ISBN: 978-981-18-1791-5
2021 the 11th International Workshop on Computer Science and Engineering (WCSE 2021)
doi: 10.18178/wcse.2021.06.050

Research on Intelligent Processing Technology of Alarm in Power Monitoring System

Li Zeke [1], Wang Chunyan [2, 3+], Xu Zhiguang [1]and Liang Ye [2,3]

[1] State Grid Fujian Electric Power Co., Ltd., Fuzhou 350001 China

[2]State Grid Electric Power Research Institute Nanjing 210003 China

[3] Beijing Kedong Electric Power Control System Co., Ltd., Beijing 100192 China

Abstract. In the power monitoring system, the control center collects a large amount of alarm and status information from the main station system and the plants under its jurisdiction every day. Most of duty officers deal with the alarms based on experience, so that it is difficult to ensure the correct judgment and handling of the alarms. This paper proposes a knowledge base-based alarm processing and solution recommendation function, using big data storage,data mining technology,machine learning technology to achieve the extraction of alarm attribute characteristics, online real-time analysis and reasoning of alarm processing methods or suggestions. Adopt the method of constructing knowledge base to assist on-duty personnel to analyze and process alarms in time And intelligently recommend alarm solutions, which are of great significance to ensure the safe operation of power grids and equipment, and significantly improve the comprehensive management and control capabilities of power monitoring systems for security threats.

Keywords: power monitoring system, network threat management and control,knowledge base,big data analysis technology, automated operation and maintenance, machine learning, intelligent recommendation algorithm.

1. Introduction

At present, the power monitoring system control center is responsible for the operation monitoring of all plants and stations, all the monitored and collected operating information data and alarm information data of the plant and station are uploaded to the network security management platform of the power monitoring system. When handling the alarm, the duty officer needs to judge and resolve the alarm through experience. If the personnel on duty have not seen a certain alarm, or have insufficient knowledge of hardware and software, it will directly lead to wrong judgments and wrong handling of the alarms, which will result in the alarms being not handled correctly, or the efficiency of alarm handling low.

In response to the above problems, this article designed an intelligent processing function for alarm information. This function provides intelligent recommendations based on the machine learning-based recommendation algorithm for the received alarm processing requirements, and provides guidance and suggestions for alarm processing, and assists on-duty personnel in analyzing and processing alarms in a timely manner. The supporting platform and intelligent processing technology required to realize this application function are given below.

2. Design of Knowledge Base for Intelligent Alarm Processing

The alarm intelligent processing knowledge base adopts big data analysis and machine learning technology to learn and process from different dimensions, calculate the risk probability of the selected plan and execute it, and according to the content of the alarm information to be processed, the plan can be intelligently recommended through the machine learning algorithm Give the alarm processing module to realize the correct handling of the alarm.

[+] Corresponding author. Tel.: 13522534927.
E-mail address: wsygr2002@163.com.

3. Knowledge Base Frame Structure

The construction of the knowledge base for intelligent processing of alarm information provides a powerful tool for reducing the daily alarm handling pressure of operation and maintenance personnel on duty, and is also a treasure house for users to acquire knowledge [1-2].At the same time, the construction of the knowledge base provides a variety of alarm handling solutions for the attendants, and gives users the convenience of free choice. When the network is unblocked, the staff on duty can directly find the required answers from the knowledge base when they make a request, which improves the efficiency and accuracy of alarm handling. Based on the long-term experience of operation and maintenance personnel or according to the processing method of the expert database, the alarm handling plan is designed to form a knowledge base according to templates, standards, and specifications, and with reference to practicability and convenience, so that the on-duty personnel can directly call and quote.

The alarm information intelligent processing knowledge base is constructed based on the big data analysis platform, and the big data technology is used to filter, integrate, mine and analyze information. The functional architecture of the knowledge base. As shown below:

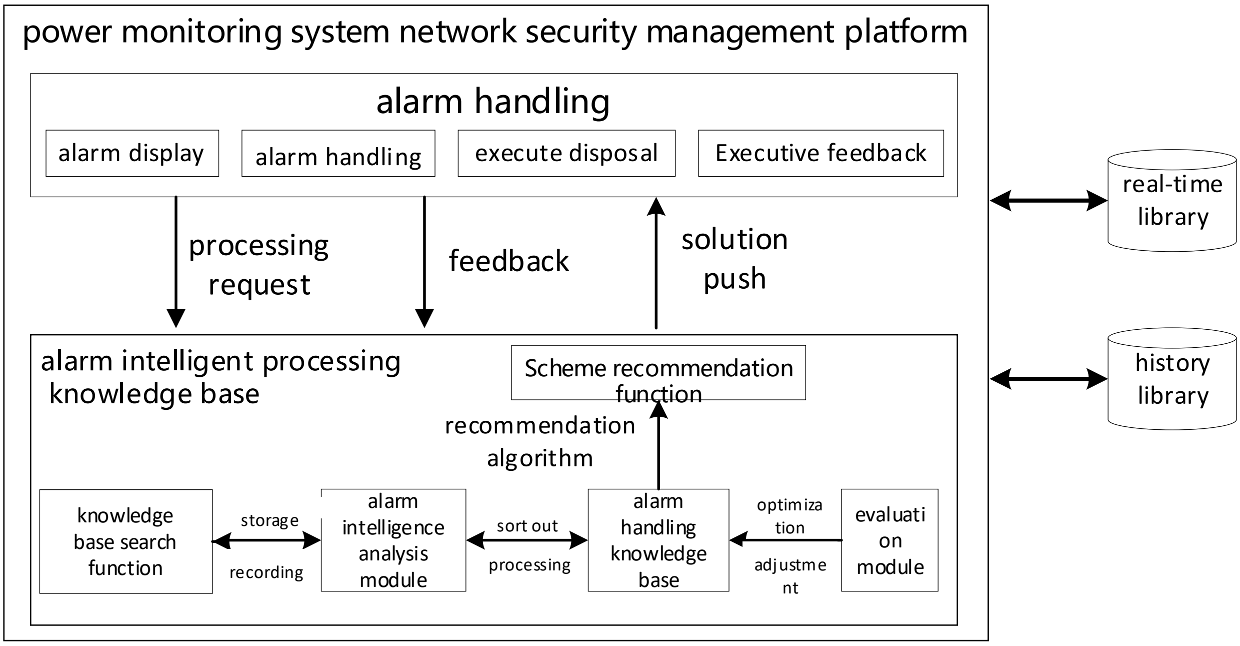


Fig. 1: The functional architecture of the alarm information intelligent processing knowledge base

By optimizing and integrating various information resources, the knowledge base provides solutions for the alarm handling in the daily operation and maintenance work of the on-duty staff, including alarm handling and alarm intelligent handling knowledge base modules. The alarm intelligent analysis module in the knowledge base automatically collects and processes to generate a corresponding solution library for users to retrieve, browse and call based on the alarm processing request raised by the attendant, referring to past processing experience or solutions given by some expert libraries; The evaluation module is used for the evaluation and feedback given by the duty staff after the implementation of the program, to reflect the evaluation and feedback on the effectiveness of the program provided by the knowledge base, and facilitate the adjustment and improvement of the knowledge base; The scheme recommendation function recommends the optimal scheme to the alarm processing module according to the recommended algorithm for the reference and execution of the staff on duty.

4. Knowledge Base Intelligent Recommendation Algorithm

The knowledge base intelligently recommends a processing plan to the alarm processing module, and the choice of the intelligent recommendation algorithm is the key [3-6]. The intelligent recommendation algorithm of this knowledge base mainly analyzes the alarm information to be processed, and combines the current network topology and physical model to obtain feasible solutions for analyzing alarms. It mainly recommends solutions and treatment methods, which can be combined with alarm processing modules and evaluation modules. The feedback information continuously improves the quality of solution recommendations.

The knowledge base recommendation algorithm adopts tag-based recommendation, topic-based recommendation, content-based recommendation, and rule-based recommendation. Tag-based recommendation divides the knowledge base into broad categories according to the classification method of the electric power industry. The category name is the label. For example, the category is divided into network security, data security, vulnerability mining, threat intelligence, cloud security, etc., and the knowledge base is matched by the category of the alarm. Tags in, recommended solutions; Based on topic recommendation, extract the monitored object information according to the alarm log and define it as a topic, match the topic defined by the alarm log with the knowledge base, and give a recommendation plan;;The content-based recommendation algorithm only makes recommendations based on content information. By obtaining the alarm content, matching the alarm information with the content of the solution in the knowledge base can generate a recommendation list; The data source of the rule-based recommendation algorithm is mainly the alarm information to be processed, and the operator's defined rules are used to analyze and mine, and the recommended plan is obtained according to the rules. The rules here can be defined as risk evaluation, risk Coefficient, execution times, historical execution praise rate, etc., according to the alarm information and defined rules to match the scheme in the knowledge base, and recommend a suitable scheme.

The intelligent recommendation strategy of the knowledge base integrates the 4 recommended methods introduced above and provides multiple recommendation methods depending on the processed alarm information. The recommended strategy diagram:

