ATLANTIS PRESS

Advances in Engineering Research, volume 166

3rd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2018)

Research on and Analysis of Data network security state of Henan Electric power system

Lijie WU[1,a], Yinlin REN[2], Wencui LI[1], Zhiyuan AN[1], NingningZHANG[1]

[1]Information & Telecommunication Co. of State Grid Henan Electric Power Company, Zhengzhou, 450052, China,

[2]Henan University of Technology, Zhengzhou, 450052, China

[a]email:374663965@qq.com

Keywords: Data network, Risk assessment, Status analysis

Abstract. With the expansion of the electric power system data business requirements, study the security of electric power data network is more and more, the safety of the structure and function of the network itself got extensive attention. This paper studies the accord with the characteristics of Henan electric power data network security technology, network state analysis method is proposed, and formulated the Henan electric power data network security testing plan, summary analysis of the data network running status, ensure that Henan electric power data network can safe, reliable, stable and efficient operation, provide a reliable platform for electric power production and management support.

Introduction

The rapid development of power industry, has become the important pillar of the national economy, electric power industry of data network security also becomes very important, but the electric power data network security technology is based on the business side more of information security policies, such as intrusion detection, virus protection, vulnerability scanning, Multi-level protection, etc. and the imperfection of the safety management system of the network itself, the network level of security awareness is not strong, also lead to corresponding technical guidance and management system. In view of these shortcomings, this paper puts forward the safety test plan of Henan electric power data network, comprehensively considers all aspects, and guides the safety test of the network. And support on the basis of deep analysis of the result of the test, data network running status summary analysis, to the further construction of data network, optimization, improvement works, such as theoretical basis and practical scheme is put forward.

Design of Risk Assessment System for Data Network

The depth of the data network presents the complexity of the bearing relationship and presents the network with wide domain characteristics in the breadth of the network. The depth of the bearing relationship includes transmission network, exchange network, data bearing network, Internet and terminal system, etc. The scope of scale includes international, provincial, provincial and local urban network [1]. Risk assessment was carried out on the data network to get huge assets system, business system, system threat, vulnerability, technical index system, management index system and the corresponding laws and regulations, etc. Therefore, the research data network risk assessment method will face the following technical difficulties:

Classification Methods and Types of Assets, Vulnerabilities and Threats. In the traditional system of information security risk assessment in the guide, classification methods and types are not in view of the data network, for small systems, so use this way of classification processing data network, based on the analysis of the breadth and depth, there will be obvious. At the same time, at present, both at home and abroad for the research is still in the exploratory stage, there is no guidelines or criteria to define the data network assets, vulnerability and type of threat, so how do you determine the data network assets, vulnerability and kinds of threat is the technical difficulties

in the project. This project will be according to the characteristics of the data network and security problems, and combined with the existing risk assessment, vulnerability and threat classification methods and types, research suitable for kinds of classification methods and data network.

Vulnerability Detection Technology. This project will be based on the vulnerability of all the data networks that have been developed, and the research will be operable for each vulnerability detection method [2]. Key technical difficulties include: access control vulnerability detection technology; Identification of vulnerability detection technology; Hidden channel vulnerability detection technology; Object reuse vulnerability detection technology; Audit vulnerability detection technology; Trusted path vulnerability detection technology and system executable program protection function vulnerability detection technology.

Valuation of Assets, Vulnerabilities, and Threats. In the traditional system of information security risk assessment in the guide, the principle of assignment is not for data network, and there is no sure to define each corresponding threat, vulnerability to determine each vulnerability corresponding threat to need to rely on human experience, without the basis of criteria and guidelines, so the research in view of the data network assets, vulnerability and threat the assignment method and definition of each of the vulnerability corresponding threat is the technical difficulties.

Research on Network Security Test Scheme

In this paper, a network security test scheme which can be used for the actual safety testing is developed according to the Henan power data network. Cover the topology of the grid data of network security, network equipment security, network traffic, security, network management, security testing evaluation, based on the given network, business and other safety situation analysis and reinforcement proposals. It mainly includes:

(1) Asset identification.
(2) Network topology vulnerability assessment of grid data network.
(3) Grid data network equipment security check.
(4) Security check of network management platform.
(5) Network protocol and traffic safety analysis.
(6) Evaluation and analysis of safety management system.
(7) Safety measure effectiveness analysis.

