ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T M.3383 (04/2023)

SERIES M: Telecommunication management, including TMN and network maintenance

Telecommunications management network

Requirements for log analysis in telecom management with artificial intelligence

ITU-T M-SERIES RECOMMENDATIONS

Telecommunication management, including TMN and network maintenance

Introduction and general principles of maintenance and maintenance organization	M.10-M.299
International transmission systems	M.300-M.559
International telephone circuits	M.560-M.759
Common channel signalling systems	M.760-M.799
International telegraph systems and phototelegraph transmission	M.800-M.899
International leased group and supergroup links	M.900-M.999
International leased circuits	M.1000-M.1099
Mobile telecommunication systems and services	M.1100-M.1199
International public telephone network	M.1200-M.1299
International data transmission systems	M.1300-M.1399
Designations and information exchange	M.1400-M.1999
International transport network	M.2000-M.2999
Telecommunications management network	**M.3000-M.3599**
Integrated services digital networks	M.3600-M.3999
Common channel signalling systems	M.4000-M.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T M.3383

Requirements for log analysis in telecom management with artificial intelligence

Summary

Recommendation ITU-T M.3383 introduces the requirements for log analysis in telecom management with artificial intelligence (AI) and includes a functional framework, functional requirements, and typical scenarios of log analysis in telecom management with AI. This Recommendation gives examples of some log types and characteristics. This Recommendation also describes use cases of log analysis in telecom management with AI.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T M.3383	2023-04-29	2	11.1002/1000/15516

Keywords

AI log data, AI log acquisition, data processing, log analysis, telecom management with AI.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T M.3383

Requirements for log analysis in telecom management with artificial intelligence

1 Scope

This Recommendation specifies, for log analysis in telecom management with artificial intelligence (AI), including functional framework, functional requirements, and typical scenarios of log analysis in telecom management with AI. This Recommendation is applicable to the design, development, and application of log analysis in telecom management with AI.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3080] Recommendation ITU-T M.3080 (2021), *Framework of artificial intelligence enhanced telecom operation and management (AITOM)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 artificial intelligence capability set [ITU-T M.3080]: A set of functions that are provided based on orchestrated artificial intelligence (AI) models to meet the requirement of some specific application scenarios.

NOTE 1 – Specific application scenarios are to realize quality assurance, efficiency improvement, cost management, security assurance and industry applications, which are used for telecom operation and management.

NOTE 2 – An AI capability can be generated through AI model orchestration based on the requirement of a specific application scenario.

NOTE 3 – These functions may, but do not have to, be used based on the requirements of specific application scenarios.

3.1.2 artificial intelligence engine [ITU-T M.3080]: The realization and mechanization, in software or hardware, of one or more functions dedicated to performing a specific artificial intelligence (AI) task.

3.1.3 artificial intelligence model [ITU-T M.3080]: The model created by applying artificial intelligence (AI) technology to data to learn from.

3.1.4 artificial intelligence pipeline [ITU-T M.3080]: A set of logical nodes, each with specific functionalities, that can be combined to form an artificial intelligence (AI) application in systems of telecom operation and management.

3.1.5 artificial intelligence sandbox [ITU-T M.3080]: An environment in which artificial intelligence (AI) models can be trained and tested, and their effects on the network are evaluated.

3.1.6 customer-oriented marketplace [ITU-T M.3080]: A collection of functional sets that exposes capability to external telecom customers, especially enterprises and industries. The exposed capability includes applications, services, data, and artificial intelligence (AI) capability.

3.1.7 management [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at fulfilment, assurance, and billing of services, network functions, and resources in both physical and virtual infrastructure including compute, storage, and network resources.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

5GC	5G Core network
AI	Artificial Intelligence
AITOM	AI enhanced Telecom Operation and Management
BSS	Business Support System
EPC	Evolved Packet Core
ETH	Ethernet
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
HDFS	Hadoop Distributed File System
LTE	Long-Term Evolution
NG-RAN	Next Generation Radio Access Network
NMS	Network Management System
NoSQL	Not Only SQL
OS	Operations System
OSS	Operation Support Systems
OTN	Optical Transmission Network
RAB	Radio Access Bearer
RAN	Radio Access Network
RDBMS	Relational Database Management System
RRC	Radio Resource Control
SQL	Structured Query Language
SVM	Support vector machine
UMTS	Universal Mobile Telecommunications System

5 Convention

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

With the rapid development of network scale, operation and maintenance management have become more complicated. During the operation of the network and management information system such as network management system (NMS), operation support systems (OSS), etc., a large amount of log data will be generated, including network connection status, system database operating status, service process operating status and so on.

There are many sources to collect logs, such as operations system (OS) server logs, network element logs, etc. Each type of log records different behaviours in the network elements or management systems. For example, network element logs focus on recording network behaviours at the network layer, while OS server logs record the running status and operation records of OS applications.

