stc ANL Core Network Reliability Evidence

Overall scoring

1. Core Network Fault Management

				Evaluation	
High-Value Scenario	**Cognitive Activity (AADE)**	**Service Capability**	**Weight**	Equipment	Communication and Quality of service
Core Network - Fault Mgmt.	**Awareness**	Data collection Alarm correlation	10%	A	A
	Analysis	Fault identification	10%	A	A
		Risk prediction	10%	A	A
		Demarcation	15%	A	A
		Locating	15%	A	A
	Decision	Failure recovery solution generation	10%	A	A
		Solution pre-verification	10%	B	A
	Executions	Solution implementation	10%	B	B
		Service verification	10%	A	A
				3.63	

2. Core Network Stability

				Evaluation
High-Value Scenario	**Cognitive Activity**	**Service Capability**	**Weight**	**stc**
Core Network - Stability	**Basic stability**	Stable deployment architecture	10%	B
		Control plane disaster recovery	15%	A
		User-plane disaster recovery	15%	A
		Infrastructure disaster recovery	15%	B
		Anti-signaling surge capability	15%	A
	Intelligent stability	Risk prediction	15%	A
		Service degradation recovery	15%	B
				3.6

Data Collection/Alarm Correlation

Question:

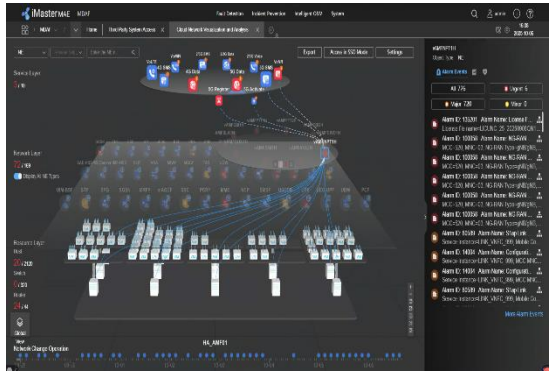
Capability or Task	Weight	Questions
Data collection Alarm correlation	10%	Does your system automatically collect data? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

Options:

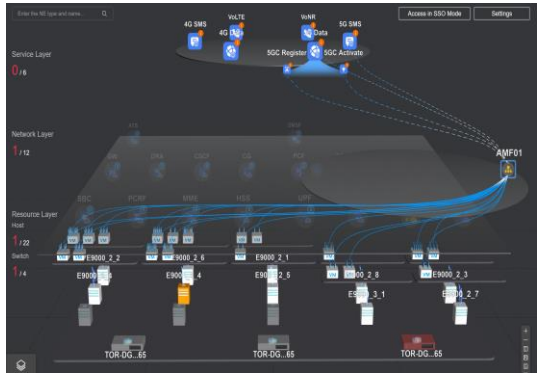
✓ Option A	Option B	Option C
Yes. The system can automatically collect data (alarms, configuration data, and performance data etc.) and sort alarms. The data should be at the module level, including NF modules, cloud OS (VMs or pods), hardware (hosts and ports), detected KPIs indicating slight service 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 VNF level and cloud OS (VMs or pods).	No. The system supports manual data collection.

Evidence:

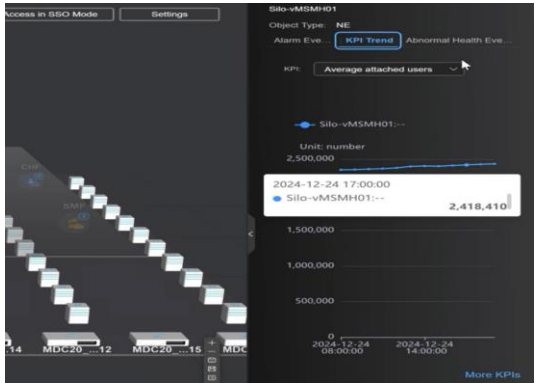
This question evaluates whether the core network Fault management system can automatically collect network data and the detailed level of the collected data.
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):



NF modules, cloud OS (VMs or pods)



infrastructure-layer hardware data (servers, storage devices, EOR/TOR devices and IP core).



KPI, alram

Fault identification

Question:

Capability or Task	Weight	Questions
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 VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs) 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.

Options:

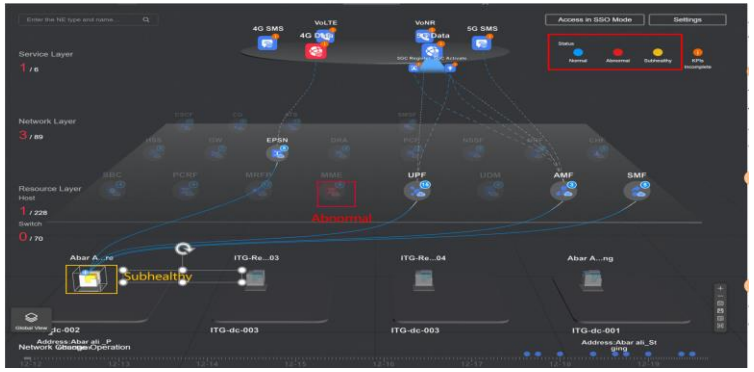
✓ Option A	Option B	Option C
The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault Mgmt. supports visualization of the following management capabilities in one view of VNFs/NFs and the telecom cloud. 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF 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 Mgmt. supports visualization of the following management capabilities: 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF 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.

Fault identification

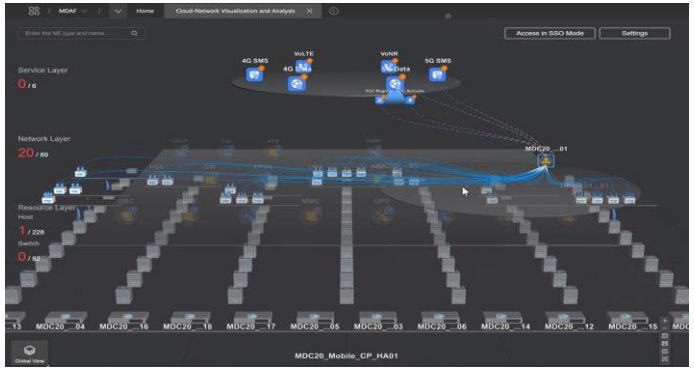
Evidence: This question evaluates whether the core network Fault Mgmt. system can identify faults and visualize device health status
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

Example evidence for option A (support by MDAF, cover all the Equipment and Communication and Quality of service**):**

VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization

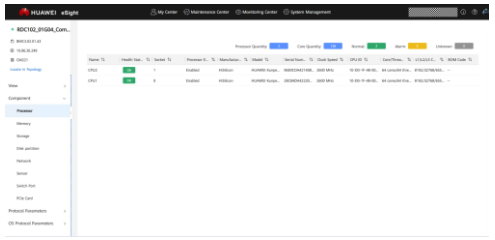


VNF health status visualization

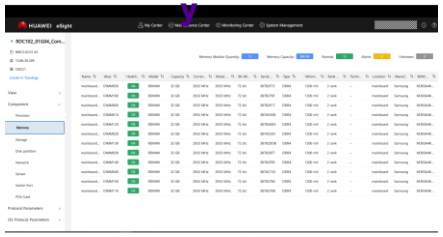


Visualized status (faulty or normal) of VMs and pods in the telecom cloud.

