GB1059D IP Network Fault Management Questionnaire Evidence

China Mobile Group Guangdong Co., Ltd.

2025.10

Proportion of tickets for each fault sub-scenario in Guangdong Mobile's IP/SPN network

Option	Fault Category	Sub-scenairos	Ticket Ratio
The IP/SPN network of Guangdong Mobile	Physical Port Failure	Sub-scenairo-4: Port Failure	59.20%
	Device Offline Failure	Sub-scenairo-2: Device Offline	20.78%
	Board Failure	Sub-scenairo-1: Hardware Failure	1.72%
	Optical Power Abnormal	Sub-scenairo-3: Optical Module Failure or Optical Power Abnormal	9.65%
	The Bit Error Rate Failure	Sub-scenairo-5: High Error Rate	1.57%
	Static L3VPN Service Failure	Sub-scenairo-8: VPN Interruption	1.14%
	Logical Port Failure	Sub-scenairo-4: Port Failure	1.03%
	Tunnel APS Protection Failure	Sub-scenairo-7: VPN Degradation	0.26%
	Optical Module Failure	Sub-scenairo-3: Optical Module Failure or Optical Power Abnormal	0.08%
	Fan Failure/Abnormal Temperature	Sub-scenairo-1: Hardware Failure	0.02%

The total number of tickets for these fault sub-scenarios accounts for over 90%.

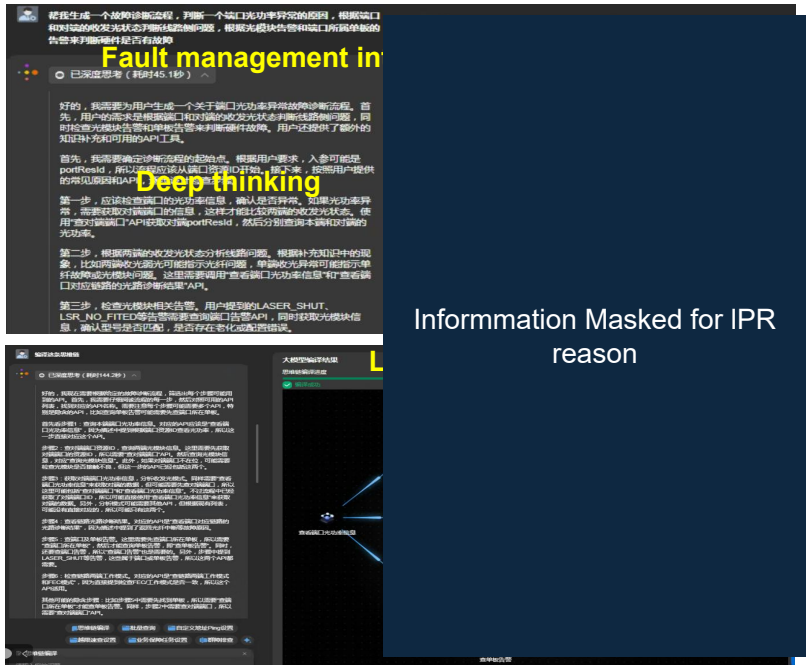
Cognitive Activity (IAADE)	Service Capability	Weight	Question	Answer								Final score
				Hardware Failure (should include but not limit to board failure, fan failure)	Device Offline	Optical Module Failure or Optical Power Abnormal	Port Failure	High Error Rate	Protocol State Abnormal (should include but not limit to IGP and BGP peer state abnormal, BFD session abnormal)	VPN Degradation	VPN Interruption	
				1.72%	20.78%	9.73%	59.20%	1.57%		0.26%	1.14%	
Intent	Fault management target formulation	10%	Does the system support automatic generation of fault management targets? Note: 1) Intent could be fault management requirements such as MTTR (mean time to repair) , troubleshooting priority (e.g., emergency restoration in highest priority), customized troubleshooting preference based on fault impact scope and severity, etc. 2) Fault management target include alarm severity, alarm threshold, alarm aggregation rules, fault notification rules, etc.	A	A	A	A	A	A	A	A	
Awareness	Data Collection	10%	Does the system support automatic collection and aggregation of fault-related indicators \? Note: 1) fault include device offline, physical port down, optical module failure, etc. 2) All types of faults memtioned in 1) and fault-related indicators memtioned in options should be covered when choosing a related option	A	A	A	A	A	A	A	A	
Analysis	Risk identification	10%	Does the system support automatic identification of risks? Note: 1) existing risks include ip configuration conflict, ACL redundancy, receiving frequency weak optical power, etc. 2) petential risks inculde abnormal memory usage of device, abnormal BGP route number, etc.	A	A	A	A	A	A	A	A	**4**
	Fault identification	10%	Does the system support automatic identification of risks? Note: 1) existing risks include ip configuration conflict, ACL redundancy, receiving frequency weak optical power, etc. 2) petential risks inculde abnormal memory usage of device, abnormal BGP route number, etc.	A	A	A	A	A	A	A	A	
	Demarcation of faults and risks	20%	Does the system support automatic demarcation of faults and risks?	A	A	A	A	A	A	A	A	
	Locating of faults and risks	15%	Does the system support automatic root cause analysis for network faults and risks?	A	A	A	A	A	A	A	A	
Decision	Generation and evaluation of solutions	15%	Does the system support automatic generation and evaluation of emergency restoration and repair solution? Note: 1) Emergency restoration solution may be compute alternative paths based on service SLA requirement. 2) Repair solution may be repair power supply.	A	A	A	A	A	A	A	A	
Execution	Execution and verification	10%	Does the system support automatic execution and verification?	A	A	A	A	A	A	A	A	

Fault management target formulation

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Fault management target formulation	10%	Does the system support automatic generation of fault management targets? Note: 1) Intent could be fault management requirements such as MTTR (mean time to repair) , troubleshooting priority (e.g., emergency restoration in highest priority), customized troubleshooting preference based on fault impact scope and severity, etc. 2) Fault management target include alarm severity, alarm threshold alarm aggregation rules, fault notification rules, etc	The system supports the input of fault management **intent by simplified human-system interaction** (e.g., nature language user interface provided by system), system automatically translates the intent into fault management targets .	The system supports manual configuration of fault management targets with **custom rule-based templates**. Manually adjustment and confirmation is needed.	The system generates fault management targets based on predefined template. Manually confirmation is needed.	Manually set fault management targets based on expertise(such as setting alarm severity and classification) .

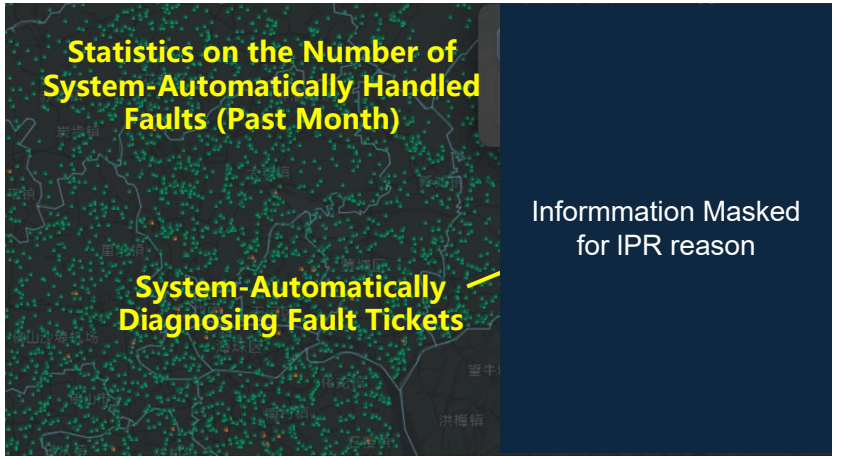
Example evidence for option A:

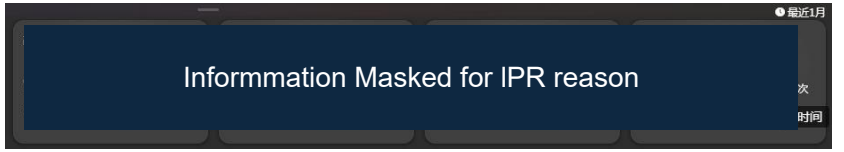
1、The system interprets natural language descriptions of fault management intent, auto-generating a system-executable fault diagnosis thought chain (CoT).



2、The system supports fault management and provides diagnostic CoT for various types of faults. The supported fault CoT includes Port Failure, Hardware Failure ,Optical Module Failure, Optical Power Abnormal, Bit Error, Device Offline, VPN Degradation/Interruption, 1588 Clock, DCN, Temperature etc.

3、When a fault occurs, the system automatically takes over the fault ticket, understands the intent of the ticket, automatically loads the corresponding fault diagnosis CoT, performs fault demarcation and localization, and generates a repair solution, thereby realizing the automated disposal of the fault process.





System Automatic Diagnosis-Related Statistics (Past Month):
Fault Ticket Automatic Diagnosis Rate, Average Diagnosis Duration, etc.

