**3GPP TSG-SA5 Meeting #144-e *S5-224180rev1***

**e-meeting, 27 June – 1 July 2022**

**Source: CMCC, Huawei**

**Title: pCR TR 28.830 Add relation description with existing MnS**

**Document for: Approval**

**Agenda Item: 6.7.7.2**

# 1 Decision/action requested

***The group is asked to discuss and approve the proposal.***

# 2 References

[1] SP-220153: "New SID on Fault Supervision Evolution"

[2] S5-222733: "draft TR 28.830 Fault supervision evolution"; v0.1.0

# 3 Rationale

Existing fault management has some problems, such as lack of cross-domain coordination, independent fault management, performance management, and configuration management, lack of risk detection and prediction capabilities, and lack of service impact analysis and automatic fault recovery capabilities. Technologies such as 5G network architecture and air interface evolution also raise evolution requirements for fault management, for example, fast fault recovery and prediction of performance degradation and risks in advance. This document describes the objectives and requirements of fault management evolution and introduces the concept of anomaly event and new capabilities related to anomaly event management services.

It is proposed to add description of the above concepts of fault supervision evolution in draft TR 28.830.

# 4 Detailed proposal

This document proposes the following changes in TR 28.830.

|  |
| --- |
| **1st Change** |

# 4 Background and concepts

## 4.1 Background

## 4.2 Concepts

### 4.2.1 Issues in existing fault supervision

The problems of current fault management are as follows:

1) Alarms are mainly network or resource oriented rather than service-oriented, for example, the service or SLS impacts analysis information are not reported.

2) It lacks cross-domain collaboration or correlation analysis of multiple management services, including coordination of fault management, performance management, and configuration management. As a result, cross-domain service and network anomaly or risks cannot be identified, located, and resolved in a timely manner. For example, hardware failure of a transport link may result in a large amount of different alarms in multiple domains, a single fault name indicating the hardware failure is expected from the cross domain management. In exsiting fault management, the correlated alarms are included in alarm notification. However, they are based on alarms, if no alarms are generated, e.g. predictive information or pre-failure performance measurements etc, there will be no such information.

3) Lack of service failure detection and prediction capabilities, leading to passive fault management. Proactive and predicative fault management capabilities are expected.

As 5G networks evolve to new architectures, new air interfaces, new technologies, and new devices, the network complexity is increased to a new level, and customers have higher requirements on experience, which poses new requirements on existing fault management. For example, quick fault recovery, quick SLA response, and performance and risk prediction and mitigation.

Requirements and objectives of fault management evolution:

Based on the preceding background and problems, the requirements for fault management evolution are as follows:

(1) The system can identify anomaly events that affect services and need to be handled from a large number of alarms, and accurately locate root causes.

2) The system can manage multiple devices, multiple management domains, and multiple management functions (or capabilities) from a high-level perspective.

Based on the preceding requirements, the objectives of fault management evolution are as follows:

1) Automatically discover, locate, and diagnose events, faults, exceptions, and risks in the system by introducing automation and intelligence capabilities.

2) Complement cross-domain and service-oriented comprehensive O&M. From reactive response to proactive prevention, identify potential service quality risks and rectify them in a timely manner to ensure normal service operation and improve network reliability and effectiveness.

3) Correlate data from multi-dimensional sources, identify and rectify problems that affect services or are about to affect services in a timely manner, and introduce AI and automation technologies to drive the evolution of network O&M to AN (autonomous network).

### 4.2.2 Concept of anomaly event and fault supervision evolution

Based on the objective of fault management evolution, the term "anomaly event" is used to indicate anomaly (anomaly) that affects or is about to affect services and which requires corresponding actions to be taken to rectify the anomaly issues. This terminology is used as an aggregation name to indicate the anomaly issue to be precisely monitored and resolved. For example, anomaly event such as device faults, parameter abnormalities, connection interruption, line deterioration, external environment factors, and external emergencies occur or will affect services, service processing capability deterioration, service interruption, and user experience deteriorition.



Figure 1: relationship between event, alarms and anomaly events

Figure 1 depicts the concepts relationship among event, alarms and anomaly event. An anomaly event may originate from an alarm of a device or service, a performance/quality/experience indicator TCA (Threshold Crossing Alarm), an operation exception, or a system exception, and/or a combination thereof.

Anomaly event could be classified in two ways:

by impact severity, including interruption (network or service unavailability), deterioration (performance or experience deterioration), and risks. (i.e. disruption, deterioration, or customer complaint).

By impacted object, including resource-layer anomaly events (NEs and network-layer incidents), service-layer anomaly events (data and voice events), and customer-layer anomaly events (customer complaints and experience events).

Correspondingly, the fault management evolution takes anomaly events as managed objects. Based on multi-dimensional data and AI/ML technologies, the anomaly event identification, analysis, decision, and execution process are used to detect and resolve events. This eliminates the impact on services and ensures normal network and service O&M.

Compared with existing fault management, the evolution of fault management includes the following changes:

(1) Device/network-oriented -> Service-oriented

(2) Reactive response - > proactive prevention

(3) Single data source -> Multi-dimensional data sources

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

.

|  |
| --- |
| **End of change** |