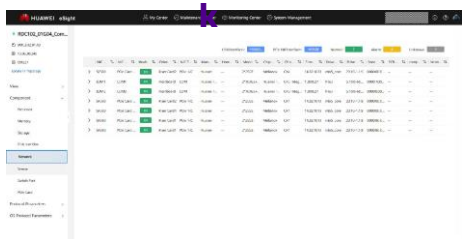
CPU



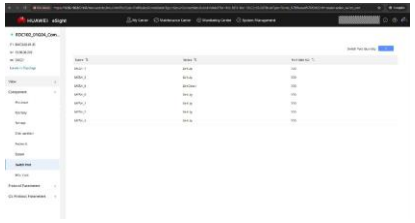
Memory



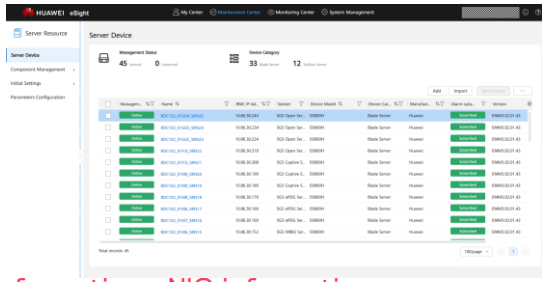
network



Switch port



Server



Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information. vNIC information and rack information can be get via eSight

Risk prediction

Question:

Capability or Task	Weight	Questions
Risk prediction	10%	Does your system automatically detect and prevent risks of VNF faults? Assessment object: management entities Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

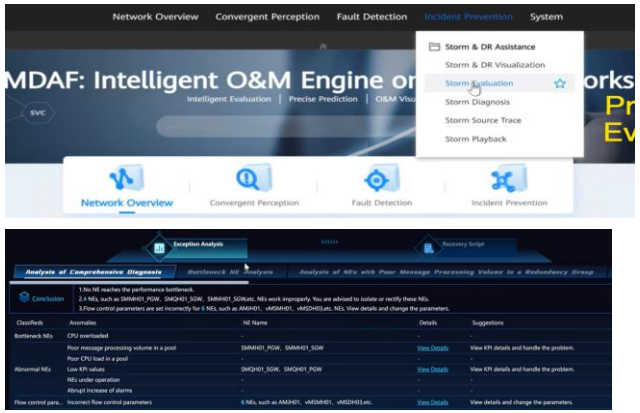
Options:

✓ Option A	Option B	Option C	Option D
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.

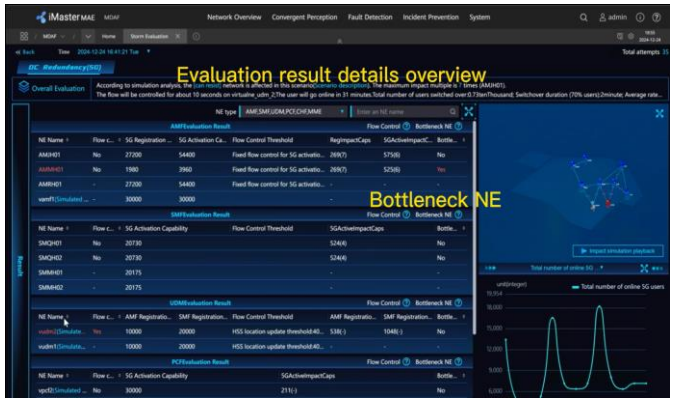
Risk prediction

Evidence: This question evaluates whether the core network Fault Mgmt. system can identify potential faults and prevent faults
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

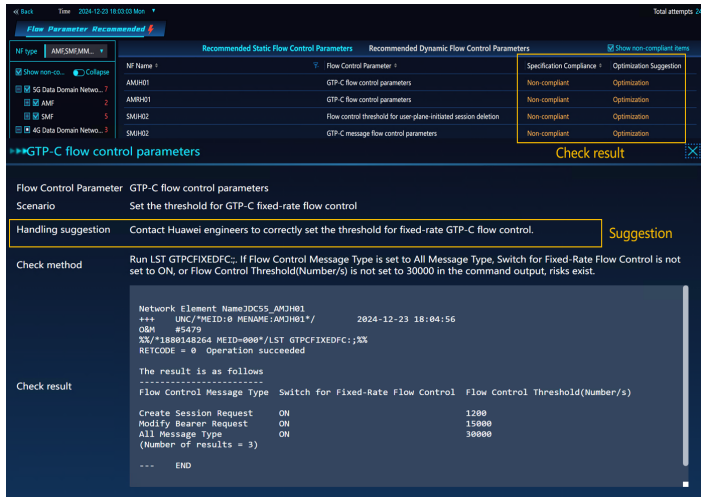
Example evidence for option A (support by MDAF, cover all the Equipment and Communication and Quality of service)**:**



Impact simulation in typical fault, emergency drill, holiday assurance, and signaling storm scenarios is supported to intelligently identify potential network risks in advance(based on capacity, links, signaling storms, DR, and hardware.



Network bottlenecks in switchover scenarios, as well as bottleneck VNFs and flow-controlled VNFs are identified in advance, and signaling storms and DR risks are prevented.



Optimal flow control parameters are recommended flow control specifications and AI algorithms to prevent signaling storms.

Demarcation

Question:

Capability or Task	Weight	Questions
Demarcation	15%	Does your system support automatic demarcation of core network faults? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs and IMS VNFs)

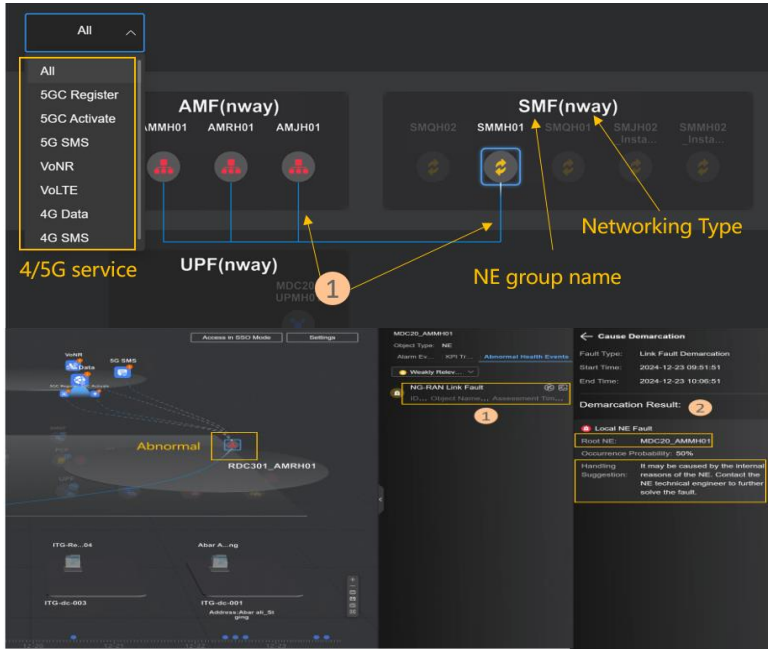
Options:

✓ Option A	Option B	Option C	Option D
Yes. The intelligent system supports automatic fault demarcation without manual intervention (e.g., core network VNFs 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 VNFs 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 VNFs 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.

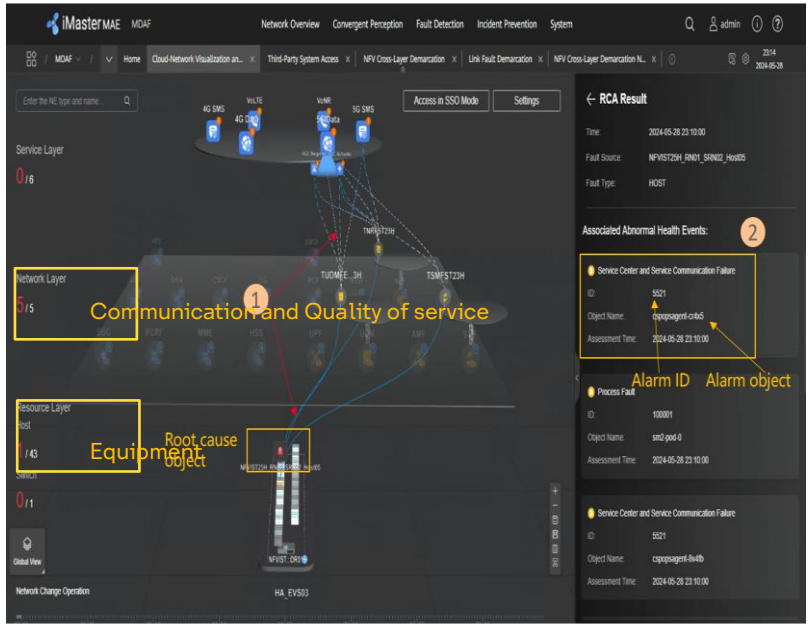
Demarcation

Evidence: This question evaluates whether the automatic core network fault demarcation and locating capabilities are developed
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

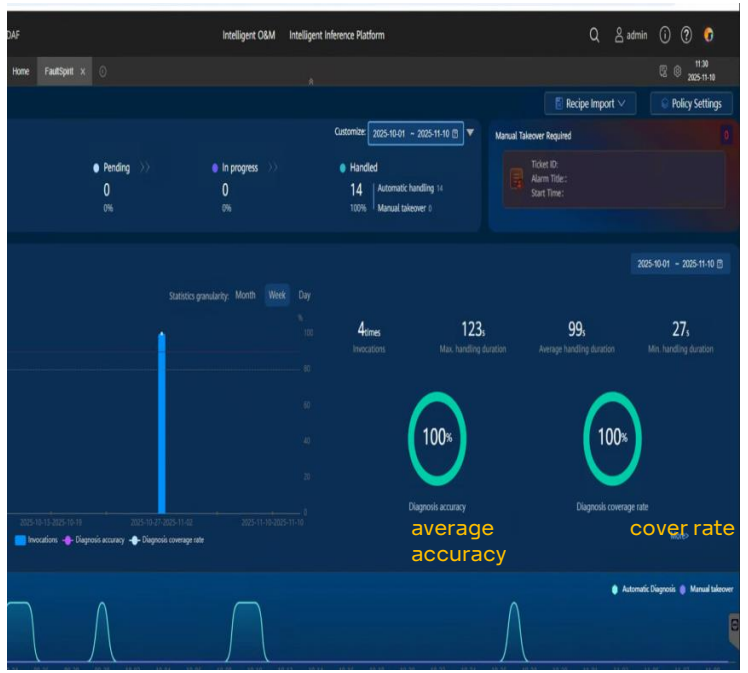
Example evidence for option A (support by MDAF, cover all the Equipment and Communication and Quality of service**):**



Horizontal demarcation for VNFs in the core network domain.



