Application Scenarios Of Knowledge Graph In IT Operation

Ziqian Li¹, Xusheng Liu¹, Yeteng An¹, Lintan Sun¹, Yintie Zhang²*, Jing Wan²

¹State Grid Customer Service Center
²Nanjing Data Foundation Technology Co, Ltd.

*Corresponding author e-mail: 569649415@qq.com

Abstract. Since Google optimized its search service by using knowledge graph, the application of knowledge graph has developed rapidly, especially in the aspect of information system operation and maintenance. CMDB (configuration management) built based on knowledge graph plays an excellent role in fault location of information system. However, the operation and maintenance data generated during the operation of the information system are diverse, not limited to configuration, correlation, and alarm information, and include all data generated during the operation and maintenance of the system. The knowledge map technology is used to effectively correlate various types of operation and maintenance data, which is more conducive to identifying core application scenarios of the information system, thereby further improving the global control ability in the operation and maintenance process. Therefore, this paper explores the rich application scenarios and prospects of knowledge graph application in the field of information operation and maintenance.

1. Introduction

Knowledge map is a relational network obtained by connecting all kinds of information, also called semantic network, including entities, attributes and relationships among entities in the real world. The knowledge map used in information operation and maintenance is to build domain knowledge map, especially in the operation and maintenance of enterprise-level information systems, the knowledge map technology is used to build the relationship network of all stakeholders in enterprise operation and maintenance of information technology. It is not limited to the single application scenario of configuration relationship and fault location, but applies the knowledge map to the overall situation of information operation and maintenance. Therefore, this paper mainly discusses the application scenarios and prospects of knowledge map application in the field of information operation and maintenance, instead of discussing the practical technology of knowledge map.

2. The concept of system operation and maintenance data [1]

Enterprise information systems are mainly run in enterprise data centers, so maintaining enterprise information systems involves four levels of operation and maintenance of information technology objects, including basic environment, infrastructure, infrastructure and business applications. The specific division is shown in Figure 1. Among them, the basic environment is the physical location of the data center, that is, the location of the buildings and the surrounding areas where the data center is located, which is the foundation of the existence of information systems. Infrastructure is the equipment running in the basic environment, which does not directly produce information value, but is an...
information asset with veto attribute. Infrastructure is IT equipment running in infrastructure environment, including virtual equipment, which directly generates information value and provides information system with resources. Business application is a software program running in the infrastructure, including platform software, business application software, operation and maintenance platform software, safety control software, etc., to directly realize information service.

![Diagram of Object Scope of Operation and Maintenance Data](image.jpg)

**Figure 1.** Object scope of operation and maintenance data.

The common concept of operation and maintenance data in information system operation and maintenance refers to all data information generated by all the above operation and maintenance objects in daily operation and maintenance. Such as operation logs, alarm information, performance indicators, maintenance documents, scheduling information, process information, etc., are collectively referred to as operation and maintenance data. The data type of data information can be structured, semi-structured or unstructured. Thus, operation and maintenance data is a very broad concept. Due to the diversity of maintenance objects at different levels, it is difficult to fully grasp the operation and maintenance data. Common operation and maintenance of information systems carry out differential maintenance by grouping maintenance objects. Maintenance hosts do not pay attention to network and database conditions, maintenance networks do not pay attention to business application software scheduling, etc. This directly increases the complexity of information system operation and maintenance, making it often difficult to locate faults in operation and maintenance.

### 3. Application Ideas of Knowledge Mapping

The concept of operation and maintenance data for information system operation and maintenance has been clarified. The key to breaking the common dilemma of information operation and maintenance is to establish the global correlation of operation and maintenance data by using knowledge map, and to control the situation of all operation and maintenance objects through a relational network, which is not limited to the single-point scenario of configuration management and fault location. The specific application ideas are: firstly, clustering the types of operation and maintenance data; secondly, extracting relevant knowledge by using the concept of knowledge map; and thirdly, constructing an application scenario of a global relationship network by using knowledge.

#### 3.1. Cluster operation and maintenance data

The content reflected by operation and maintenance data generated by all operation and maintenance objects can be divided into three categories: objects, activities and results. Therefore, operation and maintenance data can be clustered according to these three directions.

1. **Configuration class data**
Configuration data is used to explain the object problems in operation and maintenance. The core of information system operation and maintenance is configuration management, which needs to collect all the configuration information of hardware assets and software assets in the configuration database. The core of configuration data is three kinds of configuration information of four layer objects, which are configuration item, attribute and relationship. Configuration item refers to the configuration name of each item of entity information asset or virtual information asset. Attribute refers to the specific parameter of configuration name, and relationship refers to the relationship between configuration items. This three information are the basis of building the knowledge map. The more detailed the configuration item, the history of attribute value reservation, and the dynamic generation of relationship, the clearer the establishment of the knowledge map, and the three information need to be actively discovered and dynamically maintained.

(2) Log data
Log data is used to explain the activities in operation and maintenance. All objects are generating logs at all times during operation, recording what objects are doing at all times. No matter the operation logs, audit logs, security logs, etc., no matter the correct confirmation and error reporting information, they need to be classified together. The common log analysis is based on these data for machine learning. Log information is the basis of building knowledge map. There is association of object activities in massive logs, which needs to be automatically discovered by log mining.

