Interactive Sharing Method of Power Grid Dispatching and Control Operation Data Based on Data Classification and Grading

Lin Xie[1(✉)], Ruili Ye[1], Yan Wang[1], Chaohan Feng[1], Dapeng Li[1], Xiangyu Zhang[2], Can Cui[1], Qiong Feng[1], Zhoujie Zhang[1], and Xinxin Sheng[1]

[1] Beijing Key Laboratory of Research and System Evaluation of Power Dispatching Automation Technology, China Electric Power Research Institute, Beijing, China
xielin519@163.com

[2] Economic and Technological Research Institute, State Grid Shanxi Electric Power Company, Taiyuan, China

Abstract. The era of big data is characterized by rapid information change, large volume of data, many dimensions, and various types, which requires enterprises to classify and grade data management. Especially in the critical period of new power system construction, a method is needed to classify and share power grid dispatching and operation data safely. This paper analyzes the business characteristics of power grid dispatching and control data, and designs the classification principle of power grid dispatching and control operation data, and builds a data sharing open directory based on this principle, and proposes a method of interaction and sharing of power grid dispatching and control operation data. Finally, this paper realizes the internal sharing and external circulation of power grid dispatching and control data through the interaction process.

Keywords: Power grid dispatching and control operation data · Data classification and grading · Data sharing and open directory · Data interaction and sharing

1 Instruction

With the speeding up of the construction of extra-high voltage AC/DC interconnection grid, the centralized access of large-scale new energy, the deepening of power market reform, and the goal of "carbon peaking, carbon neutral" and "building a new power system", the grid operation has formed and accumulated rich data resources. These data resources have become important assets of the enterprise [1, 2]. The full exploitation of the value of these data assets can greatly promote the grid intelligent perception, internal control capabilities and customer service efficiency. Power grid dispatching and operation data sharing can also bring convenience to power production and marketing, etc. However, as the national critical infrastructure, power data is related to national security, and it is be easy to become the target of network attacks and theft. Once with these business data loss, damage or leakage, it may cause power system failure or

G. Zhai et al. (Eds.): IFTC 2022, CCIS 1766, pp. 502–511, 2023.
https://doi.org/10.1007/978-981-99-0856-1_37

major security incidents, and bring huge economic losses to the country and enterprises. Therefore, power enterprises must strengthen the security protection of power sensitive data assets and solve the security problems of value data exchange and sharing and data mining.

Data classification and grading is the cornerstone for promoting data sharing and data security construction, and sorting out data with different attributes and implementing differentiated opening strategies is the premise of data security sharing [3]. In February 2020, the Ministry of Industry and Information Technology issued the Guide to Industrial Data Classification and Grading (for Trial Implementation), which divides industrial data into three security levels and guides enterprises to comprehensively sort out their own industrial data and improve data grading management capabilities, but the guide is a guideline for the whole industrial field, which is relatively broad in rule design and has limitations for guiding the practical operation of the electric power industry [4]. In addition, various industries have successively proposed principles for data classification and grading. In September 2020, the People's Bank of China released JR/T0197–2020 "Financial Data Security Data Security Grading Guide", which gives principles for data security grading and divides financial data into 5 levels. In December 2020, the Ministry of Industry and Information Technology released YD/T3813- 2020 "Data Classification and Grading Methods for Basic Telecommunications Enterprises", which stipulates the principles of data classification and grading for basic telecommunications enterprises as well as the workflow and methods of data classification. at the end of 2020, the "Technical Specification for General Data Security Requirements of Southern Power Grid (for Trial Implementation)" was released, which puts forward the basic principles for data classification and grading work. The goal of data classification and grading is to ensure that information is appropriately protected and open according to its importance to the organization, so proposing a classification and grading method for grid dispatching and operation data is an important basis for open data sharing.

Based on the characteristics of instantaneous, reusable and multi-attributed power grid operation data, a scientific and reasonable classification of power grid dispatching and operation data and the design of "different and equal" sharing methods are indispensable tools to promote data sharing and data protection in the digital economy. This paper proposes a sharing and interaction method for power grid dispatching and control cloud data through a data sharing open directory to classify and display dispatching and operation data, and realize internal sharing and external circulation of enterprise data.