Faults are automatically analyzed based on multi-source data, and Demarcation between VNFs and vertical demarcation for the telecom cloud



Automatic fault demarcation covering 95% or higher of faults. The average accuracy per month is above 90%.

Locating

Question:

Capability or Task	Weight	Questions
Locating	15%	Does your system support automatic locating related to core network Fault Mgmt.? Assessment object: the core network management function and network function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

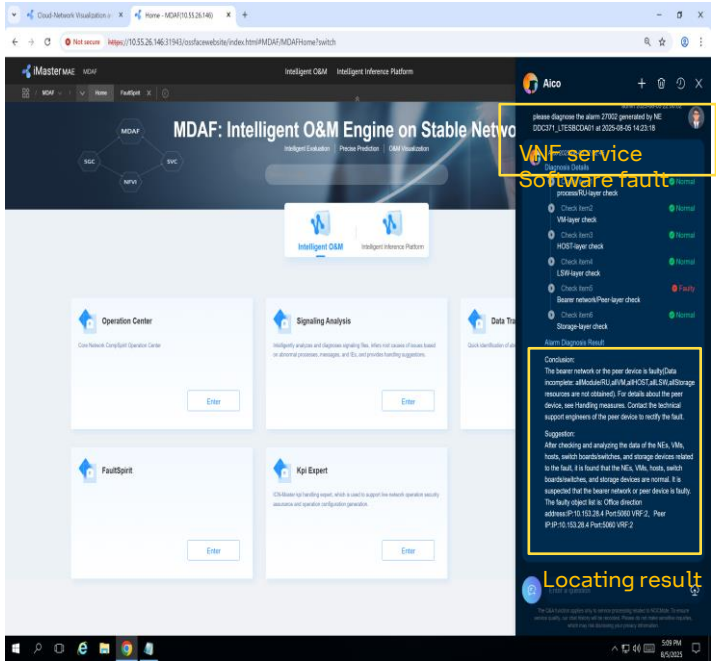
Options:

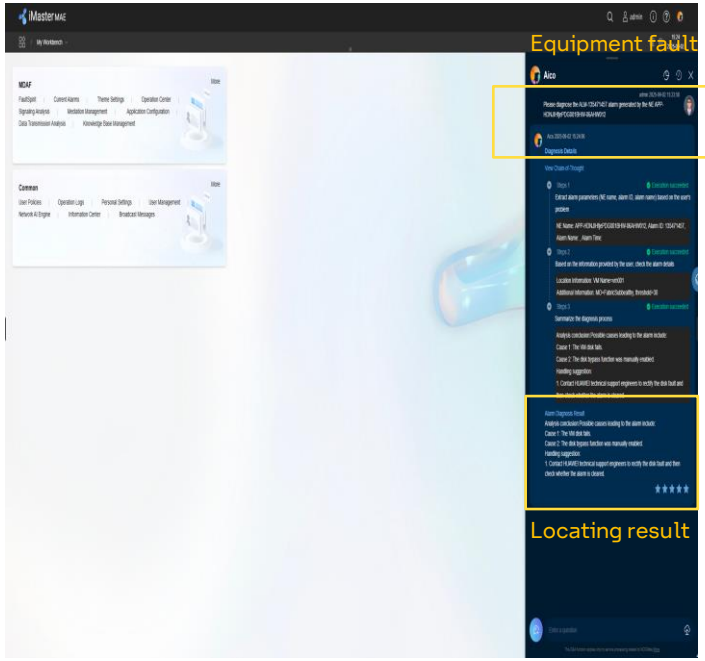
✓ Option A	Option B	Option C	Option D
Yes. Intelligent fault diagnosis is capable of automatically providing precise locating (e.g., detailed causes of identified faults, including minimum units, software modules, and ports) of faults, covering 95% or higher of live network faults without human intervention. 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.

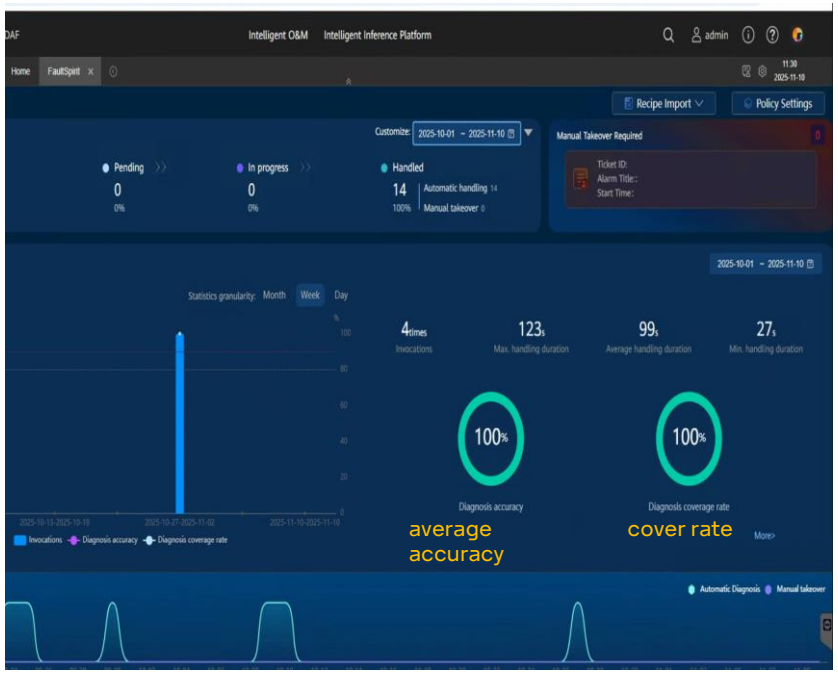
Locating

Evidence: This question evaluates whether the automatic core network fault location and demarcation capabilities are developed
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

Example evidence for option A (support by MDAF, cover all the Equipment and Communication and Quality of service**):**







Intelligent fault diagnosis can automatically provide information about accurate fault locations faults (only for the alarms after aggregation and alarms generated based on KPI monitoring) (The average monthly accuracy exceeds 95%.)

Fault rectification solution generation

Question:

Capability or Task	Weight	Questions
Fault rectification solution generation	10%	Does your system automatically generate the fault rectification solution? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