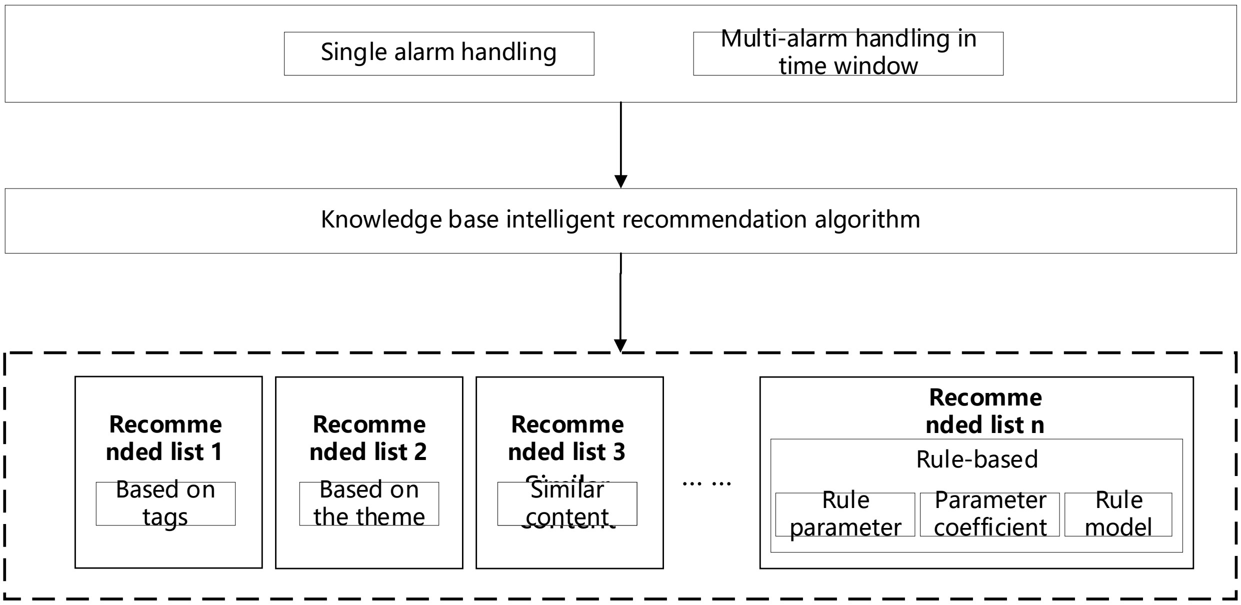


Fig. 2: Knowledge base recommendation strategy

Based on the above recommendation strategy, a recommendation process based on the knowledge base is given:

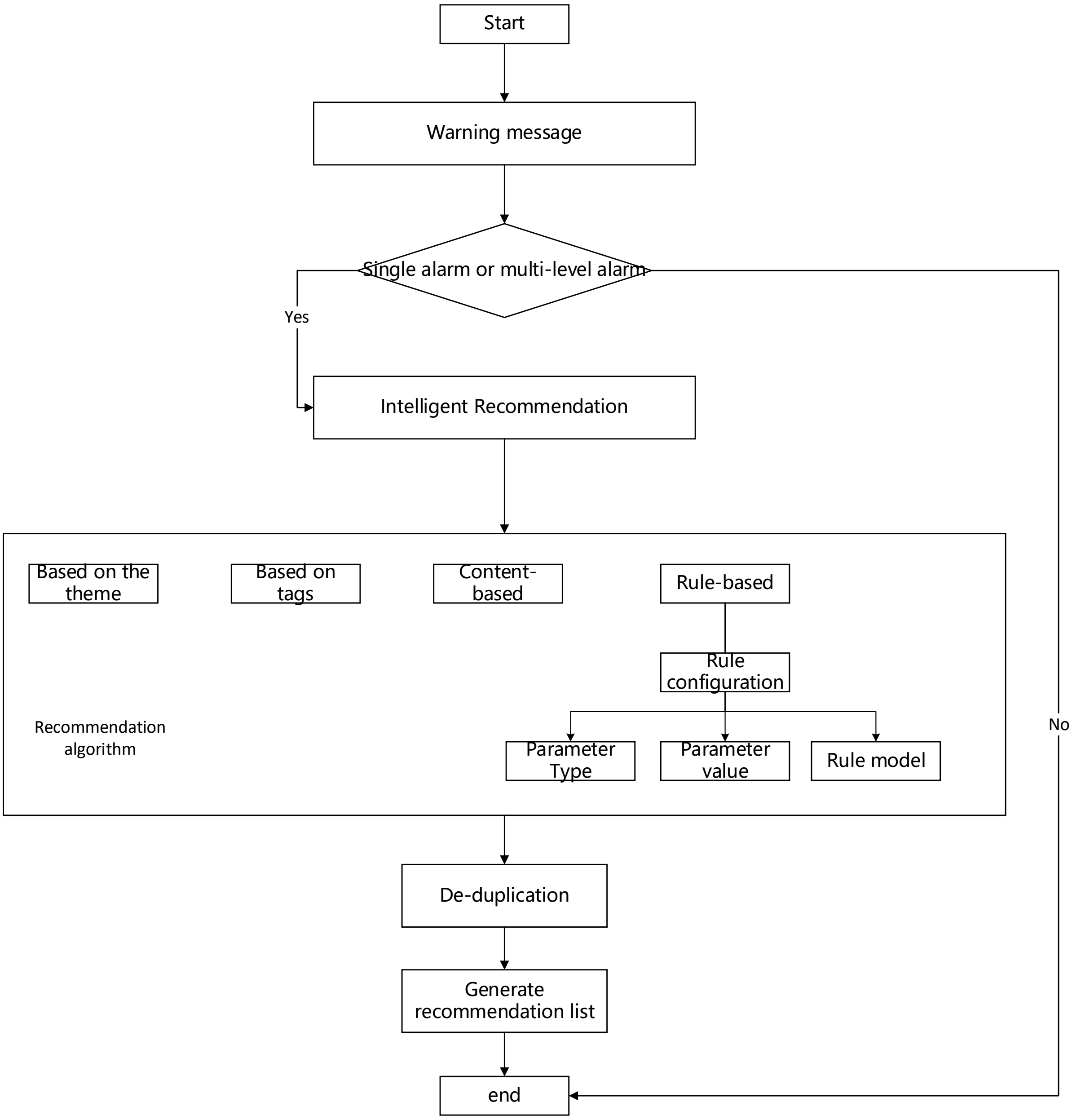


Fig. 3 : Knowledge base recommendation process

When the attendant on duty handles the alarm, recommend the optimal solution through the recommendation algorithm of the knowledge base.