Data Collection

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Data Collection	10%	Does the system support automatic collection of fault-related indicators, including alarms, logs, performance, and OAM data etc.? Note: 1) fault should include but not limit to device offline, physical port down, optical module failure, etc. 2) All types of faults mentioned in 1) and fault-related indicators mentioned in options should be covered when choosing a related option	The system **automatically collects** fault-related indicators including alarms, logs, performance, and OAM data, detecting service and network status **in minutes**.	The system **automatically collects** fault-related indicators including alarms, logs, performance, detecting service and network status **within 15 minutes or 24 hours**.	The system **automatically collects alarms and logs.**	

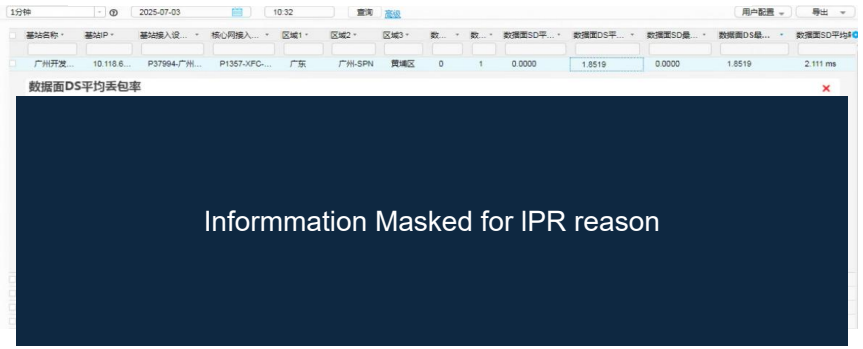
Example evidence for option A:

Real-time Fault & Performance Alarm Management

Log Management

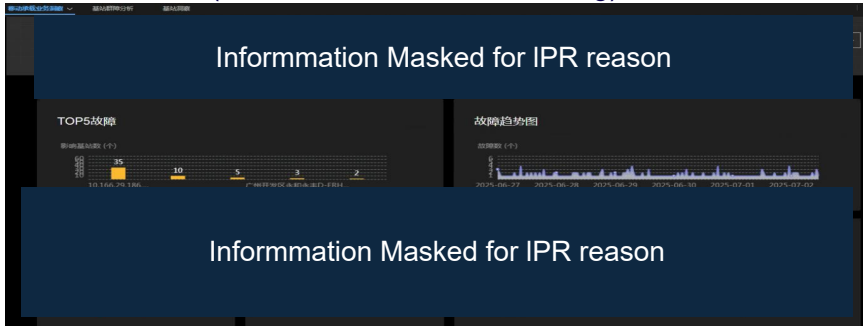
Minute-level Performance

(Traffic, Packet Loss, Delay, Jitter, etc.)



Service Fault Dashboard

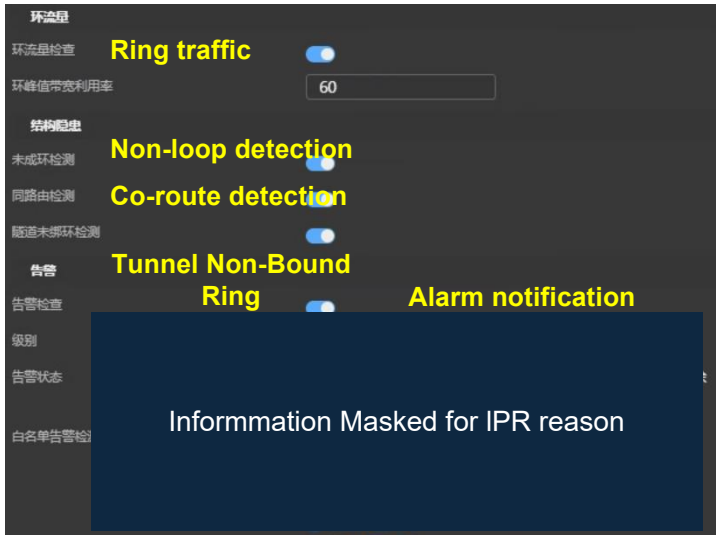
(Base station service monitoring)



Risk identification

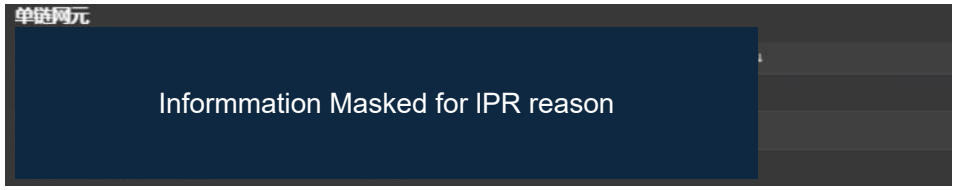
Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Risk identification	10%	Does the system support automatic identification of risks? Note: 1) **existing risks can be reported in alarm/event**, including but not limited to **network element and link anomalies,** . For example, board temperature, ip configuration conflict, optical module with weak optical power, etc. 2) potential risks can't be reported directly in alarm/event, including but not limited to network element resource and capacity anomalies, network configuration anomalies, and routing anomalies. For example, abnormal memory usage of device, incorrect static route configuration and incorrect BGP configuration, abnormal BGP route number, etc.	The system supports **automatic** identification of **existing risks** and **prediction of potential risks**.	The system supports **automatic** identification of **existing risks.**	The system identifies risks based on **manually pre-defined rules**.	**Manually** identify risks based on expertise.

Example evidence for option A:

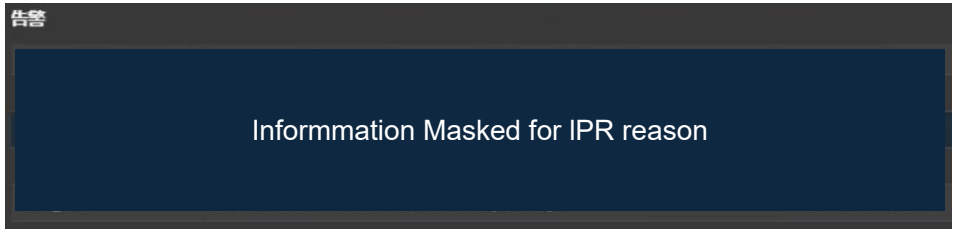


System supports network risk detection, such as Non-loop detection, Co-route detection, Tunnel Non-Bound Ring detection, Ring traffic threshold-crossing detection, Alarm detection.

Query the network risk check results using natural languages. A risk check result diagram is generated, showing the risk type and quantity.



Risk: Single-Linked NE



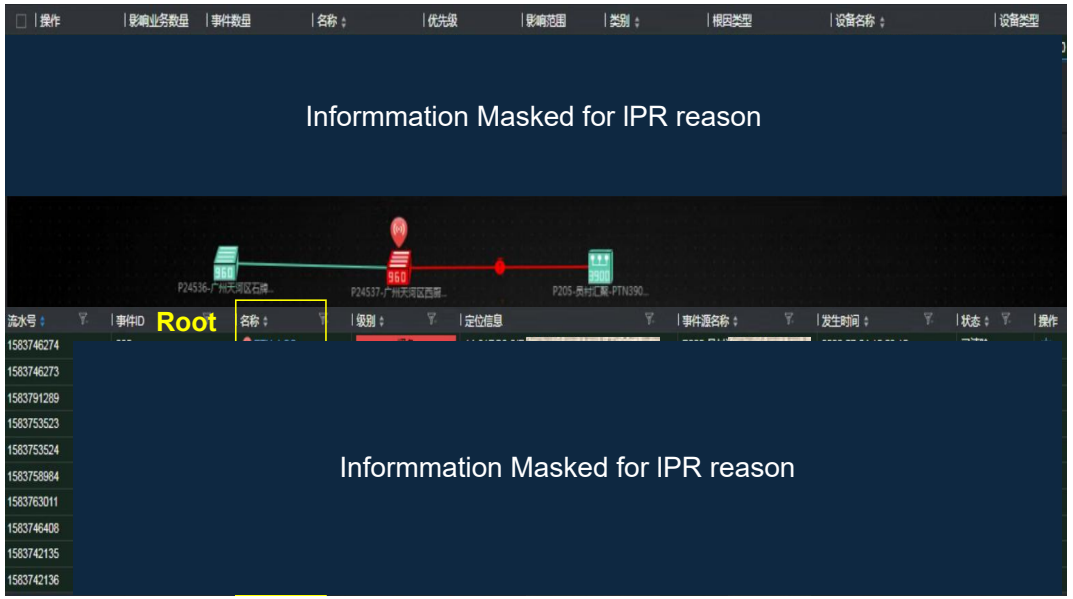
Risk: Critical Alarm List

Click View details to view the specific location of the risks. Click Export to generate a check result statistics table in XLS format.

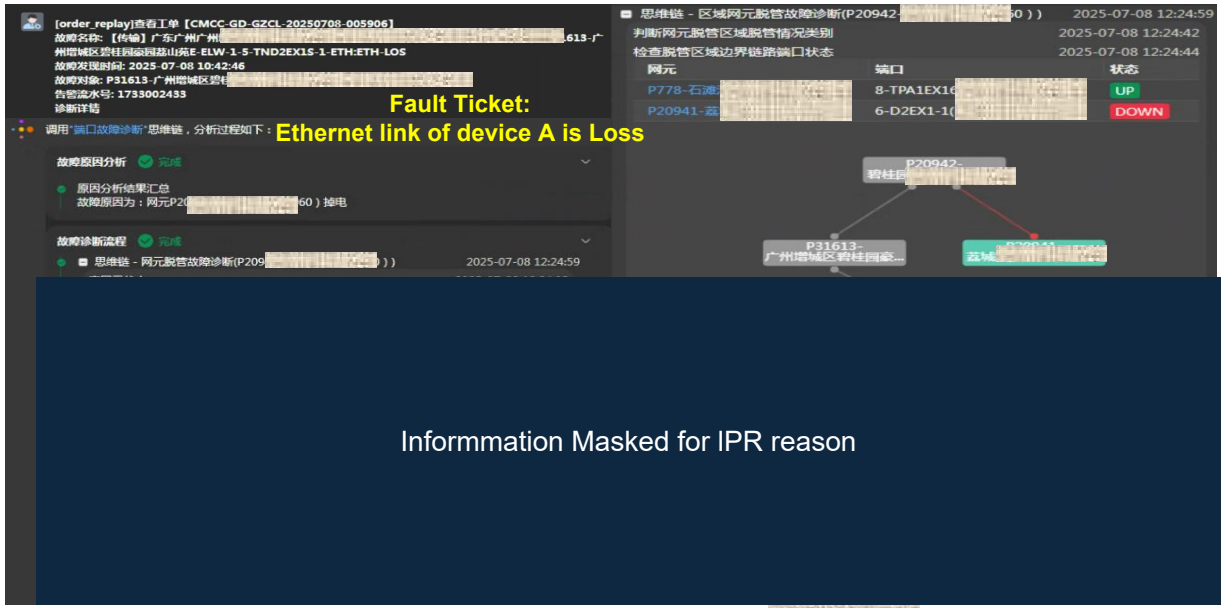
Fault identification & Impact analysis

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Fault identification and impact analysis	10%	Does the system support automatic and intelligent identification of faults? Note: 1) fault should include but not limit to device offline, physical port down, optical module failure, etc. 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc	The system supports automatic fault identification by **intelligent aggregating** of multiple data source (alarms, logs, performance data, OAM data, etc.). System provides the impacted services with severity.	The system support automatic fault identification based on **custom rules**, results need manually confirmation.	The system supports automatic fault identification based on predefined rules, results need manually confirmation.	Manually identify faults based on expertise.

