|  |
| --- |
| 3GPP TR 28.830 V18.1.0 (2024-06) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on fault supervision evolution;(Release 18) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttps://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Background 7

5 Issues and potential solutions 9

5.1 Issue 1: Missing definitions 9

5.1.1 Description 9

5.1.2 Potential solutions 9

5.1.3 Conclusion - Impact on normative work 9

5.2 Issue 2: Potential enhancements for fault related analysis 9

5.2.1 Description 9

5.2.2 Potential solutions 10

5.2.2.1 Potential solution 1: Failure prediction enhancement 10

5.2.2.1.1 Introduction 10

5.2.2.1.2 Description 10

5.2.2.1 Potential solution 2: Fault impact analysis 10

5.2.2.2.1 Introduction 10

5.2.2.2.2 Description 10

5.2.2.3 Potential solution 3: Fault cause analysis enhancement 11

5.2.2.3.1 Introduction 11

5.2.2.3.2 Description 11

5.2.3 Conclusion - Impact on normative work 11

6 Fault supervision evolution relation and interaction with MDA and closed loop control 11

7 Conclusions and recommendations 12

Annex A (informative): Change history 13

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document investigates potential use cases, requirements and solutions for the fault supervision evolution, its relation with performance management and fault supervision, relation and interaction with MDAS and COSLA, and potential enhancements for MDA assisted fault management. The present document provides conclusions and recommendations on the normative work.

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

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

[3] 3GPP 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] 3GPP TS 28.532: "Generic management services".

[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] 3GPP TS 28.552: "5G performance measurements".

[9] 3GPP TS 28.554: "5G end to end Key Performance Indicators (KPI)".

[10] 3GPP TS 28.111: "Fault management".

[11] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics (MDA)".

[12] 3GPP TS 28.535: "Management and orchestration; Management services for communication service assurance; Requirements".

[13] 3GPP TS 28.536: "Management and orchestration; Management services for communication service assurance; Stage 2 and stage 3".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

## 3.2 Symbols

None.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1]. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

# 4 Background

Since several decades the telecommunication management network offers a multitude of possibilities to inform about specific states of the system [2] and [3], errors and faults by using alarms [4] and [5], and about the performance related indications like counters, KPI 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. Any new proposal has to consider already existing solutions in order to avoid diverging, non-interoperable frameworks.

ITU-T Recommendation X.733 [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. Correlation in existing specifications mainly covers alarm notifications, although 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 management would be able to reduce the number of alarm messages 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, although the mechanism described above have been standardized by ITU-T in 1992, such mechanisms are not applied in currents systems. Reducing the number of alarms in the network elements by simple filtering of alarms imposes the risk to miss important information that might be needed by other management functions. Therefore, it requires the network elements to perform thorough correlation of notifications and state information in order to suppress redundant information only, but not to suppress information that is needed by higher level management tools.

It is an unfortunate fact that -since ever- the management systems as well as the human operators are choking in alarms, although a combination of alarm reporting and state management would offer a technical means to reduce the number of alarms. As a matter of fact, the determination whether an abnormal behavior is caused by an entity itself or by another entity (or subsystem) requires sophisticated correlation functions that are able to be reliable in order to avoid erroneous correlations resulting in false statements about the root cause. Implementation of such functions require high implementation effort because it requires the knowledge of all dependencies.

An additional problem is that TS 28.532 [5], clause 11.2, which defines the Fault Supervision MnS, does not provide the necessary definitions and descriptions required to understand the current state of art as to alarm management. This is because much of the material specified and available for the IRP Framework was not moved to SBMA.

For that reason, this study investigates which definitions and descriptions need to be added to TS 28.532 [5], clause 11.2 to make this clause understandable without need to consult other specifications. Besides descriptions for alarm management, the role and importance of state management are highlighted as well.

It is also in scope of this study to look at possibilities to clarify in TS 28.532 [5] that internal behavior of functions is not subject to standardization. For example, the algorithm used to accomplish alarm correlation is outside the scope of standards. This implies that deliberations on if AI/ML is used for correlation or not is also outside the scope of standards. It is a vendor decision to use AI/ML or not.

