Vulnerability Assessment of Shipboard Electric Power Information Network

Han Yang[1, a], Zhihao Ye[1], Dan Mei[2], Han Xiao[1]

[1] National Key laboratory of Science and Technology on Vessel Integrated Power System, Naval University of Engineering, Wuhan 430033, China

[2] College of science, Naval University of Engineering, Wuhan 430033, China

[a]email: icyyoung2010@163.com

Keywords: Shipboard; Complex Network; Electric Power Information Network; Delay; Business Importance; Vulnerability

Abstract. With the development of the Ship Power Network automation, the relationship between the Ship Information Network and the Ship Power Network becoming more and more closed, and it causes information factors will impact the ship's fragile of Power Information Network at the same time, but there are not totally proven technique and method to evaluate the vulnerability of Ship Power Information network from the different angle like topology and information factors at the same time. In the process of forming a new index to assess the vulnerability of the Ship Power Information, considering a complex network theory-based structural vulnerability firstly, and then also discussed the network running the business importance, fiber or equipment, fiber delay or other factors delay and other equipment affect network performance which contains more factors. Compared to the traditional topology vulnerability indicators, this new vulnerability indicators can be more comprehensive assess the network vulnerability.

Introduction

Power information network vulnerability becomes a new problem in recent years in the field of information and electrical power. The operation of the network, substation automation, distribution automation, power plant monitoring system and so on, has become a necessary part to ensure the normal operation of power network. Electricity networks and information integration network has gradually become a highly integrated network integration. Information technology in facilitating the operation of the electricity network, but also will bring adverse effects to the electricity network.

Vulnerability also be called vulnerabilities that can be used by the attacker or intruder, and cause economic and security issues. In 2000, the United States somewhere plant control system receives signals from unknown attacks, resulting in the generator set in 7 seconds lost 900Mw load almost crash the system [1]; In October 2000, the control system crashes caused by Ertan Hydropower Plant load rejection 890MW, making Chongqing a wide range of grid outage, the direct interconnection network control systems and office automation system network is a factor leading to an unsafe network according to the accident analysis [2]. Synthesis of the above mentioned problems and the case of the accident we can know that despite the unavoidable power information network inherent vulnerability, but try the best to find a more full index to assess the vulnerability of electric power information network, analyzed the current vulnerability of becoming urgent needs to guarantee the safe operation of the electricity network. Similarly, in the ship field, ship information network has become more and more close with the ship power network and it made the vulnerability and the vulnerability assessment issue of the ship information network and the ship power information network has become increasingly concerned.

To achieve the correct assessment of the power information network vulnerability is conductive to discovery the most vulnerable part of the network. If the relevant design departments for these more vulnerable part of some appropriate amendments, the performance and efficiency of electricity network will be greatly improved. Firstly, according to ship electricity network to establish a network and get the appropriate information power information network integration model, combined with

the complex network theory to obtain structural vulnerability of the ship power information network, and to consider further the information network service importance, the probability of a link failure, delay and other factors, finally get a comprehensive evaluation index of integrated network vulnerability assessment.

Marine Electric Information Network Modeling

Ship Power Network modeling

According to the actual ring structure diagram ship power grid, the grid elements will be generators, power distribution boards, load and other abstract complex nodes in the network, the connection relationship between the elements abstract grid side, the establishment of ship power network equivalent topology model Figure.1. Where G represents the generator node, S represents switchboard node, F represents the feeder cable node, L represents the load node.