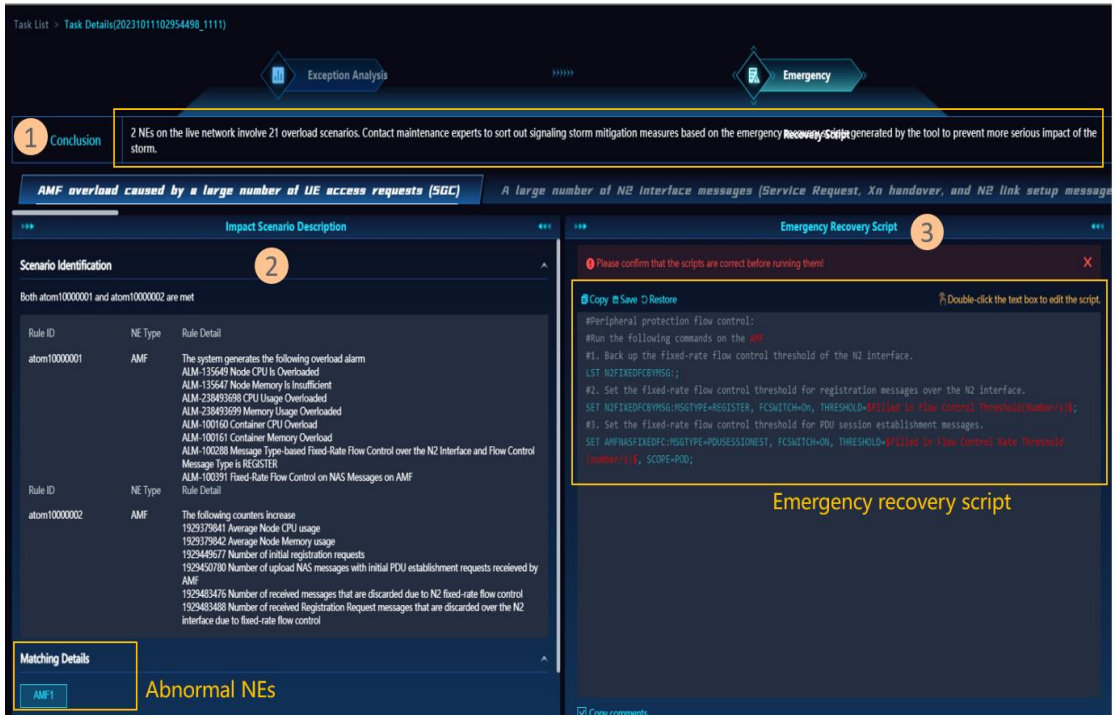
Options:

✓ Option A	Option B	Option C	Option D
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.

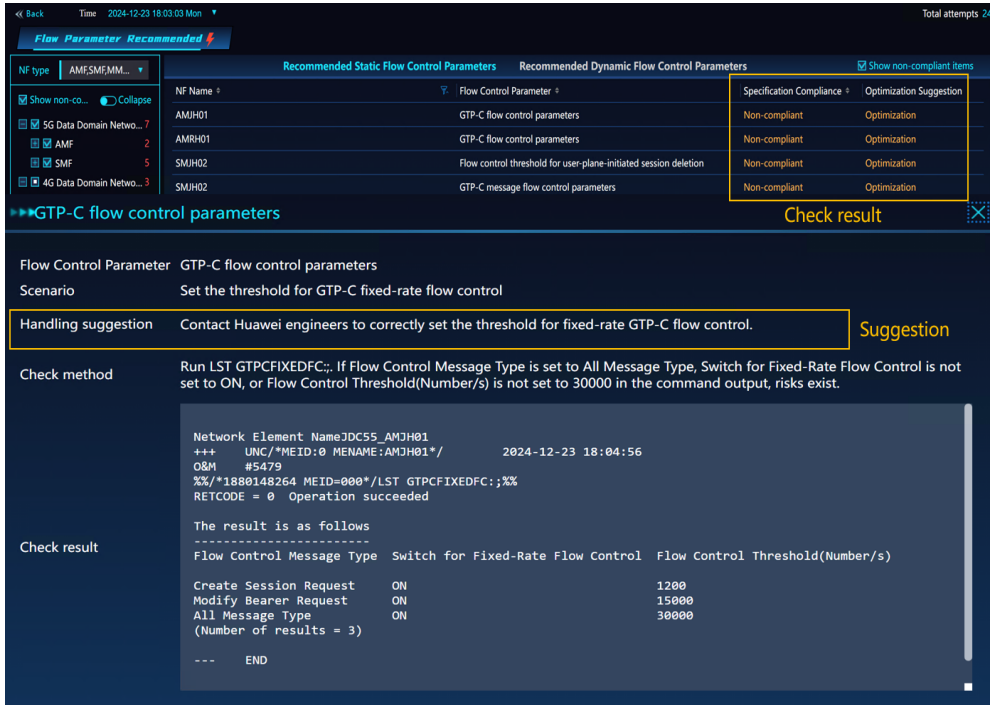
Fault rectification solution generation

Evidence: This question evaluates whether the core network Fault Mgmt. system can automatically generate fault rectification solutions. Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

Example evidence for option A (support by MDAF, cover all the Equipment and Communication and Quality of service**):**



Emergency rectification scripts are automatically generated after signaling storm exception analysis.
Providing a DR solution in case of accidents or natural disasters.



System can generate optimization to network for failure (e.g., signaling storm etc.) automatically.

Solution pre-verification

Question:

Capability or Task	Weight	Questions
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 VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

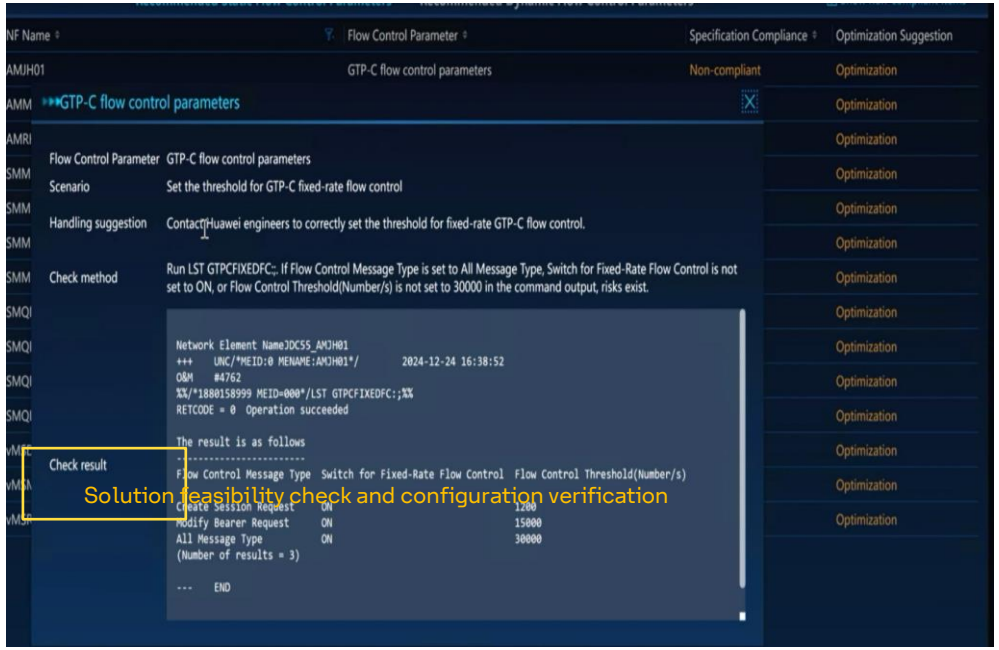
Options:

✓ Option A	Option B ✓	Option C	Option D
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.

Solution pre-verification

Evidence: This question evaluates whether the core network Fault Mgmt. system supports automatic evaluation and verification on the feasibility of fault rectification sc
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

Example evidence for option A (support by MDAF, cover all the Equipment and Communication and Quality of service**):**



The construction of network impact models is supported to digitally simulate the actual impact scenarios on the live network, generate simulation results, and optimize the result comparison in a visualized manner based on various flow control parameters， the system support automatic decision-making.

Solution Implementation

Question:

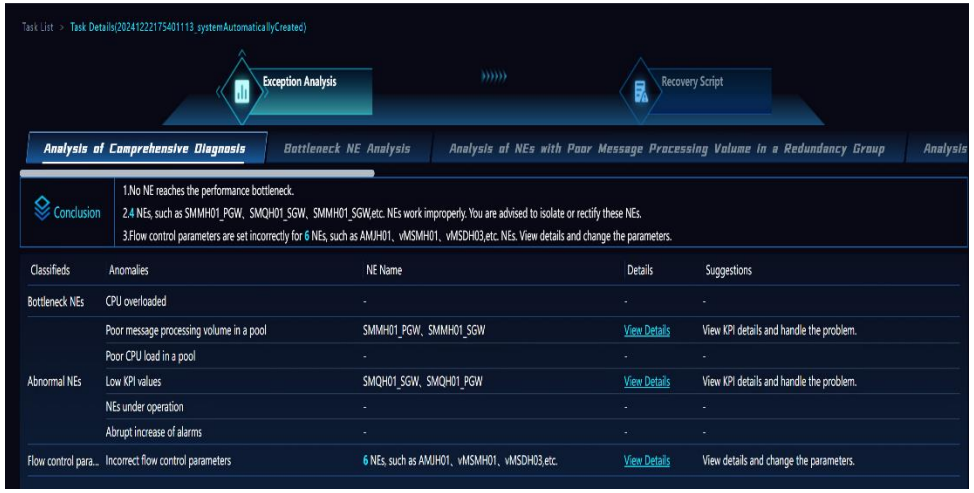
Capability or Task	Weight	Questions
Solution implementation	10%	Does your system support automatic fault rectification? Assessment object: the core network management function and network element Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs).

