ISG ZSM PoC Proposal:

1 PoC Project Details

1.1 PoC Project

PoC Number:	18
PoC Project Name:	Agent based Network Fault and Root Cause
PoC Project Host:	China telecom;
Short Description:	This PoC demonstrates the use case of agent-based autonomous network fault diagnosis and root cause analysis. The scope of this PoC is to validate the normative architectural extensions for Agent-Based Entities defined in ZSM020 [2] that enable intelligent fault management. It will verify how these agent-based mechanisms perform fault data collection, execute diagnostic algorithms, and interact to localize root causes within network operation frameworks. The PoC will also demonstrate the verification of analysis results and the associated security mechanisms, showcasing scenario-based solutions for network operators, OTT services, and third-party management systems as defined in the corresponding use cases. The implementation of the solution in this PoC uses the relevant ZSM specifications as a reference. The design architecture of the use case follows the ZSM framework (ZSM 002) and incorporates the agent-based entity concepts from ZSM020 to realize the defined requirements for autonomous fault and root cause analysis.

1.2 PoC Team Members

	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	China Telecom	yes	Mrs. Jingwen Ning ningjw09@chinatelecom.cn Yu Zeng zengyu@chinatelecom.cn Xiao Zhou zhouxiao.js@chinatelecom.cn Ping Shen shenping.js@chinatelecom.cn Zheng Zhang zhangzheng1.js@chinatelecom.cn Yongpan Zhang zhangyongpan.js@chinatelecom.cn YuHan Chen chenyh54@chinatelecom.cn Qiang Cheng chengqiang.js@chinatelecom.cn You Lv lvyou1.js@chinatelecom.cn Ling Lin linling.js@chinatelecom.cn Yunkai Zhao zhaoyk1@chinatelecom.cn Feng Zhang zhangfeng11.js@chinatelecom.cn WenXing Zhang zhangwx12@chinatelecom.cn Yingfeng Xie xieyf8@chinatelecom.cn	X	Service Provider	-User Stories/ Use Case -PoC development -PoC documentation -PoC demos
2	Asiainfo		Dr. Zhongke Zhang Zhangzk10@asiainfo.com		Vendor	- Help with architecture verification
3	CAICT		Ziruo Liu liuzhiruo@caict.ac.cn		Academic	-help with simulation and architecture optimization
4	ZTE		Manchang Ju Ju.manchang@zte.com.cn		Vendor	-help with concept refinement and use case

All the PoC Team members listed above declare that the information in this proposal is conformant to their plans at this date and commit to inform ETSI timely in case of changes in the PoC Team, scope or timeline.

1.3 PoC Project Scope

1.3.1 PoC Topics

PoC Topics identified in this clause need to be taken for the PoC Topic List identified by ISG ZSM and publicly available in the ZSM WIKI. PoC Teams addressing these topics commit to submit the expected contributions in a timely manner.

PoC Topic Code	PoC Topic Description	Related WI	Expected Contribution	Target Date
	Agent based Network Fault and Root Cause	ZSM020 , ZSM002	Demo	Dec 2026

1.3.2 Other topics in scope

List here any additional topic for which the PoC plans to provide input/feedback to the ISG ZSM.

PoC Topic Code	PoC Topic Description	Related WG/WI	Expected Contribution	Target Date
A				
B				
<…>				

1.4 PoC Project Milestones

PoC Milestone	Milestone description	Target Date	Additional Info
P.S	PoC Proposal submission	Mar 2026	Official PoC proposal submission.
P.D	PoC Expected Contribution (Demo)	May 2026	Demonstrates the use case of agent-based autonomous network fault diagnosis and root cause analysis
P.R	PoC Report	Jul 2026	PoC Project Feedback.
P.E	PoC Project End	Sep 2026	Publication

NOTE: Milestones need to be entered in chronological order.

1.5 Additional Details

We prefer to present the demonstrations at ZSM's meetings (Demo in ZSM#35) and submit the contributions and report which include demo scenarios. The PoC demo will be presented in the form of PPT.