Traditional operation and maintenance management does not make full use of log data and is mostly based on relatively simple processing algorithms such as statistical analysis and association rules. It relies more on the experience of maintenance personnel and experts, and the value of log data is not yet fully explored. With the development of artificial intelligence technology, it is necessary to use AI technology to realize the intelligent processing of log analysis, realize more efficient abnormal monitoring and early warning based on log analysis, and improve the level of operation and maintenance management. So, with the development of network scale, it is urgent to use artificial intelligence technology to realize the intelligent processing of log analysis, realize more efficient abnormal monitoring and early warning based on log analysis, and improve the level of operation and maintenance management.

Appendix I gives some examples of different log types and characteristics which also contains some possible abnormal behaviours. Appendix II gives some use cases and scenarios of log analysis in telecom management with AI.

7 Function framework for log analysis in telecom management with AI

The function framework of log analysis in telecom management with AI is shown in Figure 1.

The input data for log analysis in telecom management with AI include log records collected from network elements such as optical transmission network (OTN) terminal multiplexing device, etc. and OS servers that run management systems such as NMS, OSS, etc.

After log analysis with AI, the analysis results such as anomaly monitoring information, fault classification information, and fault prediction information are formed to provide a decision-making basis for operation and maintenance personnel. It can improve the efficiency and quality of operation and maintenance work.

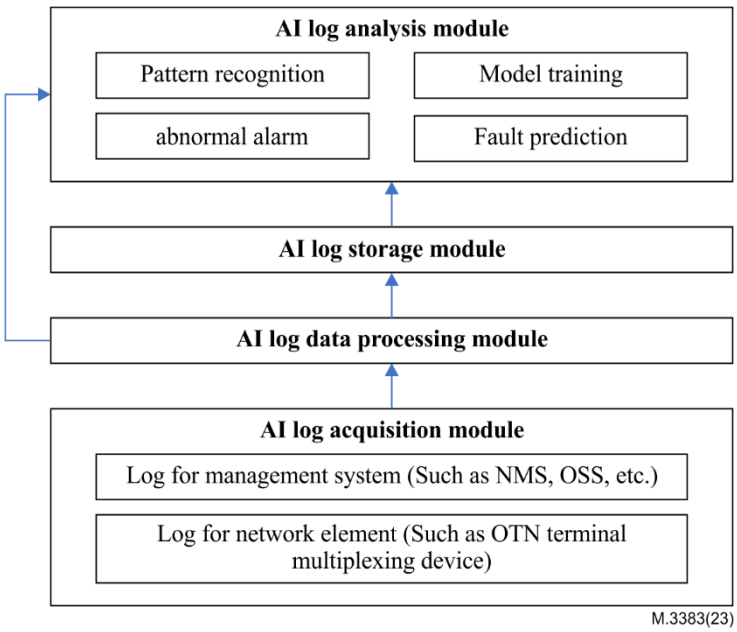


Figure 1 – Function framework for log analysis in telecom management with AI

7.1 AI log acquisition module

This module is used to collect various types of logs. In order to distinguish the types of logs and understand the contents of logs, the module should have the ability to collect and use various types of logs to train AI models, such as OS server logs and network element logs. The collected information includes alarm ID/name, alarm type, alarm severity, alarm source, occurrence time, etc. For a specific alarm, the detailed illustration (definition, type, impact) is reported as context. Dealing with alarm data is important for failure management, including alarm compression, alarm correlation analysis, and alarm root cause identification.

7.2 AI log data processing module

This module is used to extract valid information in a log. Based on the characteristics of different types of log information, it converts unstructured or semi-structured multi-source heterogeneous log files into structured files and stores parameter values in the AI log storage module, so as to facilitate data mining and learning in the AI log analysis module. This module has the ability to identify and match the data according to the format and structure of data characteristics, and quickly extract the effective information in the data by referring to the extraction method of historical data.

7.3 AI log storage module

This module is used for storage data. The AI log storage module will record the knowledge information processed by the AI log data processing module to assist knowledge reasoning and data analysis in AI log analysis module.

7.4 AI log analysis module

This function module includes the basic AI functions that must be possessed for log analysis with AI. AI log analysis module models and trains log data, deeply excavates the hidden information and potential of the log and generates analysis results to guide the operation and maintenance of the network. AI log analysis module supports the choosing of different built-in function modules in different scenarios. This module collects the pre-processed log information in certain scenarios from the AI log storage module and the use in order to train the model and realize the pattern recognition and adjust and improve the parameter and performance of the models after making clear the usage scenario.

– Model training: Train and test the model based on pre-processed log data and common AI models according to the requirements from the customer-oriented marketplace layer and other layers. Adjust and improve the parameter and performance of the models.

  NOTE – The functions of the customer-oriented marketplace layer are a reference to [ITU-T M.3080] which include a standardized capability directory and capability customization. The customer-oriented marketplace layer can build and maintain the AI capability requirements of external customers and expose applications, services, data and AI capability set to external customers.

– Pattern recognition: Realize pattern recognition to mine the pre-processed data, find the hidden patterns and extract abnormal information from the log based on trained models. The abnormal information involves abnormal log number, abnormal log total number, abnormal log keyword, and so on. This process involves algorithms such as statistical analysis, clustering, classification, association rules, and sequential pattern recognition.

– Fault prediction: Predict potential faults and performance failures ahead of time based on the trained models and excavated information.