(3) Action data
Action-type data is used to explain the activity problems in operation and maintenance. The difference between this type of action data and log data is that the log is an objectively generated record of the object itself. Action data is data generated by human subjective actions, mainly referring to who, what time, what object, and what operation was performed. Among them, the operation may be a maintenance operation or an operation of a business operation. Action information is also the basis for constructing a knowledge map. Action information is implicitly related to other operation and maintenance data. It needs to be solidified by management means and established automatically.

(4) Performance data
Performance data is used to explain the problem of results in operation and maintenance. It mainly refers to the monitoring of various performance indicators in the normal state, and the data generated is divided into two categories: cross-section data and time series data. Among them, the cross-section data is the current state of the reaction log and the result of the action; the time-series data is the change of the reaction object over a period of time. Performance information is a difficult point in constructing a knowledge graph. In theory, all actions and behaviors of maintenance objects should reflect performance, even if it does not cause changes in performance indicators. The fact that it is constant is also a reaction state, and the connection needs to be automatically discovered through data mining.

(5) File data
File-type data is used to explain the results in operation and maintenance. It is mainly data in all file formats generated during operation and maintenance, which can be execution work orders, report files, implementation plans, emergency manuals, etc., or video files, picture files, etc. These are the result files that need to be archived before, during, and after the operation and maintenance work is started. Document-type information is an extension of the construction of a knowledge graph, which is to transform existing experience and knowledge into a global information source. It needs to have the ability to automatically operate files and file contents.

3.2. Select related knowledge [2]
The global relationship network of information system operation and maintenance can identify the correlation between various types of operation and maintenance data, so the triple expression of knowledge map is fully utilized to extract all the correlations of operation and maintenance data. Among them, triplets are a common representation of knowledge maps, and their basic forms can be divided into two types, as described in the following expression.

Expression 1: "Object-Attribute-Attribute Value", an expression of the meaning of the data itself;
Expression 2: "Object-Relation-Object", an expression of the relation between data.

Two types of expressions are used to express global knowledge across different operation and maintenance data categories, and ten types of global knowledge can be extracted in total, as described below.

1. The first type of knowledge, between the configuration class and the log class

   Extract the relational expression of "attribute-relationship-log", that is, the attributes of the configuration item itself are linked to the occurrence of which logs. Extract the relational expression of "attribute value-relationship-log volume", that is, the linkage between the change in attribute value and the change in the number of logs. The meaning expression of "configuration item-attribute value-log volume" is extracted, that is, a logical interpretation of configuration management and log generation is established.

2. The second type of knowledge, between configuration and action

   Extract the relationship expression of "attribute-relationship-action", that is, identify which maintenance actions are associated with which attributes. The relational expression of "attribute value-relationship-performance" is extracted, that is, identify which performance index changes will be caused by different configurations of the system. Extract the relationship expression of "attribute value-relationship-performance value", that is, classify the relationship between different configuration values and performance time series data. Extract the meaning expression of "configuration item-attribute value-performance value", that is, to establish a logical interpretation of configuration changes and performance capacity.

3. The third type of knowledge, between configuration and performance

   Extract the relational expression of "attribute-relationship-performance", that is, identify which performance index changes will be caused by different configurations of the system. Extract the meaning expression of "configuration item-attribute value-performance", that is, classify the relationship between different configuration values and performance time series data. Extract the meaning expression of "configuration item-attribute value-performance volume", that is, establish the interpretation logic of different action results and logs.

4. The fourth type of knowledge, between file and configuration

   Extract the relationship expression of "file relationship configuration item", that is, identify which files are related to which configuration. The meaning expression of "file configuration item attribute value" is extracted, that is to say, which documents are involved in the generation process of different configuration values.

5. The fifth type of knowledge, between log and action

   Extract the relationship expression of "action relationship log", that is, identify what logs will be generated by different maintenance actions. Extract the relationship expression of "action relationship log change", that is, identify the log changes caused by different maintenance actions. Extract the meaning expression of "action result log", that is, establish the interpretation logic of different action results and logs.

6. The sixth type of knowledge, between log and performance

   Extract the relationship expression of "performance indicator relationship log", that is, the relationship between different performance indicators and log generation. Extract the meaning expression of "performance change log content", that is, establish the interpretation of log content and performance capacity change.

7. The seventh type of knowledge, between log and file

   Extract the relationship expression of "file relationship log", that is, identify which log indicators are involved in different file contents. Extract the meaning expression of "file log log content", that is, master the interpretation of different schemes and other files and logs.

8. Type 8 knowledge, between action and performance

   Extract the relationship expression of "action-relationship-performance", that is, identify which indicators are associated with different actions. Extract the relationship expression of "action-relationship-performance change", that is, identify the change relationship of the index caused by different actions. Extract the meaning expression of "performance change-action-result", that is, grasp the explanation between different performance time series data trends and maintenance actions.

9. Type 9 knowledge, between action and document
Extract the relational expression of "action-relationship-file", that is, identify the execution basis of different actions.