The knowledge base intelligent recommendation algorithm adopts machine learning algorithms suitable for such needs. The algorithm integrates and innovates on the existing mainstream methods to realize that the machine learning model itself can adapt to the data environment, and through continuous confrontation between models Evolve to maintain the accuracy of data prediction at a high level for a long time. The input of this model is alarm information, and the output corresponds to the recommended scheme. The modeling flowchart is as follows:

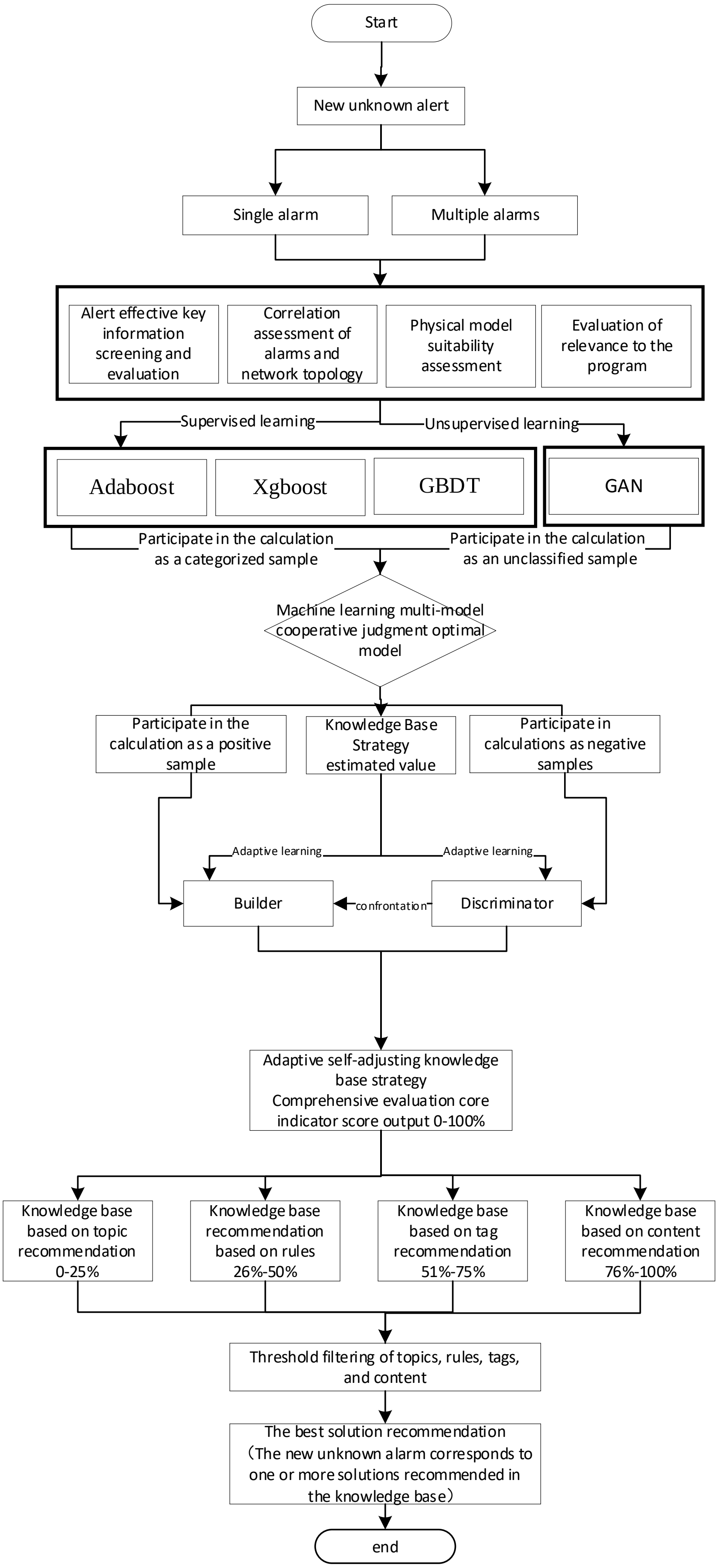

Start
New unknown alert
Single alarm
Multiple alarms
Alert effective key information screening and evaluation
Correlation assessment of alarms and network topology
Physical model suitability assessment
Evaluation of relevance to the program
Supervised learning
Unsupervised learning
Adaboost
Xgboost
GBDT
GAN
Participate in the calculation as a categorized sample
Participate in the calculation as an unclassified sample
Machine learning multi-model cooperative judgment optimal model
Participate in the calculation as a positive sample
Knowledge Base Strategy estimated value
Participate in calculations as negative samples
Adaptive learning
Adaptive learning
Builder
confrontation
Discriminator
Adaptive self-adjusting knowledge base strategy Comprehensive evaluation core indicator score output 0-100%
Knowledge base based on topic recommendation 0-25%
Knowledge base recommendation based on rules 26%-50%
Knowledge base based on tag recommendation 51%-75%
Knowledge base based on content recommendation 76%-100%
Threshold filtering of topics, rules, tags, and content
The best solution recommendation（The new unknown alarm corresponds to one or more solutions recommended in the knowledge base）
end