– Abnormal alarm: Alarm and report anomaly detection and prediction results based on the trained models and excavated information. The analysis results (such as log anomaly detection and log prediction results) and management and maintenance of log analysis strategy can be visualized. The abnormal alarm has the capabilities to create, configure, deliver, customize and manage the visual presentation of analysis results and analysis strategy.

8 The relationship between functional framework for log analysis in telecom management with AI and AITOM

Log analysis in telecom management with AI is a typical application scenario based on the AI enhanced telecom operation and management (AITOM) framework.

The functional framework for log analysis in telecom management with AI references and AITOM framework. The relationship between the framework for log analysis in telecom management with AI and AITOM framework in Figure 2 can be described as follows:

– The block name and functions of the "AI log acquisition module", "AI log data processing module" and "AI log storage module" correspond to "data acquisition", "data processing" and "data storage" respectively of the AITOM framework. But these three modules in this Recommendation are based on log analysis scenarios and they are extended to support AI methods.

  NOTE 1 – These three blocks correspond to red circle 1, red circle 2, and red circle 3 respectively in Figure 2.

– The block name and functions of the "AI log analysis module" corresponds to the "AI engine" of the AITOM framework. The functions of "model training" are mainly guided by that of the "AI sandbox training" of AI engine, and the orchestration of "pattern recognition", "fault prediction" and "abnormal alarm" is mainly guided by "AI capability orchestration" of the AI engine.

  NOTE 2 – This block corresponds to red circle 4 in Figure 2.

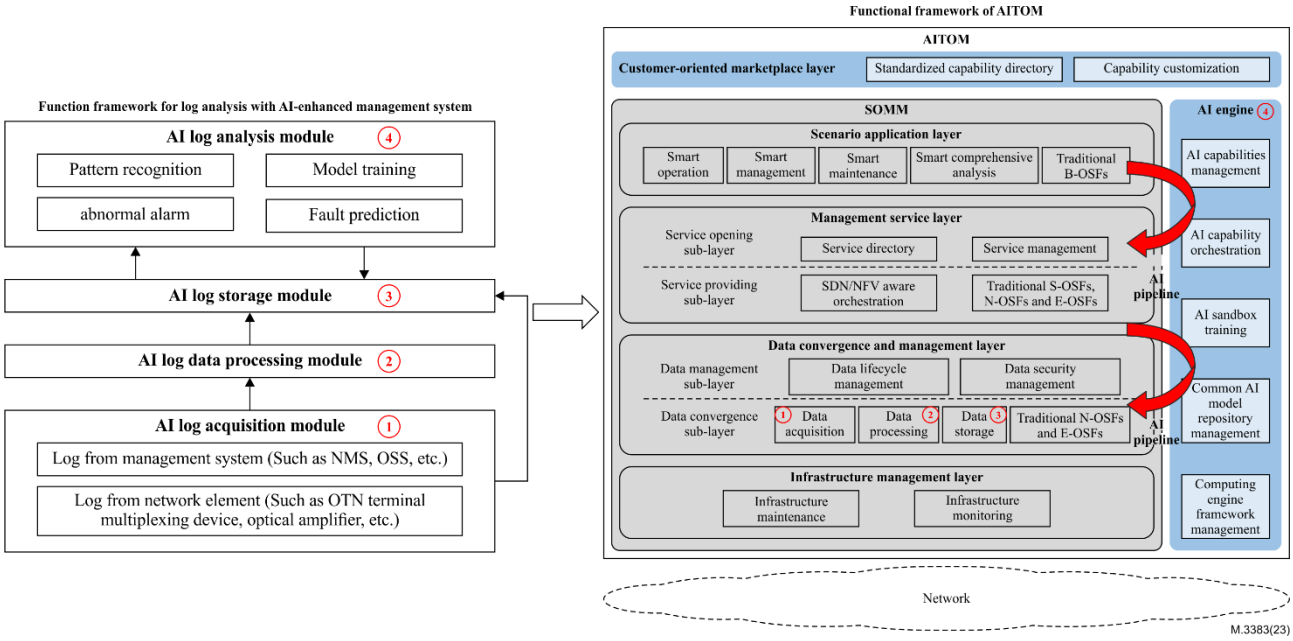


Figure 2 – Mapping relationship between functional framework for log analysis in telecom management with AI and AITOM [ITU-T M.3080]

NOTE 3 – The symbols of the red circle with a number represent the mapping relationship between the "function framework for log analysis in telecom management with AI" and the AITOM framework.

9 Requirements for log analysis in telecom management with AI

9.1 Requirements for AI log acquisition module

The requirements of the AI log acquisition module include:

1) It is required that the AI log acquisition module supports collecting multi-source heterogeneous log, such as data from network management system (NMS), element management system, and network equipment.
2) It is recommended that log data be collected in time, which can timely obtain the operation status of the managed network and provide timely data support for the decision-making of the management system.
3) It is recommended that the AI log acquisition module supports conducting preliminary analysis, including the format, storage mode and generation speed of different logs.
4) It is recommended that operation-related anomalies log be collected and pre-processed.
5) It is required that the AI log acquisition module supports the accuracy and completeness of data collection. Data loss and corruption should be prevented during acquisition.
6) It is recommended that a proper collection period should be supported in the AI log acquisition module based on the different types of logs.
7) It is recommended that the interface of AI log acquisition is open to ensure real-time and is stable for log collection.
8) It can optionally support the parallel collection of log data, and collect multi-source data simultaneously in a multi-channel parallel mode.