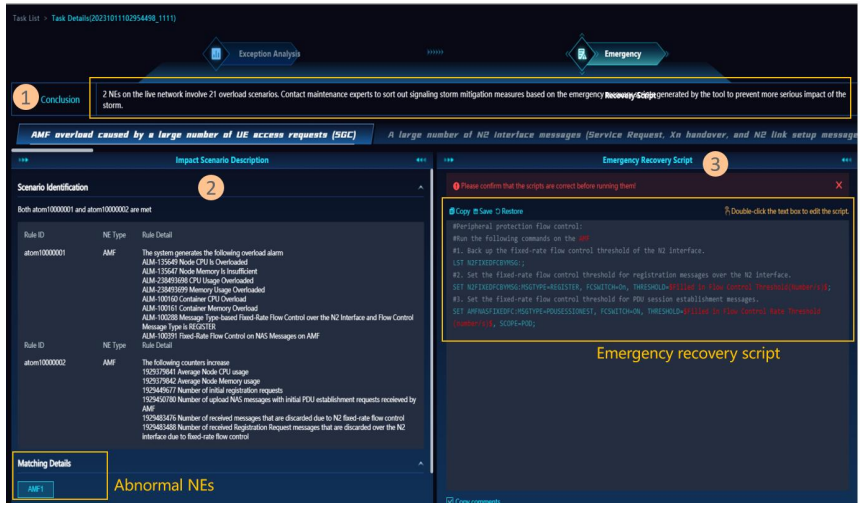
Options:

Option A	✓ Option B
Yes. The system can support automatic fault rectification in all fault rectification scenarios.	The system supports fault rectification after manual confirmation.

Evidence:

This question evaluates whether the core network Fault Mgmt. system supports automatic fault rectification in various scenarios.
Evidence for option A (support by MDAF, cover the Equipment part):





Reason why criteria in option A are not met for communication and Quality of service part : The simulation system does not support the auto implementation.

Service Verification

Question:

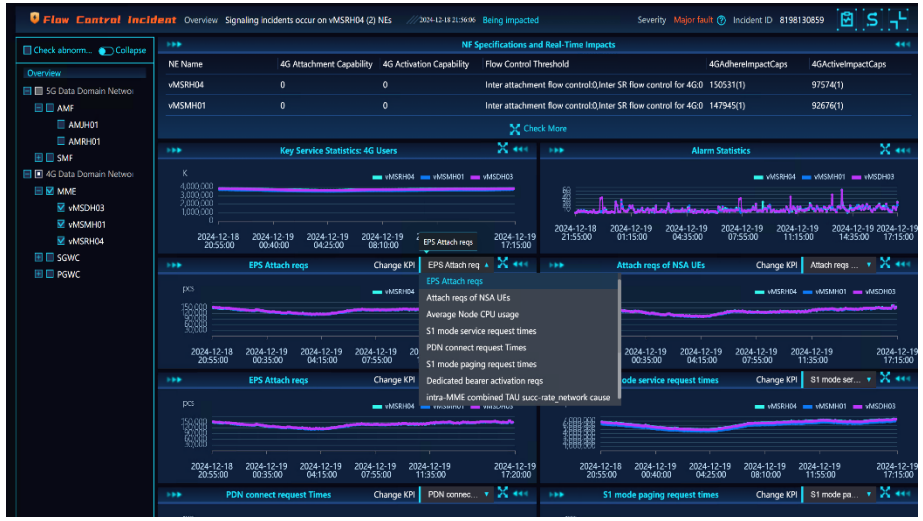
Capability or Task	Weight	Questions
Service verification	10%	Does your system support automatic service verification after faults on core networks are rectified? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

Options:

✓ Option A	Option B	Option C
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:

This question evaluates whether the core network Fault Mgmt. system supports automatic service verification after fault rectification..
Evidence for option A (support by MDAF, cover all the Equipment and the Communication and Quality of service):



DR attendance in switchover scenarios is supported to display VNF KPI changes in a visualized manner to ensure that services are restored properly.

Stable deployment architecture

Question: **Does the core network deployment architecture have a capability for redundancy modules to take over the services carried by faulty modules?**

NOTE:
- There are service processing modules, LB load sharing modules, and service data modules.

Scoring guide:
- Check whether the core network has the stable deployment architecture considered in the case of network planning

Assessment core network NE:
- 5GC NFs, EPC NEs, IMS NEs

Required evidence:
- Provide core network deployment architecture related evidence (NE service module N-Way, Distributed LB)

Options:

Option A	Option B	Option C	Option D
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 Support

Stable deployment architecture

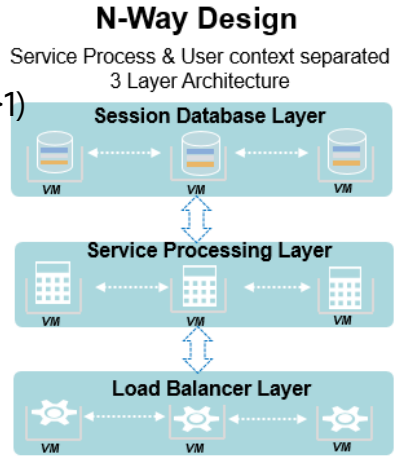
Evidence 1:

1. NE service module N-Way, by using typical N+M backup (M>1)

```
LST LICENSESWITCH:LICITEM="LKV3G5SURD01";
RDC301_UPRH01
+++    UDG/*MEID:0 MENAME:UPRH01*/        2024-04-20 14:50:24+3:00
O&M    #2737
%%/*1880004468 MEID=000*/LST LICENSESWITCH: LICITEM="LKV3G5SURD01";%%
RETCODE = 0  Operation succeeded

The result is as follows
------------------------
License Item  =  LKV3G5SURD01
License Name  =  Service Processing Unit Reliability Definition Basic Function
     Switch   =  ENABLE
(Number of results = 1)

---    END
```