Fig. 4: Machine learning modeling processes

The specific machine learning modeling process is shown in Figure 4, the input is a new unknown alarm, Data set features are divided into key features, main features and branch features, The key features are: single alarm, multiple alarms. The main feature is evaluation in four dimensions, namely, the effective key information screening evaluation of the alarm, the evaluation of the correlation between the alarm and the network topology, the evaluation of the applicability of the physical model, and the evaluation of the correlation with the scheme. Each main feature will contain branch features of subordinate items, For example: the effective key information screening and evaluation of alarms, its branch characteristics can be risk evaluation, risk coefficient, execution times, execution methods, etc., as the key relationship and basis before input characteristics and output categories. Other main features have corresponding detailed branch features, which can be increased or decreased according to different actual conditions on site.

After the data preprocessing and the data feature set are determined, it enters the machine learning multi-model cooperation stage. At this stage, this paper applies three supervised learning decision tree methods and unsupervised learning GAN model to confirm the internal characteristics of the data set. A relationship that is difficult to identify or easy to ignore. The four models will run in parallel and participate in the calculation as classified samples and unclassified samples. After that, the output of the model is the knowledge base recommendation scheme corresponding to the alarm. The flow of the optimal model determination method is shown in the following figure:

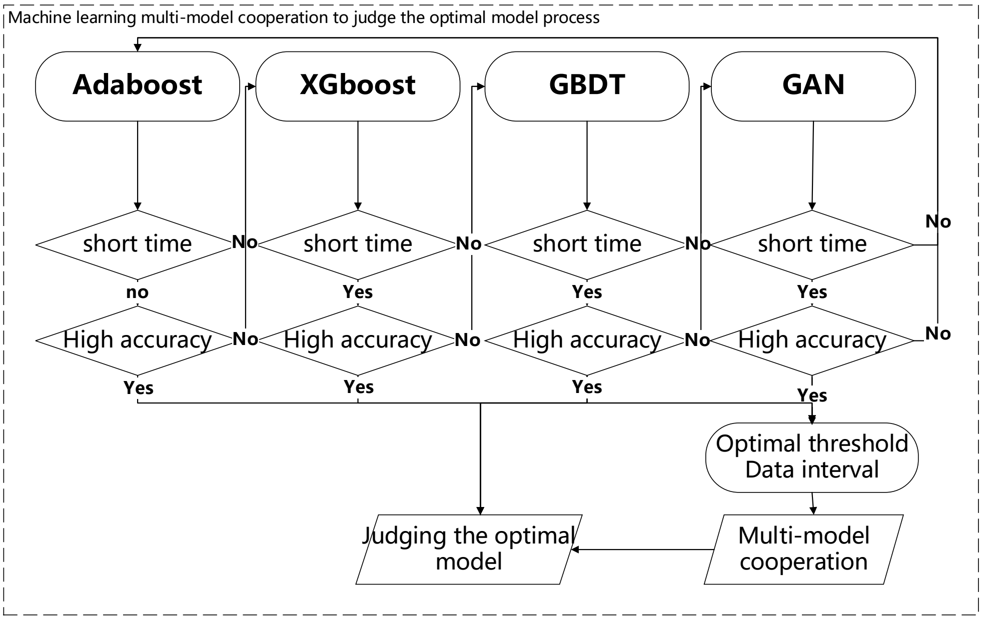


Fig. 5: Machine learning multi-model cooperation to determine optimal model process

There are two main basis for judging whether the model is optimal, one is that the running time of the model is shorter, and the other is that the accuracy is higher. The optimal selection is carried out through the above conditions, and the optimal threshold data interval is determined, so as to realize multi-model cooperation. The above method is performed in parallel with each new input, and the reasonable output is obtained through the optimal model suitable for each set of new data.

After completing the model cooperation, it enters the stage of adaptive self-adjusting machine learning model. At this stage, the estimated value of the knowledge base strategy (the result obtained from the above-mentioned machine learning algorithm) is first clarified, and the result is divided into two branches for adaptive learning and model confrontation evolution. Among them, the actual data, including the characteristics and category results, enter the generator. The generator generates data based on the actual data information. The generated data is mixed with the actual data, and the discriminator is used to determine the authenticity. When the first round of generation After the discrimination is over, the record generator generates and successfully deceives the discriminator, making the discriminator mistakenly believe that the data generated by the generator is actual data, and its weight is increased in the generator as the basis for the second round of generators to generate data And weight, In addition, the discriminator records the correct data, that is, it effectively recognizes that it is the data generated by the generator instead of the actual data, and the data is also weighted as the basis and weight of the second round of the discriminator. This is repeated for multiple rounds of confrontation and evolution cycles until the accuracy of the output data of the two models is maintained above 90%.

Finally, the model output is performed. The first output is the core index score output (0-100%) of the comprehensive evaluation of the adaptive conditional knowledge base strategy. This score can be extended to four categories of recommendation schemes, namely: knowledge base based on topic recommendation 0-25%, knowledge base based on rules, 26%-50%, knowledge base based on label recommendation, 51%-75%, knowledge The library is based on content recommendation, 76%-100%.Each category contains a large number of recommended solutions in the knowledge base, and the corresponding scores can specifically refer to the recommendations of one or more solutions, and correspond to the input of new unknown alarms. After the output of the scores is over, filter according to the set thresholds of these types of recommendations, and filter out some recommendation results.