9.2 Requirements for AI log data processing module

The requirements of the AI log data processing module include:

1) It is recommended that the AI log acquisition module supports pre-processing function, including log cleaning and missing value handling. Log cleaning is to filter the unnecessary log information, remove noise data and correct the inconsistency of the data. Missing value handling can be filled by AI algorithms to ensure data integrity.

2) It is required that the AI log data processing module supports the normalization and unification of log data format, including multi-source heterogeneous log data, for further storage and analysis.

3) It is recommended that the AI log data processing module supports analysing the user-defined analysis strategy and feature data pre-processing for the log data, so that the heterogeneous data can be converted into a standard format, including feature data selection, normalization or standardization, and feature data enhancement and enrichment, etc.

9.3 Requirements for the AI log storage module

The requirements of the AI log storage module include:

1) It is required that the AI log storage module supports the classification storage of different log types and log formats.

2) It is recommended that the AI log storage module supports the storage of intermediate output data and final analysis results.

3) It is recommended that the AI log storage module supports multiple file systems for storing logs, such as traditional relational database management system (RDBMS) or distributed cluster system not only structured query language (NoSQL), and Hadoop distributed file system (HDFS).

4) It is recommended that the AI log storage module supports full-text retrieval, phrase query, field filtering and other functions to achieve fast log search.

5) It is recommended that the AI log storage module needs a reasonable storage period based on the data collection period and data storage space to prevent storage space overflow.

9.4 Requirements for the AI log analysis module

The requirements of the AI log analysis module include:

1) It is required that the AI log analysis module supports various types and formats of logs.

2) It is recommended that the AI log analysis module supports a variety of log analysis algorithms. The AI models are stored in the common artificial intelligence model library. The log analysis algorithms include statistical analysis, association rules, clustering, classification, sequence pattern, transaction recognition, etc.

3) It is recommended that the AI log analysis module supports user-defined algorithms. The AI models are stored in the telecom specific artificial intelligence model library. The common AI models in management systems can be added for fault monitoring, root cause analysis, etc.

4) It is recommended that the AI log analysis module supports the training of log data in a sandbox. The training object is a pre-defined AI model suitable for specific situations. In the training process, it is necessary to estimate and analyse the model and predict the accuracy of the model. Through the test and evaluation of the model, constantly adjust the parameters, optimize the model, and improve the accuracy and practicability of the model.

5) It is recommended that the AI log analysis module supports fault detection.

NOTE 1 – Log analysis based on fault detection can comprehensively manage and analyse system faults. AI log analysis module can monitor the running state of the system in real time through a log analysis service. The log analysis module can automatically classify the fault logs and analyse the correlation of the system faults.

6) It is recommended that the AI log analysis module supports a variety of predictions, such as fault prediction, error prediction, user access prediction, regulatory prediction, etc.

7) It is recommended that the AI log analysis module supports pattern recognition.

NOTE 2 – Pattern recognition is a technology that uses various algorithms, rules and models to mine the pre-processed data and find the hidden patterns from the log. The algorithm includes statistical analysis, clustering, classification, association rules, sequential pattern recognition, etc.

8) It is recommended that the AI log analysis module supports anomaly assessment with logs.

NOTE 3 – Three steps need to be done to assess a log anomaly. Firstly, construct a structured log by extracting keywords and matching it to a log template that is learned from existing log files. Secondly, carry out pattern mining to extract features from structured logs. Finally, judge the log's anomaly from the quantitative perspective as well as the perceived perspective.

9) It is recommended that the AI log analysis module supports abnormal alarms based on the result of fault prediction and reports anomaly detection and prediction results in real time or regularly.

10) It is recommended that the AI log analysis module supports fast log information search and log query, including fuzzy query, range query, combined query, etc.

11) It is recommended that the AI log analysis module supports the determination of log training time, scope, process, and method according to the requirements from the customer-oriented marketplace layer and other layers.

12) It is recommended that the AI log analysis module supports the reporting of analysis results to the customer-oriented marketplace layer for customized analysis strategy.

13) It is recommended that the AI log analysis module supports the visualization of log anomaly detection and log prediction results.

14) It is recommended that the AI log analysis module supports the visualization of multiple data sources fusion.

15) It is recommended that the AI log analysis module supports real-time data display and interaction.

Appendix I

Examples of several log types and characteristics

(This appendix does not form an integral part of this Recommendation.)

AI log acquisition module can collect OS server logs, network element logs, etc. Each kind of log has its characteristics. The log records different types of behaviours in the network. Network element logs record network behaviours in the network layer, while OS server logs record the running status of system application processes and the operator's behaviours. Table I.1 shows examples of the different types of logs and the corresponding behaviours that may be detected. Table I.2 lists the characteristics of several typical logs and the possible abnormal behaviours.