2 Grid Dispatching and Control Operation Data Classification and Classification

2.1 Principles of Wide-Area Service Proxy

Grid dispatching and control operation data are various historical data generated during the operation of the grid to reflect the operating status of the grid and related primary and secondary equipment [5]. Referring to the existing domestic and international data classification system standards, the paper presents the data asset classification principles for power grid dispatching and control operation with reference to the dispatching and

control operation business data generation process and object-oriented principles. The data asset classification of power grid dispatching and control operation covers horizontally to each business information system, and vertically extends from business functions to specific power grid dispatching and control operation activities. Grid dispatching and control operation data comes from Supervisory Control and Data Acquisition, Operations Management System, Tele Meter Reading, Power Generation Plan, and other data assets. Reading, generation planning system, and other types of dispatching and control business systems [6].

In this paper, the data classification is carried out according to the idea of total division of business lines, and the business data are subdivided into 28 categories such as load, generation, current, voltage, etc., and then converged into 8 major categories such as power, electricity, planning, forecasting, alarm, event, environment, and market according to the business categories.

According to the above rules, combined with the 8 categories and 28 sub-categories of data objects, the data classification system for power grid dispatching and control operation data is designed, as shown in Fig. 1.

2.2 Data Security Intensity Grading

Data should be graded according to legal requirements, value, importance and its sensitivity to unauthorized leakage or modification [7, 8]. According to the core idea of ISO27001 system, security includes three elements of confidentiality, integrity and availability, and data asset evaluation can be judged by the assignment of the three elements, which can be calculated to reflect the business value of data according to the assignment and weight of CIA (Confidentiality, Integrity, Availability). Based on the classification, the data security grading of power grid control operation data takes the smallest data class as the grading object, takes into account the factors of power grid production and operation and dispatching professional management, and builds the data grading model from three evaluation dimensions according to the degree of damage and impact after the data is tampered, damaged, leaked or illegally obtained or illegally used, as shown in Fig. 2.

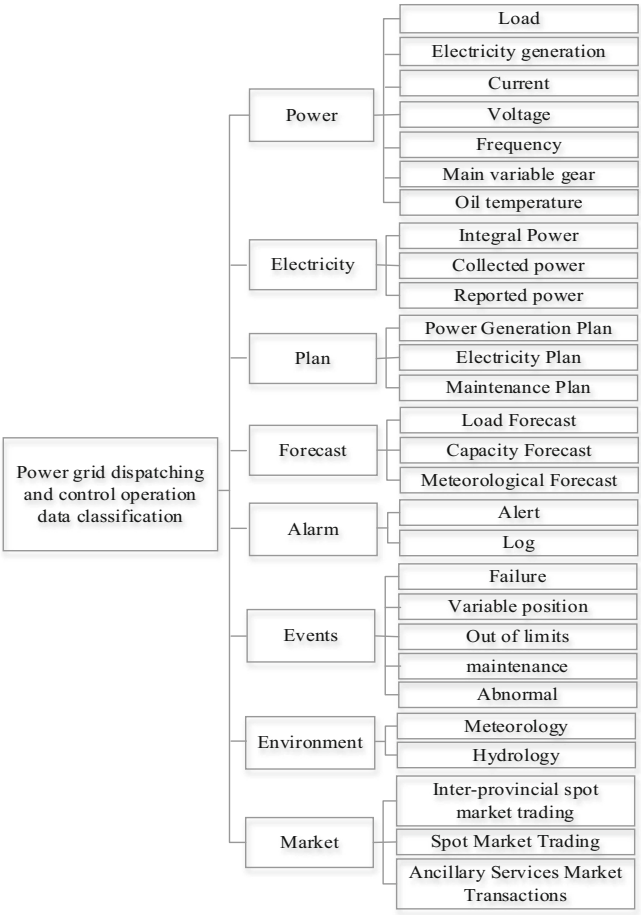

Fig. 1. Classification system of power grid dispatching and control operation data

Based on the data classification model, business data is identified and evaluated to determine the reasonable valuation of the data, and finally the data level is divided into three levels from high to low. If the first level data is tampered, damaged, leaked or illegally obtained or used, it may affect the safe operation of the power grid or the economic interests of the market players, such as remote telemetry, generation plan, protection value, market clearing data, etc. Once the secondary data is tampered with, damaged, leaked or illegally obtained or illegally used, it may affect the monitoring and analysis of the power grid, such as power consumption, telematics and telemetry data. If the tertiary data is tampered, damaged, leaked or illegally obtained or illegally used, it will not have a direct impact on the power grid operation and monitoring, such as secondary equipment operation and monitoring, meteorological data, etc. According to the above classification principles, the grid control operation data security grading control strategy matrix is formed, as shown in shown as Table 1.