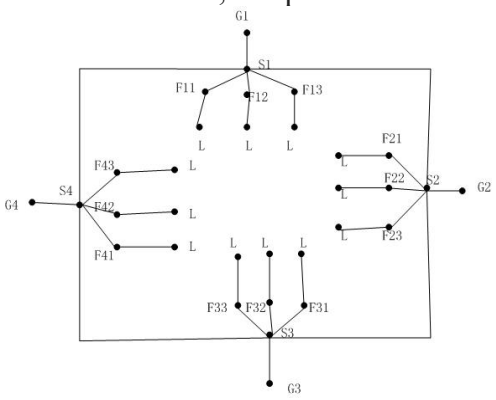

Fig.1. A ship power system topology diagram

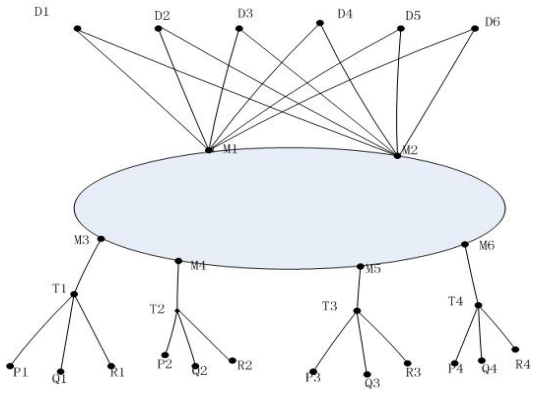

Fig.2. Power network topology information corresponding to a schematic view of a ship

Ship Information Network Modeling

Figure.2 shows a ship information network topology diagram, M represents the switch, D1 represents power quality management workstation node, D2 represents distribution operation monitoring node, D3 represents the Line relay protection system node, D4 represents power transmission equipment monitoring node , D5 indicates scheduling information management node, D6 indicates scheduling training system node, T for the CAN bus master node, P_i is stable operation and management of information nodes, Q_i to protect operating information management nodes, R_i is electric energy metering nodes.

Ship Power Information Network Modeling

Ship power information network as shown in Figure.3, According to the function of each module, the ship electric power network node is connected with the information network node correspondingly. Such as distribution operation monitoring node correspondingly connected to the switchboard node; line relay protection system is a power system to ensure stable and reliable operation, signal relay means between the high voltage transmission lines and grid protection devices automatic safety devices the distance signal transmission, the signal is required for the safe operation of the power grid, the power distribution board corresponding node connected to it; and generating node has a corresponding connection with monitoring node of transmission equipment; electric energy metering system for metering the electric energy consumption, corresponding connected to which is a load; stable operation of information management and operation of the same switchboard closely linked, it corresponds to the two nodes are connected; according to different functions, power network nodes are linked with the information network nodes on the application dotted line.

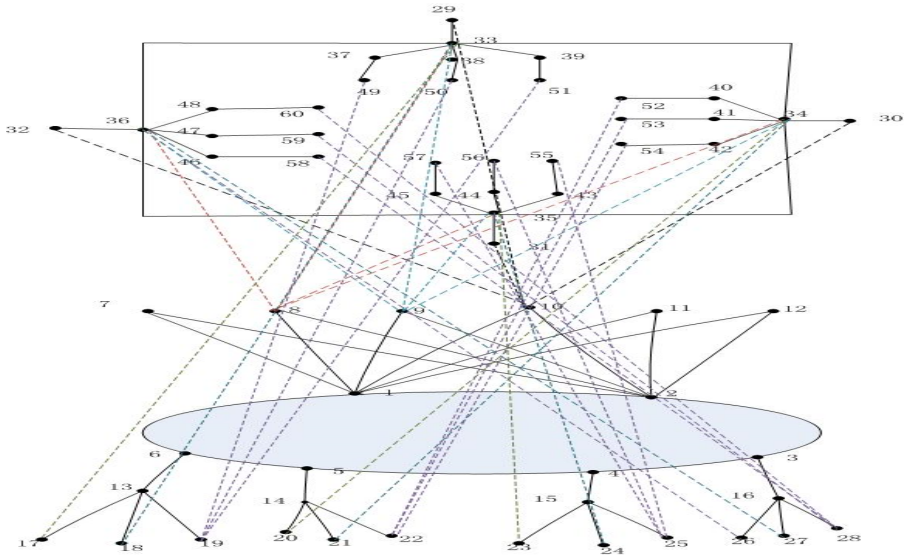

Fig.3. Integrated information model structure of the ship power network diagram

Vulnerability Index

Electricity network vulnerability was first proposed by Fouad professor and his students in 1994, based on the use of transient energy function neural network to analyze the vulnerability of the grid [3], as the impact of incidents on the electricity network in each sector growing great, scholars began to the study of power network blackouts for the goal of electricity network vulnerability, with the development of intelligent power network, the corresponding information network vulnerability research began to enter our field of vision. For the information of the network vulnerability analysis, there are based on AHP information network vulnerability analysis [4], based on the information network vulnerability analysis of complex network theory [5], based on the information network attack paths Vulnerability Analysis [6], based on attack graph information network vulnerability analysis [7] and the cloud model based on the information network vulnerability analysis [8] methods, and so on. During the process of power network, it becomes more and more depend on the information network, the vulnerability assessment of the integrated network of the two is bound to become an increasingly popular research.