Example evidence for option A:



Alarm automatically aggregate to identify root & correlated alarms.



After receiving the fault ticket, the system automatically diagnoses the root cause of the fault and the affected services.

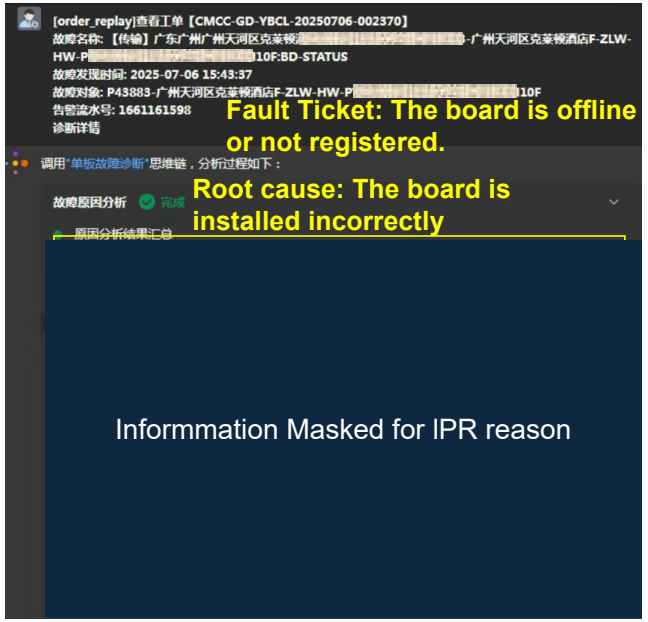
Demarcation of faults and risks -1

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Demarcation of faults and risks	20%	Does the system support automatic demarcation of faults and risks? Note: 1) Examples of demarcation involve pinpointing the exact roles of malfunctioning routers, like identifying whether they are access routers, aggregation routers, or Autonomous System Boundary Router (ASBR). 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc..	The system **automatically** demarcates the faults and risks **without manual intervention**.	The system demarcates the faults and risks based on **custom rules**, results need **manually confirmation**.	The system demarcates the faults and risks based on **predefined rules**, results need **manually confirmation**.	**Manually** demarcates the fault and risks based on data such as operation logs and captured packets.

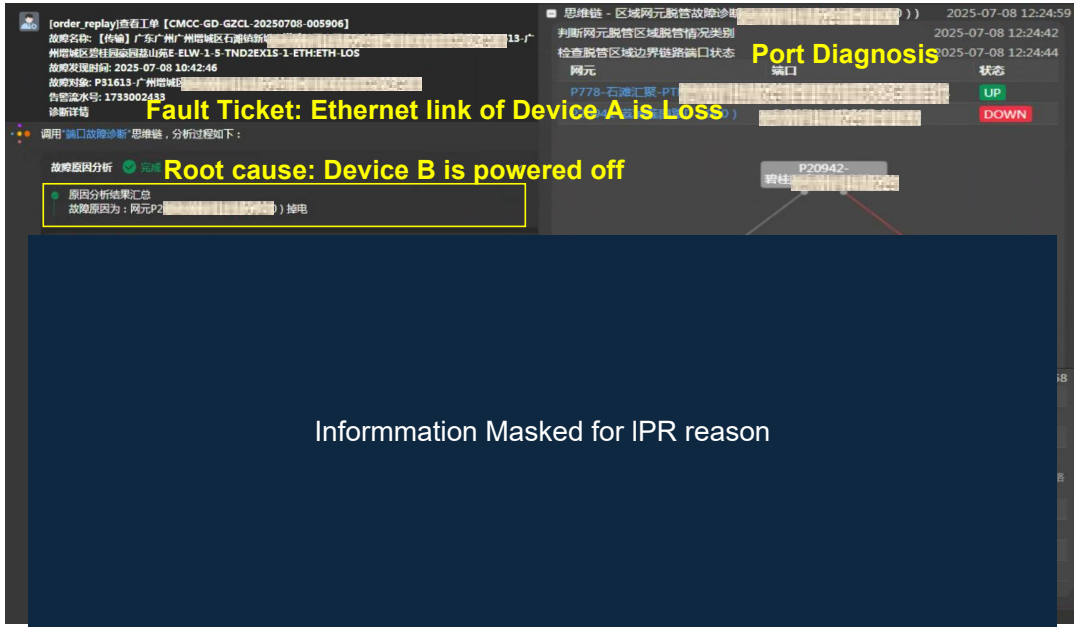
Example evidence for option A:

After receiving the fault ticket, the system automatically demarcates and locates faults.

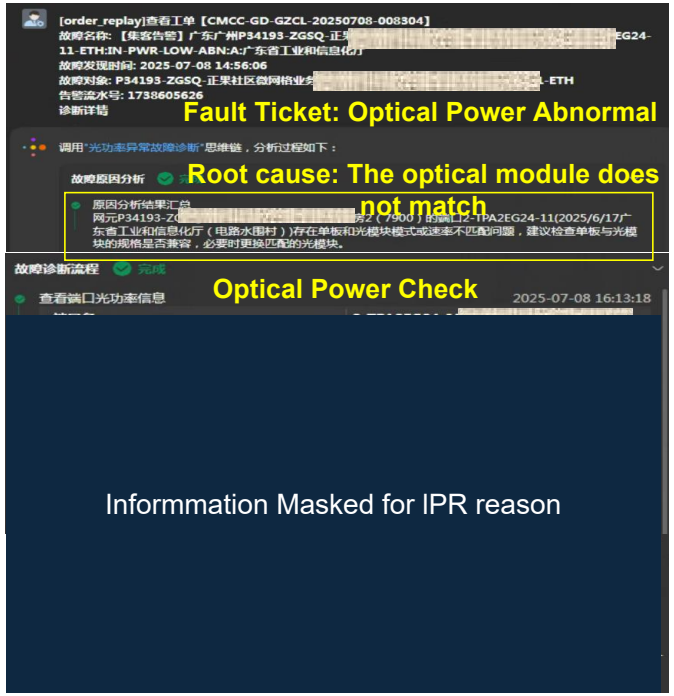
Sub-scenario-1：Hardware Failure



Sub-scenario-2：Device Offline



Sub-scenario-3：
Optical Module Failure or Optical Power Abnormal



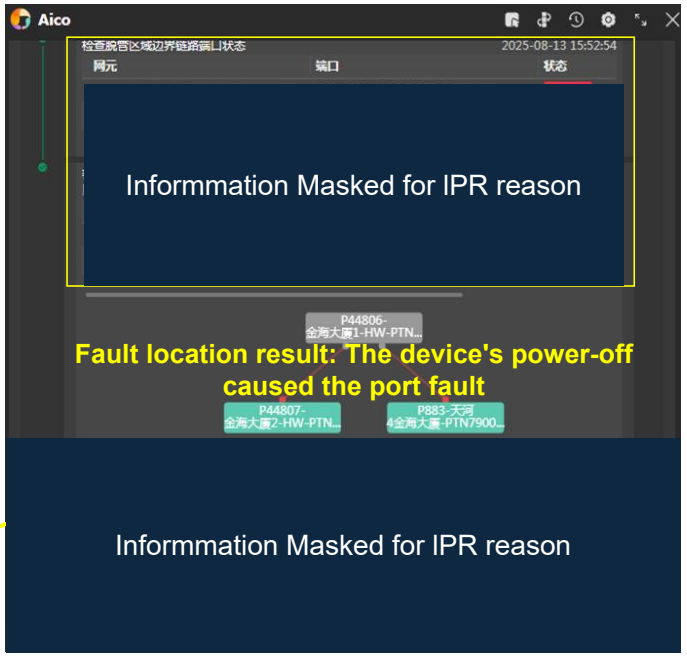
Demarcation of faults and risks -2

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Demarcation of faults and risks	20%	Does the system support automatic demarcation of faults and risks? Note: 1) Examples of demarcation involve pinpointing the exact roles of malfunctioning routers, like identifying whether they are access routers, aggregation routers, or Autonomous System Boundary Router (ASBR). 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc..	The system **automatically** demarcates the faults and risks **without manual intervention**.	The system demarcates the faults and risks based on **custom rules**, results need **manually confirmation**.	The system demarcates the faults and risks based on **predefined rules**, results need **manually confirmation**.	**Manually** demarcates the fault and risks based on data such as operation logs and captured packets.

Example evidence for option A:

After receiving the fault ticket, the system automatically demarcates and locates faults.

Sub-scenario-4： Port Failure



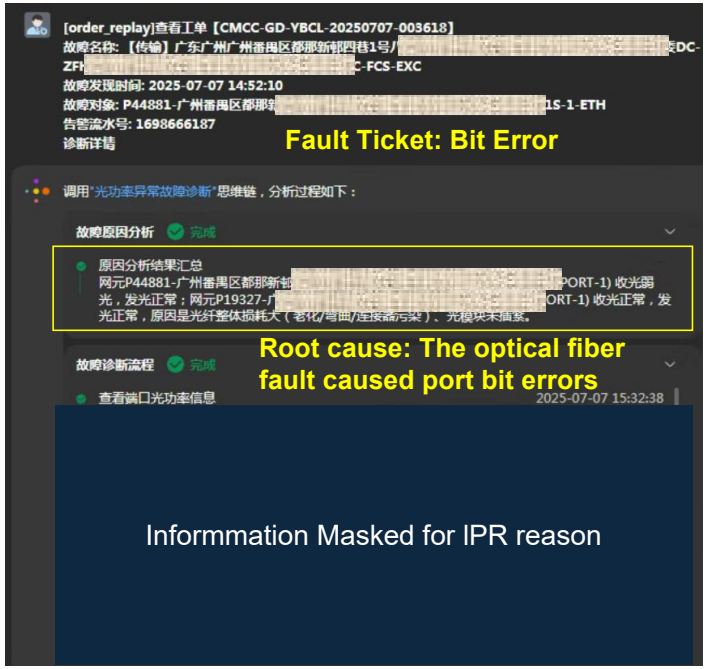
Demarcation of faults and risks -3

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Demarcation of faults and risks	20%	Does the system support automatic demarcation of faults and risks? Note: 1) Examples of demarcation involve pinpointing the exact roles of malfunctioning routers, like identifying whether they are access routers, aggregation routers, or Autonomous System Boundary Router (ASBR). 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc..	The system **automatically** demarcates the faults and risks **without manual intervention**.	The system demarcates the faults and risks based on **custom rules**, results need **manually confirmation**.	The system demarcates the faults and risks based on **predefined rules**, results need **manually confirmation**.	**Manually** demarcates the fault and risks based on data such as operation logs and captured packets.

