**3GPP TSG-SA5 Meeting #144-e *S5-224182rev1***

**e-meeting, 27 June – 1 2022**

**Source: CMCC, Huawei**

**Title: pCR TR 28.830 Add description of key issue performance degradation**

**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

5G networks provide high rates and low latency for services, but also result in high sensitivity and low tolerance of services to performance degradation. On the live network, a certain cell in a cell cluster is faulty. As a result, multiple cells generate a large number of alarms at the same time. This is because UEs in the faulty cell are handed over to different neighboring cells at the same time, causing congestion alarms and performance deterioration in multiple cells. Different types of alarms may be generated due to different fault symptoms in different cells. In the current fault management system, multiple work orders may be generated for O&M personnel to handle. In fact, only alarms of faulty cells need to be processed by work orders, which wastes human resources and takes a long time to rectify faults.

It is expected that the 3GPP management system could generate a single “anomaly event” according to the correlated alarm notificatins and the performance data etc. An anomaly event name is assigned to represent the issue or symptom that has negative impacts on network or service operations. The 3GPP management system analyzes the aggregated data and the context information to further identify the root cause and try to recover the anomaly event. The anomaly event is also generated and its progress status is recorded and reported to the operator, for the monitoring purpose. Therefore, the complexity and heavy burden of monitoring and handling of a large amount of alarms manualy from multiple management domains could be reduced greatly

In particular, the following information attributes are expected to be provided in the context of an identified anomaly event report purpose:

* Sequence number of the anomaly event, which uniquely represents an anomaly event, differentiating from a normal alarm which always needs operation by default.
* Name of the anomaly event, which represent the negative issue identified from a group of correlated alarms, and the other related data described in “data collection”.
* Description of the anomaly event, more detailed information of the anomaly event.
* Severety level of the anomaly event, which represent the urgency and sererety degree of the anomaly event, e.g. critical, high, medium, low etc.
* Create time, which represent the generation time of the anomaly event.
* Sources, which represent the associated one or multiple objects of the anomaly event.
* Affected resources, the network objects which are affected by the anomaly event, e.g. network slice, network slice subnet, network elements, network functions etc.
* (Optional) affected services, the services and users which are affected by the anomaly event, e.g., the name and range of the affected services such as VoNR, URLLC service, access of network, number of users, coverage area etc.
* Root cause of the anomaly event, e.g. the root cause and the associated source objects which result in the anomaly event corresponding to group of alarms, hardware failure, location of the root cause etc.

However, existing FM in the resource layer does not support the management of a single “anomaly event” representing a group of correlated alarms and the associated managed objects. In existing fault management (FM) in the resource layer, the alarms are associated with an EM or a NE, if faults are detected in the managed object, alarm notifications would be generated for each of managed object. A single network fault may result in the generation of multiple alarms and events from affected entities over time and spread over a wide geographical area. If possible, the OS should indicate which alarms and events are correlated to each other. Such correlation capability is described for FM in OSS layer. The correlation describes relations between network events (e.g. current alarms as those captured in AlarmList, historical alarms as those captured in NotificationLog, network configuration changes). “*correlatedNotifications*” is defined for this purpose. Moreover, “*rootCauseIndicator*” may indicate whether an alarm notification is the root alarm or not, “*ProbableCause*” may also be indicated.

While in this context, the consumer concerns more on the aggregated group of alarms as an integral issue to be tracked and handled, i.e. the nature of the end result or the symptom of the correlated alarms, instead of each individual alarms. In existing FM, the managed alarms are still multiple individual alarms and their correlated alarms, even with the alarm correlations are provided.

From the consumer’s perspective, a single “anomaly event” report is more preferred to be used to represent the group of alarms, and the lifecycle “anomaly event” is managed from its generation to clearance. The progress status of the “anomaly event” could be observed by the consumer.

In addition, the monitoring consumer needs to know the classifications of the anomaly events, their service impacts definintions, analytics information, recovering related APIs etc. in order to decide whether it is needed to take an action on it. The capabilities to convey these information are not defined in existing FM or PM.

It is proposed to add description of key issue anomaly event supervision in draft TR 28.830.

# 4 Detailed proposal

This document proposes the following changes in TR 28.830.

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

# 5 Key Issues and potential solutions

## 5.X Key Issue #2: Anomaly Event Supervision

### 5.X.1 Description

Editor’s note: This clause provides a description of the key issue.

5G networks provide high data rates and low latency services, it is high sensitive and low tolerance of performance degradation for some services. As depicted in Figure X, if the service becomes unavailable in an access cell A1 due to a kind of fault, the users in cell A1 need to be handed over to a neighboring cell (for example, A2, A3, and B2). When the traffic load of the cell cluster is too high, alarms related to performance degradation are reported, such as:

1) Alarm1: Cell A1 is unavailable.

2) Alarm2: Cell A2 (or cell A3, B1, and B2) cannot be accessed.

3) Performance alarm 1: Cell cluster service access degradation;

4) Performance alarm 2: Cell cluster service congestion and degradation.



Figure X

The preceding types of alarms are generated. However, only the Alarm1 needs to be handled. Lack of root cause analysis results in waste of resources and time-consuming rectification.

The 3GPP management system should provide the capability to resolve the preceding kinds of alarms, and analyze root causes, recommend corresponding solutions and implement the recovery actions in more efficient means. For example, the 3GPP management system obtains alarm, performance, and configuration information and performs multi-data source correlation analysis, e.g., top N degraded cell identification, KPI trend analysis etc. For example, the performance degradation anomaly event is reported. Then it demarcates and analyzes the root causes of performance degradation anomaly event, and provides corresponding solutions for recovery. Therefore, only a single anomaly event name indicating the cell A1 failure is reported by the 3GPP management system, based on the alarms and performance measurements received from existing FM and PM data etc.

FSEV\_REQ SUPERVISION1: The 3GPP management system should provide the capability to support anomaly event monitoring and report, as an integral issue to be tracked and handled, including all the correlated alarms and events.

FSEV\_REQ SUPERVISION2: The 3GPP management system should provide the capability to support anomaly event monitoring and report, providing the information over the classifications of the anomaly events, their service impacts definintions, analytics information, recovering related APIs etc..

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