Risk Quantified Evaluation Method and Platform Design for Grade Protection

Wang Tian
[1]Guangdong Power Grid Corporation Information Center, Guang Zhou, 510600
[2]Guangdong Power Grid Software Testing Lab, Guang Zhou, 510600

Wei Lihao
[1]Guangdong Power Grid Corporation Information Center, Guang Zhou, 510600
[2]Guangdong Power Grid Software Testing Lab, Guang Zhou, 510600

Zou Hong
[1]Guangdong Power Grid Corporation Information Center, Guang Zhou, 510600
[2]Guangdong Power Grid Software Testing Lab, Guang Zhou, 510600

Abstract—**Regarding all the issues that Corporation faced during the grade evaluation, e.g.lack of accuracy on risk analysis, over dependence on the capability of the evaluater, etc. We bring out a new evaluation method on grade protection and the distributed platform RQEP. With them we can quantify the risk objectively, improve the efficiency of grade evaluation, and standardize evaluation process.**

Keywords-Information Security of Power System, Grade Protection, Security Evaluation

Grade protection is our nation's critical infrastructure and assets, and maintain social stability [1]. The implementation of grade protection includes five important links: grade record, safety construction, grade assessment, safety improvement and examination. Grade assessment, run through the stages of information system construction, operation maintenance and system return, is an very important driving factor for grade protection improvement and safety construction [2,3]. This paper proposes a kind of risk quantified method for grade protection evaluation and also design a risk quantified evaluation platform for grade protection of information system(RQEP) after further research. This platform has solved a lot of problems, such as, grade protection evaluation results that affected by human factors seriously, non-standard evaluation process, evaluation with low efficiency, report with big error, data difficult to count and so on.

I. Present Situation of Grade Protection Evaluation

Information security grade protection evaluation has strong policy, the evaluation implementation process must strictly abide by national standards, which reveals the security protection capability, evaluation requirement， assessment result ect. A set of perfect grade protection standard systems are initially established in our country, there are standards for evaluation implementation to follow, the evaluation organization has been managed strictly and the assessors of grade evaluation have been required work with certificate, but there still exist problems in the process of evaluation implementation. There is a list of some typical problems as following:

1) Excessively rely on the personal ability of assessors in evaluation implementation, so that there are too high requirements for them. In the process of grade evaluation, although testing personnel abide by relevant norms and standards of grade protection, they need the help of personal experience more often. For example, when analysis IDS log, experience must be need to found invasion traces rapidly in a large number of log.

2) The risk analysis is not accurate enough in evaluation results. Report Template requires that risk analysis must done for problems of grade protection evaluation results, but the evaluation method is single, it only focus on risk vulnerability, and threats are usually not taken into consideration , so the assessment way is informal and inexact, which can not express evaluation target timely and accurately.

3) The evaluation workload is huge but efficiency is low. With the deepening of informationization degree, enterprise information systems have proliferated, especially those companies that have molecular company as Guangdong Grid Co, the evaluation workload is huge, partial evaluation work rely on manual and the process repeats, so an automatic and efficient evaluation mode is needed.

4) The evaluation data management is difficult, and it is hard to support further analysis. Grade protection evaluation data are the foundation data of enterprise information security. To analysis those data from different dimensions can provide decision support for enterprise information security. It is lack of the tools for evaluation data analysis and historical data management nowadays.

II. Risk Quantified Model for Grade Protection Evaluation

For existing typical problems of grade protection, this section proposes a quantified risk technology for grade devaluation, which use systematic, quantitative and effective methods to measure and evaluate the incapability(the partial conforming and nonconforming items in grade evaluation results) of security protection of information system, to find out the risk of information system and its influence.