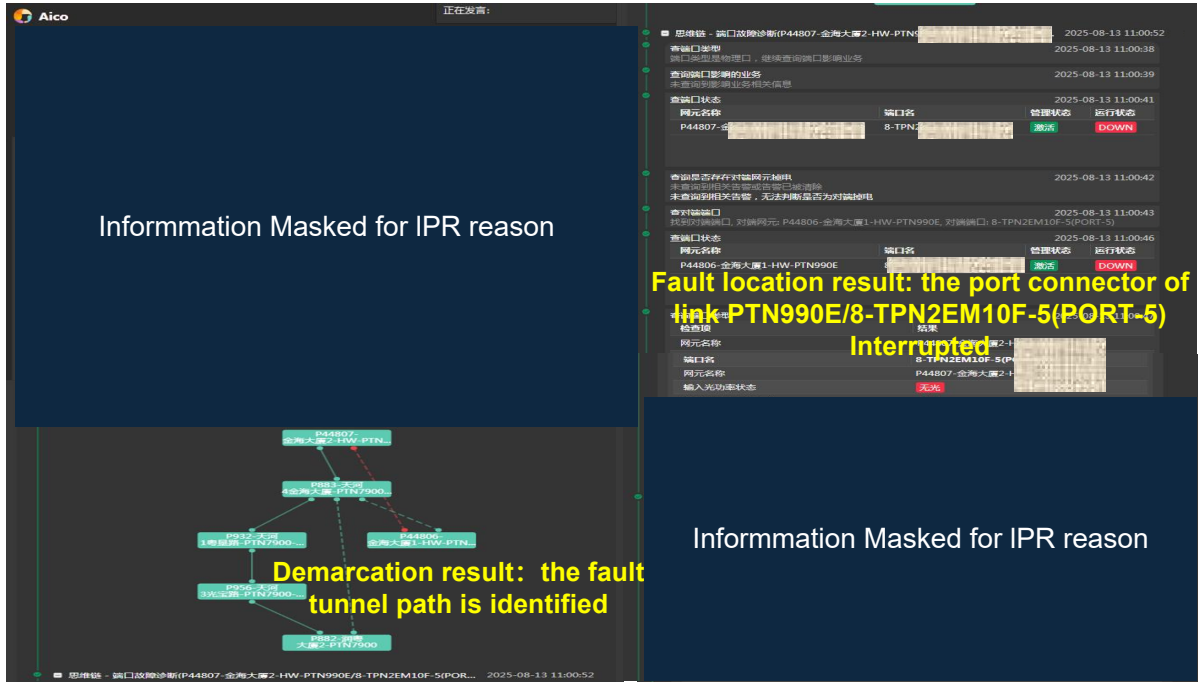
Example evidence for option A: After receiving the fault ticket, the system automatically demarcates and locates faults.

Note： For sub-scenario 6 (Protocol State Abnormal), no example evidence is provided as there are no corresponding fault tickets in the actual network.

Sub-scenario-5：
High Error Rate / Port Bit Error



Sub-scenario-7：
VPN / Tunnel Degradation



Sub-scenario-8：
VPN / Tunnel Interruption

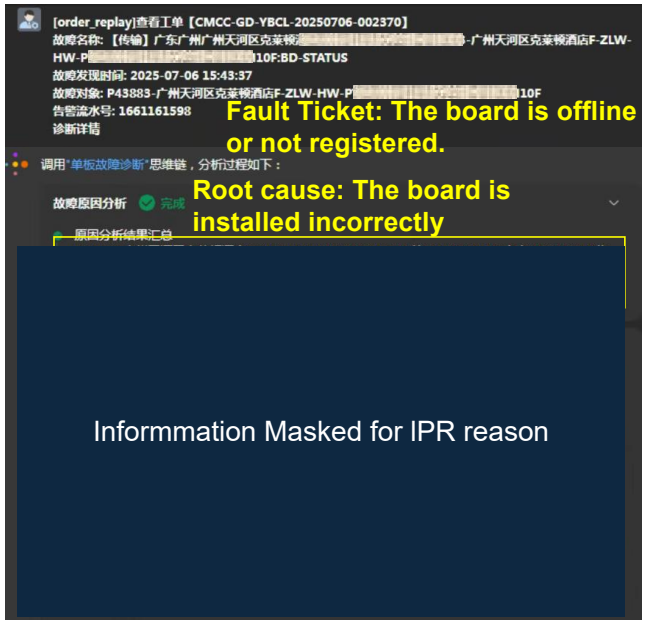
Locating of faults and risks -1

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Locating of faults and risks	15%	Does the system support automatic root cause analysis for network faults and risks? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports. 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc	The system **automatically** analyzes root cause **without manual intervention.**	The system provides one or more suspected causes based on **custom rules,** manually analyze and confirm the root cause**.**	The system provides cause analysis based on **predefined rules,** manually analyze and confirm the root cause.	**Manually** analyze root cause based on expertise.

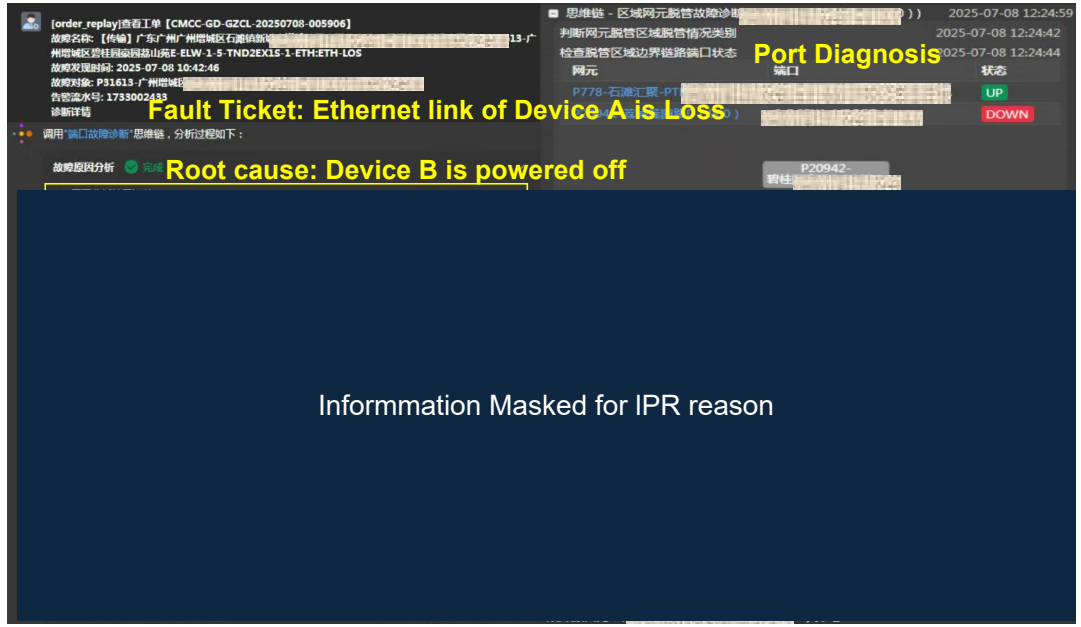
Example evidence for option A:

After receiving the fault ticket, the system automatically demarcates and locates faults.

