Research And Implementation Of Integrated Operational Monitoring System Based On Secondary System Security Protection

Dekui Lv[1]*, Miao Yu[1], Jianyu Song[1], Zifeng Cui[1], Qiang Liu[2], Ningxin Liu[3]

*1 The 28th Research Institute of China Electronics Technology Group Corporation,
Nanjing 210000, China
2 Tianfu College of SWUFE,Chengdu 610000, China
3 College of Communication Engineering, PLA University of Science and Technology,
Nanjing 210007, China
Corresponding author, e-mail: ldk114@qq.com

Keywords: Secondary System Security Protection; Operation and Maintenance Supervision; Network Management; Security Management; Alarm Management.

Abstract

With the development of network and information technology, the system network equipment structure is more and more complex and the system is more and more difficult to manage. Facing such complex equipment and network architecture, current automation systems and network management methods are still in the initial stage, which can not meet the needs of safe operation and maintenance, it is difficult to improve service management level. In this paper, based on the research and analysis of unified information base model and interface specification, unified automation system of platform security area I and II, centralized monitoring and management of network equipment and security risk management, the author designs and implements the comprehensive operational supervisory system that adapts to intelligent power stations, which solved the operational problems in the system of secondary system security protection technology. Besides, the system was validated to be effective through the experiment.

1 Introduction

At present, with the development of network and information technology, the system network equipment structure is more and more complex and the system is more and more difficult to manage. Facing such complex equipment and network architecture, current automation systems and network management methods are still in the initial stage, there are the following questions:

1) A large number of safety equipment doesn’t have centralized management, the maintenance is decentralized and workload is heavy. They identify the network structure by mutual work, which have big maintenance difficulty and are error-prone[1];

2) Staffs are unable to grasp the performance of automatic network operation and can not technically control the use of the network, there are network security risks and it’s difficult to optimize the network structure[2,3];

3) There is no uniform monitoring and management of the performance of various types of servers, which is not conducive to improving the management level;

4) There is no monitoring of long-distance dials and daily maintenance of automatic system, which exists potential safety hazard[4].

In order to achieve the above-mentioned requirements, we need to improve service management level[5]; we need to use advanced technology, adopt safe and reliable design program, integrate the secondary information systems and network management into one, and establish an automatic system and network synthesis management system[6,7]. The main content of this paper is to design and implement an integrated operational monitoring system based on secondary system security protection, which solved the problems of system operation and maintenance.

2 Research and analysis of technology

2.1 Collect once and share data everywhere

Through the collection of the alarm, performance, configuration and security data of the automation network, host computer and security equipment, the author achieves the management of IT resources such as network, system, application and security equipment. In the process of data collection of multiple systems, same data of same resource may be collected for many times. On the one hand, multiple storage of same data results in data redundancy and consistency differences. On the other hand, multiple data collection may cause performance impact on the managed resources. Therefore, it is suggested that to collect data once and change the repeated collection of alarm, performance, configuration, security incidents, vulnerabilities and asset data to one collection, using for many times.

2.2 Unified information base of the extensible IT resource model

Data of various systems is stored respectively, which results in data redundancy. Due to the fact that data collection is different from maintenance strategy, there may be inconsistency of data. In order to provide a unified, complete and accurate data, a unified management information system needs to be built as the core data structure and storage of the system, which provides an unified data bus interface for other applications and display module. The data in the management information base includes resource data, operations, views, faults, performance, raw data and knowledge base.

2.3 Graphic platform of graphic and model integration

In order to achieve the goal of real-time management and fine management and draw on the successful experiences of SCADA/power grid management and monitoring system, a graphic platform needs to be established to support unified application and display interface, integrated real-time monitoring and maintenance and statistical analysis.

2.4 Flexible and efficient system architecture

The author breaks the traditional decentralized integrated monitoring tool construction, combines with the current development status of integrated monitoring products, independently researches and develops flexible and efficient automation systems and network management platform, reserving interface for future system expansion and remote monitoring of transformer substation.

The main structure of the system takes the data bus, unified information database and graphics platform as the core.

Unified database is based on DMTFCIM standard, the author combines with the characteristics of power IT system and establishes flexible resource model suitable for power IT infrastructure, which means to adapt to different IT resource types and IT business applications of products in different manufacturers. It achieves the model integration of the entire system.