The scope of this study includes potential enhancements to MDA assisted fault management. MDA capability may be used or enhanced for the fault related analysis. The MDA capability "failure prediction" supports the prediction of the running trend of network and potential failures to intervene in advance. More alarm/fault related analysis scenarios and capabilities will be studied. Existing alarm data is needed as one of the data sources for the analysis.

# 5 Issues and potential solutions

## 5.1 Issue 1: Missing definitions

### 5.1.1 Description

TS 28.532 [5], clause 11.2, which defines the Fault Supervision MnS, does not provide the necessary definitions and descriptions required to understand the current state of art as to alarm management. This is because much of the material specified and available for the IRP Framework was not moved to SBMA.

### 5.1.2 Potential solutions

It is proposed to add the following definitions to an appropriate TS:

**Event:** Anything that occurs at a certain point in time, for example a configuration change, a threshold crossing, a transition to an error state or a transition to a failure state. Events do not have states.

**Error**: A state of the system different from the correct system state as defined by the service specification. An error may or may not lead to a service failure. An error has a begin and end time.

**Failure:** A state of inability to deliver the correct service as defined by the service specification. A service failure may be the result of an error or a poor service function design.

**Fault**: The (hypothesized or adjudged) cause for an error or a failure.

**Alarm**: An error or failure that requires attention or reaction by an operator or some machine. Alarms have state.

**Root cause:** The primary fault (cause), if any, leading to one or multiple errors or failures.

### 5.1.3 Conclusion - Impact on normative work

The proposal in clause 5.1.2 has been considered in TS 28.111 v1.0.0 [10], therefore no further normative work is needed.

## 5.2 Issue 2: Potential enhancements for fault related analysis

### 5.2.1 Description

If a potential fault/failure is predicted and reported to the consumer, the consumer would like to know the consequence. More analysis information on 3GPP system may be provided for the consumer to perform more proper actions, e.g., performance degradation analysis and predictions, KPI anomaly analysis and predictions, etc.

For example, the impacts on 3GPP system may not be perceived significantly in densely populated urban areas if there are overlapping coverage when a few sites encounter faults. However, service outage may occur due to faults in a site if there are few overlapping coverage in suburban areas. If this kind of information can be provided, the different handlings may be performed by the consumer.

### 5.2.2 Potential solutions

#### 5.2.2.1 Potential solution 1: Failure prediction enhancement

##### 5.2.2.1.1 Introduction

Some potential enhancements to failure prediction are provided. The concrete potentialFailureType is defined as standardized value of the alarmType in TS 28.532 [5].

##### 5.2.2.1.2 Description

Failure of service and network functions may occur during the network operation. It is necessary to predict potential failures and prevent more severe impacts. The MDA capability of failure prediction has been specified in TS 28.104 [11], the analytics output are as follows:

- failurePredictionObject;

- potentialFailureType;

- eventTime;

- issueID;

- perceivedSeverity.

The potentialFailureType in the failure prediction analytics output need to be defined more concretely. The potentialFailureType may reference to the standardized AlarmType. The MDA service may coordinate with fault supervision for identification and analysis of alarm types. The attribute name is also modified to predictedFailureType.

Table 5.2.2.1.2-1: Analytics output for failure prediction

|  |  |
| --- | --- |
| Attribute Name | Description |
| predictedFailureType | Indication of type of issues that can cause the failures.(see note) |
| NOTE: The values can be defined as a list of values of the alarmType described in TS 28.532 [5]. |

#### 5.2.2.1 Potential solution 2: Fault impact analysis

##### 5.2.2.2.1 Introduction

The MDA type of failure prediction may need to provide fault impact analysis information.

##### 5.2.2.2.2 Description

The scope and degree of fault impacts are evaluated and provided in MDA type of failure prediction in TS 28.104 [11]. It may contain the following aspects:

- Scope and service types which are impacted by the fault.

- A list of managed objects which are impacted by the fault.

Table5.2.2.2.2-1: MDA analytics output of fault impacts in failure prediction

|  |  |
| --- | --- |
| Attribute Name | Description |
| affectScope | Coverage areas which are affected by the fault, e.g. a list of cells, a list of tracking areas (TAs), etc.  |
| affectService | Service types which are affected by the fault, e.g. the VoNR, URLLC service types. |
| affectNumOfPDUSessions | Number of PDU sessions which are affected by the fault. |
| affectManagedObjects | The object instances which are impacted by the fault, e.g. network slice, network slice subnet, network elements, network functions, a list of gNBs, etc. |

#### 5.2.2.3 Potential solution 3: Fault cause analysis enhancement

##### 5.2.2.3.1 Introduction

The MDA may provide capability of probableCause analysis.