2 PoC Technical Details

2.1 PoC Overview

2.1.1 Use case description

In order to realize autonomous network operation and management, it is essential to move beyond traditional, rule-based fault management towards intelligent mechanisms that can diagnose and localize root causes with minimal human intervention. The Agent-Based Entities defined in ZSM020 provide a foundational concept, but normative architectural extensions are required to enable them to perform autonomous fault diagnosis and root cause analysis within intelligent network operation frameworks.

By adopting an agent-based approach in the process of network fault management, it is possible to achieve the capabilities mentioned above. Through specialized agent entities that can collect fault data, execute diagnostic algorithms, interact with each other, and verify analysis results, the mechanism can automatically identify the root cause of network issues and provide verified recommendations. This approach also incorporates necessary security mechanisms to ensure trustworthy operations.

As a first step, this PoC project will verify the key functionalities of agent-based fault and root cause analysis by implementing the normative architectural extensions defined for the Agent-Based Entities in ZSM020. The scope of this PoC includes:

1. Validating the mechanisms for fault data collection and the execution of diagnostic algorithms within agent entities.

2. Demonstrating agent interaction procedures that enable collaborative root cause localization across different network domains or management layers.

3. Verifying the process of analysis result verification and the associated security mechanisms to ensure the reliability and trustworthiness of the diagnosis.

Based on the results of the verification at this PoC, we will plan to consider a future PoC that expands the scope to include integration with higher-level management systems (e.g., E2E MD, BSS) or other automation paradigms such as intent-driven management.

This PoC uses the agent-based entity concepts defined in ZSM020 as the core building blocks. The implementation refers to the ZSM framework architecture (ZSM 002) and incorporates the requirements for fault data collection, diagnostic algorithms, agent interaction, and security as specified in the corresponding normative work. The use cases demonstrated in this PoC are derived from the scenario-based solutions defined for network operators, OTT services, and third-party management systems.

2.1.2 PoC scope

This PoC demonstrates the use case of agent-based autonomous network fault diagnosis and root cause analysis. The scope of this PoC is to validate the normative architectural extensions for Agent-Based Entities defined in ZSM020 [x] that enable intelligent fault management. It will verify how these agent-based mechanisms perform fault data collection, execute diagnostic algorithms, and interact to localize root causes within network operation frameworks. The PoC will also demonstrate the verification of analysis results and the associated security mechanisms, showcasing scenario-based solutions for network operators, OTT services, and third-party management systems as defined in the corresponding use cases.

The implementation of the solution in this PoC uses the relevant ZSM specifications as a reference. The design architecture of the use case follows the ZSM framework (ZSM 002) and incorporates the agent-based entity concepts from ZSM020 to realize the defined requirements for autonomous fault and root cause analysis.