Some fault logs can be compared to determine the current system anomalies, realizing real-time alarm and fault processing. Combining log information of different times and different types and mining the internal association of logs with AI technology, the management system can have a comprehensive understanding of the current status, potential risk, and so on.

Table I.1 – Examples of different log types and corresponding behaviours

Log types	Behaviours may be detected
OS server log	OS server log is classified into information, warning, and error levels. Most event records generated by the OS server are related to the following aspects: running status and operation records of OS applications, modifications of executable files, unsafe system reconfiguration or damage, authentication or authorization failure, etc.
OTN equipment log	OTN equipment log can record the operating status of equipment in the optical transmission network. The equipment includes OTN terminal multiplexing devices, OTN optical cross-connected devices (such as OTN electrical crossover devices, OTN optical crossover devices and devices having both OTN electrical and optical crossover functions), etc. OTN equipment log records a large number of forward events, configuration changes, outbound and inbound transfer bytes, the connection status of different devices, etc.
Optical transmission link log	Identify the transmission link information, for example, the ETH (Ethernet) end port information, automatic protection switching information, input optical power information of the link, etc.
Database log	Database log can record the operating status of the database, including error log, query log, slow query log, event log, binary log, relay log and so on. For example, the database log can record the customer interface status of the database, the execution status of the program statement (e.g., SQL) and error information.
Operation support systems (OSS) and business support system (BSS) log	The OSS and BSS log includes the module log, application log, and security log. The OSS and BSS log can record the information of the hardware, software, and system problems in the OSS and the BSS. Moreover, the OSS and BSS log can also monitor the events that occur in the OSS and BSS. The OSS and BSS log can be used to check the cause of the error and to find the traces left by the attacker when it was attacked.

Table I.1 – Examples of different log types and corresponding behaviours

Log types	Behaviours may be detected
5G core network (5GC) and evolved packet core (EPC) network function log	5GC and EPC network functions include the network elements and virtual network elements in the 5GC and EPC. The network function log includes the system log, operation log, and security log. The system log can record the running information of (virtual) network elements of 5GC and EPC. The operation log can record the operation log of (virtual) network elements of 5GC and EPC. The security log can record the security events and security audits that occur in the (virtual) network elements of 5GC and EPC.
Long-term evolution (LTE) evolved universal mobile telecommunications system (UMTS) terrestrial radio access network (E-UTRAN) and 5G next generation radio access network (NG-RAN) performance measurement log	Record the RAN performance measurement information, which includes radio resource control (RRC) connection related measurements, radio access bearer (RAB) related measurements, handover related measurements, radio source utilization related measurements, paging related measurements, equipment resource related measurements, etc.

Table I.2 – The characteristics of several typical logs and the possible abnormal behaviours

Log characteristics	Possible abnormal behaviours
OS server log generates alarm information	Identify events that may have problems in the future. For example, critical system files have been deleted and disk space is running out, abnormal program results in a device restart, a memory usage error occurs, and device memory utilization reaches the limit.
OS server log generates failure auditing information.	Identify the audited security events that did not complete successfully. For example, users cannot access network drives.
OTN transmission interrupt information	Identify events that caused the interruption, for example, an abnormal clock signal (SerDes), E1/T1 port error, etc.
OTN status abnormal information	The abnormal information collected by the OTN equipment contains a variety of fault information, including loss of continuity, path trace mismatch, payload type mismatch, forward / backward indication missing, etc.
Database abnormal information	The abnormal information collected by the database contains the abnormal frequency of keyword occurrences (e.g., error, failure), and log volume changes (e.g., sudden rise or drop).
OSS and BSS abnormal information	The abnormal information collected by the OSS and BSS contains the abnormal frequency of keyword occurrences (e.g., alarm, error), and log volume changes (e.g., sudden rise or drop).
5GC and EPC network function abnormal information	The abnormal information collected by the (virtual) network elements of 5GC and EPC contains the abnormal frequency of keyword occurrences (e.g., error, warning), and log volume changes (e.g., sudden rise or drop).
LTE E-UTRAN and 5G NG-RAN base station generates frequently performance false alarm	Usually, LTE E-UTRAN and 5G NG-RAN base station performance measurements are below the threshold predefined by the operator, an alarm will be generated, but sometimes performance fault recovery occurs by the equipment itself and the corresponding alarms are closed, the reasons may be due to transmission flash break and wind (antenna of a base station could be affected), etc. Thus, it is necessary to distinguish the true performance alarm from all of the alarms. The method of threshold adjusted, and delay set is not valid in most of the cases.

Appendix II

Use cases of log analysis in telecom management with AI

(This appendix does not form an integral part of this Recommendation.)

After log analysis with AI, the analysis results such as anomaly monitoring information, fault classification information, and fault prediction information are formed, as shown in the following tables.