JMS-based data bus configures the main data dynamically and takes IT resource model of the unified information base as the basis, which achieves the standardization exchange of real-time data such as different sources of IT configuration, performance, alarm and security. It also achieves the model integration of the entire system. Finally, the author reconstructs multi-dimensional data cored by IT resources. Through the use of asynchronous message exchange processing chain technology of cluster mode, data bus achieves the real-time data processing capability of 4000kByte/s [8].

The author fully utilizes the characteristics of the EMS system of the power grid for further improvement and adapts the FLEX technology to realize the WEB-based integrated configuration monitoring graphic package. Besides, the author combines with the real-time message pushing mechanism to meet the needs of personalized integrated real-time monitoring, which provides flexible and rich means of WYSIWYG for the entire system.

2.5 Centralized monitoring of network equipment

The author conducts real-time monitoring of IT infrastructure equipment(such as network equipment, host equipment, operating system, key process) that supports the operation of the automation system, integrates various collected information and timely finds hidden faults. Through the correlation analysis of monitoring of basic equipment and operation events and security events, the author conducts safe real-time monitoring of the overall operation of the automation system.

2.6 Real-time alarm

Fault alarm information can be timely notified to operator on duty and those responsible through SMS, web pages and other means. At the same time, operator on duty and those responsible can also timely confirm and deal with the fault alarm through a variety of ways.

2.7 Management analysis of security risks

In the secondary security protection system of power, the focus of safety management is to ensure the security of power communication and dispatching data network and automation systems such as power monitoring system and power dispatching management information system. The goal is to protect the system from malicious damage and attacks launched by various hackers, viruses, malicious code and other forms. Besides, safety management aims to protect the system from damage caused by man-made faulty operation and to prevent resulting primary system accident or a large area of electrical accidents and secondary system collapse or paralysis.

Through the construction of automation system and integrated network management platform, the operation and maintenance of the secondary system of power and the centralized management of safety can be realized. Through the analysis of the logs and the monitoring of the status, the operation status of the secondary system and the active state of the network can be known timely. Moreover, possible security accidents can be quickly located to prevent the further development of security accidents.

2.8 Centralized monitoring of automation network in security crossing zone

Due to the existence of the isolation device, the automation network in security crossing zone is separated physically, but it is logically a whole. Therefore, when it is monitored, it should not be distributed to manage from the local point of view, but be managed in a centralized and unified way, so that we can achieve full control from a global perspective and improve management efficiency and avoid repeated construction. From the technical point of view, the following issues need to be considered:

Unified network topology management. The network topology of zone I and zone II automatically generates network structure and transmits to the security zone III, forming a network topology diagram(including logical structure and physical structure) of the whole automation system. When the network has unauthorized equipment access, the system automatically detects and alarms. When the network needs to be changed, the system can verify that whether the actual system topology change is in accordance with application regarding changes or not.

Unified operation and maintenance functions of network equipment. The unified monitoring system will be constructed in zone III. Due to the presence of isolation devices, the control requests for zone I and zone II devices can not be initiated directly in zone III. Therefore, the author considers setting up a monitoring proxy server in zone I (can be combined with the above collection proxy server) which is responsible for network control commands of zone I and zone II, such as standard SNMP, private protocols and so on.

3 Systematic design

3.1 Overall design of technology

The author fully considers the current situation and goal of integrated operation and maintenance monitoring construction of information. How to take possible changes of various heterogeneous supervision systems and future integrated monitoring technology and products into consideration is the biggest challenge in the implementation of system technology. Only if we fully consider different equipment status and construct an open and extensible system architecture on the basis of various heterogeneous information systems, can we achieve the intended goal.

The flexible system architecture consists of data bus, unified information base and graphic platform. Data bus achieves standardized collection of data; unified information base achieves normalization and standardization of information; graphic platform providea personalized and flexible ways of presentation. Data bus, unified information base and graphic platform together constitute a flexible system architecture.

Flexible system architecture can also get rid of the dependence of a single product, while reducing the overall risk of automation systems and network integrated management platform. Because in the modular design, defect or failure of a single module will only be limited to affect the function of other modules, and not easily lead to the collapse of the overall platform. At the same time, it also creates favorable conditions for the upgrading of the system in the future. Functions of various modules can be enhanced or upgraded as time and funds permit, and functions can be reintegrated within the modules. This kind of plug-based design structure will make IT centralized operation monitoring system stronger and stronger.