A Basic Element Description

The basic elements of model are information system asset, threat, vulnerability, system risk. Asset is the valuable information or resource for an organization. Threat refers to the possible damage of information system asset safety, such as software failure, deliberate destruction, equipment failure or aging, eavesdropping, earthquake, typhoon, ect. Vulnerability refers to the flaw or weakness of system itself, includes: database vulnerability, operating system vulnerability， code security vulnerability of application system, management weakness and system security configuration problem. Vulnerabilities themselves are harmless, but they can be used and bring negative effect on asset after threatened [5,6].

Risk is the potential that specific threats use the vulnerability of assets and cause assets loss or damage. When threat behavior occurs on specific asset, it has impact on the assets and accompanying business.The influence degree not only depend on level of threat and vulnerability, but also the value of assets.That is, risk (R) consists of three independent elements: threat level (T), vulnerability level (V) and asset value (A). Using formula can be expressed as:

R= f（T,V,AV） .... (2-1)

Security risk consists of three parameters(T, V, A).

Risk quantification of grade evaluation is the process that aroud information system assets and grade evaluation of implementation, quantitative analysis threats and the vulnerability of system assets, host system, applications system and data, obtain the information system risk after scientific analysis.

B Evaluation Methods

According to the requirements of state grade protection policy and their own present information construction situations, we sum up the evaluating process, including three phases: evaluation preparation, site evaluation, analysis and reporting, as shown below:

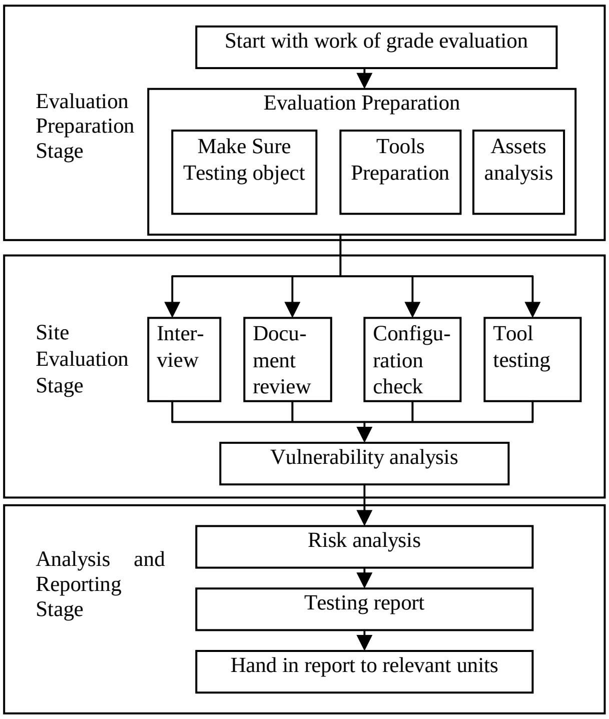

Figure 2-1 Schematics of the information security grade protection evaluation process

1) Evaluation Preparation

The major work of this stage are to prepare project plan, choose suitable project of evaluation tools, identify detected information system assets etc. to determine access point, and according to requirements to reuse or develop evaluation implementation manual finally. Unlike other general evaluation, it is needed to add asset identification content in this preparation stage. Through investigation, collect assets information, make assets attribute assignment, and form a complete asset information table. According to the standard of information security grade protection, information assets are divided into five categories: system assets, netword assets, medium assets, terminal assets and management measures, which is shown as below.

Table 2-1 Asset Classification List

Classification	General Description
System Assets	Identify the assets of business systems, including host, application, database, backup and recovery
Netword Assets	Do asset identification for internal network equipments, including core switch, router, firewall, IDS, IPS, etc.
Medium Assets	Recognize various hardware facilities and IT physical equipments that are related to business, support to install identified software and store identified system assets, including storage device, computer peripheral, mobile device, mobile storage media and wiring system etc.
Terminal Assets	Identify PC terminal
Management Measures	Recognize the responsibilities and operation measures of roles who use, operate and support all the identified system assets, netword assets, medium assets and terminal assets

2) Site Evaluation

The site evaluation include unit testing and overall testing, whose target is to comprehend the real protection situation of system, obtain sufficient evidence and found the existing security problems of system [4]. There are four kinds of methods: interview, document review, configuration check and tool testing.