5. Alarm Handling based on Knowledge Base

5.1. Alarm Information Classification

First, the alarm information is classified according to the associated equipment, and the alarm information is defined in the following table according to the requirements of the specification:

Table 1 :Alarm message definition

Alarm type	Alarm subtype	Alarm equipment	Warning level	Alarm time	Processing status
System log	CPU utilization exceeds the threshold	Firewall	general	2020-04-23 23:32:39	unsolved
System log	Memory usage exceeds the threshold	Firewall	general	2020-04-23 23:03:59	unsolved
Intelligent analysis alarm	Abnormal access to data	Firewall	important	2020-04-23 22:34:26	unsolved
Intelligent analysis alarm	Port scan	Firewall	important	2020-04-23 22:05:01	unsolved
System log	CPU utilization exceeds the threshold	Vertical encryption	general	2020-04-23 19:15:33	solved

5.2. Intelligent Recommendation Process of Knowledge Base

In the alarm processing process, based on the solutions stored in the knowledge base, and combined with the alarm content in the monitoring system, logical reasoning and analysis are carried out to infer the specific cause of the alarm, and to propose solutions according to the execution results. The knowledge base is optimized and adjusted. The following icon shows the process of intelligent alarm analysis.

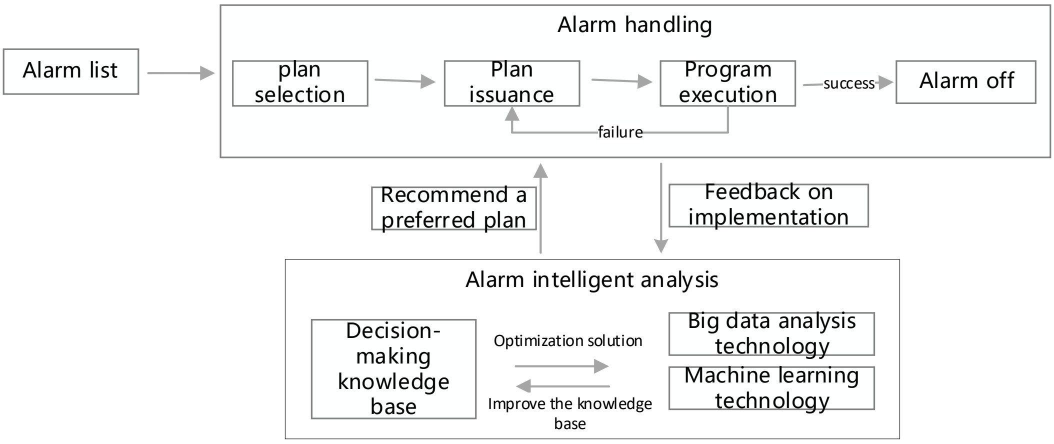

Alarm handling
Alarm list
plan selection
Plan issuance
Program execution
success
Alarm off
failure
Recommend a preferred plan
Feedback on implementation
Alarm intelligent analysis
Decision-making knowledge base
Optimization solution
Improve the knowledge base
Big data analysis technology
Machine learning technology

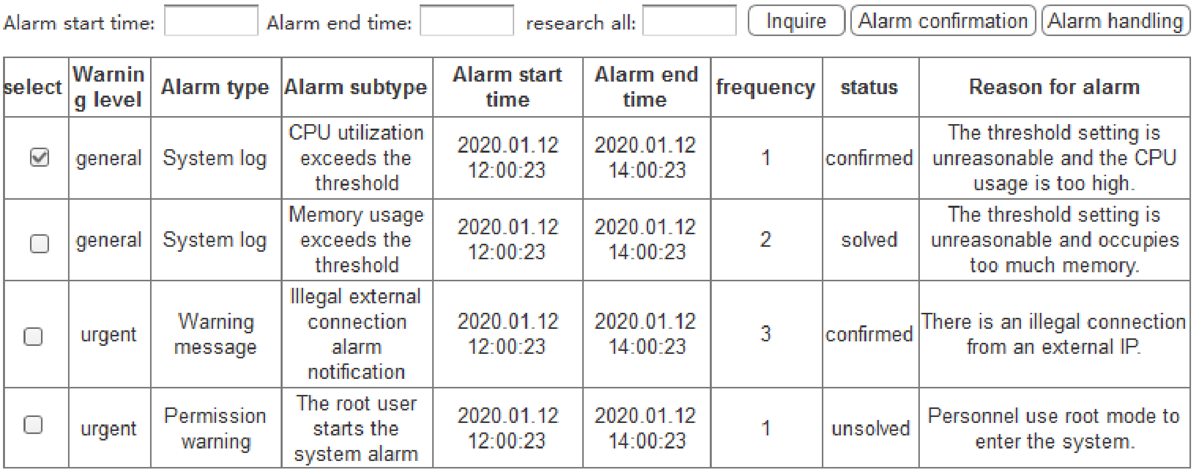
Fig. 6: Intelligent recommendation process of knowledge base solutions

The recommendation of the alarm information solution of the electric power monitoring system adopts an algorithm model based on machine learning. After the recommended plan, the staff on duty selects and executes, feeds back the implementation, and updates the plan data to achieve the purpose of improving the knowledge base.