In zone I and zone II, the author deploys a collection server respectively. In zone III, the author deploys an unified information base server and an integrated display server. Collection and monitoring of network and automation system in zone I and zone II are realized respectively through the collection servers in zone I and zone II. And real-time data collection collected in zone I and zone II is transmitted to the unified information database in zone III. The author conducts completed and integrated presentation after unified analysis and calculation. The overall deployment scheme frameworks are as follows in Figure 1:

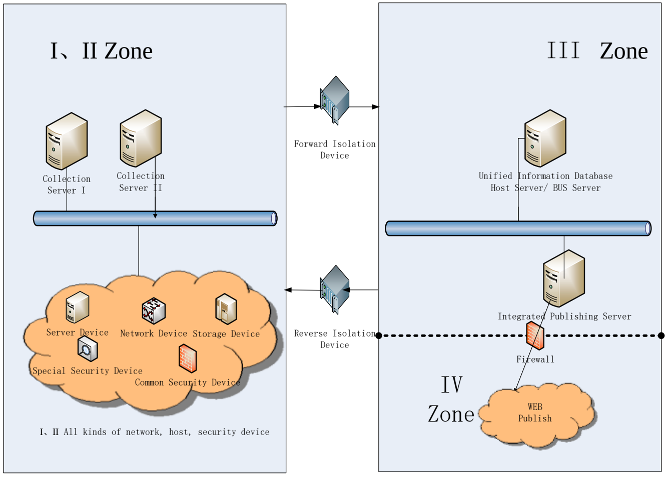


Figure 1: Overall deployment scheme framework

3.2 Design of data collection layer

The data collection function collects the data of key equipment and applications in transverse physical isolating device(positive/negative), longitudinal authenticated encryption device, firewall, intrusion detection system (IDS), anti-virus system and receiving dispatching technology support system.

The security monitoring platform mainly uses the Syslog mode to collect the log information of the security device. Special security devices(transverse physical isolating device, longitudinal authenticated encryption device) of electric power system use Syslog mode to collect data directly; general security devices(firewall, intrusion detection system, anti-virus system) converts logs to logs that accord with the standard format of electric power system through the Agent agent and collects data; dispatching technology support system converts the logs in key equipment and applications of the system to logs of standard format through the Agent agent and sends to the security monitoring platform.

3.3 Design of data processing layer

The data standardization processing function is the basic function of the security monitoring platform. When the collecting terminal receives the original log data, it is firstly identified by the protocol and then distributed to the respective content identification modules. In the content recognition modules, the data is distributed to various data analysis modules through the content pattern matching engine, then the author conducts keyword extraction and content filtering and content filling.

For the collected data, according to the rules set by the security monitoring platform, the author filters the data and only keep necessary and effective data in the scope of monitoring, so as to ensure that the security monitoring platform does not save too much redundant data. Data filtering rules can set complex matching relationship through the matching operator, matching rules use a regular expression algorithm[9].

3.4 Design of centralized show layer

The interface display function analyzes, queries and charts the collected data of the monitoring equipment in a graphical way, reports the results of the analysis and reports, manages the assets of the monitoring equipment, and manages the parameters configuration of the system itself and user privilege.

3.5 Design of systematic functions

The integrated operation and maintenance monitoring system based on the secondary security protection system aims to realize the unified monitoring and security management of the power secondary business system infrastructure supporting various management and application functions. The main business functions consist of five parts, including network management, host management, security management, engine room management and alarm management.

1) Network Management

The network management function is one of the essential functions of the information integrated monitoring system. Network management personnel are responsible for the network management, the system should achieve topology management, configuration management, fault management, performance management and other management functions.

(1) Topology Management

Topology automatic discovery function can conduct conditional automatic discovery of topology structure through the combination of SNMP, ICMP and other TCP/IP protocol stack protocols with a variety of algorithms. It can find network equipment and topology relationships among them, distinguish ports from VLAN and HSRP and OSPF, automatically summarize the redundant connection and backup connection and balanced load connection, and stores the topology map in the database. Users can customize the algorithm and polling interval for topology discovery and support physical topology discovery and logical topology discovery. Topology discovery module can discover the change of network topology at regular intervals, and can rediscover one or several subnets already found. Automatic discovery of topology structure can be realized according to one or several setting conditions such as specifying network segment, specifying resource type and other conditions. The discovered results can be displayed in accordance with the subnets. Besides, it has automatic topology refresh function.