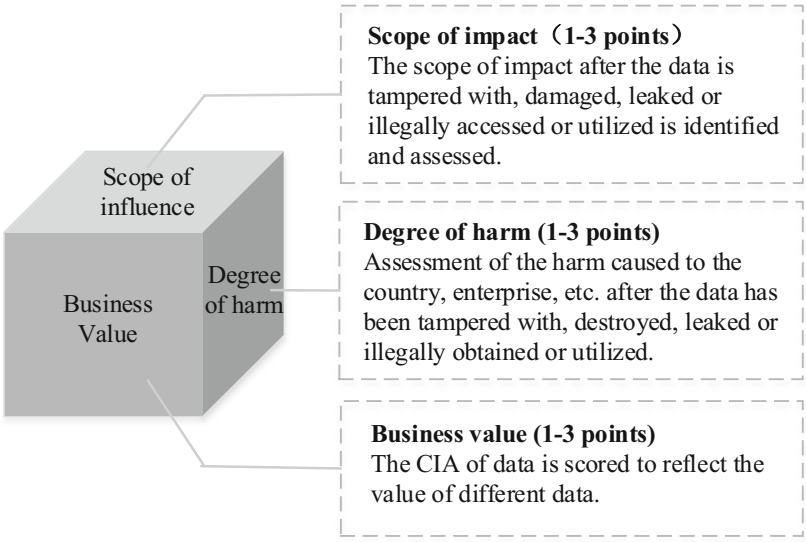

Fig. 2. Data classification model

Table 1. Data security classification and control strategy

Data grading	Impact level	Encryption principle	Desensitization principle
Level 1	Serious	Need to encrypt	Need to desensitize
Level 2	Moderate	/	Need to desensitize
Level 3	None or slight	/	/

3 Method of Sharing and Interacting with Data of Power Grid Dispatching and Control Operation

3.1 Data Sharing and Open Directory

Data sharing and open cataloging can clarify the scope and conditions of data resources for sharing and opening, and reduce the threshold for understanding system data. The shared open catalog for power grid dispatching and control cloud line data customizes the construction of data asset catalog hierarchy and describes data asset-related attributes in accordance with business requirements and enterprise standards. The shared open catalog of dispatching and operation data is organized in the form of metadata, which is a set of data sorted and coded according to certain classification methods to describe the characteristics of each data resource [9]. Then, according to different data classifications and data attributes, corresponding types of data topics are established, and different types of data catalogs are cataloged into the corresponding data topics, taking into account information such as resource dimension, security dimension and sharing dimension, which not only improves the ability to manage data, but also greatly enhances the efficiency

of users in retrieving, locating and accessing data. It includes resource dimension, security dimension and sharing dimension, etc. The process of publishing the data sharing open catalog is generally divided into three steps: data catalog archiving, data catalog auditing, and data catalog publishing, and the flow chart is shown in Fig. 3.

