**3GPP TSG-SA5 Meeting #145-e *S5-225xxx***

**e-meeting, 15 – 24 August 2022**

**Source: Huawei, CMCC**

**Title: Discussion paper on FSEV study**

**Document for: Approval**

**Agenda Item: 6.7.7.1**

# 1 Decision/action requested

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

# 2 References

[1] [SP-220153](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3693): "New SID on Fault Supervision Evolution"

[2] S5-224406: "draft TR 28.830 Fault supervision evolution"; v0.2.0

# 3 Introduction

The study of FSEV has been discussed for several meetings, including the background, concepts, relation with existing FM and PM etc, use cases and potential solutions, management framework, management requirements and potential interface impacts, etc. Some existing basic concepts are included in [2].

In the following sections, some issues are discussed to seek consensus.

# 4 Analysis of existing FM and FM

In [2], some existing concepts are included e.g., alarm, fault, root cause etc. In Table 1, some considerations are listed.

**Table 1**

|  |  |  |
| --- | --- | --- |
| No. | Concept | Considerations |
| 1 | **event notification** | A generic concept about notifications used to inform the recipient about the occurrence of an event. |
| 2 | **Alarm** | There are different serverity level of alarms, including low critical warnings. The alarms may be triggered by fault or threshold based performance issues.Some alarms have network and/or service impacts and need operator’s actions, some alarms have no or trivial network and/or service impacts and no operator’s actions are needed. Manual analysis and processing may be needed. |
| 3 | **Fault** | A deviation of a system from normal operation. Alarms may be generated, usually there are network and service impacts. Manual analysis may be needed to identify faults from alarms. |
| 4 | **Root cause analysis** | In existing FM specs, rootCauseIndicator (boolean) and probableCause are included. |

Based on analysis of some existing concepts, some issues can be observed as in Figure 1:



Figure 1

Existing FM and PM does not differentiate (1), (2) and other alarms for which there are no network or service impacts and no actions are needed. They do not support for use cases of (3) and (4) either.

It should be indicated that warnings are different from (3) and (4). Warning is considered the lowest critical alarms, e.g. error rates by means of threshold increases. The prediction has wider scope, and its severity level could be managed separately.

In use case (4), dynamic threshold, multi-parameter/KPI correlation analysis etc are examples of non static threshold types, which have been widely considered in intelligent operation solutions.

Existing FM supports alarm correlation, the “correlatedNotifications” is included in the alarm reporting interface. In figure 2, an example of alarm correlation is depicted. In existing FM, each Alarm is still managed as individual managed data (MnS component C), and their associated managed objects (MnS component B) are also managed separately. For the correlated alarms, it is expected that the group of alarms and their associated managed objects could be managed as an integral or aggregated objects, including managed data and managed objects. The term “Anomaly event” is used for the purpose of description simplification, it represents the use cases in (1), (2), (3) and (4), and used as managed data with its associated managed objects.



Figure 2

It is expected that the new aspects described above could be investigated in FSEV SI.

# 5 Use cases which may demand potential new management capabilities

## 5.1 Service outage

Service outage is a typical anomaly issue in the network, e.g., multiple gNBs may be out of service simultaneously. Multiple domains will be involved and it will cause the End to End service outage. A large amount of alarms will be reported in RAN domain and CN domain. It is complex and time consuming to identify the root cause and recover from the anomaly situation. In some existing solutions, human operators from RAN domain, CN domain and TN domain will be involved to analyse the alarms, identify the root cause and try to recover the anomaly separately from the domain perspective. As a result, it is difficult for manual fault demarcation and locating from each separate domains.

3GPP management system need to identify the service outage issue from the large amount of alarms from multiple domains and report the issue and its recovering status to the MnS consumers.

## 5.2 Performance degradation

5G networks provide high rates and low latency for services, but also result in high sensitivity and low tolerance of services to performance degradation. Multiple cells may generate a large number of alarms at the same time due to accessibility problem in one of the cells in a cluster. 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.

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 managed objects could be reduced greatly.

3GPP management system need to identify the correlation of performance degradation issue of multiple managed objects, report the issue to the MnS consumer and try to resolve it automatically.

## 5.3 Data service failure prediction

A failure of the 5G core network will affect data services on a large scale. The passive O&M operations are not very efficient for service recovery if it only responds after the faults have been reported. It is necessary to demarcate and locate cross-layer faults on the cloud-based core network.

The 3GPP management system should proactively predict 5GC service failure on the 5G core network in advance, demarcate and locate faults, and provide corresponding solutions to improve problem handling efficiency. This reduces the impact on services and ensures stable network operation. KPIs anomaly are predictively analysed to prevent potential failure in advance. This could be implemented based on single indicator trend analysis or multiple indicators correlated analysis. AI/ML technologies can be used for data analysis and proactively identify and prevent potential 5GC service failure. For the predicted service failure, associate alarms with different data sources, demarcate the NFs where the 5GC service failure may occur, and locate the affected object of the service failure prediction. Finally, solutions can be provided and implemented, or the related 5GC failure prediction anomaly event can be reported to the upper-layers.