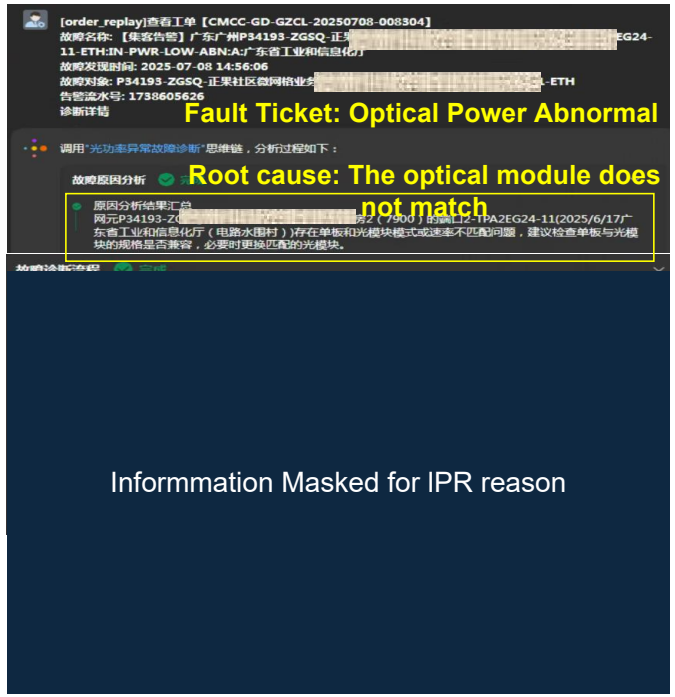
Sub-scenario-1：Hardware Failure



Sub-scenario-2：Device Offline



Sub-scenario-3：
Optical Module Failure or Optical Power Abnormal



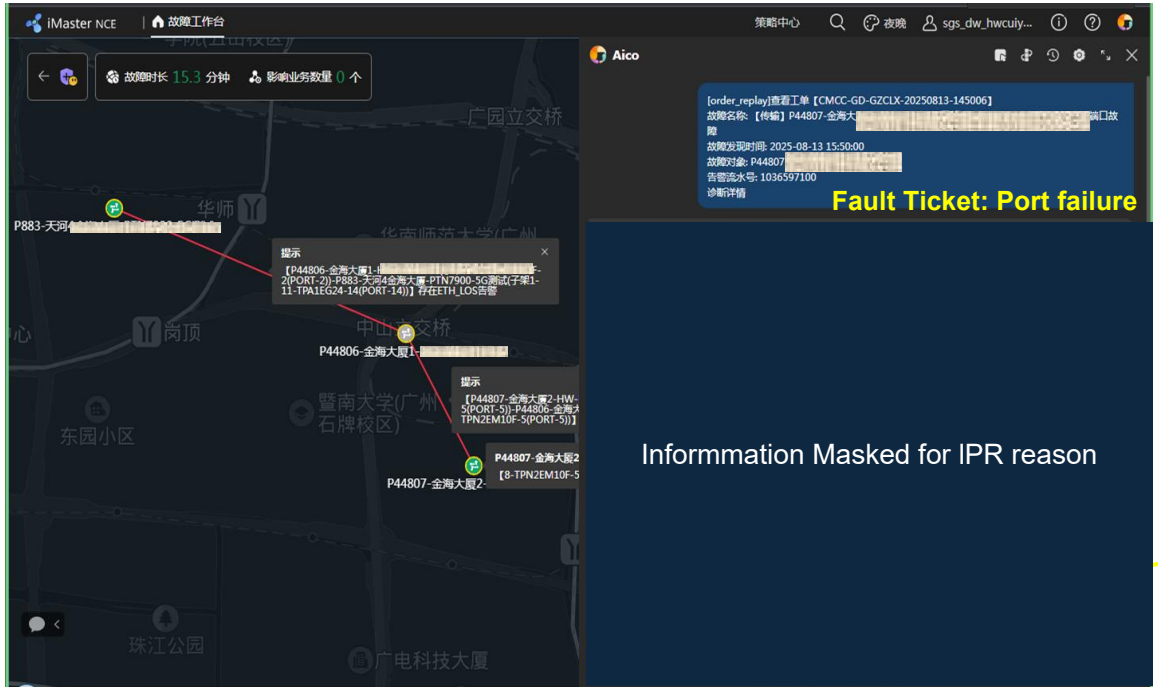
Locating of faults and risks -2

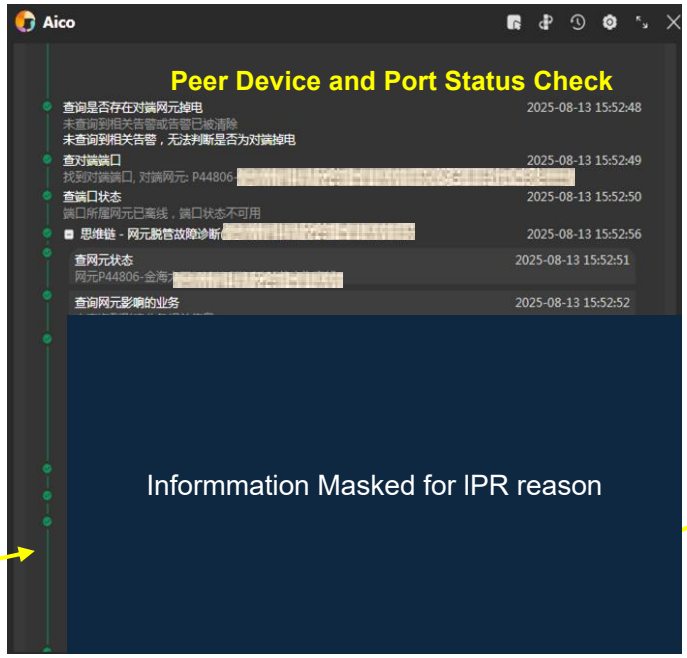
Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Locating of faults and risks	15%	Does the system support automatic root cause analysis for network faults and risks? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports. 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc	The system **automatically** analyzes root cause **without manual intervention.**	The system provides one or more suspected causes based on **custom rules,** manually analyze and confirm the root cause**.**	The system provides cause analysis based on **predefined rules,** manually analyze and confirm the root cause.	**Manually** analyze root cause based on expertise.

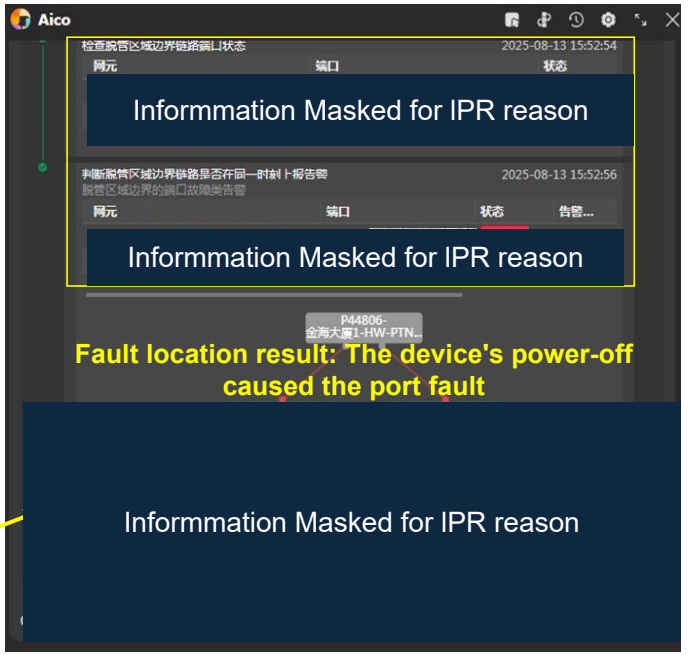
Example evidence for option A:

After receiving the fault ticket, the system automatically demarcates and locates faults.

Sub-scenario-4： Port Failure







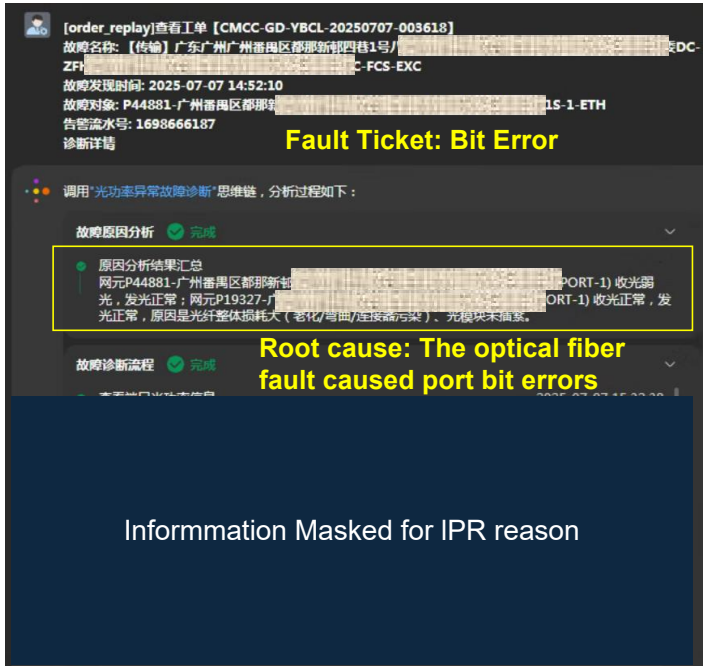
Locating of faults and risks -3

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Locating of faults and risks	15%	Does the system support automatic root cause analysis for network faults and risks? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports. 2)Custom rules include but not limited to scenario specific rules made based on data analysis on alarms, logs, performance and OAM data, etc	The system **automatically** analyzes root cause **without manual intervention.**	The system provides one or more suspected causes based on **custom rules,** manually analyze and confirm the root cause.	The system provides cause analysis based on **predefined rules,** manually analyze and confirm the root cause.	**Manually** analyze root cause based on expertise.

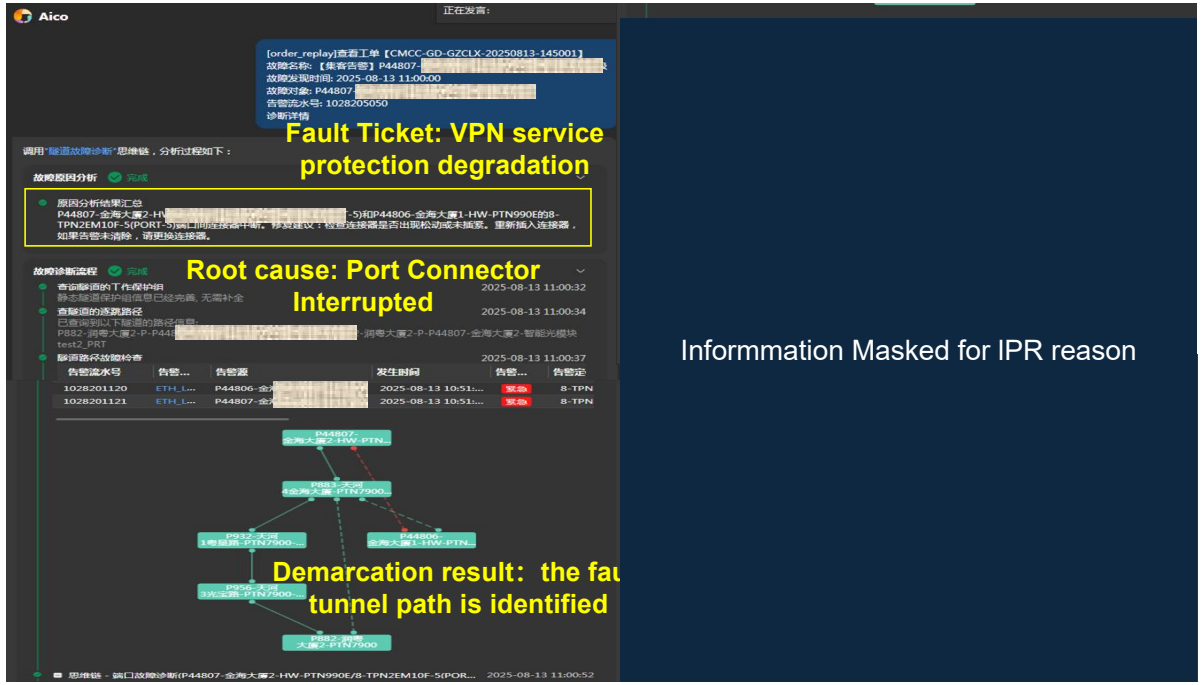
Example evidence for option A: After receiving the fault ticket, the system automatically demarcates and locates faults.