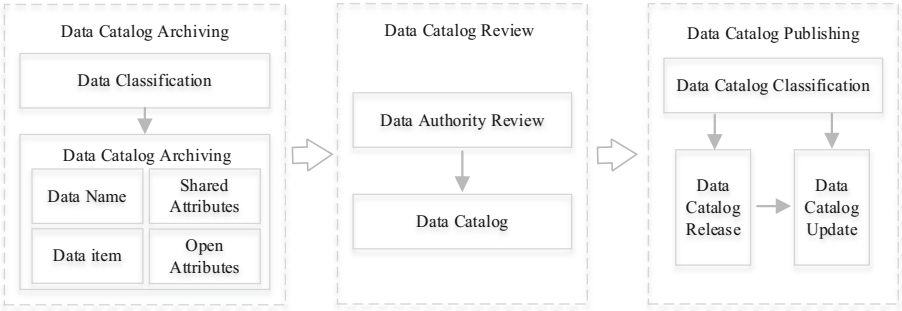

Fig. 3. Flow chart of data sharing and open catalog publication

Data catalog archiving is the process of open data archiving. Open data sources with file uploading and parsing, data sharing, data disclosure, etc. require unified data archiving functions. After data archiving, auditors from data providing departments are required to review and form data catalogs before publishing. When the data catalog is released, it needs to be classified and released according to different topics to facilitate data users to browse. After the data catalog is published, new data will be added and the data catalog will be continuously updated and maintained.

3.2 Data Sharing Methods

Grid dispatching and control operation data sharing, on the one hand, is oriented to the flow of data within the enterprise, and on the other hand, it is the act of providing data to external users such as government departments, external enterprises, organizations and individuals. This paper combines the data classification and grading principles and data opening forms, and proposes the interaction sharing method and interaction process for power grid dispatching and operation data. Users can get data from the data platform after authentication, but the content and way of data access are different for users with different authority. The internal sharing of data is the exchange of data across organizations and departments within the enterprise, which can be done through data services, database access, data files, etc.; the external sharing of data is mostly the exchange of data between enterprises, and due to the special nature of power grid dispatching and operation data, the original data is often not directly opened, and the primary and secondary data need to be protected and provided through data services. The data is provided through data services. For the data that can be provided to the public, it needs to be audited for information leakage. The interaction process for sharing data on power grid dispatching and operation is shown in Fig. 4.

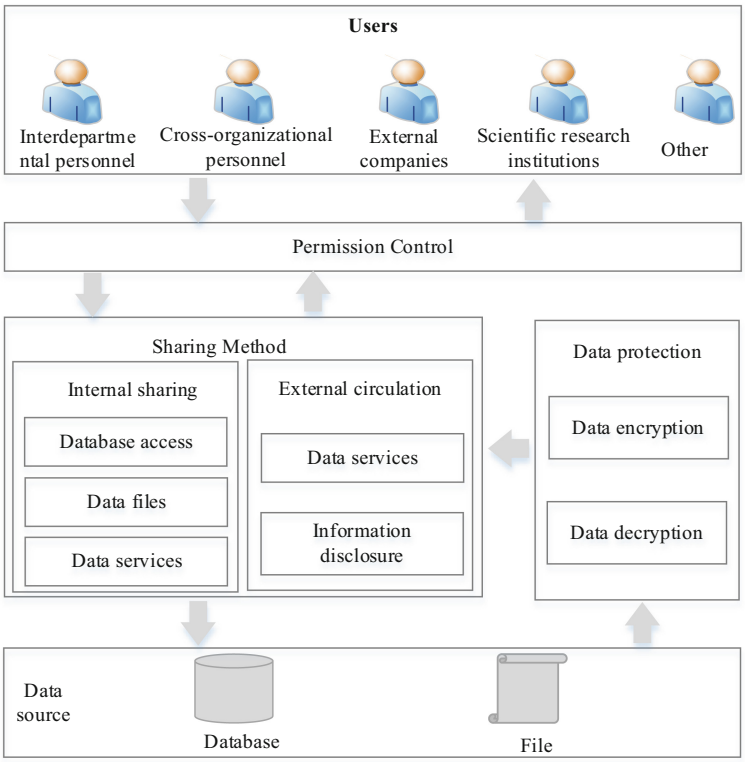

Fig. 4. Interaction flow of data sharing for grid dispatching and operation

(1) Permission control

Data permissions are a mapping relationship between users and data. Because different users enjoy permissions to different data resources, a many-to-many mapping relationship is formed. By introducing the Role-Based Access Control model [10], a mapping relationship is established between roles and data, as shown in Fig. 5(a). However, it is inappropriate to generate roles for each individual, as the mapping relationship is too large and redundant. In this paper, the control of permissions is combined with data levels, and the control of data permissions is performed by comparing user levels and data levels. Data and users are mapped to data levels to determine the data permissions that users have, as shown in Fig. 5(b). For different levels of users, the access content, access mode and data access frequency of data need to be controlled to ensure the security of data sharing.

