**3GPP TSG-SA5 Meeting #144-e *S5-224180rev2***

**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** |

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1] TR 28.830 “Fault Supervision Evolution”

[2] ITU-T Recommendation X.731 (1992) | ISO/IEC 10164-2 : 1992, *Information technology – Open Systems Interconnection – Systems Management – State management function*.

[3] TS 28.625 State Management Data Definitions

[4] ITU-T Recommendation X.733 (1992) | ISO/IEC 10164-4 : 1992, *Information technology – Open Systems Interconnection – Systems Management – Alarm reporting function*.

[5] TS 28.532 Generic management srvices

[6] ITU-T Recommendation X.739 (1993), *Information technology – Open Systems Interconnection – Systems Management – Metric Objects and attributes*.

[7] ITU-T Recommendation E.880 (1993), *Telephone network and ISDN Quality of service, network management and traffic engineering. Field data collection and evaluation on the performance of equipment, networks and services*

[8] TS 28.552 5G performance measurements

[9] TS 28.554 5G end to end Key Performance Indicators (KPI)

|  |
| --- |
| **Next modification** |

# 4 Background and concepts

## 4.1 Background

## 4.2 Concepts

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

The term "anomaly event" is used to indicate an abnormal issue related to multiple managed objects that affects or is about to affect services or network with an explicit impact analysis 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 related to potentially one or more managed objects, that needs to be precisely monitored and resolved. For example, anomaly event such as user experience deteriorition prediction based on correlation analysis with FM, PM, log data from multiple devices or network domains.

In such context, the corresponding managed data is no longer individual alarms, but the identified anomaly event (identified from a group of FM, PM and other management data by correlation and impact analysis) .

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).

In comparison, an existing alarm or warning is related to a specific managed object, and bears the related severity information only related to the managed object. While anomaly event represent an issue (already happened or about to happen) that could have a critical or major impact to the aggregated functionality provided by one or more managed objects.

Correspondingly, the fault supervision evolution takes anomaly events as managed data.

### 4.2.2 Issues in existing fault supervision

Since several decades the telecommunication management network offers a multitude of possibilities to inform about specific states of the system [2, 3], errors and faults by using alarms [4, 5], and about the performance related indications like counters, KPIm gauges, aggregations, statistics, and thresholds, e.g [6 - 9].

Already the first paragraph on the model of alarm reporting [4, clause 7] describes the importance to use thresholds and to detect trends in order to provide warnings to the managers. This means the managed systems are encouraged to use means to detect abnormal conditions as early as possible in order to inform the management system by standardized means about the situation.

[4, clause 7] also highlights the importance to correlate multiple events. While the correlation is an internal function of management systems, the interfaces are supporting the correlation by specific fields to associate multiple events to each other. This also is true for the corresponding 3GPP specifications, which to a large extent are based on the specifications by ITU-T. The correlation in existing specification mainly concern alarm notifications, other type of data e.g. normal performance measurements, KPIs, historical data etc could also be considered for more comprehensive analysis.

The combination of alarm reporting and state managent is able to reduce the number of alarm messaged very efficiently if certain best practices are followed: If alarms are used to indicate that a resource requires maintenance, and states are used to inform about the well-being of a resource.

For example, in case a backhaul link towards a gNB has a problem, many logical and physical interfaces of the gNB, many protocol layers, and all cells will experience certain abnormal conditions. If all these resources are raising alarms, then the management system will choke in alarms -although none of these alarms requires any maintenance, since the problem is caused by the link, while the base station as such has no problem at all.

If in such situation the resources would consider the rule to issue alarms only in case they require maintenance, then the base station would not send any alarm, while all affected resources would set their operational state to “disabled” and the availability state to “dependency”. In this case the human operator would be aware that the base station does not work as expected and would be also aware of the fact that the base station as such does not require any maintenance.

However such operation may be risky because the base station may not be aware the nature of the real issue by itself, and filtering of alarms may hide potential faults in the resources. In this case, a higher level management is helpful to correlate alarms and other related data to identify the anomaly issue related to one or more managed objects with impact analysis.

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

.

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