Note： For sub-scenario 6 (Protocol State Abnormal), no example evidence is provided as there are no corresponding fault tickets in the actual network.

Sub-scenario-5：
High Error Rate / Port Bit Error



Sub-scenario-7：
VPN / Tunnel Degradation



Sub-scenario-8：
VPN / Tunnel Interruption

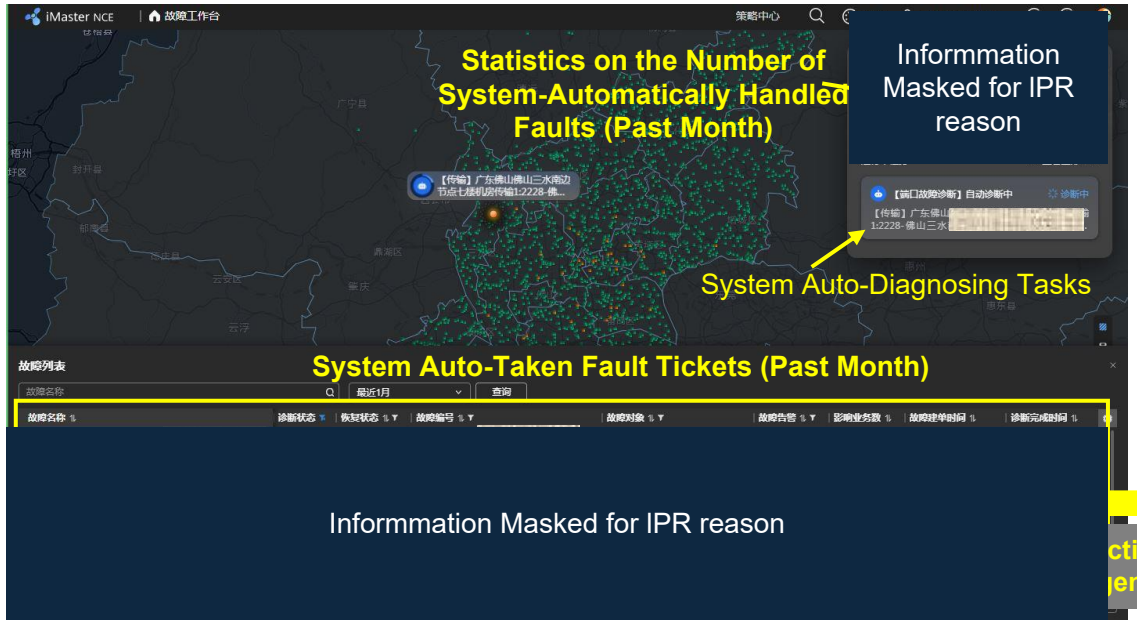
Generation and evaluation of solutions -1

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Generation and evaluation of solutions	15%	Does the system support automatic generation and evaluation of emergency restoration and repair solution? Note: 1) Emergency restoration solution may be compute alternative paths based on service SLA requirement. 2) Repair solution may be repair power supply.	The system **automatically generates** emergency restoration and repair solutions**.** The system **automatically make decision** on the alternative solutions based on **evaluation through simulation**.	The system **automatically generates** emergency restoration and repair solutions**.** **Manually** make decision on the alternative solutions.	The system gives emergency restoration **suggestions. Manually** formulate solutions and make decision.	**Manually** analyze and evaluate emergency restoration solutions based on system-collected service data**.**

Example evidence for option A: After receiving the fault ticket, the system automatically generates emergency restoration and repair solutions.

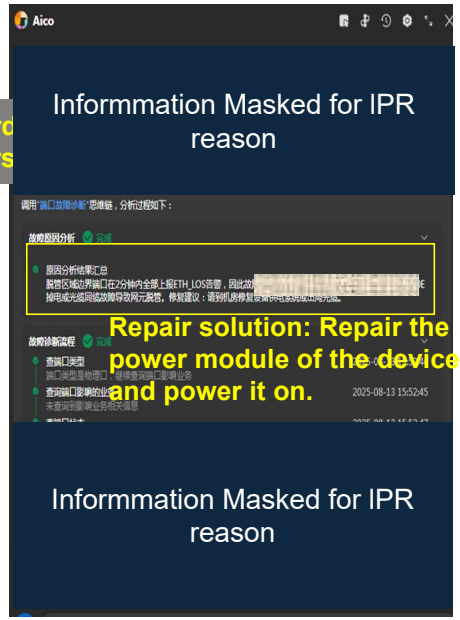
The system automatically generates an emergency repair solution based on information such as the fault cause and location. The repair solution includes capabilities for two phases:
Phase 1: For faults that the system can automatically repair, it calculates alternative paths to restore services (refer to Fault Sub-scenario 8: VPN/Tunnel Interruption).
Phase 2: For faults requiring on-site manual handling, the system provides a detailed repair plan to guide maintenance personnel in conducting accurate on-site operations, thereby improving on-site work efficiency.

Auto-takeover Fault Ticket, Localization & Repair Solution Generation

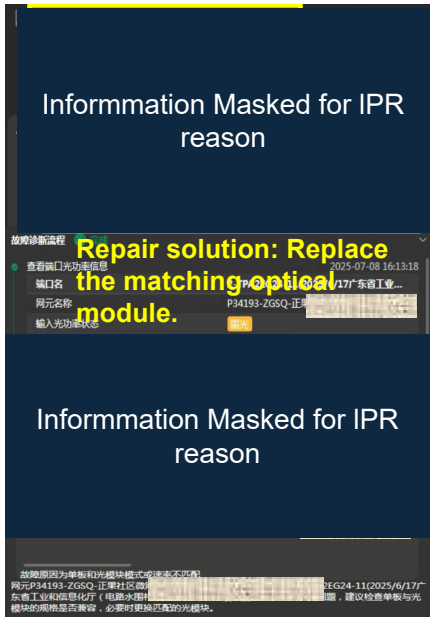


Sub-scenario-1：Hardware Failure

Sub-scenario-2：Device Offline



Sub-scenario-3：Optical Module Failure or Optical Power Abnormal



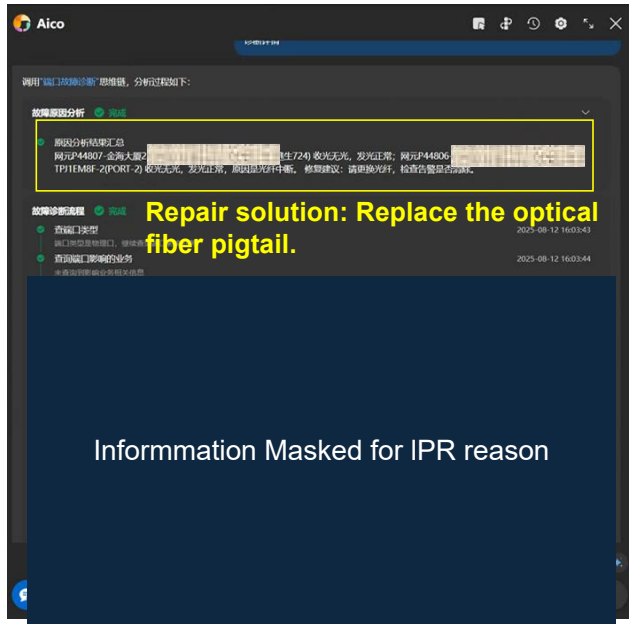
Generation and evaluation of solutions -2

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Generation and evaluation of solutions	15%	Does the system support automatic generation and evaluation of emergency restoration and repair solution? Note: 1) Emergency restoration solution may be compute alternative paths based on service SLA requirement. 2) Repair solution may be repair power supply.	The system **automatically generates** emergency restoration and repair solutions**.** The system **automatically make decision** on the alternative solutions based on **evaluation through simulation**.	The system **automatically generates** emergency restoration and repair solutions**.** **Manually** make decision on the alternative solutions.	The system gives emergency restoration **suggestions. Manually** formulate solutions and make decision.	**Manually** analyze and evaluate emergency restoration solutions based on system-collected service data**.**

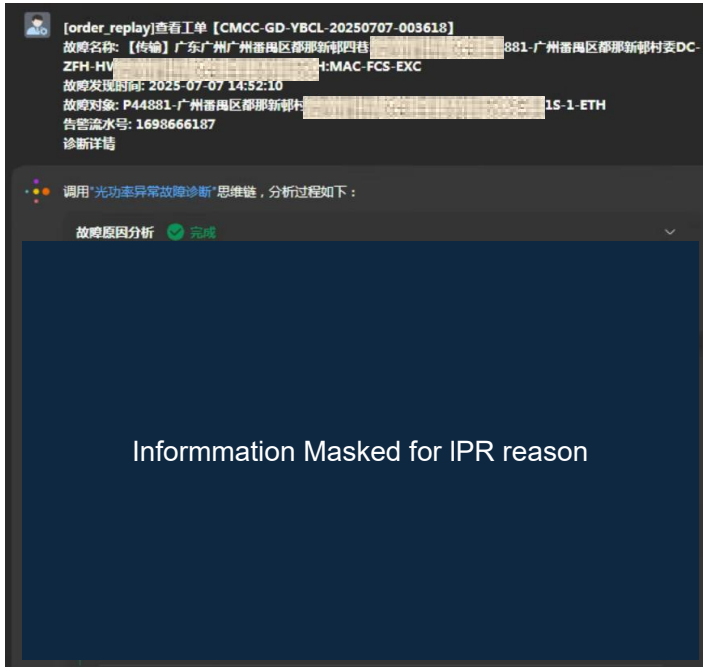
Example evidence for option A: After receiving the fault ticket, the system automatically generates emergency restoration and repair solutions.

The system automatically generates an emergency repair solution based on information such as the fault cause and location. The repair solution includes capabilities for two phases:
Phase 1: For faults that the system can automatically repair, it calculates alternative paths to restore services (refer to Fault Sub-scenario 8: VPN/Tunnel Interruption).
Phase 2: For faults requiring on-site manual handling, the system provides a detailed repair plan to guide maintenance personnel in conducting accurate on-site operations, thereby improving on-site work efficiency.