(2) Sharing method

On the basis of classification and grading of power grid dispatching and operation, the data sharing mode is opened by following the principle of minimum authority and dynamic authorization. Data internal sharing is the exchange of data across organizations and departments within the enterprise, and data can be shared through data services,

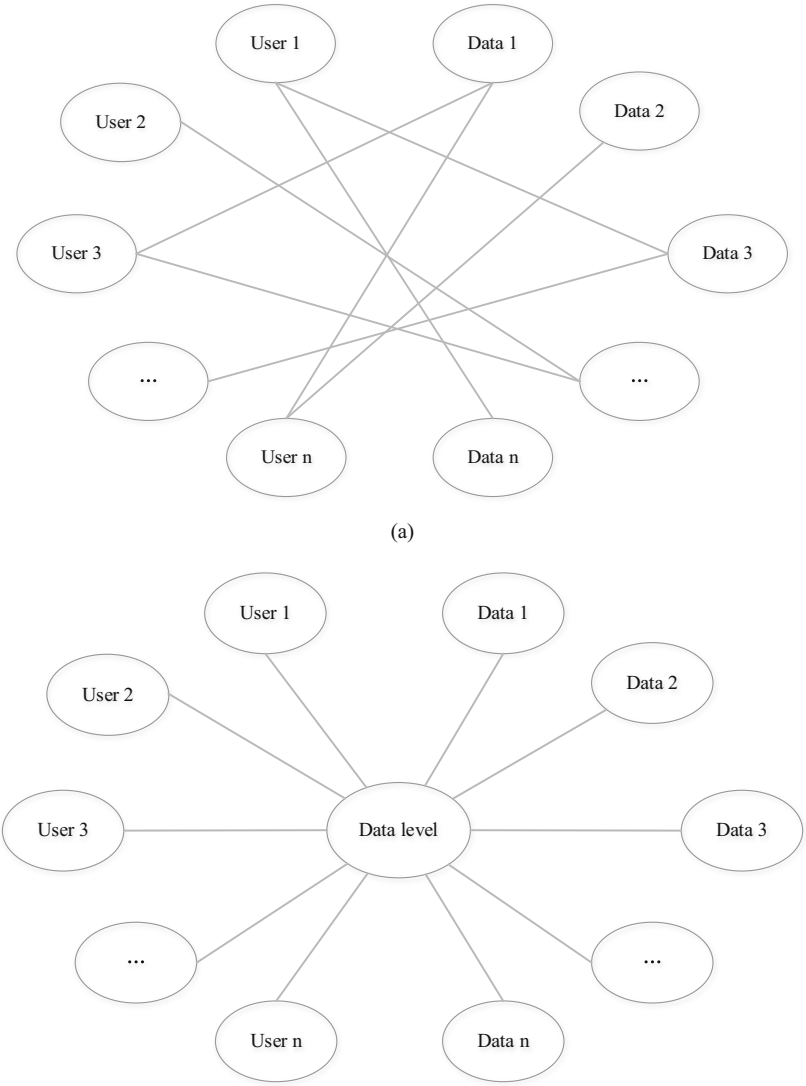

Fig. 5. User access control model

database access, data files, etc. Data services are encapsulated in the form of API interfaces for data protection of security level data. The data file approach allows data to be exported offline, encrypted, and then shared. After the data visitor obtains the data permission through permission authentication, the sharing platform provides the choice of sharing methods according to the permission. The external sharing of data is mostly for data exchange between enterprises. Due to the special nature of power grid dispatching and operation data, the original data is often not opened directly, and for primary and

secondary data, data protection processing is required and the data is provided through data services. For the data that can be provided to the public, it needs to be audited for information leakage, and the public can download and use the data.

(3) Data protection

In the data protection module, data with high security level will be encrypted and decrypted to key authorization, which enhances the security of sensitive data in the usage chain. By constructing an asymmetric encryption service AEMS, it provides an additional layer of protection for the asymmetric encryption public key in the hybrid encryption mechanism, and later uses a hybrid AES symmetric encryption algorithm and RSA encryption scheme to improve the confidentiality of data.

