Electricity communication transmission network risk calculation model design and management system achievement

Hailong Xiao[1,a] , Chunyu Liu[2,b], Yongsheng Zhang[3,c]

[1,2,3] State Grid Inner Mongolia Eastern Power Co. Information Communication Ltd.

Century Six Road, Hohhot city, Inner Mongolia province, China

[a] xiaohailong1984@163.com , [b] 83211540@qq.com , [c] cyberyosh@126.com

Keywords: Electricity communication transmission network; Risk Management; Risk calculation; Risk management and control

Abstract: Electricity communication transmission network is the key support network of the power grid. Its security has direct significance to the stable operation of the power system. The article brings out a re-definition of risk. According to the threat of natural disasters, equipment and human resources in the electricity transmission network , we identify the risk factors. The article designs risk calculation processes and models of the network nodes and business, gives specific risk management and control strategies. Finally, combining these risk management processes and methods, we implement a risk management system of electricity transmission network.

1 Introduction

Power communication network is a dedicated communication network for the national electricity system, which bears all the business of electric power system. Power communication network has a complex structure and large system, which plays a greater role in electric power dispatching and power production. Any failure could seriously threat the safe operation of the power grid. Therefore, risk management for the power communication network, real-time risk assessment of the situation and ensuring safe and stable operation of the communication network have very important significance.

At present, risk management mainly applied to areas such as the electronic commerce, the insurance industry, the operation of the power system. The target of power communication network risk management is to solve the power communication security and operation issues, to give scientific analysis and timely control for risk points of power communication network, to timely discover the weaknesses in the network and security risks that may arise, to establish management methods and processes of risk point response and elimination.

2 Risk of electricity communication transmission network

The traditional definition of risk is the probability and consequence of hazardous events, which is a forecast to the risk. But the actual system also need to consider the real-time operating state of communication networks, such as the equipment running status is normal or not, the computer room environment meets the requirements or not. So we redefine risk as real-time operating state and consequences of communication network.

Threats and the corresponding defense measures in electricity communication transmission network are as follows:

Natural disasters influence

According to the historical operation experience, the main threat of the electric power communication network comes from natural disasters. Because the electric power communication network has a large coverage, natural disasters can easily destruct the infrastructures.

For natural disasters, we can real-time monitor the computer room environment, ensure the temperature and humidity within the allowed range; communication equipment should have the

lightning protection measures, the cabinet should be grounded, power supply has overvoltage and overcurrent protection or redundant power supply. These measures can reduce impact of natural disasters on communication transmission network.

(2)Reasons of equipment itself

The failure of equipment itself can also cause risk events, so we need to take many protective measures on equipment. When we buy equipment, choose a better reputation brand and business. Transmission equipment should have configurations of dual power supply. Long time operating, serious aging equipment should be regular inspected, maintained and even replaced timely.

(3) The difference of human resources

Grid employee lack of safety consciousness and work quality is also a big threat to the communication transmission network. Therefore, we should conduct regular training for staff; staff responsibilities need to be institutionalized and behavior of employee should be transparent; improve the management system, enhance staff safety awareness and sense of responsibility.

3 Risk management processes and methods

Risk management is a risk analysis of electric power communication transmission network. The main processes include risk factors identification, risk calculation model design and risk control strategies.

3.1 Risk Factors Identification

Risk identification is the basis of risk management, which determine risk assessment indicators and identify which factors will lead to instability and even hazard of the power transmission network operation condition. Risk identification include assets, assets vulnerability and threat identification. The main source is based on the actual production .

Power communication network is a complex network system that contains a variety of business subnet. It is mainly composed by the transmission network, management network, data network and switching network. Transmission network is the core. There are a lot of SDH equipment running in transmission network, therefore, the main targets of communication transmission network risk assessment are SDH equipment and cables.

SDH equipment factors include optical port, power port, Ethernet port, operation management, human factors and computer room environment, which are primary factors.