Sub-scenario-4： Port Failure



Sub-scenario-5：High Error Rate / Port Bit Error



Sub-scenario-7：VPN / Tunnel Degradation

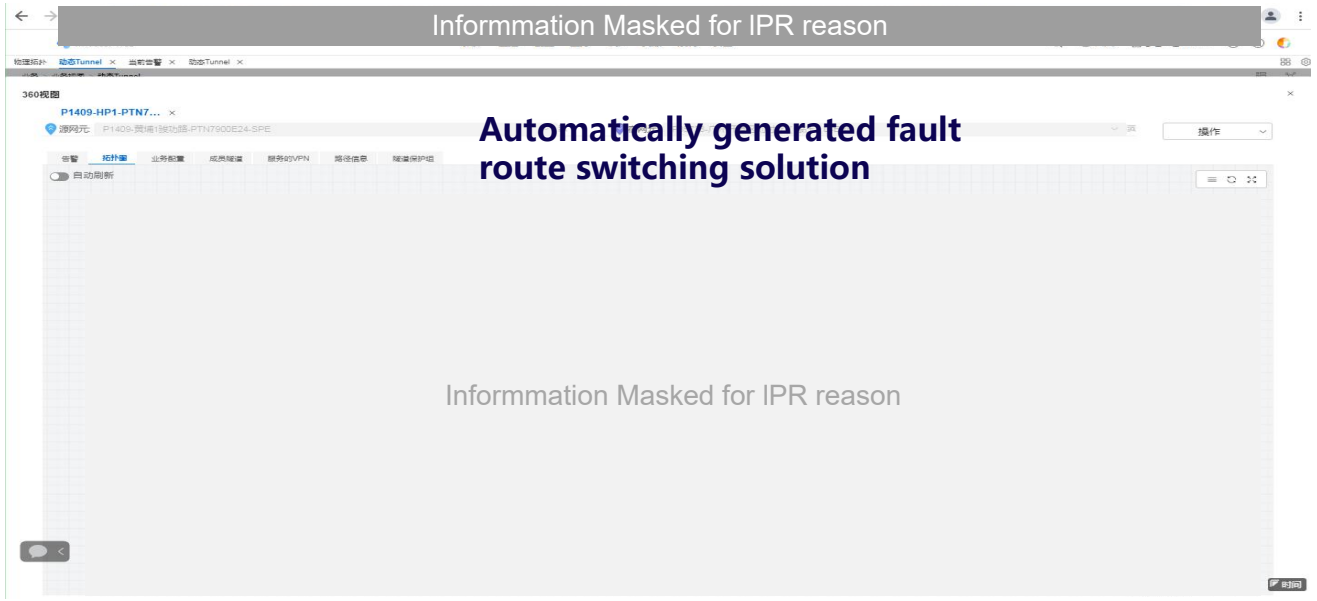
Generation and evaluation of solutions -3

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Generation and evaluation of solutions	15%	Does the system support automatic generation and evaluation of emergency restoration and repair solution? Note: 1) Emergency restoration solution may be compute alternative paths based on service SLA requirement. 2) Repair solution may be repair power supply.	The system **automatically generates** emergency restoration and repair solutions**.** The system **automatically make decision** on the alternative solutions based on **evaluation through simulation**.	The system **automatically generates** emergency restoration and repair solutions**.** **Manually** make decision on the alternative solutions.	The system gives emergency restoration **suggestions. Manually** formulate solutions and make decision.	**Manually** analyze and evaluate emergency restoration solutions based on system-collected service data**.**

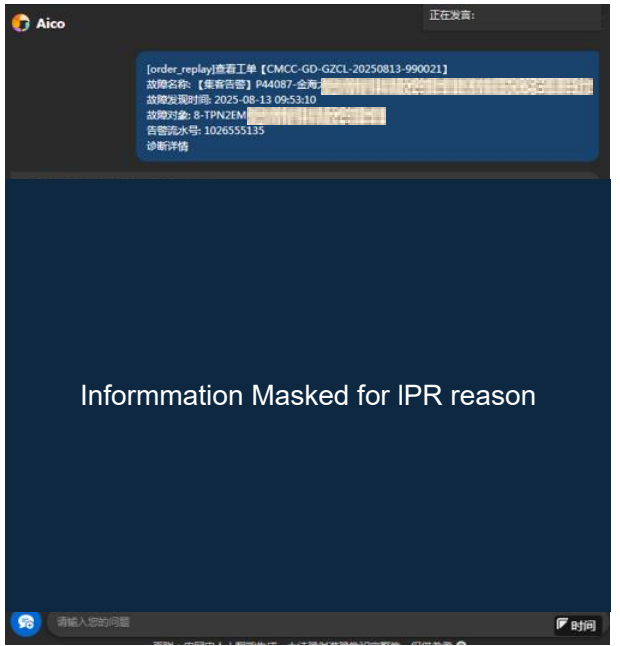
Example evidence for option A: After receiving the fault ticket, the system automatically generates emergency restoration and repair solutions.

Note: For fault sub-scenario 8 (VPN/Tunnel Interruption), the system's emergency recovery includes two phases of capabilities:
Phase 1: The system automatically generates an emergency recovery plan for the fault and calculates alternative paths to restore services.
Phase 2: For specific faulty links, the system further identifies the cause of the fault and provides a repair solution, supporting maintenance personnel to handle the issue on-site.

Sub-scenario-8 VPN / Tunnel Interruption:
Phase 1、 Automatically calculates alternative paths to restore services



Phase 2、 Further identify the root cause of the faulty link and provide a solution for on-site repair.



Execution and verification-1

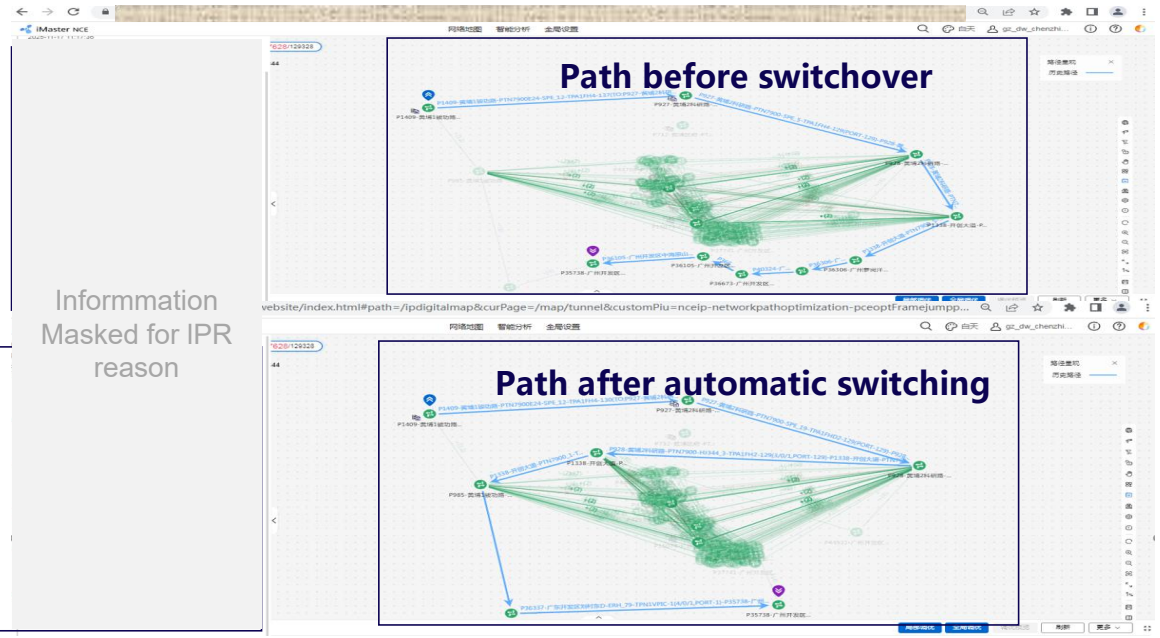
Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Execution and verification	10%	Does the system support automatic execution and verification? Does the system support assistance for on-site engineers?	1) The system supports **automatic execution and verification** of emergency restoration and repair solution. (Automatic repair excludes the faults that on-site handling is necessary, such as power supply failure, board fault, fiber cut). 2) The system support intelligent on-site instruction and efficient information query based on simplified human-system interaction.	1)The system supports **automatic execution** of emergency restoration and repair solution. **Manual verification** is needed. 2)The on-site handling are assisted by tool.	The system support **automatic** execution of emergency restoration. Manually execute repair solution. **Manually verify** by analyzing system data (e.g., alarms)	

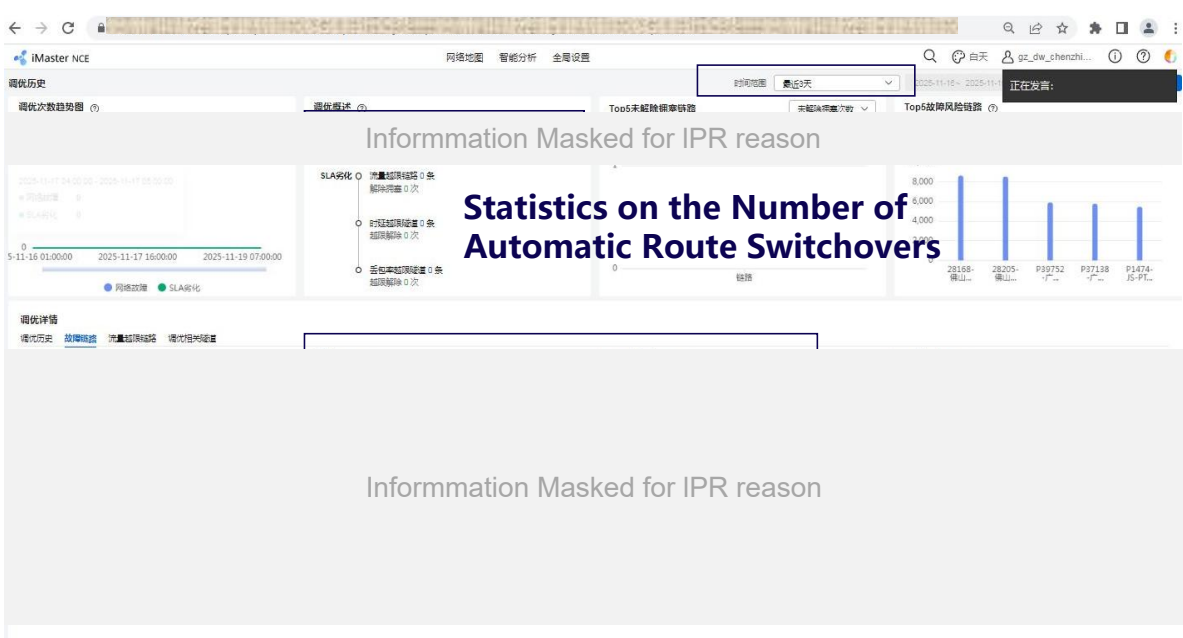
Example evidence for option A:

Scenario 1: For faults that can be automatically repaired by the system, the system automatically executes emergency plans to restore services and achieve service recovery.
Scenario 2: For faults requiring on-site manual intervention, frontline maintenance personnel can use the mobile O&M app to perform simplified human-system interaction during site visits. They can intelligently query fault work order diagnosis information, alarm status, optical power indicators, and other data on-site, enabling self-service data access.