2.2 PoC Architecture

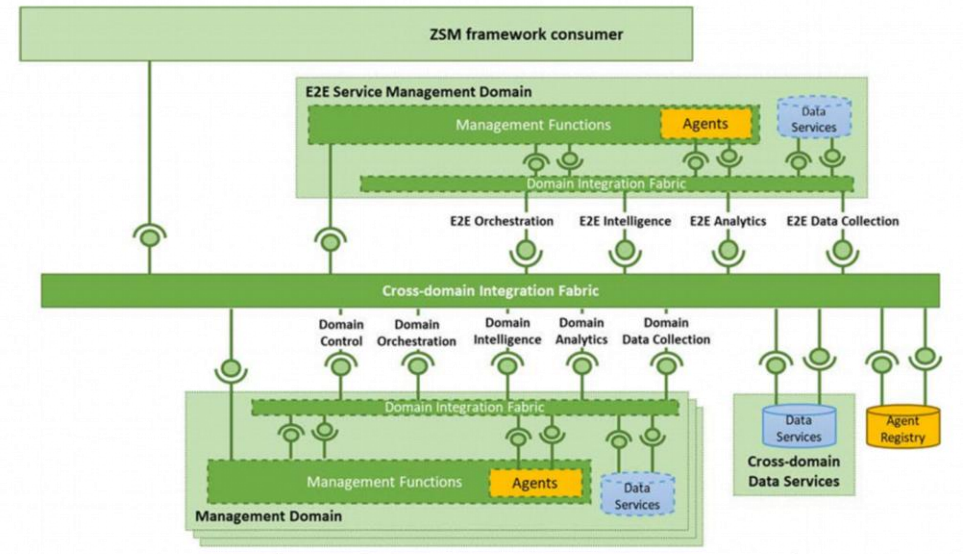

Figure 1 PoC architecture

Figure 1 shows the PoC architecture. It is same as ZSM 020 for Agents in the ZSM framework

2.2.1 Agent-Based Autonomous Fault Diagnosis Architecture

The proposed architecture for agent-based autonomous network fault diagnosis and root cause analysis is designed in accordance with the ETSI ZSM reference architecture [3] and incorporates the agent-based entity concepts defined in ZSM020. As illustrated in Figure 1, the architecture deploys autonomous agents across multiple Management Domains (MDs), including a Radio Access Network (RAN) MD, a Transport Network MD, and a Core Network MD, with a dedicated End-to-End Service (E2ES) MD agent serving as the workflow coordinator for cross-domain fault scenarios. Each domain agent is instantiated with a ZSM020-defined Agent Capability Profile (clause 6.3.1), which formalizes its functional capabilities (e.g., fault detection, data collection, diagnostic algorithms), operational context, and security attributes. These agents register their profiles with a centralized Agent Registry (clause 6.3.2) to enable dynamic capability discovery and support both centralized and decentralized discovery mechanisms as specified in clause 5.1.

2.2.2 Multi-Agent Fault Diagnosis and Root Cause Analysis Process

The fault diagnosis and root cause analysis process follows the cross-domain fault resolution scenario detailed in ZSM020 clause 5.2, enhanced with the task negotiation mechanisms from clause 5.3 and terminology alignment capabilities from clause 5.5. Upon fault detection by a domain-specific agent (e.g., RAN MD Fault Agent), the agent queries the Agent Registry to discover the E2ES MD cross-domain agent with coordination capabilities. The E2ES MD agent forms an investigation team comprising relevant domain agents based on their capability profiles and initiates collaborative diagnosis. During the investigation, agents utilize peer-to-peer and publish/subscribe communication models (clause 6.1) to exchange fault data, share diagnostic insights, and coordinate actions. If an agent encounters an abnormal state due to insufficient contextual information, it initiates the task execution information phase (clause 5.3.3), requesting additional data from other agents to resolve blocking states. The architecture also implements terminology alignment mechanisms, embedding term definitions within agent messages to ensure semantic interoperability across domains using diverse LLMs. Throughout the process, identity management capabilities (clause 6.2.1) ensure secure agent interactions with short-lived, task-specific credentials, while comprehensive audit logging enables verification of analysis results and supports security investigations. This collaborative multi-agent approach enables dynamic, adaptive fault localization and root cause analysis across heterogeneous network domains, demonstrating the ZSM020 normative extensions for autonomous network management.

2.3 PoC Process

Small-model algorithms such as ARIMA (Autoregressive Integrated Moving Average Model) and LSTM (Long Short-Term Memory Network). This solution adopts lightweight models based on the Transformer architecture, such as Log BERT. ARIMA model was used to capture data trends and fluctuations through autoregression and differencing. The PoC process can be described as following:

2.3.1 Set up Data Lake

- **Data Collection:** Upper-layer systems manage network devices and network elements, and continuously collect multi-dimensional real-time and historical data, including device alarms, operational logs, traffic, online user counts, port utilization, and more.
- **Data Integration and Orchestration**: resource status and data analysis from other systems for data acquisition and preprocessing.

2.3.2 Lightweight Small Models for Proactive Prediction

Lightweight AI small models are introduced for specific operational metrics such as traffic and user count. This enables minute-level proactive prediction and anomaly detection.

