core network can provide local area (e.g., within a region) communication for a period of time. 2. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the NEs in running status for a period of time. 3. Distributed user-plane NE deployment can reduce the impacts of user-plane NEs faults, and user-plane NE switchover can minimize the affected region. 4. When the core network subdomain experiences faults, network in the subdomain can fall back, keeping normal UE connection. (e.g., 5GC data connectivity can fall back to EPC network and EPC data connectivity can fall back to 3G PS services.)	The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the NEs in running status for a period of time.	Not supported

Evidence

Capability Introduction: China Unicom's telecom cloud pool adopts a site-level disaster recovery mechanism. Multiple sites are set up in each region, with upper-layer applications distributed across different telecom cloud pools to achieve service site disaster recovery. For example, in the current network, China Unicom's telecom cloud pools in Henan are distributed across two different data centers.
Self-assessed Capability: Option B



The diagram illustrates the core network communication cloud deployment for China Unicom's Central Region:
1、 Henan Unicom's active telecom cloud pools are deployed across two data centers. In the event of a transmission failure in one DC, services can be switched to the other, ensuring business continuity. — Support 1
2、 Network elements in the current setup are deployed with a Bypass mechanism. This ensures that core network elements can maintain operation for a period of time in case of telecom cloud infrastructure anomalies, such as storage failures. — Support 2
3、 User Plane Functions (UPFs) are distributed across different equipment rooms. This deployment minimizes the impact of a single UPF failure and reduces the scope of affected users. — Support 3
4、 In case of a failure in a core network sub-domain (e.g., the 5G sub-domain), user equipment (UE) can fall back to the 4G Evolved Packet Core (EPC) sub-domain to maintain a normal connection. — Support 4
5、 Due to the large-scale decommissioning of China Unicom's 3G base stations, voice services cannot fall back to 3G in case of an IMS sub-domain failure. Thus, it does not meet the requirement for Option A.
6、 A third data center has not yet been deployed in the current network, so it does not meet the requirement for Option A.

Question 5 Anti-signaling Surge Capability

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Anti-signaling surge capability	15%	Does your system support automatic signaling overload control to avoid core network service outage? NOTE: The terminal behaviors are affected by the software logic or server design. Since the terminal behaviors are highly consistent, wide-range signaling impact can occur. Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, NEs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end NEs can evaluate and adaptively adjust subscribers' service requests delivered to back-end network elements, so the back-end elements can remain at the optimized workload without service congestion. 3. When signaling storm occurs, core network NEs are capable to evaluate and adjust traffic to avoid impact to other domains when services fall back. The system can converge signaling storm in minutes.	The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, NEs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end NEs can reduce the service requests delivered to back-end network elements, so the back-end NE faults can be avoided. The system can converge signaling storm within 1 hour.	NEs are capable to protect its processing capability.	Not supported

Evidence

Capability Introduction: All core network elements of China Unicom support the capability to withstand signaling surges. When signaling traffic exceeds the design specifications of a network element, the element's flow control protection mechanism ensures its own stable operation and maintains service continuity. Furthermore, the system supports front-end network elements in implementing flow control to protect back-end network elements, optimizing the network-wide resilience against signaling surges and preventing service congestion. It also possesses the capability for signaling impact simulation and assessment, which supports the optimized configuration of flow control parameters and enables minute-level storm convergence.
Self-assessed Capability: Option A

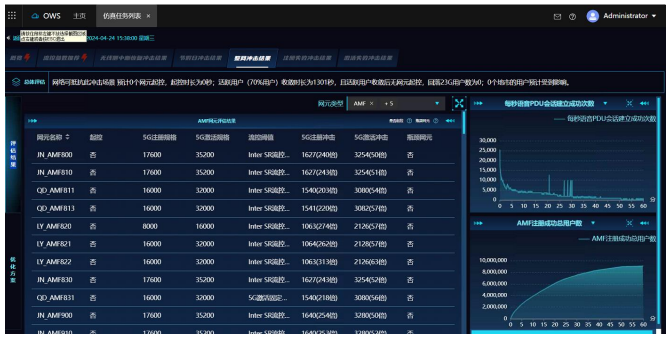
Evidence materials for Option A：

Evidence materials for Point 1/2：

Evidence of aling Surge Resili

Evidence of Signaling Surge Resilience

Evidence materials for Point 3：



Assessing signaling surge traffic

Optimization of Flow Control Parameters for Faster Storm Convergence.

Question 6 Risk Prediction

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Risk prediction	15%	Does your system automatically detect and prevent the risks of network NE faults to ensure the service continuity? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. The system can use intelligent risk identification to recognize the potential faults and automatically prevent faults, and it can do the following: 1. Prevent potential risks and analyze the specification-related risks including capacity, links, signaling storm, and DR. 2. Analyze the cause of risk and provide the recommended measures automatically.	The system can perform automatic risk identification, which requires manual confirmation, to recognize the potential faults and prevent faults, and it can do the following: 1. Prevent potential risk and analyze the specification-related risks, including capacity and links.	The system can use risk identification, which provides an automatic check list and requires periodically manual confirmation about the potential risks in this check list, to recognize the potential faults and prevent faults, and it can do the following: 1. Prevent potential risk and analyze the specification-related risks including capacity.	Not supported