Structural vulnerability

In the complex network theory, the betweenness reflects the size of the medium node throughput, traffic, capacity and level of activity nodes in the network. Corresponds to the destination network node it reflects information carrying capacity. When the link for the attack, also used the betweenness as parameters characteristic amount. Current information to the electricity network of high-capacity optical fiber transmission, the basic non-existent capacity limit. Therefore, the use of edge betweenness parameters can well describe the link vulnerability, the higher the number of dielectric fiber optic network transmission line more easily lead to vulnerability. Ship information networks generally use a bicyclic ethernet & fieldbus networking, temporarily not consider the case of line redundancy topology, we make it reduced to a single ring network representation.

Betweenness: betweenness is divided into two kinds of node count mediator mediated side, it is a global feature amount reflects the entire network node or edge in the role and influence. B_i node betweenness is defined as

$$B_i = \sum_{\substack{\text{所有} j,l \\ j \neq l \neq i}} [N_{jl}(i) / N_{jl}] \tag{1}$$

Where N_{jl} represents the number of shortest paths between nodes v_j and v_l, $N_{jl}(i)$ represents the shortest path between the node v_j and v_l passing a number of nodes v_i. Similarly, the number of referrals B_{ij} defined for the network edge all the shortest paths through the ratio of the number of edge e_{ij}

$$B_{ij} = \sum_{\substack{\text{所有} l,m;l\neq m \\ \{l,m\}\neq\{i,j\}}} [N_{lm}(e_{ij})/N_{lm}] \quad (2)$$

Wherein, N_{lm} represents the number of shortest paths between nodes v_l and v_m, N_{lm} (e_{ij}) represents the shortest path between the node v_l and v_m after several edges of e_j.

Business Vulnerability

Business concept of vulnerability: the vulnerability of business includes the probability of the network running the business importance, fiber or equipment failure, delays or fiber optic delay device vulnerability of these three factors caused by the Power Information Network, the introducing the concept in favor of a more comprehensive expansion of information network vulnerability analysis. Business vulnerability contains the link business vulnerability C_{ij} and the node business vulnerability C_i.

Business vulnerability indicators C_{ij}, C_i is calculated as follows:

$$C_{ij} = r_{ij} \times p_{k1} \times \varepsilon_1 \quad (3)$$

Wherein, r_{ij} indicates that the circuit is running the business class i and Si is business importance; p_{k1} is the probability of occurrence of a link L_k failure; ε_1 is ratio of real time delay t1 and intrinsic delay T1 for link transmission. Currently electric power communication network commonly used fiber optic cable as a transmission link, the probability of failure and the cable laying, cable type, running time, the surrounding environment and other related value of the link failure probability p_k should consider the actual situation of each cable, according to statistics determine.

$$C_i = (\sum_{m=1}^{x} r_m) \times p_{k2} \times \varepsilon_2 \quad (4)$$

Wherein, m represents the node running through the i-type Si business of importance; p_{k2} is the probability of occurrence for a node N_k fault; ε_2 node apparatus transmission delay actual ratio t_2 inherent delay of T_2.