Table II.1 – An intelligent system of real-time monitoring and anomaly warning

Title	An intelligent system of real-time monitoring and anomaly warning
Description	This case is an intelligent system with real-time monitoring and anomaly warning function. Each log has its unique characteristics. For example, when automatic protection warning occurs, the OTN transmission link log information will be created. With these feature behaviours of the managed elements, whether there is real automatic protection anomaly, can be determined. 1) Collect log data including possible fault information from OS servers and network elements through the AI log acquisition module. 2) Analyse the log analysis strategy and pre-process log data to convert it into a standard format in the AI log data processing module. NOTE 1 – The information can be extracted directly from some log data which has a fixed format (e.g., IP address, etc.). 3) Store the pre-processed data in the AI log storage module. 4) Acquire the pre-processed data from the database, knowledge base and diagnosis database of the expert system in the AI log storage module and form the training data and test data sets. 5) Train the model in AI log analysis module according to the train data sets and update the parameter of the model by test data sets. 6) Acquire online log data which has been collected, pre-processed and stored, then match the pre-processed log to a log template based on the trained models. 7) Carry out pattern mining on unmatched log data to extract log features from pre-processed logs. 8) Extract anomaly detection to carry out real-time monitoring. 9) Visualize the anomaly results and anomaly warning. 10) The online data is used to retrain existing models to improve model quality. NOTE 2 – Existing models also can be incrementally retrained, and parameters are updated to improve model quality by periodically updating the training data.

Table II.1 – An intelligent system of real-time monitoring and anomaly warning

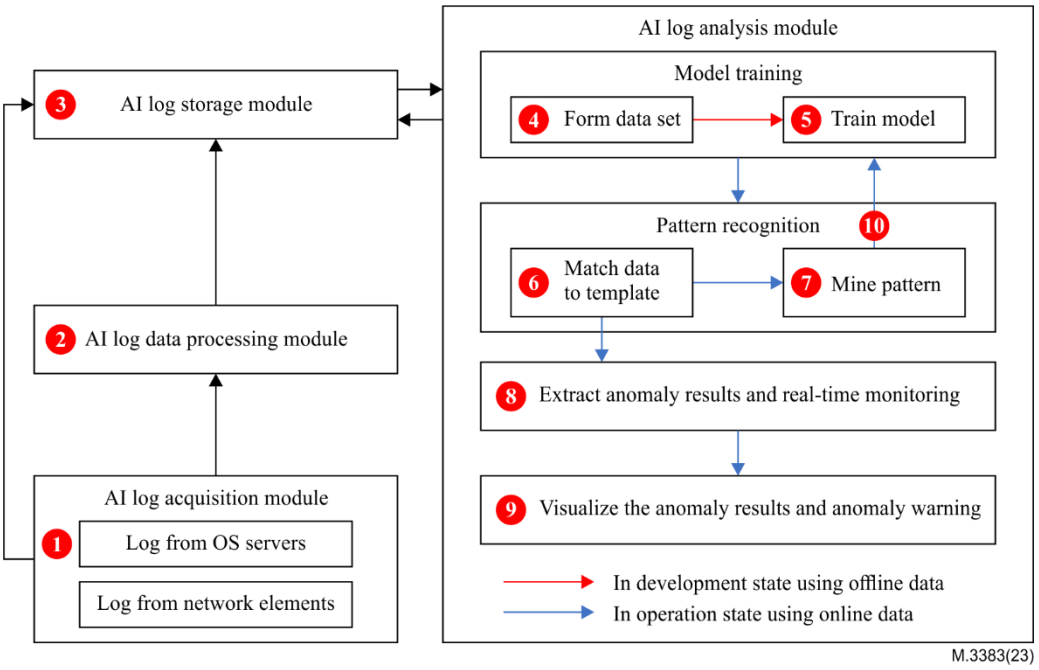
Title	An intelligent system of real-time monitoring and anomaly warning
Figure II.1	

Table II.2 – An intelligent system of fault prediction

Title	An intelligent system of fault prediction
Description	This case is an intelligent system with a fault prediction function. AI log collection module will collect information (including possible fault information) from the OS server log and network element log in the AI log storage module after being structured and normalized by the AI log data processing module. AI log analysis module will use the AI model stored in a common artificial intelligence model library or telecom specific artificial intelligence model library for fault prediction according to the requirements. 1) Collect the current log with potential faults from the OS servers and network elements through the AI log acquisition module. 2) Analyse the log analysis strategy and pre-process log data to convert it into a standard format in the AI log data processing module. NOTE 1 – The information can be extracted directly from some log data which has a fixed format (e.g., IP address, etc.). 3) Store the pre-processed data in the AI log storage module. 4) Acquire the pre-processed data from the database, knowledge base and diagnosis database of the expert system in the AI log storage module, which includes the normal log with the label "1" and fault log with the label "0", to form the training data and test data sets. 5) Train the model in AI log analysis module according to the train data sets and update the parameter of the model by test data sets. 6) Generate the predicted value based on the trained model. 7) Compare the predicted value with the threshold. 8) If the value is larger than the threshold, which means a potential fault is identified. NOTE 2 – Existing models also can be incrementally retrained, and parameters are updated to improve model quality by periodically updating the training data.