Network browsing functions mainly include: the background map of the topological graph can be customized, the topological graph should be able to be enlarged and shrunk and can be moved up and down, left and right, and different icons are used to identify different types of nodes(network element, network tuple, subnet, etc.) on the topology graph; the topological graph should reflect the actual networking situation accurately and the linking relation among various network elements of subnets of all levels; the topological graph should reflect various performance conditions of loading of network elements, network tuples, subnets and connected lines in real time through various ways such as color, subscript, tooltip and so on; the topological graph can be used with the navigation tree to find network elements, tuples or subnets; through the corresponding topological graph, configuration information of network elements and tuples and subnets can be checked.

The topology monitoring function should be able to display the running status of the managed network dynamically and in real time. The system can respond to the real-time service alarm events timely and display the alarm-related business channels deeply, In the topological graph, forms of corresponding link discoloring and mode flashing are used to give alarms. If the alarm information is not confirmed, the system should prompt the user in some way. The system should provide the voice prompts of the alarm information.

(2) Performance Management

The performance management function is mainly for the performance monitoring and analysis of all kinds of network devices. It should have the following sub-functions, including performance monitoring management, performance data reporting management, performance data management, performance threshold management and performance analysis.

(3) Fault Management

The system should display the alarm information clearly and intuitively on the network topological graph, the position of the alarm and the level of the alarm should be displayed on the topological graph, and the system should prompt the user to confirm the alarm information. At the same time, the system should support to send the alarm information to the user's e-mail or short message through the alarm center.

(4) Network Configuration Management

The system provides the uploading and downloading function of configuration files of network equipment, which can edit and compare the configuration files. Besides, it provides unified export and storage function and edition control function of configuration files in real time, which is convenient for network administrators to quickly switch and adjust and recover the network configuration.

2) Server Host Management

Server host management monitoring objects are automation systems used in all host equipment in zone I and zone II of the Songjianghe Power Plant. Host management will comprehensively display a variety of monitoring information, which provides the regulators with basic data support, covers product life-cycle management of assets and fully realizes the monitoring informatization.

Real-time performance monitoring of host equipment: real-time performance monitoring provides the monitoring of CPU, RAM and disk of these devices, displaying the service condition of components and other indicators. The system saves the historical service conditions of the devices and provides the basis for the performance analysis of the devices. When there is an alarm, the system provides the alarm correlation query function, which not only can locate the device from the physical layer, but also can make location analysis of the device from the application layer and estimate the impact level of equipment alarms, thus providing assistance for supervisors.

Server host equipment asset information monitoring: the equipment configuration data, the back panel, asset data and historical statistics are monitored to display, which realizes the product life-cycle management of the equipment.

Monitoring page of the host equipment asset information consists of many tabs, including basic information panel, change status, maintenance history, historical alerts, asset information, configuration and so on.

(1) Basic information panel displays basic information about the device, including the device owner, model and configuration.

(2) The back panel of configuration and asset information provides the basic information about the asset and resource of the device, including the audit information of the asset and the configuration information of the resource.

(3) The back panel of maintenance history provides historical maintenance records for the device and provides integrated information that combines with historical records of work-ticket and operation-ticket.

3) Security Management

In the second power system, security products generally include firewall, intrusion detection system, anti-virus system, VPN, horizontal isolation device, vertical encryption device, vulnerability scanning.

Security management can be centralized and unified management of a variety of security products. On the one hand, it collects the events of each security product, filters and merges the massive events of many security products, analyzes the events in conjunction with business assets, makes correlation analysis among the events to discover network security threats more timely and effectively, and makes the appropriate response. On the other hand, it can develop and issue unified security strategies, conduct configuration management of security products, and monitor the running status of security products in real time to ensure stable and effective operation.

On the basis on the secondary security protection system, the automation system and the security management module in the network integrated management platform mainly include following functions, including information asset management, security incident management, risk management, security product monitoring and security policy management.