Comprehensive Vulnerability

Information network vulnerability contains the node fragility of V_i and link vulnerability V_{ij}, and link the vulnerability by structural vulnerability B_{ij} and C_{ij} link traffic vulnerability to obtain comprehensive, and link traffic vulnerability by running link channel effect importance r_i business and the SDH link transmission delay and other factors; node vulnerability obtained by the structural fragility of B_i and operational vulnerability C_i, node vulnerability is limited by business operations through all the important nodes the degree of influence and SDH network element equipment transmission delay and other factors. B_i, C_i, B_{ij}, C_{ij} indicators are dimensionless units, composite vulnerability index V_i, V_{ij} is calculated as follows

$$V_i = (B_i + C_i)/2 \quad (5)$$

$$V_{ij} = (B_{ij} + C_{ij})/2 \quad (6)$$

Numerical example

Figure.3 is a ship electric information network, based on the target network to establish the corresponding adjacency matrix, using MATLAB software simulation calculates the parameters required to obtain the changes of the nodes vulnerability of only considering the topology and taking into account the impact of information network factors, the results are shown in Table 1.

Table 1

NO	Structural Vulnerability	Comprehensive Vulnerability	Equipment No	NO	Structural Vulnerability	Comprehensive Vulnerability	Equipment No
1	0.0924	0.157344	M1	15	0.0389	0.068504	T3
2	0.0924	0.157344	M2	16	0.039	0.068554	T4
3	0.051	0.075084	M6	17	0.0133	0.025546	P1
4	0.0441	0.071634	M5	18	0.0133	0.01961	Q1
5	0.0441	0.071634	M4	19	0.0174	0.015834	R1
6	0.0509	0.075034	M3	20	0.0149	0.026346	P2
7	0	0.031412	D1	21	0.0149	0.02041	Q2
8	0.0001	0.034654	D2	22	0.0161	0.015184	R2
9	0.1926	0.134944	D3	23	0.0149	0.026346	P3
10	0.0344	0.03222	D4	24	0.0149	0.02041	Q3
11	0	0.036644	D5	25	0.0161	0.015184	R3
12	0	0.011172	D6	26	0.0133	0.025546	P4
13	0.039	0.068554	T1	27	0.0133	0.01961	Q4
14	0.0389	0.068504	T2	28	0.0174	0.015834	R4

Table 2 below size for individual taking into account the structural vulnerability factors and also considerate information networks link composite vulnerability of the calculated value.

Table 2

NO	structural vulnerability	Comprehensive Vulnerability	node	NO	structural vulnerability	Comprehensive Vulnerability	node
1	0.038853616	0.243719648	(1, 2)	18	0.231137851	0.339861766	(4, 5)
2	0.306795648	0.377690664	(1, 6)	19	0.234190048	0.230420024	(4, 15)
3	0.098333333	0.227154912	(1, 7)	20	0.251313505	0.349949593	(5, 6)
4	0.098333333	0.245241582	(1, 8)	21	0.234168262	0.230409131	(5, 14)
5	0.445904995	0.441919063	(1, 9)	22	0.239701746	0.233175873	(6, 13)
6	0.101640212	0.135927181	(1, 10)	23	0.110485048	0.269381444	(13, 17)
7	0.098333333	0.256800732	(1, 11)	24	0.110485048	0.202111724	(13, 18)
8	0.098333333	0.112470012	(1, 12)	25	0.19637819	0.17903515	(13, 19)
9	0.307144232	0.377864956	(2, 3)	26	0.117073413	0.272675626	(14, 20)
10	0.098333333	0.227154912	(2, 7)	27	0.117073413	0.205405906	(14, 21)
11	0.098703704	0.245426767	(2, 8)	28	0.186796569	0.174244339	(14, 22)
12	0.445883209	0.441908169	(2, 9)	29	0.117084306	0.272681073	(15, 23)
13	0.101640212	0.135927181	(2, 10)	30	0.117084306	0.205411353	(15, 24)
14	0.098333333	0.256800732	(2, 11)	31	0.186796569	0.174244339	(15, 25)
15	0.098333333	0.112470012	(2, 12)	32	0.110419688	0.269348764	(16, 26)
16	0.251291719	0.349938699	(3, 4)	33	0.110419688	0.202079044	(16, 27)
17	0.240028543	0.233339271	(3, 16)	34	0.196574269	0.179133189	(16, 28)

In order to make a more direct comparison between the two indicators of vulnerability assessment, the data in the table above is converted to the following graph in Figure.4, Figure.5.