① Interview. Testing personnel communicate with measured system related personnel (person / group), obtain relevant evidence and information.

② Document review. According to GB/T22239-2008, check whether there are the documentations of regulation, strategy and operation procedures or not, check whether there are complete records of regulation implementation, such as register record , electronic records, the use records of key equipment of high grade system, check the completeness and consistency of documentation via review and analysis.

③ Configuration check. Using validation to check whether the configuration of application system, host system, database system and network device are properly or not.

④ Tool testing. According to evaluation implementation manual, use technology tools, including the vulnerability scanning based on network detection, permeability testing, virus and Trojan horse killing and equipment performance testing to test the system and backup test results finally. The main measurement tools including: portable computer, host system vulnerability scanning tools, application system scanner, database scanner, network capture tools and script testing tools, ect. In specific evaluation implementation process, use various methods synthetically according to demand.

In site evaluation stage, use the above evaluation techniques, comparative analysis with Baseline, to conform of the partial conforming and nonconforming items of system, and form the vulnerability identification table, as shown in the table below.

Table 2-2 Vulnerability List Sample

System	Vulnerability
Human Resource Management Information System	04AP01 Authentication strength inadequacy
	04AP03 Security audit incomplete
	04AP04 Communication integrity vulnerability
	04AP05 Communication security vulnerability
	04AP06 Software fault tolerant vulnerability

3) Analysis and Reporting

The major task are according to information security classified protection requirements and site evaluation results, use the methods of single evaluation result, unit evaluation result, overall evaluation result and risk analysis, to find out the gap between the whole system security protection status and the requirements of appropriate level protection, analyze measured system risk which is cause by these gaps, to get grade evaluation conclusion and format evaluation report finally.

Risk analysis calculation is that in considering the existing safety measures, use proper methods and tools to identify the possibility of security incidents cause by asset vulnerability, to collect results of assets assessment, threat assessment and vulnerability assessment, combine the impact of security attributes damage to make sure the information assets risk.

C risk analysis and calculation

According to formula (2-1), risk calculation first need to analyze assets value. Considering the information asset value (AV) is closely related the assets confidentiality (C), integrity(I) and availability(A), their relation can show as formula (2-2)

$$AV = f_2(C,I,A) = \ln\frac{e^C + e^I + e^A}{3} \quad \text{……………….(2-2)}$$

Where C,I,A $\in \{1,2,3,4,5\}$. Vulnerability (V) is divided into 5 grades, V$\in \{1,2,3,4,5\}$. The assignment of threat should comprehensively consider threats probability and severity. Possible assignment (T1): the assignment refers to threat probability. Severity(T2): the severity that threats affect security attributes (confidentiality, integrity, availability). Where T1,T2$\in \{1,2,3,4,5\}$, the threat T can be calculated by T1 and T2,and the formula is as follows:

$$T=\frac{T_1+T_2}{2}, \quad T\in\{1,2,3,4,5\} \quad \text{…………(2-3)}$$

The higher value of T, the higher frequency the threat represents, and may cause more serious influence.Risk value (R) can calculate by the following formula：

$$R = f(V,T,AV) = \sqrt{V*T} * \sqrt{AV*V} \quad \text{…………(2-4)}$$

The value of technical risk calculation results between 1~25, which can be divided into 5 grades: very low (1~5), low (5~10), middle(10~15), high (15~20), very high (20~25). The risk calculation table of human resource system as an example as shown below:

Table 2-3 The Example of Technology Risk Calculation

Property value			Risk assessment		Risk calculation					
C	I	A	Threat vulnerability and attachment object	Vulnerability classification	Threat name	Assets value (AV）	Threat (T)	Vulnerab-ility (V)	Risk (R)	Risk grade
3	3	4	Human resource system	Communication security vulnerability	Eavesdropping	3.5	2.5	4	11.8	Middle

III. The Architecture Design of RQEP

This section presents a quantitative risk assessment tool (RQEP), realize a variety functions of evaluation process, such as standardization management, report automatic generation, evaluation data analysis, ect. It can be used as special tool for information security grade protection evaluation.