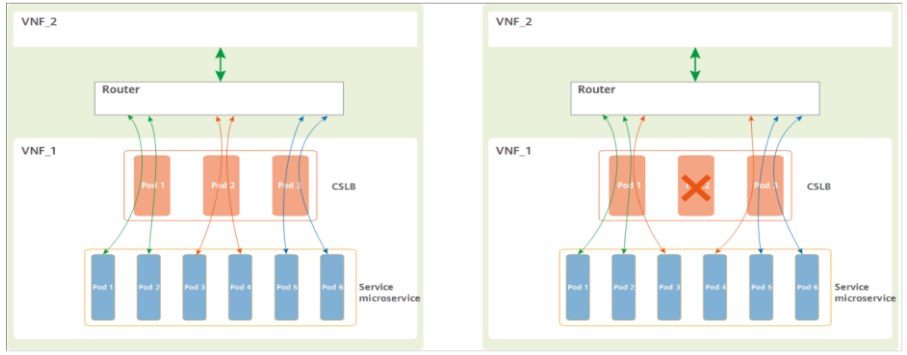

```
+++    UDG/*MEID:0 MENAME:UPRH01*/        2024-04-20 14:52:03+3:00
O&M    #2742
%%/*1880004470 MEID=000*/DSP NODE: APPID=0;%%
RETCODE = 0  Operation succeeded

The result is as follows
------------------------
ME ID  Vdu Type   Node Name       Node IP         VM Name                 Host Name                Operating Status  Management Status

0      ISU_C48_M  192.168.36.99   192.168.36.99   UPRH01_ISU_C48_M__3     RDC301_02D07_Compute028  Normal            Active
0      OMU_L1     192.168.35.162  192.168.35.162  UPRH01_OMU_L1__0        RDC301_02D07_Compute028  Normal            Active
0      PBU_A      192.168.35.193  192.168.35.193  UPRH01_PBU_A__1         RDC301_02D07_Compute028  Normal            Active
0      PBU_B      192.168.35.232  192.168.35.232  UPRH01_PBU_B__2         RDC301_02D07_Compute028  Normal            Active
0      PBU_P-L    192.168.32.91   192.168.32.91   UPRH01_PBU_P-L__4       RDC301_02D07_Compute028  Normal            Active
0      PBU_P-L    192.168.35.168  192.168.35.168  UPRH01_PBU_P-L__5       RDC301_02D07_Compute028  Normal            Active
0      PBU_P-M1   192.168.34.61   192.168.34.61   UPRH01_PBU_P-M1__0      RDC301_02D07_Compute028  Normal            Active
0      SDU        192.168.32.252  192.168.32.252  UPRH01_SDU__1           RDC301_02D07_Compute028  Normal            Active
0      OMU_L1     192.168.33.190  192.168.33.190  UPRH01_OMU_L1__1        RDC301_02D07_Compute029  Normal            Active
0      OMU        192.168.36.67   192.168.36.67   UPRH01_OMU__1           RDC301_02D07_Compute029  Normal            Active
0      PBU_A      192.168.33.212  192.168.33.212  UPRH01_PBU_A__0         RDC301_02D07_Compute029  Normal            Active
0      PBU_B      192.168.32.242  192.168.32.242  UPRH01_PBU_B__1         RDC301_02D07_Compute029  Normal            Active
0      PBU_P-L    192.168.34.30   192.168.34.30   UPRH01_PBU_P-L__1       RDC301_02D07_Compute029  Normal            Active
0      PBU_P-L    192.168.32.135  192.168.32.135  UPRH01_PBU_P-L__2       RDC301_02D07_Compute029  Normal            Active
0      SDU        192.168.32.73   192.168.32.73   UPRH01_SDU__0           RDC301_02D07_Compute029  Normal            Active
0      ISU_C48_M  192.168.33.221  192.168.33.221  UPRH01_ISU_C48_M__0     RDC301_02D07_Compute030  Normal            Active
0      PBU_A      192.168.35.26   192.168.35.26   UPRH01_PBU_A__2         RDC301_02D07_Compute030  Normal            Active
0      PBU_P-L    192.168.35.237  192.168.35.237  UPRH01_PBU_P-L__0       RDC301_02D07_Compute030  Normal            Active
0      PBU_P-L    192.168.34.57   192.168.34.57   UPRH01_PBU_P-L__6       RDC301_02D07_Compute030  Normal            Active
0      SDU        192.168.35.40   192.168.35.40   UPRH01_SDU__4           RDC301_02D07_Compute030  Normal            Active
0      ISU_C48_M  192.168.34.44   192.168.34.44   UPRH01_ISU_C48_M__13    RDC301_02D07_Compute031  Normal            Active
0      OMU        192.168.36.208  192.168.36.208  UPRH01_OMU__0           RDC301_02D07_Compute031  Normal            Active
0      PBU_B      192.168.33.55   192.168.33.55   UPRH01_PBU_B__0         RDC301_02D07_Compute031  Normal            Active
0      PBU_P-L    192.168.36.126  192.168.36.126  UPRH01_PBU_P-L__7       RDC301_02D07_Compute031  Normal            Active
0      PBU_P-M1   192.168.35.6    192.168.35.6    UPRH01_PBU_P-M1__1      RDC301_02D07_Compute031  Normal            Active
0      SDU        192.168.35.79   192.168.35.79   UPRH01_SDU__2           RDC301_02D07_Compute031  Normal            Active
```

Evidence 2:

Distributed LB




```
DSP POD:
RDC301_UPRH01
+++    UDG/*MEID:0 MENAME:UPRH01*/        2024-04-20 14:51:33+3:00
O&M    #2740
%%/*1880004469 MEID=000*/DSP POD:;%%
RETCODE = 0  Operation succeeded

The result is as follows
------------------------
Pod Name                                Pod Type          Pod Status  Node Name       Host Name                Pod Running Duration

acs-pod-0                               acs-pod           Running     192.168.36.67   RDC301_02D07_Compute029  243d
acs-pod-1                               acs-pod           Running     192.168.36.208  RDC301_02D07_Compute031  243d
auditlog-676f755476-486qx               auditlog          Running     192.168.36.67   RDC301_02D07_Compute029  26d
auditlog-676f755476-4rmgc               auditlog          Running     192.168.36.208  RDC301_02D07_Compute031  26d
backupmgr-754768b657-cjmgk              backupmgr         Running     192.168.36.67   RDC301_02D07_Compute029  26d
backupmgr-754768b657-x5dz4              backupmgr         Running     192.168.36.208  RDC301_02D07_Compute031  26d
certmgr-6c4dc796d4-2zs94                certmgr           Running     192.168.36.67   RDC301_02D07_Compute029  26d
certmgr-6c4dc796d4-5n8gg                certmgr           Running     192.168.36.208  RDC301_02D07_Compute031  26d
collectandcheck-6cbc75db9c-bmvhq        collectandcheck   Running     192.168.36.67   RDC301_02D07_Compute029  26d
collectandcheck-6cbc75db9c-qj8rn        collectandcheck   Running     192.168.36.208  RDC301_02D07_Compute031  26d
cpm-pod-684c44d5d6-8bmx7                cpm-pod           Running     192.168.35.193  RDC301_02D07_Compute028  243d
cpm-pod-684c44d5d6-q4g29                cpm-pod           Running     192.168.33.212  RDC301_02D07_Compute029  243d
cpm-pod-684c44d5d6-q9phr                cpm-pod           Running     192.168.35.26   RDC301_02D07_Compute030  243d
csdb-pod-0                              csdb-pod          Running     192.168.32.73   RDC301_02D07_Compute029  243d
csdb-pod-1                              csdb-pod          Running     192.168.32.252  RDC301_02D07_Compute028  243d
csdb-pod-2                              csdb-pod          Running     192.168.35.79   RDC301_02D07_Compute031  243d
csdb-pod-3                              csdb-pod          Running     192.168.35.40   RDC301_02D07_Compute030  243d
csdb-pod-4                              csdb-pod          Running     192.168.36.155  RDC301_02D07_Compute037  243d
csdb2-pod-0                             csdb2-pod         Running     192.168.34.61   RDC301_02D07_Compute028  243d
csdb2-pod-1                             csdb2-pod         Running     192.168.35.6    RDC301_02D07_Compute031  243d
csdbom-pod-0                            csdbom-pod        Running     192.168.36.67   RDC301_02D07_Compute029  243d
csdbom-pod-1                            csdbom-pod        Running     192.168.36.208  RDC301_02D07_Compute031  243d
```

The LB and DB on the live network are deployed in distributed mode, which minimizes the impacts of redundancy takeover on communication services.

Control plane disaster recovery Capability

Question: **Does your system support automatic control-plane DR for DR NEs to take over communication services without service interruption?**

Scoring guide:
- Check whether the core network has the Control-plane disaster recovery (DR) capability requirement considered in the case of network planning

Assessment core network NE:
- Core network NEs (e.g., 5GC Control-plane NFs (AMF, SMF, PCF, UDM, NRF, SCP etc.), EPC NEs (SGW, MME, etc.), IMS NEs)

Required evidence:
- Provide Control Plane NE disaster recovery deployment related evidence (Three-Level Reliability Design, Hot Backup, MME Chain Redundancy, UDM 3 Sites Redundancy)

Options:

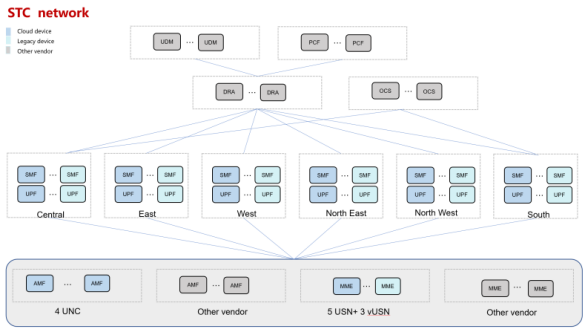
Option A ✓	Option B	Option C	Option D
Yes. The control-plane DR NEs and DR DCs can take over all services based on the following DR scenarios in minutes and UEs remain connected. 1. When an accident or natural disaster occurs, core network NEs can switch over services across DCs and the backup NEs can 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.

Three-Level Reliability Design, Implementing Service Restoration Upon VNF Faults

Evidence 1:

Spanning 9 DCs across 6 regions, it supports diverse services and cutting-edge technologies

stc network(Pool)



DR evaluate

Control-plane VNFs on the live network are pooled for DR, and DC DR is implemented physically. If an accident occurs, core network VNFs can switch over services across DCs, and the backup VNFs can take over all services successfully. — Support 1 and Support 2

Evidence 3:

Control-plane VNF bypass.xlsx

Control-plane VNFs on the live network support bypass-based DR. If critical control-plane VNFs (UDM, PCF/PCRF, or OCS/CHF) are faulty, control-plane VNFs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). — Support 3

Evidence 4:

Management-pl
ıe VNF bypass.xl

Management-plane VNFs on the live network support bypass-based DR. If a management entity is faulty, control-plane VNFs can maintain subscribers' communication active for a period of time (hours or above). — Support 4

User-plane disaster recovery Capability

Question: **Does your system support automatic user-plane DR to take over all services without service interruption?**

NOTE:
- The user-plane DR scenario indicates that the backup UP NE (UPF) can take over the services in the fault scenario.