4) 3D Machine Room

3D machine room monitoring integrates advanced technologies such as virtual reality and computer graphics into one, uses metadata [10-13] in the IT centralized operational monitoring system to accurately monitor room status in real time. Besides, it provides 3D view that simulates the actual environment of the room, displays the running status and configuration condition of room equipment. Users can have a dynamical and real-time and three-dimensional view of all aspects of the running data of the room to improve the degree of data visualization.

5) Alarm Management

Alarm management includes real-time monitoring of the secondary power system operation and the whole process from alarm predication to alarm elimination; alarm system collects alarms of infrastructures such as the host, network equipment, security equipment and monitoring equipment, and displays the information on the alarm list, including operation exceptions automatically acquired by the system and the prediction exception of the system.

According to the monitoring of the collected data and the collection of related information, the system analyzes the operation status of various systems on the basis of the corresponding models, so as to predict the hidden risks of the system. When the risk level exceeds a certain threshold, risk prediction alarm will be triggered.

At the same time, the system receives the collected data, conducts actual alarms and merger and association of the operating conditions of various systems, so as to form an unified alarm in the system. An unified presentation module is used to display the system operation events, alarms, fault conditions and processing state. And unified notification methods are used to announce alarms to users.

4 System implementation

In this paper, the author provides X power plant of X Power Grid Co., Ltd. with a solution of integrated overall monitoring platform. A set of centralized integrated monitoring system is used to conduct unified monitoring and centralized operation, which means to improve the capabilities of prevention, emergency response and fault location processing to ensure the safe and stable operation of the information system.

Aiming at the problems existing in the operation and management of the power plant and the content that needs to be studied, the author puts forward the system architecture construction plan of the integrated monitoring platform, which mainly means to implement the operational monitoring function of the integrated monitoring platform that includes all the devices in zone I and zone II from the network environment to the host and safety devices. The abnormalities and failures can be timely informed to professionals and managers through a variety of ways, so as to make the key business run normally and provide solid technology support for service capacity of automation operation. Part of the effect pictures are as follows, Figure 2 shows schematic diagram of comprehensive operational monitoring, Figure 3 shows schematic diagram of network topology of three zones, Figure 4 shows schematic diagram of alarm monitoring, and Figure 5 shows schematic diagram of operational monitoring of the machine room.

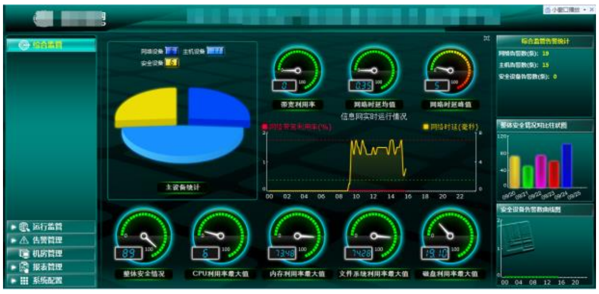


Figure 2: Schematic diagram of comprehensive operational monitoring

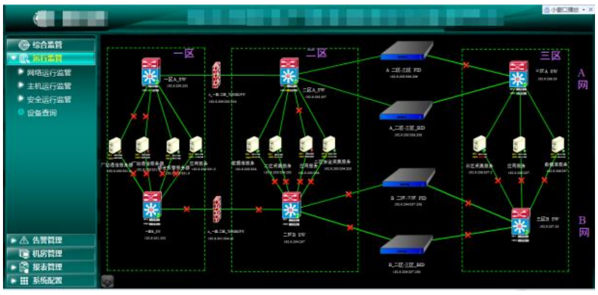
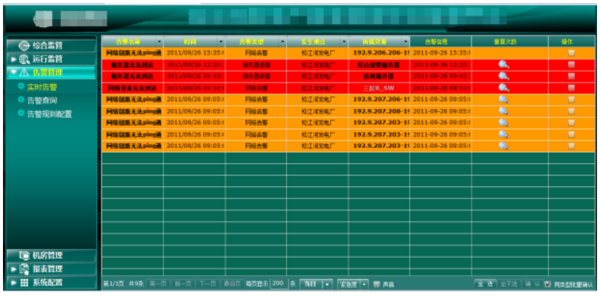