A The Architecture of RQEP

The design ideas of RQEP is according to the standards of national information security grade protection. The work is pulled out in five stages: determination for evaluation object, evaluation plans, site evaluation, information security construction (/rectification), reassessment (rectification after assessment), continuously improve related work, form the information security circulation model with plan, do, check and action. The diagram of RQEP architecture as shown below:

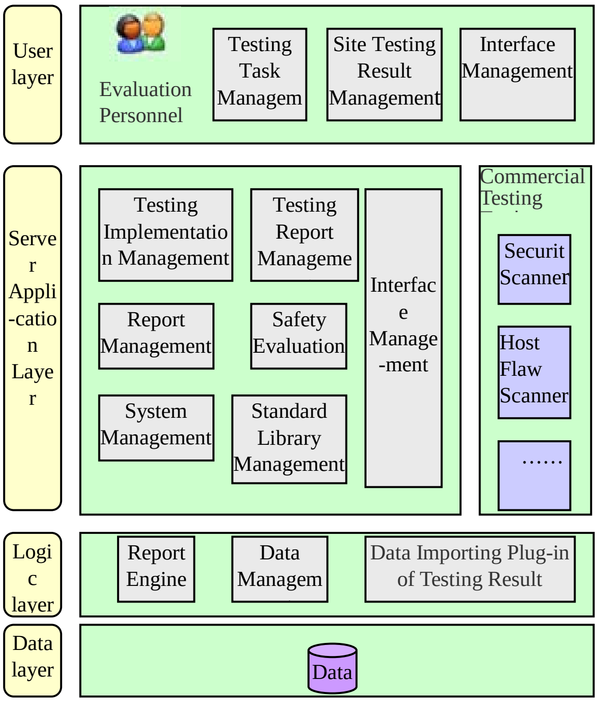

Figure 3-1 The Architecture of RQEP

1) User layer: function module for site evaluation.

2) Application layer: the main function module of system, as well as related commercial test kits that are being used, including security scanner, host system scanner, ect.

3) Logic layer: it mainly service for the function module of system, to achieve the basic functions of business logic.

4): Data layer: this layer service for data storage.

RQEP have a set of packages based on the basic requirements of information system classified protection, establish a set of rules base, compliance inspection&scenes and report template for 2 class above systems.

B The deployment mode of RQEP

RQEP adopts distributed deployment mode, including test center and test terminal. The deployment topology as shown as fig.3-2:

Evaluation center consists of high performance application server, database and storage array, which are responsible for the collection and storage of terminal feedback evaluation record, evidence and other related material, on the basis of these to finish profound data analysis, report preparation, statistical reports and other works. Testing terminal work for portable computing terminals, provides functions of scanning interface call, comparison analysis and evaluation record. The evaluation terminal can rapidly and efficiently access to system safety compliance and generate test records automatically. The distributed deployment RQEP can be adapted to the evaluation way that many people at the same time, people in different place, and asynchronous collaborative, it has a high flexibility.