Scoring guide:
- Check whether the core network has the User-plane disaster recovery capability requirement considered in the case of network planning

Assessment core network NE:
- Core network NEs (e.g., 5GC NFs (UPF), EPC NEs (PGW), IMS NEs (SBC))

Required evidence:
- Provide User Plane NE disaster recovery deployment related evidence.

Options:

Option A ✓	Option B	Option C	Option D
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.

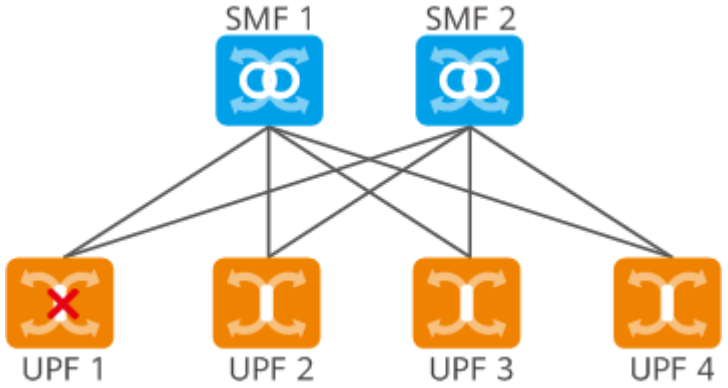
UPF Redundancy (Pool Redundancy)

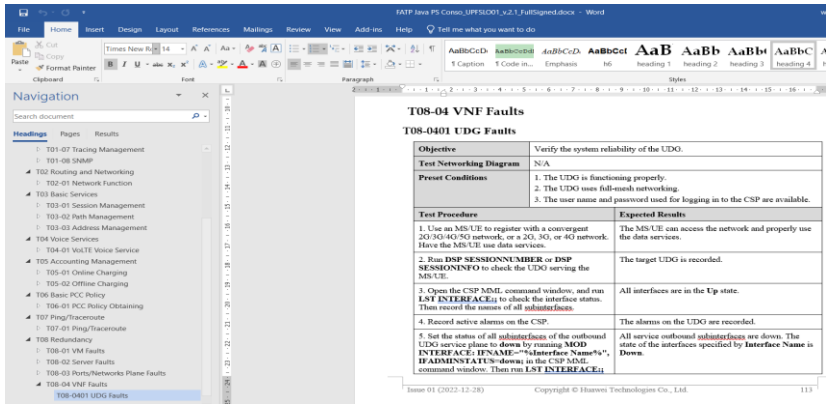
Evidence 1:

Full Mesh Networking

UPFs are pooled and fully meshed with SMFs. An SMF manages all UPFs, and a UPF belongs to all SMFs. If an SMF is faulty, it only affects the services of activated subscribers who access the network through the faulty SMF. If a UPF is faulty, only its services are affected. Homogeneous SMFs are used on the control plane, and each of them covers entire full mesh networking. UPFs are planned and deployed based on the scale of services and subscribers in the coverage area.

UPF Fault in Full Mesh Networking





Full-mesh networking for the UDG DR on the user plane

If all SMFs detect a UPF 1 fault through heartbeat messages over the N4 interface, they will deactivate the UEs on UPF 1. The SMF selects another available UPF when a UE needs to be re-activated.

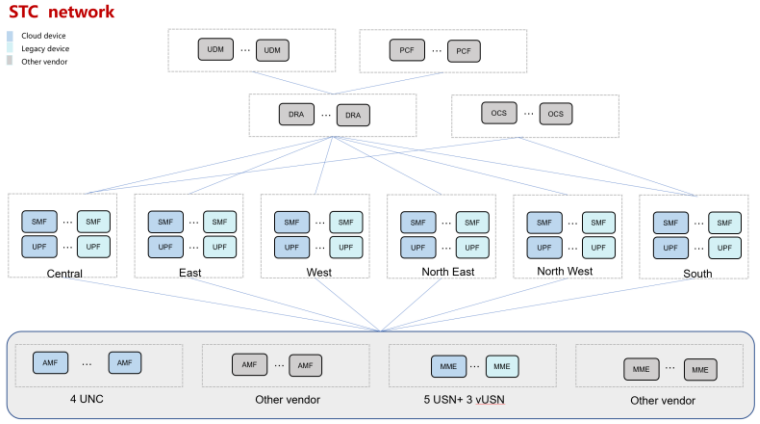
If SMFs detect no UPF 1 fault, they keep sending signaling messages to UPF 1. If they receive no response within the specified time, they will deactivate the UEs on UPF 1. The SMF selects another available UPF when a UE needs to be re-activated.

UPF Redundancy (Pool Redundancy)

Evidence 2:

Spanning 9 DCs across 6 regions, it supports diverse services and cutting-edge technologies

stc network(User plane Pool)



1. User-plane VNFs on the live network form a pool for redundancy. When an accident or natural disaster occurs, the user-plane VNF pool supports minute-level traffic switchover. -- Support 1
2. The user-plane VNF UDG is deployed in full-mesh redundancy mode. The user-plane DR VNF and DR DC can take over all services without interrupting services. -- Support 2 and 3
3. With the user-plane VNF bypass redundancy feature on the live network, the user-plane DR VNF and DR DC can take over all services without interruption. -- Support 2 and 3

Infrastructure disaster recovery

Question: **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.

Scoring guide:
- Check whether the core network has the Infrastructure disaster recovery capability requirement considered in the case of network planning

Assessment core network NE:
- Core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs)

Required evidence:
- Provide disaster recovery networking deployment capability related evidence.

Options:

Option A	✓ Option B	Option C	Option D
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

Storage Bypass: Ensure the Service Continuity

Evidence 1:

- stc 6 regional
- stc has seamless region-level disaster recovery design.

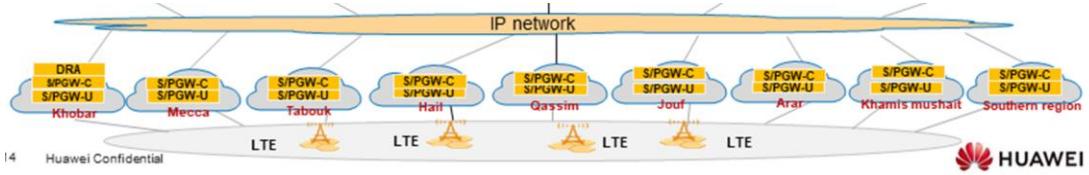
1The stc is a regional DC disaster recovery. When the DC transmission is faulty, the core network can provide communication in a local area (for example, within an area) within a period of time. - Support 1

Evidence 2:

Storage fault bypass.xlsx

With the bypass function enabled for core network infrastructure, core network VNFs can run for a period of time even if Telco Cloud infrastructure encounters a fault (for example, a storage fault). — Support 2

Evidence 3:



The stc user-plane devices support the CU separation feature. When a user-plane NE is faulty, the CU separation feature reduces the impact of the user-plane NE fault and reduces the affected area by user-plane NE switchover.
— — Support 3

Evidence 4:

Huawei 5G Core devices of Saudi Arabia stc are capable of EPS Fallback. When a 5G core network subdomain is faulty, UEs in this network can fall back, maintaining normal network connectivity for the UEs. — Support 4

Anti-signaling Surge Capability

Question:

Capability or Task	Weight	Questions
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 VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

Options:

✓ Option A	Option B	Option C	Option D
Yes. The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, VNFs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end VNFs 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 VNFs 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, VNFs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end VNFs can reduce the service requests delivered to back-end network elements, so the back-end VNF faults can be avoided. The system can converge signaling storm within 1 hour.	VNFs are capable to protect its processing capability.	Not supported

Anti-signaling Surge Capability

Evidence:

This question evaluates whether the capabilities for withstanding the signaling surge impact are supported on the core networks..
Evidence for option A(support by MDAF, cover all the Equipment and the Communication and Quality of service):