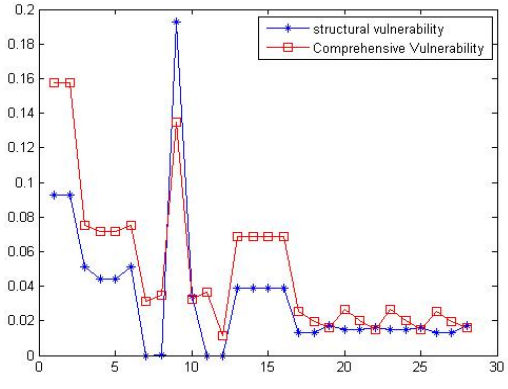

Figure.4

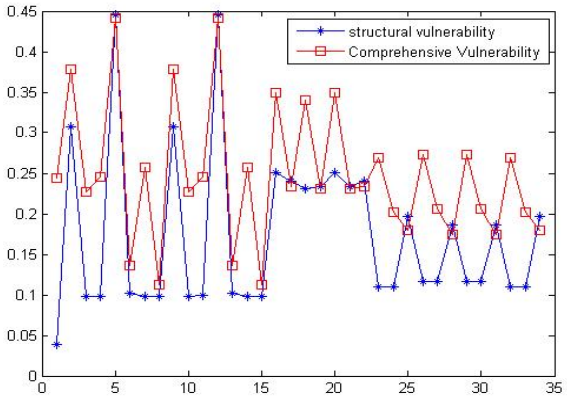

Figure.5

As seen in Figure.4, when considering separately from the topological structure, on the 9th node (Line relay protection system nodes) for the most vulnerable node, but after considering the equipment failure rate, delay, and important business and other factors No. 1& No. 2 node (1,2 switch node) to be the most vulnerable node, it means the description of the 9th node (line protection system nodes) structurally weak high value, but the value of business vulnerability isn't very high, after considering the information factors, its value of comprehensive vulnerability decreases inversely.

From Figure.4 and Figure.5, it can be seen that after considering the information network of factors, most vulnerable link node fragile values and value increased, it was found that the equipment failure rate information networks, and delay important business and other factors lead to Power Information Network node link vulnerability and greater vulnerability, which is the factor information network may increase the risk of power network failure.

Conclusion

Traditional vulnerability analysis method uses of more common method which is based on complex network theory analysis of the topology of the vulnerability of the target network, a handful of vulnerability analysis, taking into account the fragility of line or device topology itself and channel business and other factors lead to vulnerability. Vulnerability assessment indicators presented above, taking into account a variety of factors affect the vulnerability of the network, thereby enabling a more comprehensive information on the electricity network vulnerability assessment reasonable.

Acknowledgement

In this paper, the research was sponsored by the Nature Science Foundation of Hubei Province (Project No. 51377167)

References

[1] Frances Cleveland. Enhancing the reliability and security of the information Infrastructure used to manage the Power system. Security subcommittee Presentations and papers, PSCC and PSSC, IEEEPES, 2007.

[2] Yaozhong XIN. New Century dispatching automation technology trends. Power System Technology, 2001 (12): 1-10.

[3] Chen G, Dong Z Y, Hill D J, et al. Attack structural vulnerability of power grids: A hybrid approach based on complex networks [J]. Physica A: Statistical Mechanics and its Applications, 2010, 389(3): 595-603.

[4] Baoli Liu, Xiaochun Xiao, Gendu Zhang. Based on AHP Information System Vulnerability Assessment [J]. Computer Science, 2006, 33 (12): 62-64.

[5] Chi Guo. Vulnerability of Internet-based complex networks [D]. Wuhan University, 2010.

[6] Chao Qin, Nike Gui. Security vulnerability analysis based on information system attacks path [C]. National Computer Security Symposium 2009.

[7] Bao Zhao. Research on vulnerability analysis technique based network attack graph[D]. National University of Defense Technology, 2009.

[8] Qizeng Li, Zanfu Xie. A method of analyzing a fragile information systems based on cloud model[J].Guangdong Polytechnic Normal University: Natural Science Edition, 2010, 31 (6): 15-18.