6. Applications

6.1. Implementation Process

The following takes the daily handling of alarm information by attendants as an example to illustrate the knowledge-based alarm handling method designed in this article. On the platform alarm management page, select the alarm information. The alarm page displays key information such as alarm level and alarm equipment, as shown in the following figure:

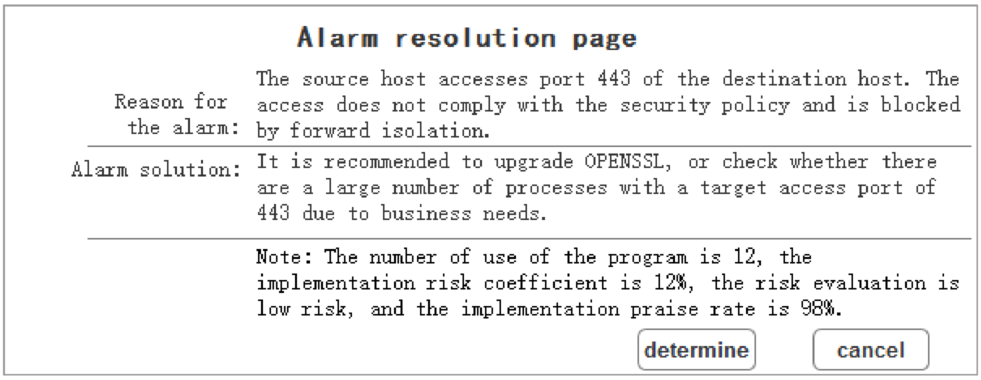


Alarm start time: ______ Alarm end time: ______ research all: ______ Inquire | Alarm confirmation | Alarm handling

select	Warning level	Alarm type	Alarm subtype	Alarm start time	Alarm end time	frequency	status	Reason for alarm
☑	general	System log	CPU utilization exceeds the threshold	2020.01.12 12:00:23	2020.01.12 14:00:23	1	confirmed	The threshold setting is unreasonable and the CPU usage is too high.
□	general	System log	Memory usage exceeds the threshold	2020.01.12 12:00:23	2020.01.12 14:00:23	2	solved	The threshold setting is unreasonable and occupies too much memory.
□	urgent	Warning message	Illegal external connection alarm notification	2020.01.12 12:00:23	2020.01.12 14:00:23	3	confirmed	There is an illegal connection from an external IP.
□	urgent	Permission warning	The root user starts the system alarm	2020.01.12 12:00:23	2020.01.12 14:00:23	1	unsolved	Personnel use root mode to enter the system.

Fig. 7: alarm information management

Select the alarm information and execute the "alarm handling". At this time, the pending alarm is sent to the alarm intelligent analysis module, and the solution recommendation algorithm in the module is called. The recommended algorithm selects the most effective solution for the alarm based on the alarm information and sends it to the knowledge base Alarm intelligent analysis module, the module gives the judgment of the alarm processing method or processing suggestion, and transmits it to the alarm processing module, as shown in the figure below.



Alarm resolution page

Reason for the alarm: The source host accesses port 443 of the destination host. The access does not comply with the security policy and is blocked by forward isolation.

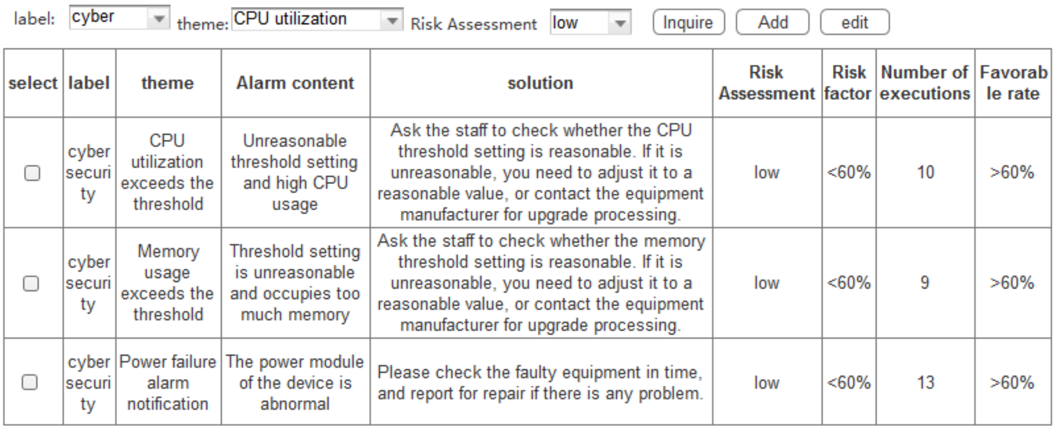
Alarm solution: It is recommended to upgrade OPENSSL, or check whether there are a large number of processes with a target access port of 443 due to business needs.

Note: The number of use of the program is 12, the implementation risk coefficient is 12%, the risk evaluation is low risk, and the implementation praise rate is 98%.

Fig. 8: Single alarm handling

The plan page gives the alarm reason, solution and message reminder for the reference of the duty officer. After the execution is completed, the alarm status, execution times, praise rate and other data are updated.