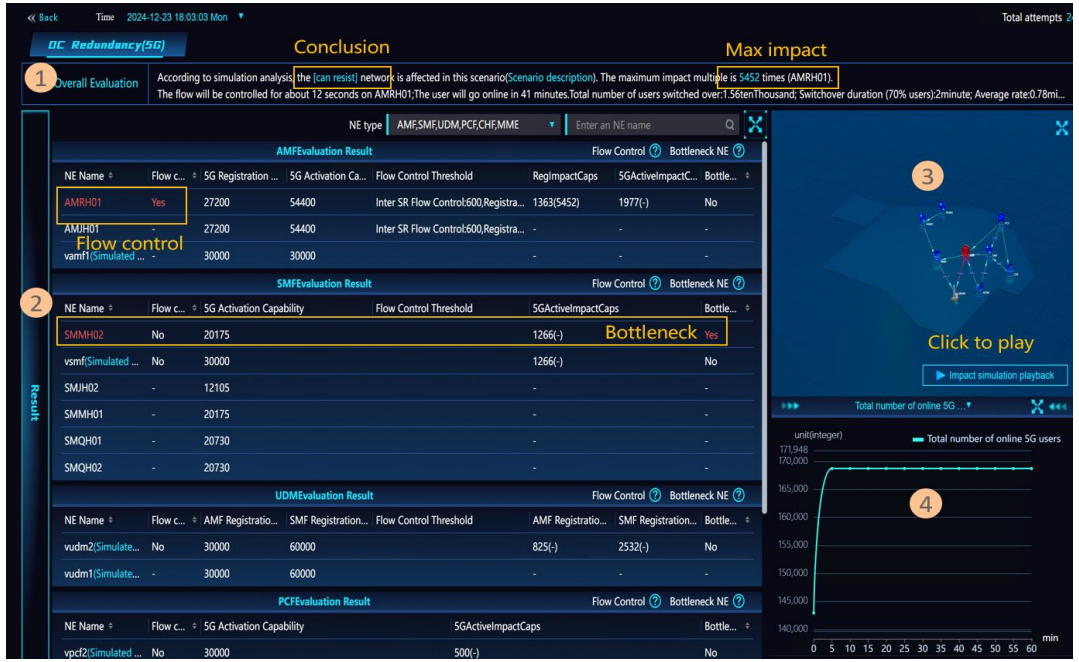
Example evidence for option A：

Peripheral VNFs are protected, HTR flow control configurations are queried or licenses are obtained in surge scenarios.

NE Flow Control Function

AMF HTR.docx

The flow control functions are supported for the VNFs on the live network



The construction of network impact models is supported to digitally simulate the actual impact scenarios on the live network, generate simulation results, and optimize the result comparison in a visualized manner based on various flow control parameters.

Risk prediction Capability

Awareness	Analysis	Decision	Executions	Basic Stability	Intelligent Stability

Question:

Capability or Task	Weight	Questions
Risk prediction	10%	Does your system automatically detect and prevent the risks of network VNF faults to ensure the service continuity? Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)

Options:

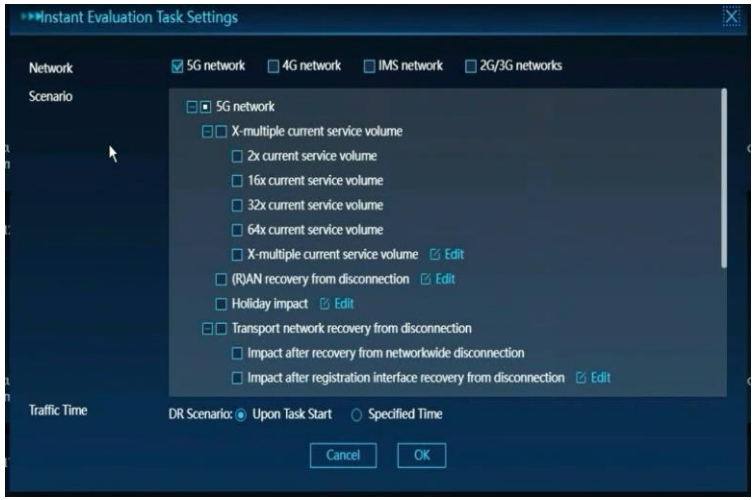
✓ Option A	Option B	Option C	Option D
Yes. The system can use intelligent risk identification to recognize the potential faults and automatically prevent faults, and it can do the following: 1. Prevent potential risks and analyze the specification-related risks including capacity, links, signaling storm, 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

Risk prediction Capability

Evidence: This question evaluates whether the VNF fault risk prediction capabilities of the core networks are developed.

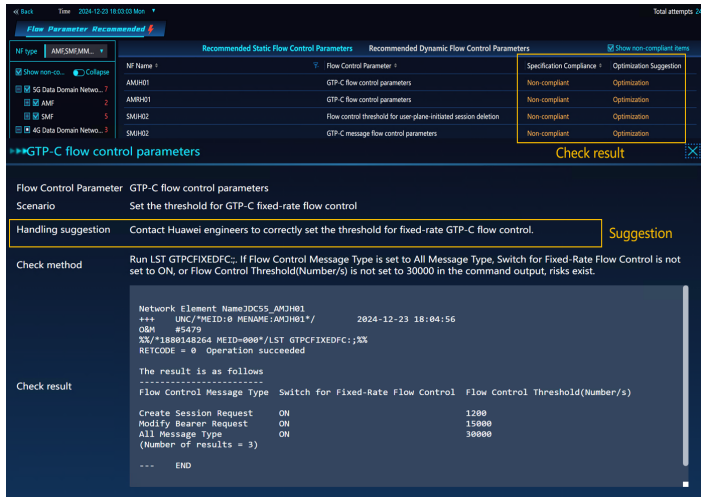
The core networks in Saudi stc automatically detect and prevent VNF fault risks, check potential risks, and analyze risks in terms of capacity, links, signaling storms, DR. Automatic risk cause analysis is carried out, and suggestions regarding the requirements of each scenario in option A are provided

Example evidence for option A :



Impact simulation is supported in typical fault, emergency drill, holiday assurance, and signaling storm scenarios to intelligently identify potential network risks in advance.

Network bottlenecks are identified in switchover scenarios in advance, bottleneck VNFs and flow-controlled VNFs are identified, and signaling storms and DR risks are prevented.



Optimal flow control parameters are recommended flow control specifications and AI algorithms to prevent signaling storms.

Service degradation recovery Capability

Question: **Does your system support automatic detection and recovery from service degradation related to core network NEs/NFs?**

Scoring guide:
- Check whether the core network has the service degradation recovery capability requirement considered in the case of network planning for Intelligent Stability purpose.

Assessment core network NE:
- Core network NEs (e.g., 5GC NFs, EPC NEs, and IMS NEs).

Required evidence:
- Provide evidence of the service degradation recovery capability.

Options:

Option A	✓ Option B	Option C	Option D
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.

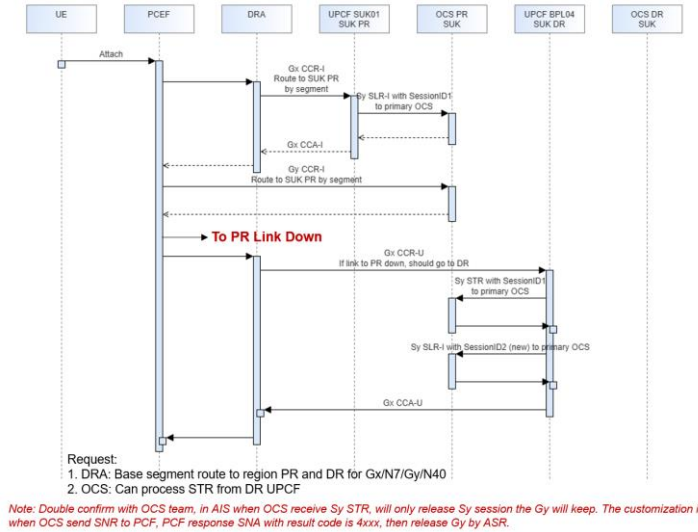
Service degradation recovery Capability

Evidence

The stc core network supports automatic detection of service deterioration related to core network NEs and NFs through the OWS system. (such as CPU overload, interconnection problems, and slight service loss) and automatic restoration after one-click restoration after manual confirmation, including the scenarios and functions required by option B.

Example of evidence for Option B:

Voice service session backup solution



5GC redundance and service fast recovery solution

5GC redundance service fast reco

1. The SmartCare supports network-wide service performance deterioration monitoring. The SmartCare provides recovery suggestions regardless of whether a fault alarm is generated. Manual recovery is supported. The value B is supported.

thank you!