Table II.2 – An intelligent system of fault prediction

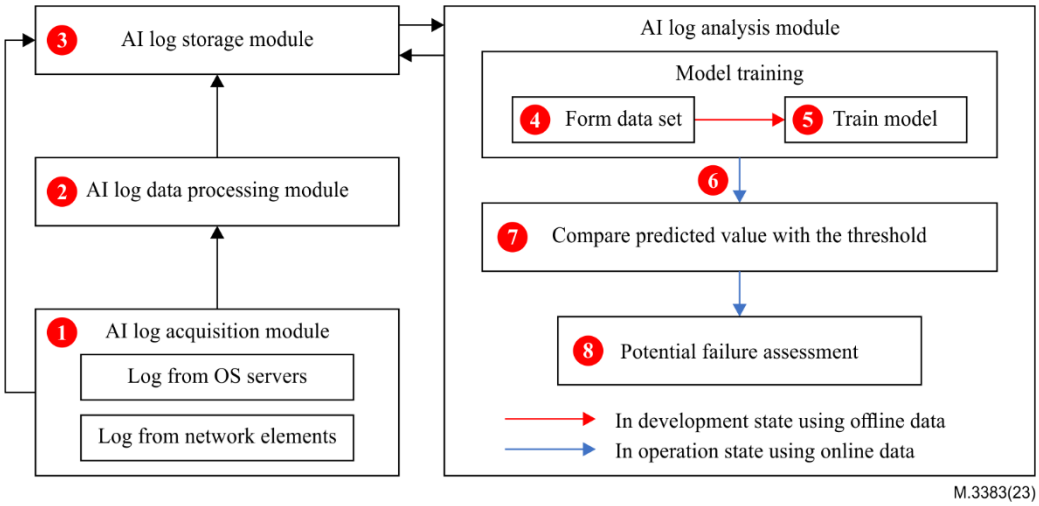
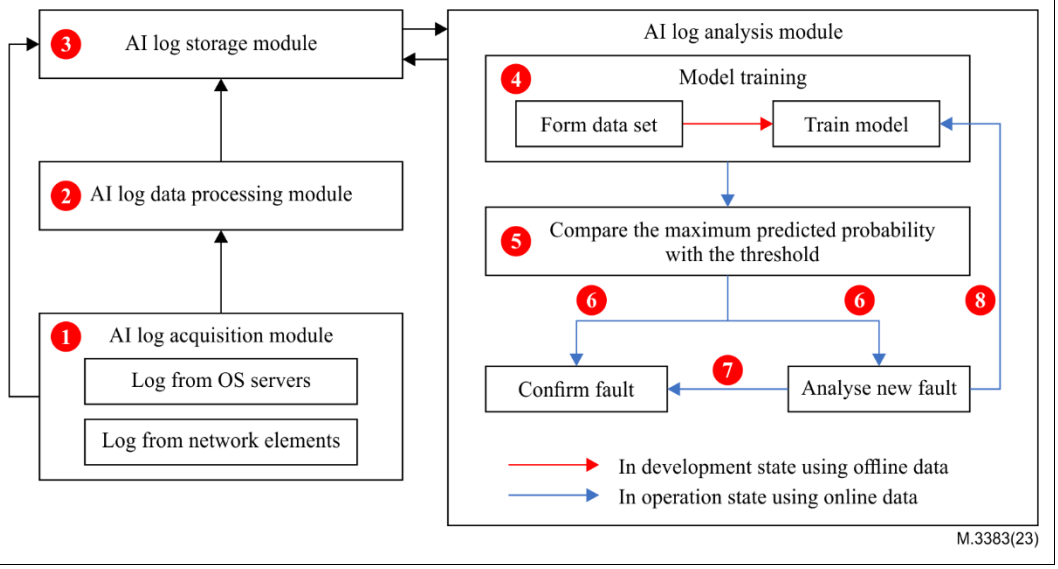
Title	An intelligent system of fault prediction
Figure II.2	

Table II.3 – An intelligent system of fault classification

Title	An intelligent system of fault classification
Description	This case is an intelligent system with a fault classification function. The AI log acquisition module collects real-time log data, inputs the processed data into the AI log analysis module, and finally outputs the fault classification results to realize the classification of the fault. 1) Collect all the abnormal events and attack events on the current network, including fault information from the OS servers and network elements through the AI log acquisition module. 2) Analyse the log analysis strategy and pre-process log data to convert it into a standard format in the AI log data processing module. NOTE 1 – The information can be extracted directly from some log data which has a fixed format (e.g., IP address, etc.). 3) Store the pre-processed data in the AI log storage module. 4) Acquire the pre-processed data from the diagnosis database of the expert system in the AI log storage module and form the training data and test data sets to train the model. Apply the model to classify the current log. 5) Compare the value of the maximum matching probability with the specified threshold. 6) If the value is larger than the threshold, the current fault is identified as the maximum matching fault; while the value is smaller than the threshold, the current is identified as a new fault, which will be deeply analysed. 7) Confirm new fault types with expert experience and cluster analysis. 8) The online data is used to retrain the existing model to improve model quality with a new fault type label. NOTE 2 – Existing models also can be incrementally retrained, and parameters are updated to improve model quality by periodically updating the training data.