In view of the above work, needs to be completed asset identification, threat recognition, vulnerability identification, safety measures, balance the impact analysis, threat analysis, vulnerability analysis, validity analysis, key business security analysis, security system structure analysis, the comprehensive risk analysis and security reinforcement proposals.

Network Security Test Implementation Technology Research

According to the above safety test plan and the network security assessment tool, the systematic and normal safety assessment test of Henan electric power data network was conducted. In the case of the least impact on the network business, the data network should be tested in a comprehensive way [3]. This paper summarizes and analysis the operation state of power data network in Henan province, and supports the improvement of safety state analysis and security strategy of Henan power data network.

Data network security test implementation process is shown inFig.1, need according to the situation of Henan power grid data network, security testing evaluation work is divided into five stages: preparation stage, the recognition stage, analysis stage, risk control planning stage and summary stage.

Preparation Stage. This stage is mainly determine the scope of the evaluation, establishing assessment organization, determine assessment tools, determine the risk assessment process of risk control strategy, making risk assessment plan, risk assessment, training and evaluation objects such as backup, ensure the smooth and orderly implementation of the risk assessment can be according to

the plan, and risk control;

Identification Stage. This stage mainly completes the work of asset identification, threat identification, vulnerability identification and security measure identification, and provides basis for the analysis stage;

Analysis Stage. This stage in the identification on the basis of a large number of arrangement and analysis, analysis of assets, threat analysis, vulnerability analysis, security analysis and comprehensive risk analysis, to the Guangdong power grid data network security risk level conclusions;

Risk Control Planning Stage. According to the result of risk analysis, combined with the relevant state laws, regulations and industry requirements, and the special requirements of Guangdong power grid network system and risk, sums up the current safety requirements; According to the priority of safety requirements and relevant standards, a suitable safety planning scheme is developed to provide reference for the future security construction of Guangdong power grid data network.

Summary Stage. this stage is mainly to the paper summarizes implementation process of risk assessment, risk assessment, and to the state of Guangdong power grid data network security evaluation strategy and analysis report, head of the research project [4].

This project is mainly to carry out the physical equipment safety testing, network architecture safety test, safety and environment test, data security, network security based on distributed probe measurement technology tools and implementation of the implementation of the contents of the research and test report form data network security.