Scenario 1、The system automatically executes the emergency recovery plan to restore services.

Automatic route switching history during failures, records traceable for review.





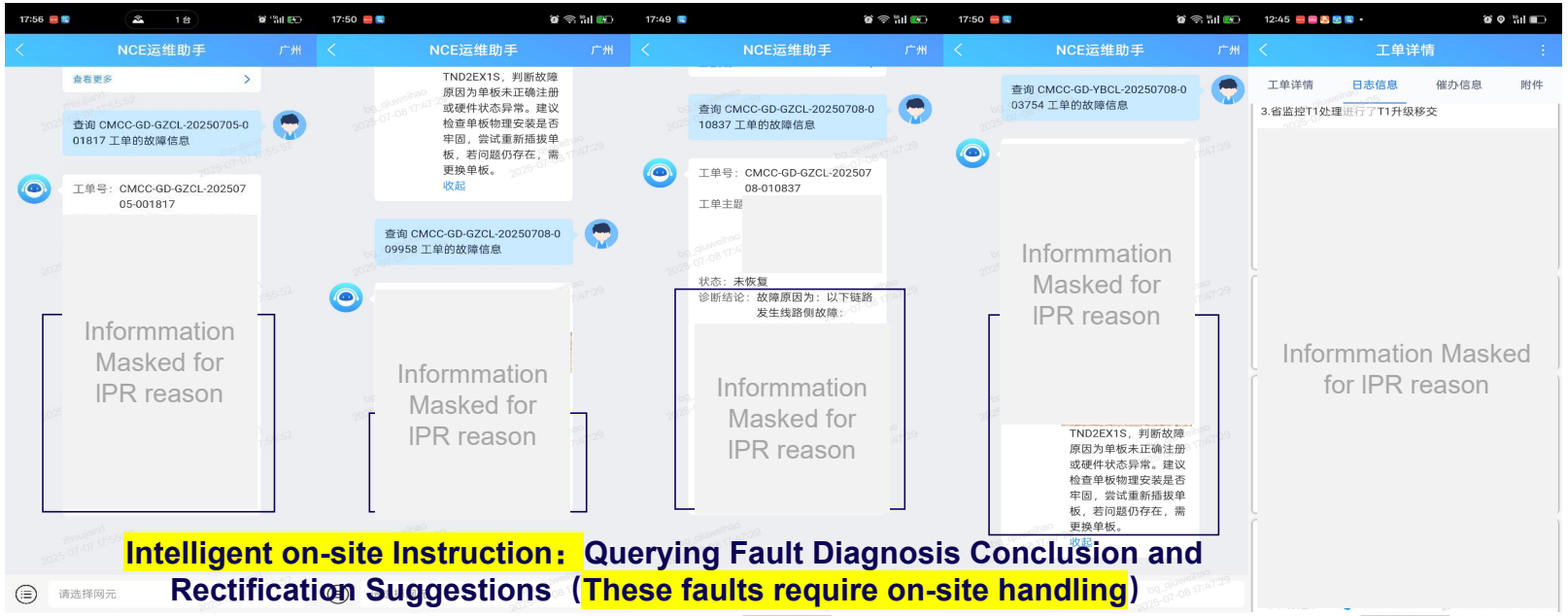
Execution and verification-2

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Execution and verification	10%	Does the system support automatic execution and verification? Does the system support assistance for on-site engineers?	1) The system supports **automatic execution and verification** of emergency restoration and repair solution. (Automatic repair excludes the faults that on-site handling is necessary, such as power supply failure, board fault, fiber cut). 2) The system support intelligent on-site instruction and efficient information query based on simplified human-system interaction.	1)The system supports **automatic execution** of emergency restoration and repair solution. **Manual verification** is needed. 2)The on-site handling are assisted by tool.	The system support **automatic** execution of emergency restoration. Manually execute repair solution. **Manually verify** by analyzing system data (e.g., alarms)	

Example evidence for option A:

Scenario 1: For faults that can be automatically repaired by the system, the system automatically executes emergency plans to restore services and achieve service recovery.
Scenario 2: For faults requiring on-site manual intervention, frontline maintenance personnel can use the mobile O&M app to perform simplified human-system interaction during site visits. They can intelligently query fault work order diagnosis information, alarm status, optical power indicators, and other data on-site, enabling self-service data access.

Scenario 2、Intelligent On-Site AI Assistant: Querying Fault Diagnosis Information，etc.



Intelligent on-site Instruction：Querying Fault Diagnosis Conclusion and Rectification Suggestions（These faults require on-site handling）

Efficient on-site Information Query：Querying the optical power、alarms、port status, etc.

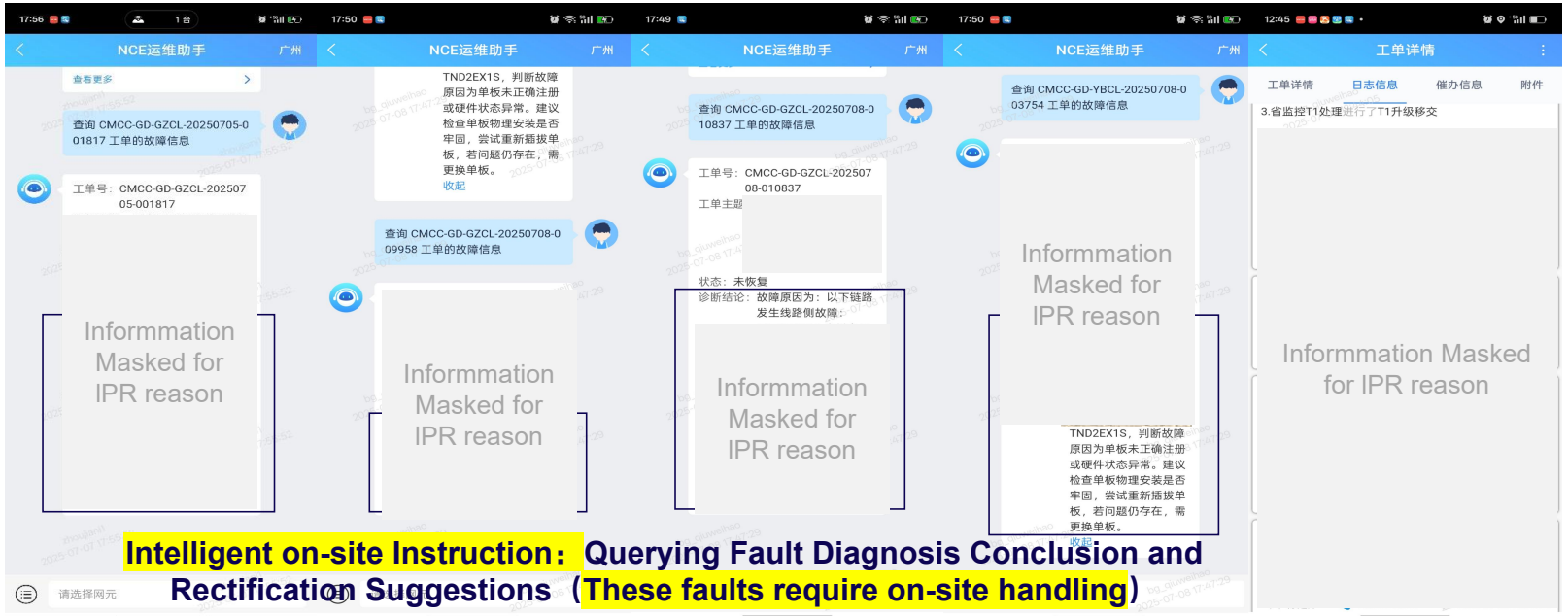
Execution and verification-2

Service capability	Weight	Question	√ Option A	Option B	Option C	Option D
Execution and verification	10%	Does the system support automatic execution and verification? Does the system support assistance for on-site engineers?	1) The system supports **automatic execution and verification** of emergency restoration and repair solution. (Automatic repair excludes the faults that on-site handling is necessary, such as power supply failure, board fault, fiber cut). 2) The system support intelligent on-site instruction and efficient information query based on simplified human-system interaction.	1)The system supports **automatic execution** of emergency restoration and repair solution. **Manual verification** is needed. 2)The on-site handling are assisted by tool.	The system support **automatic** execution of emergency restoration. Manually execute repair solution. **Manually verify** by analyzing system data (e.g., alarms)	

Example evidence for option A:

Scenario 1: For faults that can be automatically repaired by the system, the system automatically executes emergency plans to restore services and achieve service recovery.
Scenario 2: For faults requiring on-site manual intervention, frontline maintenance personnel can use the mobile O&M app to perform simplified human-system interaction during site visits. They can intelligently query fault work order diagnosis information, alarm status, optical power indicators, and other data on-site, enabling self-service data access.

Scenario 2、Intelligent On-Site AI Assistant: Querying Fault Diagnosis Information，etc.



Intelligent on-site Instruction：Querying Fault Diagnosis Conclusion and Rectification Suggestions（These faults require on-site handling）

Efficient on-site Information Query：Querying the optical power、alarms、port status, etc.

Thank you