Table II.3 – An intelligent system of fault classification

Title	An intelligent system of fault classification
Figure II.3	

Here we provide several scenarios of log analysis with AI that could help network operators manage and maintain the network better.

Scenario 1: managed element alarm optimization

Data type: Bit error rate data of communication transmission network and optical power monitoring log data of transmission equipment.

Apply scenario: Communication transmission network.

Requirement description: Due to the problems of real-time measurement error, network error code and packet loss in the communication transmission network, the bad data will affect the real-time status evaluation results of the transmission network, and then lead to wrong operation and maintenance decisions.

Processing method: By using the bad data evaluation algorithm, the mining algorithm based on the relative density is used to mine the measured data, the historical log data, and the corresponding network alarm information. Based on the results of the bad data mining, the running state of the transmission network is evaluated and comprehensively analysed.

Contribution: The influence of real-time measurement error, network error code, and packet loss on the bit error rate of communication network and optical power of transmission equipment is solved, and the occurrence of error alarm is reduced.

Scenario 2: operation and maintenance of optical cable

Data type: Operation and maintenance log data of optical cable of the communication network.

Apply scenario: Optical transmission network.

Requirement description: Due to the lack of real-time data analysis of resource performance, equipment aging, and fault information are difficult to timely monitor. The lack of external weather data makes it difficult to prevent cable failure in extreme weather.

Processing method: Based on the analysis of fibre optic cable performance log data, fibre optic cable operation and maintenance log data, and fibre optic cable environment meteorological log data, the relevant performance data and environmental data were extracted to model the operation of a fibre optic cable, and classification algorithms such as decision tree and support vector machine (SVM)

combined algorithms such as bagging and boosting were used to carry out fault warning for fibre optic cable.

Contribution: Real-time monitoring and early warning of optical cable deterioration can be realized to reduce the risk of optical cable failure caused by meteorological disasters.

Scenario 3: managed element temperature monitoring

Data type: Temperature monitoring log data of communication network elements.

Apply scenario: All kinds of communication network elements.

Requirement description: The original alarm method by setting the temperature detection threshold of the power environment in the communication room is sensitive to the distance between the monitoring point and the communication equipment, which is easy to lead to a large temperature measurement deviation. At the same time, the accuracy of the temperature alarm is difficult to control because of the different equipment specifications and sensitivity of each network element manufacturer.

Processing method: The temperature parameters are extracted from the massive log data generated by the integrated temperature measurement module, and the analysis and early warning of historical data are realized through temperature data collection, model normalization, data analysis, and function presentation by using the processing technology and idea of big data processing methods (such as the ARMA model).

Contribution: Compared with the traditional monitoring and processing methods, the temperature monitoring system based on the log file historical record of the communication network is more sensitive to temperature changes, can detect temperature anomalies in advance, can reduce the accident level of substation and communication room, and improve the system security.

Scenario 4: OTN fault diagnosis

Data type: OTN alarm log data.

Apply scenario: OTN.

Requirement description: Traditional alarm methods get a lot of interference, redundancy, and incomplete information in OTN alarm information, and cost a long time to locate the problem. In practical application, it is necessary to properly determine the location, type, and cause of the fault within the shortest time, to repair or isolate the fault in time.

Processing method: Through analysing OTN alarm log files, the algorithm adopts alarm time synchronization processing, alarm information sorting and field extraction, alarm compression, and other methods to realize the standardized processing of alarm information, and finally transforms the alarm transaction database. By using neural network and data characteristics of association rule alarm transaction database, alarm events are modelled, and fault diagnosis of alarm events is realized.

Contribution: With the help of real-time data and historical data in OTN alarm logs, the standardized management of alarms for optical transmission network equipment of different manufacturers is realized, and the correlation of log data is analysed by using data mining technology, and the intelligent alarm cause diagnosis is realized.

Scenario 5: LTE E-UTRAN and 5G NG-RAN base station false alarm distinguished

Data type: Base station false alarm log data.

Apply scenario: LTE E-UTRAN and 5G NG-RAN base station.

Requirement description: Traditional LTE E-UTRAN and 5G NG-RAN base station false alarm distinguished methods that performance threshold adjusted, and time windows set are not valid to most of the cases, it leads to a lot of effort for the operator to distinguish them by hand, and the

accuracy is low. Since the number of base stations is large for operators, it is necessary to find a new way to distinguish fault alarms quickly and accurately.

Processing method: LTE E-UTRAN and 5G NG-RAN base station performance measurement log files are analysed by an AI-enhanced management system, the process includes performance indicators data extraction, standard format transformation, loaded to the database and the AI method applied. In the data pre-processing phase, data features are calculated from the statistical characteristics, fitting features and radio service features, and combined by serial or parallel concatenation. In the AI processing phase, the decision tree and LightGBM method are used, and the parameters are optimised according to experience.

Contribution: With the help of real-time data and historical data in LTE E-UTRAN and 5G NG-RAN base station performance logs, the standardized management of performance false alarms for LTE E-UTRAN and 5G NG-RAN base station equipment of different manufacturers is realized, and the false alarm is analysed by using data mining technology quickly and accurately.

Bibliography

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	**Telecommunication management, including TMN and network maintenance**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023