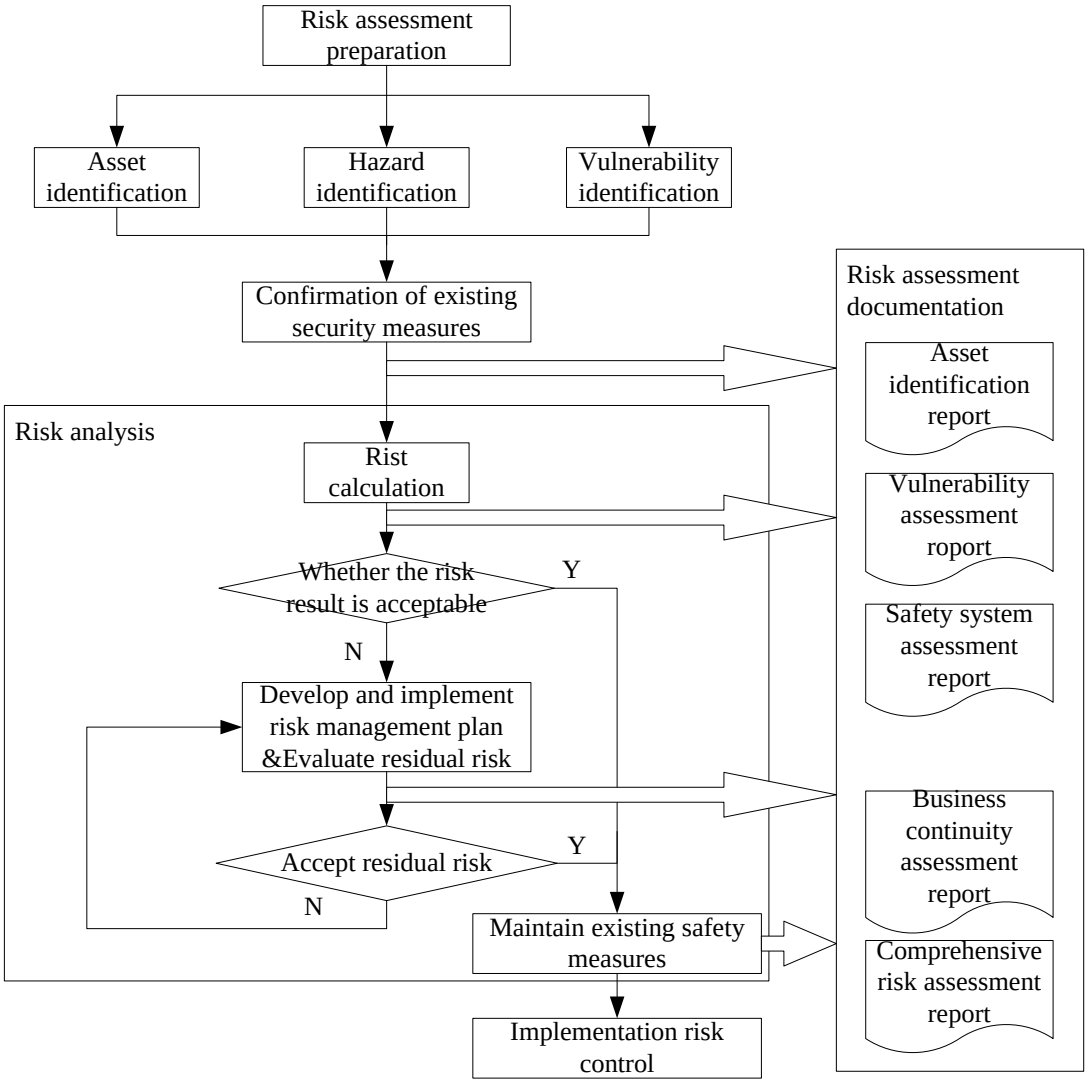

Fig.1Security test implementation workflow diagram

Research on Network Security Analysis Situation Technology

For information security risk, key information extraction, integration, analysis the security of the current state of the data network, and the data network in the future for a period of time period (e.g., year, quarter, month, week, etc.) on the prediction of the trend of overall security within, such as various types of security threats (DNS, DDOS attack, SQL injection, XSS, etc.) of the probability of occurrence, influence range and so on to make predictions [5]. Research and analysis process, including field test report data extraction, security vulnerabilities and threats analysis, safety situation assessment, management system, technical system and strengthening technology, such as research data network security evaluation model for power grid, form data network security situation analysis report.

Based on the corresponding security assessment strategy and supporting tools, the following methods are used to analysis the operation status of data network:

Data Network Operation State Analysis Target. The basic goal of the analysis of the operation state of the power grid data network is to find the security hidden danger in the network operation in time, avoid the security risk, and achieve the target.Data network running state analysis involving data network based network environment, network equipment, business system and so on several aspects, and defects of these units and system of their means of attack is state analysis results may include object.

Network Operation Situation Analysis based on Security Test Results. The security test results of the network can verify some behavior that have already occurred or are about to be jeopardized. These are real network system security threats.Further analysis of these results, or correlation analysis of the multiple unit system, can further find that hidden deep security threat, which is based on the security situation analysis of test results.Based on the safety analysis methods including the trend of test results based on the statistical analysis of safety inspection tools or further data mining, based on the comprehensive analysis of the network equipment log information, based on the analysis of the problems similar unit system, etc.

Analysis of Network Vulnerability based on Network Topology Analysis. The weakness of network structure is very big for the network stable operation, the simple attack on a key node can cause the whole network system to be paralyzed.For the depth analysis of network topology, it is possible to find the weakness of network system structure.One example is the critical node of cascading collapse, which can eventually result in a large-scale failure of the entire network system performance if a malicious attack occurs against this node.