Among them, the factors of optical port comprise transmitting optical power, received optical power, side mode suppression ratio, input jitter and output jitter, input offset, background block error, error rate, AU pointer counting and alarms. Factors of power port include outlet bit rate, input offset, input attenuation, input jitter, error seconds and alarms. Factors in Ethernet port are transmitting optical power, throughput, packet loss, delay and alarms. Factors of the operation management include equipment maintenance execution, communication equipment testing completeness, equipment spare parts completeness, equipment defect elimination completion, technical information completeness, management information completeness, communication contingency plans and completeness. Human factors include staff training conditions, staffing conditions, workers' age structures and academic situations, workers labor remuneration, team harmony situation. Computer room environment factors comprise temperature, humidity, hygienic condition, lightning protection measures, anti-static measures, air-conditioning spare situation. These are all secondary factors.

3.2 Risk calculation model design

Risk calculation is an important part of risk assessment. It uses the vulnerability of the asset and threat emerging frequency to get risk events states, and determine the system risk in accordance with the asset value.It is mainly to calculate risk of network nodes and businesses. The specific processes are shown in Figure 1 and Figure2.

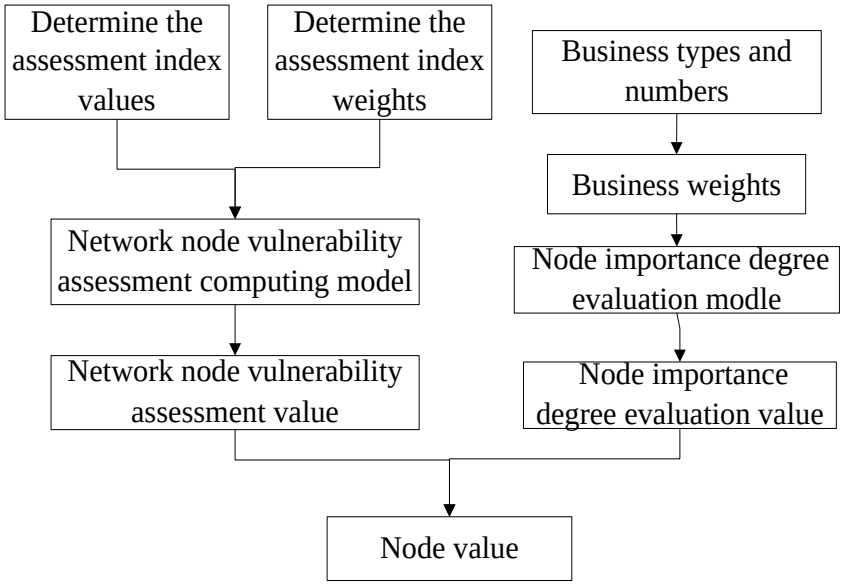

Figure 1 Network node risk calculation

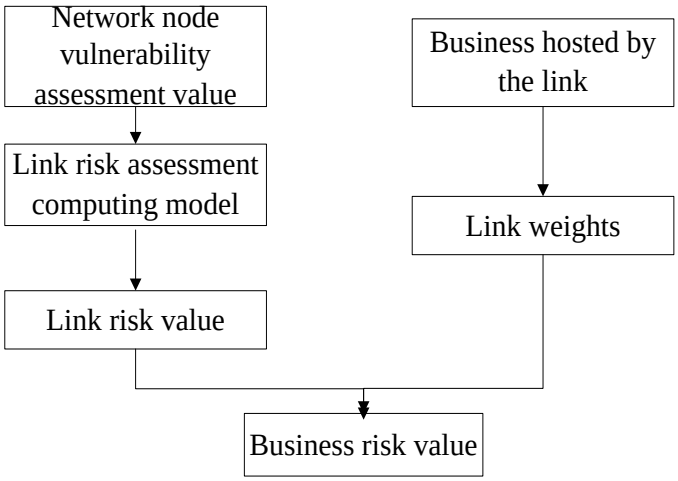

Figure 2 Business risk calculation

Vulnerability assessments to network node (SDH equipment and fiber) include determining the assessment index values (scoring the evaluation index), determining the assessment index weights, determining the network node vulnerability assessment computing model. To assess the importance degree of network nodes, we should know the business types and numbers that hosted by network nodes, identify business weights, determine importance degree evaluation algorithm. The risk of network nodes is determined both by the vulnerability value and the important degree of nodes.