Figure 3: Schematic diagram of network topology of three zones



告警名称	时间	告警类型	发生地点	所属资源	告警信息	重复次数	操作
网络链路无法ping通	2011/09/26 15:35:	网络告警	松江河发电厂	192.9.206.206-1	2011-09-26 15:35:		□
服务器无法到达	2011/09/26 12:20:	服务器告警	松江河发电厂	综合报警服务器	2011-09-26 12:20:	🔍	□
服务器无法到达	2011/09/26 09:45:	服务器告警	松江河发电厂	应用服务器	2011-09-26 09:45:	🔍	□
网络设备无法到达	2011/09/26 09:10:	网络告警	松江河发电厂	三区B_SW	2011-09-26 09:10:	🔍	□
网络链路无法ping通	2011/09/26 09:05:	网络告警	松江河发电厂	192.9.207.206-1	2011-09-26 09:05:	🔍	□
网络链路无法ping通	2011/09/26 09:05:	网络告警	松江河发电厂	192.9.207.208-1	2011-09-26 09:05:	🔍	□
网络链路无法ping通	2011/09/26 09:05:	网络告警	松江河发电厂	192.9.207.203-1	2011-09-26 09:05:	🔍	□
网络链路无法ping通	2011/09/26 09:05:	网络告警	松江河发电厂	192.9.207.203-1	2011-09-26 09:05:	🔍	□
网络链路无法ping通	2011/09/26 09:05:	网络告警	松江河发电厂	192.9.207.203-1	2011-09-26 09:05:	🔍	□

Figure 4: Schematic diagram of alarm monitoring

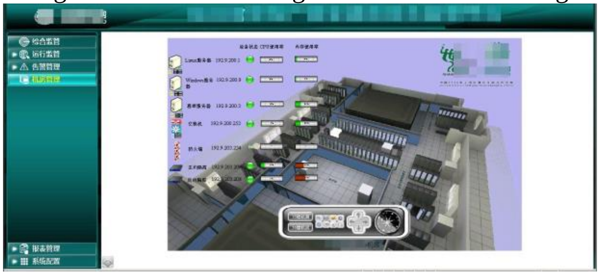


Figure 5: Schematic diagram of operational monitoring of the machine room

5 Conclusion

Aiming at the problems existing in the operation and management of the power plant and the content needing to be studied, the author puts forward the system architecture construction plan of the integrated monitoring platform. The author mainly researches and unifies the database model and interface specification, conducts unified and centralized monitoring management of automation network and network equipment in security zone I and zone II. Besides, the author realizes the function of supporting management and analysis of security risks. Through the application in the power plant, the author provides solid technical support for the service capability of automation operation, which has certain application prospect.

Acknowledgements

The authors would like to express appreciations to colleagues in our research institute for their valuable comments and other helps.

References

[1] WANGZhi-qiang. Surveillance System Design in Power Supply Environment of Computer Room [J]. VIDEO ENGINEERING, 2008, 32(8):74-75.

[2] HAN Xue-qi, WANG Feng. Research and Implementation of Show System of IT Operation and Maintenance Data [J]. Computer Science, 2012, 39(s2):232-235.

[3] QIN Hongxia, WU fangying, etc. New technology research on secondary equipment operation maintenance for smart grid [J]. Power System Protection and Control, 2015, 43(22):35-40.

[4] YU Feng. Construction of Enterprise Information Management and Control System [J]. Command Information System And Technology, 2012, 3(2):38-43.

[5] Zang Qi, etc. Grid dispatching automation secondary system safety protection practice [J]. Electronic Design Engineering, 2011, 19(20):47-49.

[6] JIN Xuecheng, SUN Wei, etc. Design and Implementation of Inner Net Security Monitoring Platform in Power Secondary Systems [J]. Automation of Electric Power Systems, 2011, 35(16):99-104.

[7] LI Dongyang, ZHANG Shuliang, etc. The Primary Exploration of Data Operation Platform for Digital City [J]. Bulletin of Surveying and Mapping, 2015(11):88-91.

[8] LIU Zhong-qing. Qt/Embedded-based environment monitoring system for laboratory[J]. Modern Electronics Technique, 2014 (8).

[9] ZHANG Yadong. Realiziation of Automatic Monitor for Machine Room of Power Sources and Its Environment in Electric Power Industry [J]. ELECTRIC POWER CONSTRUCTION, 2005, 26(4):66-68.