Data Network Security Configuration Baseline Management and Analysis System Research

This paper presents a network security configuration baseline data management and analysis system, the system will be according to the electric power data network operation and safety requirements, and the benchmark of configuration, including all kinds of routers, switches, link port, service node configuration and status information correctly, to version management of configuration files, and status information, and the use of logging.The configuration check scope includes: IP address and routing, protocol configuration, Route map and ACL, security protocol, VPN/ configuration, etc.By scanning, parsing, and matching the configuration files, the configuration of the static checking system is different from that of the baseline configuration, and the configuration is determined to meet the baseline requirements [6]. By the state of the output device information, check the equipment of the routing table, ARP table, MAC published, adjacency list, protocol state information, etc., check whether the various protocol state information is correct, the analysis results are final judgment, recording, modification scheme is put forward.The architecture of the system is shown in Fig.2.

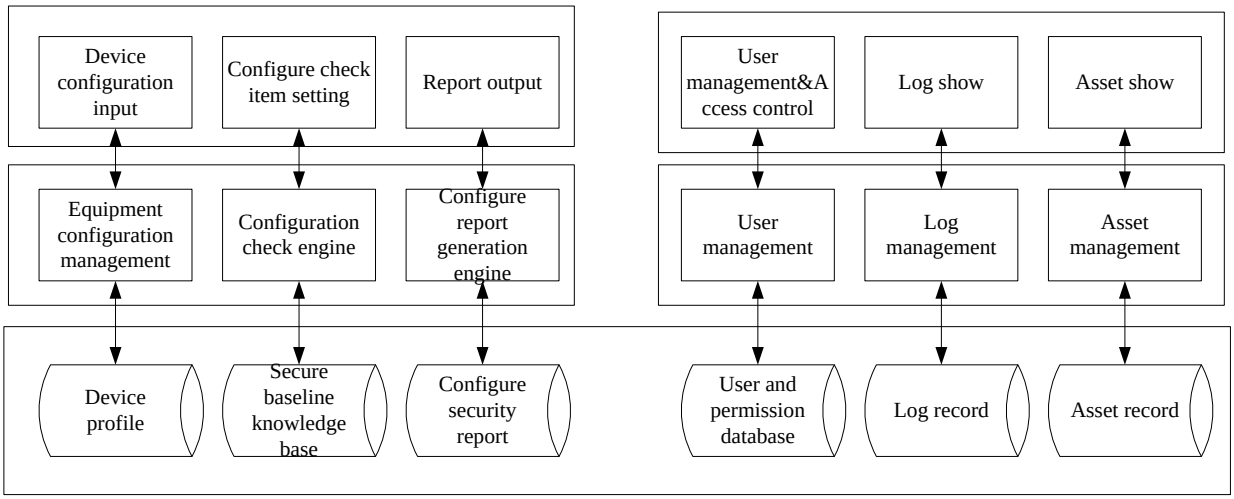

Fig.2System functional architecture

Conclusion

Based on the analysis of the current situation of data network, this paper firstly studies the network security technology which conforms to the characteristics of Henan power data network, and has the operability and practicability.Second, the network state analysis method is proposed, and in the case of minimal impact on the network business, Henan electric power data network security test plan formulation, the network security testing, data network running status summary analysis, guide the grid data of network security status analysis and running status evaluation, thus for the further construction, optimization, improvement of data network works, such as theoretical basis and practical scheme is put forward.

References

[1] Hou Hong-mei, A brief discussion on network security problems and countermeasures in the automatic operation of power dispatching[J]. China high-tech enterprise, 2017, 21(32):141-142.

[2] DOUGLAS E C. Compuer network and interncts[M].New Jersey, USA: Prentice Hall,inc,1997.

[3] STALLINGS W. Operating System: internals and design principles[M].New Jersey, USA: Prentice Hall.Inc,1998.

[4] Li Hui-Jie, An OPNET-based 3-tier network simulation architecture[A].Bering, China. Piscataway, NJ, USA:IEEE Computer Society,2005:767-770.

[5] AURA T. Strategies against replay attacks[A].Rockport, MA, USA. Los Alamitos, CA, USA: IEEE Computer Society,1997:59-68.

[6] SERPANOS D N,LIPTON R J. Defense against man-in-the-middle attack in client-server system[A]. Hammamet, Tunisia. Piscataway, NJ. USA: IEEE Computer Society, 2005:767-770.