Risk assessments of electricity transmission network focus on assessing business risk. Computing the risk of network node prepares for business risk calculation. Business risk assessment include links risk assessment and business weight assessment. Finally, we can use the risk of network nodes (SDH equipment and fiber optic cable) to get the link risk value by series and parallel calculating.

3.2.1 Vulnerability assessment model of network node

The system consists of two level index factors, so the vulnerability assessment algorithm of network nodes is in Eq. 1.

$$V = \sum_{i=1}^{n}[\sum_{j=1}^{m}(Pij * Wij)] * Wi \quad (1)$$

In formula 1, i denotes the number i factor of level 1, n represents the total number of level 1index factors, j represents the number j factor of level 2. Pij denotes the vulnerability assessment value of the number j level 2 factor of the number i level 1 factor (scored by operation maintenance person, field experts considering the actual situation of factors), Wij is the weight of the number j level 2

factor of, Wi represents the weight of the number i level 1 factor. Weight determination method: the use of judgment matrix and matrix related operations mathematical methods to determine the relative weight of relevant elements in this hierarchy to the upper layer elements.

The bigger of the network node vulnerability assessment value, the worse of the node running condition and the higher the risk.

3.2.2 Node importance calculation model

Business carrying in electricity transmission network include PCM business, dispatching telephone, power remote, teleconference, scheduling data network, relay, etc. Different business has different influence on stable operation of power systems, so it is important for a variety of business in different weight values. Business type and number hosted by per network node is different. So according to business importance degree and the corresponding number, node importance calculation method is in Eq. 2:

$$S = \sum_{i=1}^{m} Wi * Ni \quad (2)$$

In formula 2, i denotes the number i type of hosting business, m represents the total number of service bearer, Wi represents the weight of number i business type , Ni says the amount of this carrying business type.

The greater the node importance value, the larger the asset value of the node or the greater the impact on the stability of the system, the higher the risk.

3.2.3 Link risk calculation model

There are two cases when calculating link risk by node vulnerability: the nodes in series and nodes in parallel. When node series, we only need to sum the node vulnerability assessment values to get the value of this link risk. When nodes in parallel, the calculation method of the link risk R is in Eq. 3.

$$R = {}^{1}/_{\sum \frac{1}{vi}} \quad (3)$$

In formula 3, Vi represents the vulnerability assessment value in parallel nodes.

3.3 Risk control strategies

risk of operating procedures, environment and equipment. We can eliminate the risks by defect-elimination, modification and equipment replacement.

Risk management and control methods include risk prevention, risk aversion, risk suppression, risk transfer, risk tolerance.

There are different control strategies for different risk factors and different risk levels in electricity transmission network. Specific programs as shown in Table 1.

Table 1 Specific control strategy

Level 1 factors	Level 2 factors	Deduction situation（P）	Policy type	Policy description
Optical port	Transmitting (received) optical power	$0 \leq P \leq 2$	Risk tolerance	Don't take any action.
		$2 < P \leq 10$	Risk suppression	Check the remote and the local optical modules, fiber optic lines are normal
	Error rate	$0 \leq P \leq 2$	Risk tolerance	Don't take any action.
		$2 < P \leq 10$	Risk suppression	Modify the configuration and re-send; replace the board.
	Alarms	$0 \leq P \leq 2$	Risk tolerance	Don't take any action.
		$2 < P \leq 10$	Risk suppression	Check the specific alarm information and process.
Operation management	Equipment testing completeness	$0 \leq P \leq 2$	Risk prevention	Test every communication equipment regularly, identify problems and timely deal with them.
		$2 < P \leq 10$	Risk suppression	Timely testing equipment.
	Equipment spare parts completeness	$0 \leq P \leq 2$	Risk prevention	Regularly patrol the room, network management, equipment and facilities, check whether the equipment spare parts are intact.
		$2 < P \leq 10$	Risk suppression	Immediately make a full spare parts.
	Technical information completeness	$0 \leq P \leq 2$	Risk prevention	Check regularly whether all relevant technical information is complete.
		$2 < P \leq 10$	Risk suppression	Complete technical information for staff reference.
…	…	…	…	…