Evidence

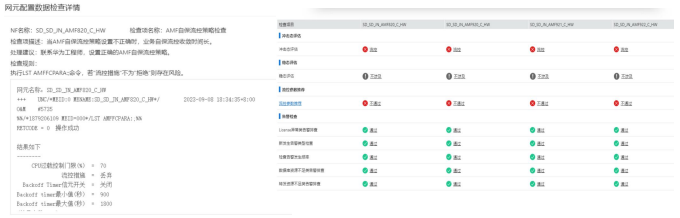
Capability Introduction: The system supports risk identification based on golden service KPIs, 5GC/vIMS prediction and prevention, and signaling storm detection. Based on identified risks, the system diagnoses risks based on CHR data and provides risk rectification suggestions.
Self-assessed Capability: Option A

Prediction and prevention risk identification

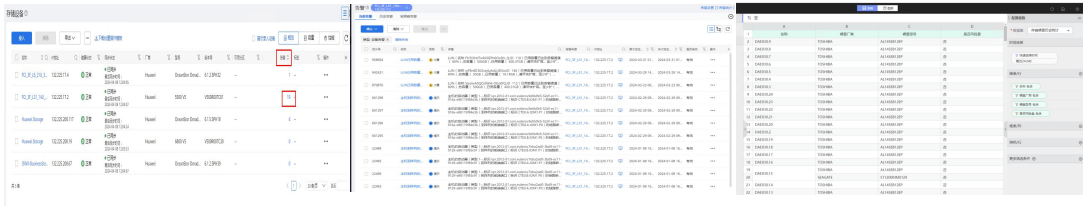
Signaling storm detection

Potential capacity identification

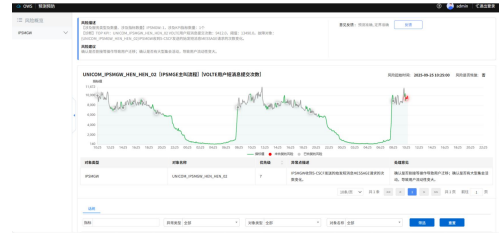
Link risk identification



Disaster recovery risk identification



Hardware risk identification (DC disk)



Provide handling suggestions

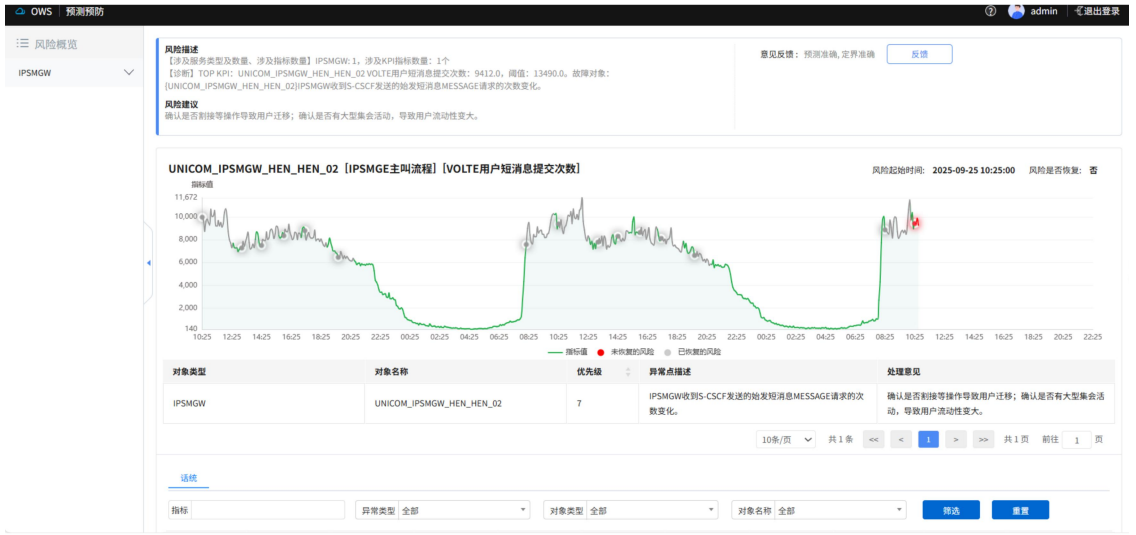
Question 7 Service Degradation Recovery

Service Capability	Weight	Question	Option A	Option B	Option C	Option D
Service degradation recovery	15%	Does your system support automatic detection and recovery from service degradation related to core network NEs/NFs? Core network NEs or NFs for assessment: core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)	Yes. When abnormal situations (for example, CPU overload, interconnection issues, and slight service damage) occur without any fault alarms generated (for example, the heartbeat is normal), the system supports automatic detection and diagnosis of service degradation, provides recovery recommendations, and enables autonomous execution without human intervention.	When abnormal situations (for example, CPU overload, interconnection issues, and slight service damage) occur without any fault alarms generated (for example, the heartbeat is normal), the system supports automatic detection and diagnosis of service degradation, provides recovery recommendations, and supports manual recovery.	When abnormal situations (for example, CPU overload, interconnection issues, and slight service damage) occur without any fault alarms generated (for example, the heartbeat is normal), the system supports automatic detection of service degradation.	Not supported.

Evidence

Capability Introduction: Leveraging big data AI learning and modeling, this capability enables proactive risk prediction and prevention for China Unicom's 5GC/vIMS networks. It establishes dynamic threshold models and performs real-time comparisons with call detail records (CDR) collected online to identify potential risks. Through a business rules engine, it automatically executes fault localization and root cause analysis procedures by integrating real-time operational data—including CDR, CHR, alarms, configurations, and logs—delivering analytical results and recovery recommendations.
Self-assessed Capability: Option B

Prediction and prevention risk identification



Provide handling suggestions

中国联通
China unicom

THANK YOU!