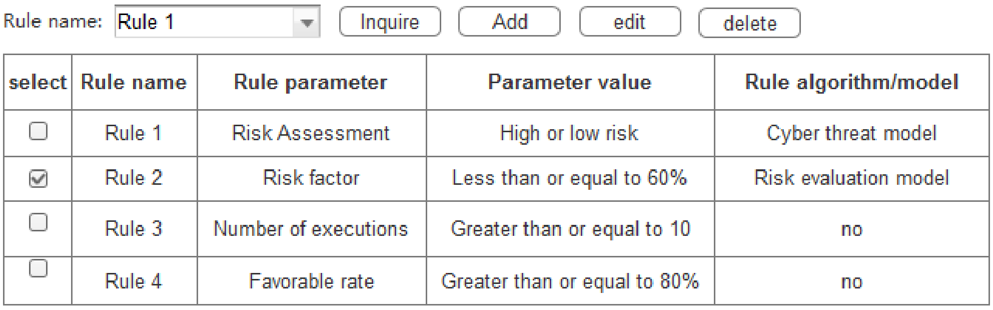
The knowledge base is continuously enriched and expanded during use. For this reason, the maintenance function of the knowledge base is also provided, as shown in the following figure:


label: cyber theme: CPU utilization Risk Assessment low

select	label	theme	Alarm content	solution	Risk Assessment	Risk factor	Number of executions	Favorable rate
☐	cyber security	CPU utilization exceeds the threshold	Unreasonable threshold setting and high CPU usage	Ask the staff to check whether the CPU threshold setting is reasonable. If it is unreasonable, you need to adjust it to a reasonable value, or contact the equipment manufacturer for upgrade processing.	low	<60%	10	>60%
☐	cyber security	Memory usage exceeds the threshold	Threshold setting is unreasonable and occupies too much memory	Ask the staff to check whether the memory threshold setting is reasonable. If it is unreasonable, you need to adjust it to a reasonable value, or contact the equipment manufacturer for upgrade processing.	low	<60%	9	>60%
☐	cyber security	Power failure alarm notification	The power module of the device is abnormal	Please check the faulty equipment in time, and report for repair if there is any problem.	low	<60%	13	>60%

Fig. 9 Knowledge Base Maintenance

In addition, the recommendation algorithm in the alarm intelligent analysis module is also an important and core part. The most important thing is that the rule maintenance in the recommendation algorithm is also a process of continuous enrichment and optimization. This article provides the rule maintenance function in the recommendation algorithm, as shown in the following figure:


Rule name: Rule 1

select	Rule name	Rule parameter	Parameter value	Rule algorithm/model
☐	Rule 1	Risk Assessment	High or low risk	Cyber threat model
☑	Rule 2	Risk factor	Less than or equal to 60%	Risk evaluation model
☐	Rule 3	Number of executions	Greater than or equal to 10	no
☐	Rule 4	Favorable rate	Greater than or equal to 80%	no

Fig. 10. Maintenance of rule base in recommendation algorithm

6.2. Application Effect Analysis

The use of the above-mentioned knowledge-based alarm processing method can help on-duty personnel to deal with on-site threat alarms, transition from manual processing to knowledge-based intelligent recommendation, and greatly improve the efficiency and accuracy of alarm processing. It usually takes 3 minutes to process an alarm, but now it only takes 20 seconds to complete. The operation and maintenance monitoring of a master station requires 5 people on duty, and now only 3 people are needed, which greatly reduces the power monitoring system of the master station and the plant. The cost of operation and maintenance has good economic benefits.

7. Conclusions and Prospects

This article proposes a knowledge base-based alarm processing method, which can help the supervisor on duty in the monitoring center monitor the on-site operation and maintenance system, assist in alarm analysis, and handle alarms. This greatly improves work efficiency and ensures that all and potential threats are obtained in the shortest time. Or abnormal handling methods, assist the on-duty staff to accurately analyze and handle in time, reduce the impact of potential threats on the system, and reduce the hazards of abnormalities. At the same time, in order to improve the quality of recommendation, the recommendation rules and algorithms need to be extended and deepened.

8. Acknowledgements

This work is supported by State Grid Corporation Headquarters Technology Project (Research on Key Technologies of Comprehensive Management and Control of Network Security Threats and Process Deduction for Power Monitoring).

9. References

[1] Wan Wenjuan, Wu Gao. Analysis of the problems and strategies of the content construction of Chinese institutional repositories[J]. Library, 2013, (1): 110-113.

[2] Si Li, Chen Xuanning. Investigation and analysis of the status quo of the construction of scientific research data institutions[J]. Library, 2017(4): 6-11.

[3] Guo Fangyu. Research and application of personalized information recommendation system for institutional repositories [D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[4] Yang Bo, Zhao Pengfei. Overview of recommendation algorithms [J]. Journal of Shanxi University (Natural Science Edition), 2011, (3): 337-350.

[5] Shi Linbin. Research on the recommendation method of review experts based on subject analysis [D]. Kunming: Kunming University of Science and Technology, 2014.

[6] He Ming, Liu Weishi, Zhang Jiang. Association rule recommendation algorithm supporting non-empty rate recommendation[J]. Journal on Communications, 2017, 38(10): 18-25.