3GPP management system need to predict data service failure risks, report the issue to the MnS consumer and try to resolve it automatically.

## 5.4 Summary of some potential new management capabilities

If a new term “anomaly event” is used to cover the issues in the use cases in this clause, classified as (1), (2), (3) and (4) in clause 4, some new management capabilities can be observed as follows:

* Anomaly event identification and automatically recovering in the domain management and cross domain management.
* Anomaly event transmission to request for further handling from the domain management to the cross domain management.
* Life cycle management of the anomaly event in the domain management and cross domain management, including anomaly event creation, update and clearance upon recovering.
* Anomaly event and its status monitoring, statistics, querying and subscription for both domain management and cross domain management.

# 6 What new information may need to be reported

3GPP management system may need to support anomaly event reporting and querying, including at least the following attributes:

* Sequence number of the anomaly event, which uniquely represents an anomaly event.
* 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 scope 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.

# 7 Whether to introduce new management aspects in existing FM or PM, or introduce new MnS producer

Based on discussions above, it is considered that there is no proper concept or terminology that can cover all the different abnormal use cases asdescribed in clause 5. Some new management capabilities may need to be considered as described in clauses 5.4 and 6.

(1) Correlation analysis and processing for a group of relevant alarms or predicted issues and their associated managed objects as an aggregated managed data and managed object. The existing alarm information is managed separately for an individual managed object. Although the interface may report correlatedNotifications, each alarm is independent and its status changes are managed separately. Therefore, MnS consumers may need to manually analyze the alarms and their correlations.

(2) Threshold-based performance alarms are statically configured and cannot be flexibly analyzed based on different service types and scenarios. Dynamic threshold-based alarms are not supported. Some performance alarms need to be correlated with multiple KPIs for joint analysis to determine whether an exception occurs. The existing static threshold based performance alarm mechanism does not support such capability.

(3) The alarm reporting interface does not support indication of fault, performance degradation, or risk prediction which have network and/or service impacts from a large amount of ambiguous alarms. Currently, warning indicates low severity level alarms and cannot indicate the prediction of major potential problems. It is expected to manage severity level of predicted issues separately.

(4) Lack of network and service impact analysis, for example, the specific impact of an anomaly event on the network or user services, the impact scope, and the impact degree.

(5) Lack of closed-loop management capabilities for the anomaly events, such as automatic analysis, demarcation and locating, and rectification capabilities.

New concepts or terms and management capabilities may need to be introduced. The existing FM or the PM are independent management services. The above scenarios involve the management services of the FM, PM and other related MnS producers. FM or PM solely may not be able to handle all the above scenarios. Therefore, introducing a new management service to cover all the above situations is a more simplified approach and avoids major modifications to the existing management system, which may cause backward compatibility issues and higher costs.

Therefore, it is recommended that a new MnS producer is introduced to support the preceding use cases and scenarios. Outputs of existing FM, PM and other related MnS producers can be used as different data sources for the new MnS producer for further processing. The anomaly event would be identified, reported and managed. Its lifecycle management and closed loop handling forms the govenance functions of the new MnS producer. Existing provisioning management can be invoked for support of corrective actions.

# 8 If new MnS producer is introduced, its potential framework

The anomaly event MnS producer is introduced and it provides the following external capabilities:

* Anomaly event monitoring such as the name, status, network and/or service impacts and correlation information of the anomaly event.
* Anomaly event subscription and query.
* Anomaly event governance, including lifecycle management of anomaly event, and potentially configurecustomized policies for anomaly event management etc.

As depicted in Figure 3, the anomaly event MnS producer is introduced for the closed loop handling of anomaly event. The anomaly event is identified based on correlated group of alarms and the related performance data, configuration data, historical data etc. An anomaly event name is assigned to represent the issue that has negative impacts on network or service operations. The anomaly event MnS producer 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 MnS consumer. Existing alarm notifications and performance measurements are operated as today however the MnS consumer could choose to filter them out and focus on anomaly events and their processing status, therefore, the complexity and heavy burden of monitoring and handling a large amount of alarms manualy from multiple management domains could be reduced greately.



**Figure 3: 3GPP Management architecture with the introduction of anomaly event MnS producer**

The Anomaly event MnS producer in domain management tries to identify and automatically recover the anomaly event in its own domain, and may report the generated anomaly event to the anomaly event MnS producer in the cross domain management based on subscription or only reported if it cannot be handled by its own domain, e.g. in the case which may involve other management domains.

# 9 Detailed proposal

It is proposed to discuss the FSEV study in the following aspects:

* Whether existing FM and PM are sufficient to handle the use cases and issues listed above.
* Whether new management capabilities are needed to identify and resolve the anomaly events and the network and/or service impacts?

Based on the above answers, it can be further discussed that:

* Firstly to focus on the technical descriptions of concepts, use cases, issues, management capabilities and potential interface impacts;
* Then to discuss whether to extend existing FM and/or PM MnS separately or introduce new MnS to cover all potential new aspects;