- **Metric Degradation Prediction Based on Time Series Forecasting Models**: For time-series data like network traffic and user count, small model algorithms such as ARIMA (Autoregressive Integrated Moving Average Model) and LSTM (Long Short-Term Memory) are applied. These models learn from historical traffic data to accurately predict future traffic trends. If real-time traffic data shows a significant and persistent deviation from the predicted value, the system can proactively identify a potential "metric degradation" trend. It can issue a warning before users experience latency or packet loss.
- **Anomaly Detection Based on Log Analysis**: with massive, unstructured log data generated by devices, traditional

keyword matching is inefficient. Log BERT are employed to pre-train on sequences of normal logs to learn inherent patterns and semantics, enabling them to identify abnormal log entries that deviate from normal patterns. Realize a shift from "passively receiving alarms" to "actively discovering anomalies".

2.3.3 Large Language Models for Knowledge-Driven Operations

- **Multi-Modal Data Fusion Analysis**: When the system receives a warning from a small model or an alarm from traditional network, it triggers the LLM analysis engine. Real-time, multi-modal cloud-network data (such as associated alarm lists, abnormal log snippets, current user count, traffic curves, etc.) is composed into a coherent "case description" and submitted to the LLM. The LLM can analyze across different data types, conducting an analysis to preliminarily determine the fault's impact scope and possible root cause.
- **Historical Experience Retrieval Based on RAG**: An operations knowledge base can be constructed. This database contains unstructured documents such as historical fault handling reports, expert experience manuals, and device configuration specifications. Using RAG (Retrieval-Augmented Generation) technology, the system automatically retrieves the most relevant historical cases and solution snippets from the knowledge base based on the current fault scenario and provides them as context to the LLM.
- **Intelligent Matching and Solution Generation**: The LLM integrates the "current on-site situation" with "historical experiences and lessons learned," performing deep correlation and comparison to ultimately generate a structured fault analysis report. The report generates preliminary handling suggestions or operational steps. This process significantly reducing the difficulty of fault localization and the dependence on specific experts.
- **Knowledge Graph**: Composed of three entity nodes: fault description, localization, and solution. Presenting prompts in a graph format supports traceability and addresses the issue of divergence in traditional prompts.

2.3.4 Self-Evolving Operations Knowledge System

To ensure the long-term viability of the solution and achieve continuous optimization, the operational closed-loop mechanism is used for the system to learn from each fault handling process and continuously improve its accuracy.

- **Continuous Accumulation of the Corpus**: After each fault handling is completed, the system archives the event. This includes: the final solution, the extraction of general features and vectorization of multi-dimensional raw data (such as abnormal logs, traffic curves, user count fluctuations, alarm sequences, etc.). This forms a standardized "fault feature vector," which is then associated with the validated effective solution and stored in the platform's corpus.
- **Intelligent Correlation and Matching**: When a new fault occurs, the system calculates in real-time the similarity between the feature vector of the current network state and the vectors of all historical cases in the corpus. Through vector retrieval, the most similar historical scenarios can be found.
- **Achieving a Fully Closed Loop**: The corpus continuously expands and enriches with each fault handling, making retrieval results increasingly precise. Simultaneously, through manual verification and correction of the solutions recommended by the system, historical corpus entries can be annotated and optimized. This enables the system’s self-update , equipping the operations system with learning capabilities.

2.4 PoC Success Criteria

Explain how the proposal intends to verify that the goals are presented in clause A.1.2 have been met

EXAMPLE: Functional (demonstration shown network fault and root cause of PoC proposal worked),

Performance (comparing to current application, the proposed PoC can achieve agent based 1 minute to detect, 5 minutes to locate network ability),

Availability(can be improved by multi domain optimization).

2.5 Additional information

The references used throughout this document are listed below.

[1] ETSI GS ZSM 002: Zero-touch network and Service Management (ZSM); Reference Architecture".
[2] ETSI GS ZSM 020: "Study on the Utilization of Agents in Autonomous Networks;".
[3] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".