(10) The tenth category of knowledge, performance and file
Extract the relationship expression of "file-relation-performance", that is, identify which performance indicators are involved in the content of different files; extract the meaning expression of "performance change-file-file content", that is, construct the interpretation of performance trends and existing file contents.

3.3. Knowledge Mapping Application Scenarios
The state of information system operation and maintenance can be simply summarized into two types, one is the daily operation state when there are no events, and the other is the time processing state when there are events. Therefore, based on the combination of identified knowledge map relationships, the operation and maintenance scenarios that can be applied can be divided into two types, as shown in Table 1 and Table 2. Among them, the application of knowledge map of daily state focuses on the interpretation of data itself, while the application of knowledge map of event state focuses on the use of data relations.

![Table 1. Application scenarios of daily state knowledge map.](image)

| Serial number | Scene               | Target                        | Application of knowledge points                                                                 |
|---------------|---------------------|-------------------------------|-------------------------------------------------------------------------------------------------|
| 1             | Panoramic monitoring| Do not split the overall situation | Use the first, third and sixth categories of knowledge to explain the overall risks.                |
| 2             | Risk management     | Master that there are anomalies  | Use the second, fifth and eighth categories of knowledge to explain behavioral risks            |
| 3             | Configuration management | Master configuration impact  | Use the first, second, third and fourth types of knowledge to explain configuration risks        |
| 4             | Capacity management | Master capacity impact        | Use the third, sixth, eighth and tenth categories of knowledge to explain resource risks.        |
| 5             | Resource management | Master the impact of changes   | Use the third, sixth, eighth and tenth categories of knowledge to explain resource risks.        |
| 6             | Program Management  | Master the priority level      | Use the second, fourth, fifth, seventh, eighth and ninth categories of knowledge to explain behavioral risks |

![Table 2. Application scenarios of event state knowledge graph.](image)

| Serial number | Scene               | Target                        | Application of knowledge points                                                                 |
|---------------|---------------------|-------------------------------|-------------------------------------------------------------------------------------------------|
| 1             | Alarm location      | Filter useless alarms         | Use the first, third, fifth, sixth, seventh, eighth and ninth types of knowledge to connect all alarms in series |
| 2             | Cause analysis      | Judge possible causes         | Use the second, fifth, eighth and ninth types of knowledge to investigate possible behaviors    |
4. Prospects for Core Application Scenarios [3]

4.1. Risk management scenario

In daily situations, risk identification is a very important work. The continuous operation and availability of information systems does not mean that there is no risk in the system. Identifying risks and optimizing them as soon as possible are the key to active operation and maintenance. The core of the application of knowledge map in this scenario is to judge the cause of the discovered abnormality. If the abnormality cannot be explained by knowledge map, it is defined as risk. On the contrary, if abnormalities can be explained by knowledge maps, they are defined as controllable phenomena. For example, when a load anomaly is discovered from the performance data, it shows that there is a constant regular load every day, as shown in Figure 2. Global knowledge map retrieval excludes the existing possibilities of related personnel behavior, business behavior, log status, similar schemes, etc. Therefore, we can define this anomaly as new, and we need to continuously pay attention to its changes and continue to expand the related knowledge in the atlas until we can explain its phenomenon.

Figure 2. Prospect of risk management scenarios.
4.2. Maintenance suggestion scenario
When an incident occurs, the management role needs to arrange the maintenance plan reasonably. The knowledge map will be used to retrieve the information related to its content, such as the optimal executor, the similar situation of historical maintenance, and the related contents in the existing documents, etc. The information operation and maintenance foundation can be used to automatically generate the personnel arrangement of the maintenance plan and refer to the implementation plan, making the arrangement of the maintenance plan more reasonable and efficient.

4.3. Result verification scenario
In system operation and maintenance, it is more important to judge whether the business function itself has been restored. Through the global information established by the knowledge map, all operation and maintenance data with the maintenance object as the core can be checked once. The verified data are the data information before overhaul and the data information after overhaul, which indexes are affected by overhaul contents can be quickly judged, and knowledge iteration enters the overhaul history as the judgment basis in the future.

5. Summary
Knowledge map is applied in information system operation and maintenance. The most important thing is to cover all operation and maintenance data, extract triplet information of various data, retrieve related knowledge content and form scenes, so as to improve the overall control ability of operation and maintenance. The application scenario is open and not limited to the use of a few scenarios. The demand for related knowledge of operation and maintenance data in different scenarios is also increasing. Extracting knowledge from operation and maintenance data center can enrich application scenarios, and the quality of operation and maintenance data can also be inferred from application scenarios.

References
[1] Hu Yang, Lin Zhida, et al. Comprehensive performance evaluation method of IT assets [J]. Information technology and informatization, 2016 (11): 34-36
[2] Fu Shan, Lu AI Lin, Yan Shu. Concept and application of knowledge map [J]. Telecommunication network technology, 2019, 000 (005): 10-13
[3] Zhang yintie, Wang Jun. evaluation method of information system operation and maintenance [J]. Information technology and informatization (11): 33-36