For sensitive data, static desensitization policy and dynamic desensitization policy are designed to realize the configuration of desensitization policy for each type and scenario. Static desensitization policy is generally used in non-production environment or in cases where data is used separately from the native business system, such as development testing and scientific research process [11]. In development and testing scenarios, such as power grid regulation and operation and other sensitive information systems contain sensitive information such as names, identities, and account numbers, but development and testing need to use these real data, so it is necessary to ensure that sensitive data are not leaked through desensitization means. Secondly, the data sharing scenario is usually under some specific needs to share the data with other departments or external enterprises. At this time, some sensitive data needs to be retained and specific sensitive data needs to be processed. Finally, scientific research scenarios usually center on the statistical analysis of data and the use of the results for scientific research, requiring the data to be desensitized while still retaining the original characteristics and content necessary for scientific research. Dynamic data desensitization is often used in the case of accessing sensitive data for immediate desensitization, and different levels of desensitization are required depending on the situation when the same sensitive data is read. In the case of interface call or data flow between business systems, the actual call can be executed and the desensitized data returned after receiving the data access request through dynamic desensitization agent conversion to ensure data security. In this paper, we design the desensitization policy configuration by considering the permission control and sharing methods, judge the data users according to the user's permission, and use the desensitization algorithm dynamically and senselessly by the selected sharing method to ensure the security of data sharing.

4 Conclusions

In order to solve the security sharing of power grid dispatching and control operation data, this paper combines the business characteristics of power grid dispatching and control data, designs the principle of grading and classification of power grid dispatching and control operation data, and builds a data sharing open directory based on the grading and classification of data, proposes a dynamic interaction sharing method of power grid dispatching and control operation data, and finally realizes the internal sharing and external circulation of power grid dispatching and control data through the interaction process. The paper puts forward some ideas and methods for grading and classification

of power grid dispatching and control operation data as well as safe sharing, and the next step will be to continue the research on safe sharing of dispatching and control operation data with new technologies such as blockchain.

Acknowledgment. This work is supported by Science and Technology Program of State Grid Corporation of China under Grant No. 5442DZ210027 (Research on Asset Value Assessment Method for Power Grid Dispatching and Control Operation Data).

References

1. Hongqiang, X., Cai, Y., Xiong, W., et al.: Architecture and key technologies for big data platform in power grid. Power Syst. Technol. **45**(12), 4798–4807 (2021)
2. Ming, Z., Chi, S., Chenghua, W., et al.: Research on power data security classification algorithm under the Internet of things environment. Mach. Des. Manuf. Eng. **50**(4), 52–56 (2021)
3. Chang, W., Ya, Z.: Discussion on classification and classification of tobacco industry data and security protection methods. Inner Mongolia Sci. Technol. Econ. 1(443), 31–32+57 (2020)
4. Qiongli, Z., Yi, C.: Research of data classification model and practice. Technol. Market **29**(8), 150–153 (2022)
5. Hongqiang, X.U.: Structured design and application of power dispatching universal data object for dispatching and control cloud. Power Syst. Technol. **42**(7), 2248–2254 (2018)
6. Hongqiang, X.U.: Architecture of dispatching and control cloud and its application prospect. Power Syst. Technol. **41**(10), 3104–3111 (2017)
7. ZhenWei, T.: Discussion on classified management strategy of enterprise sensitive confidential data. Mod. Ind. Econ. Informationization **9**(10), 79–80 (2019)
8. Jie, C., Tingyun, W., Wang, Qian, et al.: Research on the path of enterprise data classification and hierarchical management. Netw. Secur. Technol. Appl. (04), 70–71 (2022)
9. Vilminko-Heikkinen, R., Pekkola, S.: Master data management and its organizational implementation. J. Enterp. Inf. Manage. (3) 2017
10. Damiani, M.L., Bertino, E., Catania, B., Perlasca, P.: GEO-RBAC. ACM Trans. Inf. Syst. Secur. (TISSEC),(1) (2007)
11. Yiping, L., Chen, W.: Research on sensitive data protection of big data platform. Telecom Eng. Tech. Stand. **30**(11), 35–38 (2017)