In order to control the risks better ,the system established the perfect standard operating procedures ,which can be quickly shorten the process time ,easier to understand the progress of the work ,enhance the efficiency of the internal communication transmission .Based on analysis of the risks, the risk which needs to deal with will trigger the to-do transaction to start the whole process ,including application, approval, execution ,verification ,archive. First the system will remind relevant personnel to do processing, so relevant personnel can generate application information based on the risk information, after through the approval by responsible leadership, handling personnel can may refer to the contents of the knowledge base for processing. After processing is complete verification, archiving. After the control ,it still needs inspection and evaluation for the implementation of the risk control, so personnel can put forward measures and methods to reform and improve.

4 Implementation of risk management system

After landing risk management system of electicity communication network , there are four functional modules: risk management, alarm query statistics, resource management, and operation maintenance. Risk management includes risk calculations, showing the results of the risk assessment, risk management and control operations, documentation management and risk allocation. Alarm query statistics can query the information about current alarms and history alarm. Resource management mainly maintains the personnel information and network assets basic information (basic resources, space resources, cable resources, routing resources and network resources). Operation maintenance module can add, delete,change and query staff duty records and spare parts information.

5 Conclusion

Electricity transmission network has numerous assets, due to the impact of natural disasters,

device itself factors, the differences between human resource, and the other factors, the system may have a variety of security threats. Electric power communication network risk management has important practical guiding significance for power communication management. Based on the actual situation of electric power communication network, this paper establishes the evaluation index set, for the factors of index set to do the security risk analysis and risk management control, and establishes a complete electric power communication transmission network risk management system and shows the critical pages of the system.

References

[1] Huisheng Gao, Congcong Li. *Calculation model of electricity power communication network security risk*. Relay, 2007,14:50-53+76.

[2] Peng Peng, Yujun He, Yu He. *Security risk assessment system design and implementation of the electric power communication network*. The electric power information and communication technology, 2014,03:53-59.

[3] Kangming Jiang, Ying Ceng, Boren Deng, Liangrui Tang. *The electric power communication network risk assessment method based on business*. Power system protection and control, 2013,24:101-106.

[4] Nian Liu , Jianhua Zhang , Xu Wu. *Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems-Part II: Application in Substation*. IEEE Transactions on Power Delivery. 2010. 26(2): 876-881.

[5] Zhendong Zhao, Yunyong Lou, Ya-dong Zhang. *Structure of reliability evaluation model for electric power communication network*. Electric Power Technology, 2010, 19(9): 74–77.

[6] Jian Xu， Shaoyong Guo. *Risk evaluation mechanism based on AHP for power communication network*. Telecommunications Technology, 2013(3): 73–75.

[7] Jordi Cabero,Mariano Ventosa. *A medium-Term integrated risk management modle for a hydrothernal generation company*. IEEE Transaetions on Power Systems,20(3),2005.1579-1388.

[8] Jungwon Huh,Aehintya Haldar. *A Novel Risk Assessment for Complex Struetural Systems*. IEEE Transaetions on Reliability, 60(l), 2011.210-218.

[9] Changzhong Xu. *Risk prevention strategy research on Langfang electric power communication network security*. North China Electric Power University (Beijing), 2011.

[10] Jinbiao Chen. *Risk management strategy research on a rolling enterprise electrical equipment*. Shandong University, 2013.