##### 5.2.2.3.2 Description

In TS 28.532 [5], the alarm notification can provide information of probableCause. The attribute probableCause uses the definitions in ITU-T Recommendation X. 733 [4]. The MDA analytics report may add the probableCause, therefore the fault supervision management service producer may use this probableCause of MDA analytics output for the next coming alarm notification of the same alarm type. The values can refer to the Probable Causes list in Annex A (normative) in TS 28.111 [10]. The attribute of probableCause may be added to existing MDA Type MDAAssistedFaultManagement.FailurePrediction.

Table 5.2.2.3.2-1: MDA analytics output of probableCause in failure prediction

|  |  |
| --- | --- |
| Attribute Name | Description |
| probableCause | Provide the analysis report of the probableCause as listed in Annex A (normative) in TS 28.111 [10]. |

### 5.2.3 Conclusion - Impact on normative work

It is proposed to study the issue further in the Study on Management Data Analytics (MDA) – Phase 3, objective Fault management related analytics and alarm prediction.

# 6 Fault supervision evolution relation and interaction with MDA and closed loop control

TS 28.104 [11] provides the description of MDA role in management loop in clause 6. The attribute of MDA type specified in TS 28.104 [11] provides the indicator in analytics outputs for particular management capability. The clause 7.2.3 of TS 28.104 [11] includes the use case(s) and requirements of MDA assisted fault management. Some MDA capability enhancements to provide more analytics information related to fault management are described in clause 5.2 in the present document.

Currently, the closed control loop specified in TS 28.535 [12] and TS 28.536 [13] only concerns communication service assurance scenarios (including network slice and network slice subnet). It is to be studied if the scope of closed control loop can be extended to cover the fault management case.

# 7 Conclusions and recommendations

The present document investigated missing definitions, potential enhancements of fault supervision, and its interaction with MDA. The work is proposed in clause 5.2.3.

Annex A:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-04 | SA5#142e | S5-222371 | - | - | - | Initial skeleton | 0.0.0 |
| 2022-04 | SA5#142e | S5-222625S5-222526 | - | - | - | 1. Add TR structure2. Add scope  | 0.1.0 |
| 2022-07 | SA5#144e | S5-224383 | - | - | - | Add key issue on definition of terms | 0.2.0 |
| 2022-08 | SA5#145e | S5-225713 | - | - | - | 1. Add clause Background2. Align TR front page title with SA WG5 official title | 0.3.0 |
| 2023-03 | SA5#147 | S5-233156 | - | - | - | 1. update scope of the study2. propose basic definitions | 0.4.0 |
| 2023-03 | SA5#147 | S5-233157 | - | - | - | add description of fault related analysis | 0.4.0 |
| 2023-08 | SA5#150 | S5-236079 | - | - | - | Add description of failure prediction enhancement | 0.5.0 |
| 2023-10 | SA5#151 | S5-237178S5-237179 | - | - | - | 1. S5-237178 pCR TR 28.830 Add solution of fault impact analysis2. S5-237179 pCR TR 28.830 Add description for MDA and close loop control | 0.6.0 |
| 2023-11 | SA5#152 | S5-238265 |  |  |  | Add solution of fault cause analysis enhancement | 0.7.0 |
| 2024-02 | SA5#153 | S5-240412S5-240413S5-240921 |  |  |  | 1.S5-240412 pCR TR 28.830 Add conclusion of issue1 Missing definitions2.S5-240413 pCR TR 28.830 Rapporteur clean up3.S5-240921 pCR TR 28.830 Add conclusion of issue2 Potential enhancements for fault related analysis | 0.8.0 |
| 2024-03 | SA#103 | SP-240262 |  |  |  | Draft after editHelp review and submitted to SA plenary for information and approval | 1.0.0 |
| 2024-03 | SA#103 |  |  |  |  | Upgrade to change control version | 18.0.0 |
| 2024-06 | SA#104 |  | 0001 | - | F | Rel-18 CR for TR 28.830 Update fault supervision evolution background descriptions | 18.1.0 |