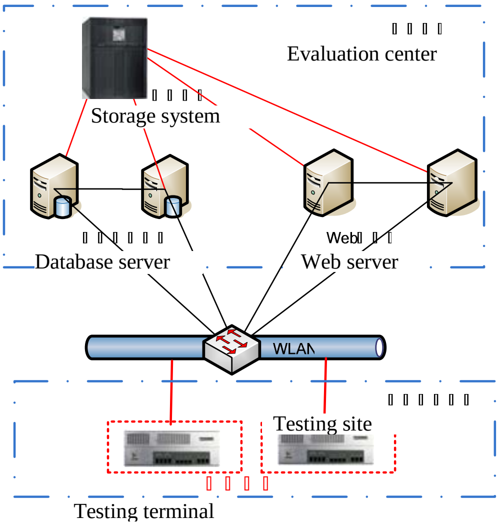

Figure 3-2 RQEP Deployment Diagram

C the function module of RQEP

1) Standard library management module: Play an important role in minimizing the impact of human factors. provide evaluation standard library of national level protection, ISO27001, enterprise baseline and various types of information security standard promulgated by SERC. According to implementation experience, refine evaluation indicators, provide evaluation steps and judging standard of examination items in detail, to make the process of assessment as objective and accurate as possible. The refinement of evaluation index is mainly based on application system, operating system and database category.

2) Evaluation implementation management module: Perpetuate the process of protection evaluation, provide functions of evaluation task allocation, evaluation tracking, evaluation result statistics, risk quantitative analysis and reporting, realize the whole life cycle management of evaluation task from initialization, implementation to close, change the previous manual audit work into automated testing and generate all kinds of security reports automatically.

3) Safety evaluation module: Using scientific methods, provide quantitative safety evaluation for evaluation results and risk, customize evaluation algorithm. Safety assessment mainly identify enterprise security status, it has promoting significance for enterprise safety level.

4) Report management module: Establish history database for information system security testing, provide advanced data analysis, according to demand to generate diverse statements, such as: enterprise safety trend analysis, safety short board analysis, etc. provide a basis for information security decision-making.

5) System management module: Provide user authority management of role-based access control, provide the funtions of user management, role management, authority management and log management and so on.

6) Interface management module: Provide interface

module for tools, such as application security scanner, scanning system of host system vulnerability and database security scan system. Realize direct call for tools and direct input the report generated by tool. Importing the analysis function by scanning external data, provide a rule driven event analysis engine, based on the engine, system can do comparative analysis for testing items and scan result, automaticly identify the testing item of grade protection. It not only can realize the sharing of evaluation result data effectively, but also reduce the workload of testing personnel greatly.

IV. Summary and Prospect

With the development of information system grade protection，problems in the process of evaluation, such as lower accuracy of risk analysis, low evaluation efficiency, lack of deep analysis for evaluation results, evaluation quality over depende on evaluation personnel’s ability and experience, are attracting more and more attention.

This paper presents a risk quantified evaluation method, through the analysis and calculation of asset vulnerability to obtain quantifed risk value. RQEP realise functions of standard library management, measurement management, safety evaluation, report management, interface management and so on. Using RQEP can greatly enhance the efficiency of grade evaluation and make the evaluation process more standardization. It has certain value on the work of information safety grade assessment.

References

[1] Shen Changxiang.Study on strengthening information security assurance system[Z].The anthology of the 17th Conference on National Computer Security and E-government Security.2002,10.

[2] Wang Tian,Xu Hui,Wei Lihao,Yang Hao.Study on Information Security Assurance System of Electric Power[J].GuangDong Electric Power.2010(5):38-42.

[3] Huang Jingzhi. Enterprise of Electric Power Grid Enforces the Security Classifyion Protection for Information System[J]. Computer Security.2010(07):80-82.

[4] ZHOU You-yuan, ZHANG Xiao-mei .Information Security Management Implementation Process of Multi-level Protection[J]. CHINA INFORMATION SECURITY. 2009(9):66-68.

[5] ZHANG Tao,MU De-jun,REN Shuai,YAO Lei. Risk assessment model of information security based on risk matrix[J]. COMPUTER ENGINEERING AND APPLICATIONS.2011(46):93-95.

[6] CHEN Qing-ming, ZHANG Jun-yan. Tools for and Their Applications in Information Security Risk Assessment[J]. CHINA INFORMATION SECURITY. 2010(1):93-95.