Research on WBS-RBS Oriented Security Risk Assessment Index System for Space Domain Private Network

Journal of Physics: Conference Series **2489** (2023) 012021 doi:10.1088/1742-6596/2489/1/012021

Research on WBS-RBS Oriented Security Risk Assessment Index System for Space Domain Private Network

Rui Wang

Air Force Engineering University

317275959@qq.com

Abstract: To solve the problems such as unclear overall situations, incomplete risk analysis, and lack of targeted evaluation indicators of the security of the special network in the aerospace field, this paper takes the special network in the aerospace field as the research object, uses the WBS-RBS method to analyze the risk of network security, and uses the OSM model to establish an evaluation indicator system for the identified risks, to provide an indicator model for the subsequent security detection and evaluation of the special network in the aerospace field.

1. Introduction

With the continuous development of China's space industry, space launch missions have increased significantly year by year, and the amount of China's orbit spacecraft has exceeded 500. The special network in the space field is the core backbone network that carries the space launch and long-term spacecraft management tasks and is the key infrastructure of the space system. It is facing unprecedented challenges at the level of technical development and strategic security. As the underlying support network system for safeguarding the use of national space assets management, it is very likely to be selected as the potential target of network attacks. In September this year, the national official media and Beijing Qihu Technology Co., Ltd. released an investigation report on the network attacks on Western Polytechnic University by foreign countries, revealing that the "Specific Intrusion Action Office" under the US National Security Agency continued to attack and steal secrets from North-western Polytechnic University, stealing more than 140GB of its core data. This cyber security incident has profoundly revealed that cyberspace has become a key area of military, economic, and technological development, and competition among countries, and has also sounded an alarm bell for the security of special networks in the space field.

Given the current severe and complex network security situation, it is urgent to research and design a scientific and effective network security detection and evaluation index model, comprehensively detect, explore, and evaluate the security vulnerabilities and weaknesses of the special network in the aerospace field, and purposefully improve the comprehensive network security protection level to ensure the safe, stable, and reliable operation of the aerospace system.

At present, the research of network security evaluation indicators in China mainly focuses on the establishment of an organizational framework and business system, and the relevant technical system and standard system are still in the research stage. Among them, Zhang Xugao [1] proposed an information system security situation assessment model based on the interval matrix correction method given the problems existing in the current information system security situation assessment model. Zhou Chao [2] explored the application of a quantum neural network algorithm in information

security risk assessment and proposed an information security risk assessment method based on a quantum gate circuit neural network. The information security evaluation index model established by Cai Yue [3] uses the analytic hierarchy process and the information entropy theory to evaluate the dual model fuzzy evaluation method. Xin Qian [4] adopted the unit evaluation model of entropy weight neural network and the overall evaluation model based on the fuzzy comprehensive evaluation method to achieve the goal of hierarchical evaluation of information systems. Chen Zheyu and Lin Mingwei [5] proposed a hesitation fuzzy language envelope analysis model based on an analytic hierarchy process to evaluate the network security of edge nodes. Gao Yunyun [6] explored the method of using the K-means algorithm to conduct mining analysis for clustering analysis, and finally obtained clustering results by clustering scores, and proposed corresponding security strategies according to the characteristics of each category. Zhang Chunjie [7] proposed a security risk assessment method based on incomplete information static attack and defense game model for the uncertainty between attack and defense in the control system. Zhao Chen [8] built the information system security evaluation model by using the analytic hierarchy process and fuzzy evaluation method. Wang Yuhe [9] proposed an evidential reasoning algorithm and BRB security assessment method.

The author comprehensively analyzed several mainstream security assessment methods and model algorithms in the industry, combined with the characteristics of the special network security system in the aerospace field and the actual security protection requirements, studied and designed the method of using WBS (Work Breakdown Structure) and RBS (Risk Breakdown Structure) to visualize multi-dimensional network security risk indicators, and analyzed and sorted them out, The hierarchical structure of "Object Strategy Measure" (OSM) is introduced, and finally, the idea of constructing a WBS-RBS based security risk analysis and evaluation index system for special networks in the aerospace field is proposed.

2. WBS-RBS-oriented security risk indicators for special networks in the aerospace field

2.1. Build WBS structure for special network security work in the aerospace field

WBS is mainly used to decompose the overall project task into specific work elements. It is generally used to refine and decompose the work with complex structures, to facilitate the implementation, inspection, and evaluation of specific work. According to the special network security in-depth protection system and security protection objects in the aerospace field, the WBS work breakdown structure is used to divide the network security protection tasks into five elements, including information transmission security, carrier network security, information terminal security, application software security, and security management system, according to the top-down creation method. Information transmission involves ground circuits and satellite communication circuits. The bearer network involves network equipment and network protocols, and the application software involves data and software. The specific security WBS work breakdown structure is shown in Figure 1.

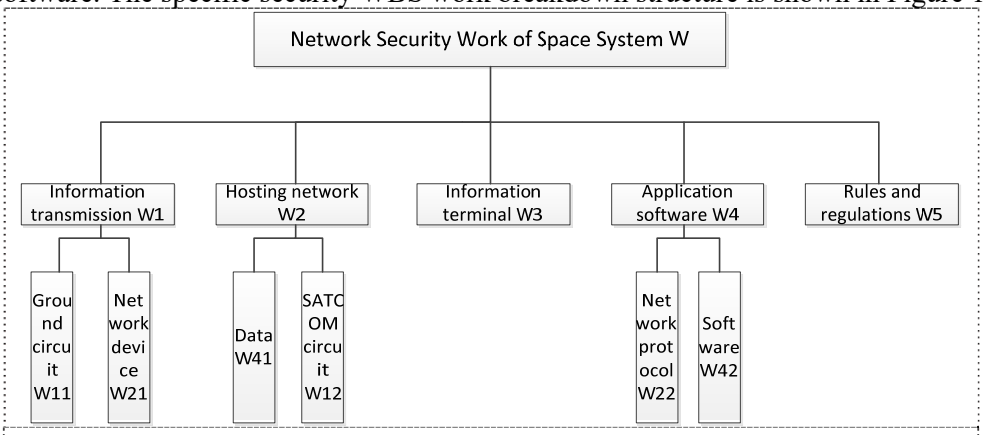

Figure 1. WBS work breakdown structure of special network security in the aerospace field

2.2. Build RBS structure of special network security risk in the aerospace field

RBS mainly decomposes the hierarchical structure of identified risks according to the risk category. Using the RBS risk decomposition structure, it decomposes the special network security risks in the aerospace field into five elements: physical environment security risks, communication network security risks, regional boundary security risks, computing environment security risks, and network security management risks. The security risks of the physical environment mainly come from the security of the channel and the computer room environment. Communication network security risk mainly comes from the security of network interaction and communication protocol, regional boundary security risk comes from the risk of intranet data interaction and international site access, computing environment security risk comes from the risk of the terminal, software, data, network, and security equipment, and network security management risk mainly comes from the risk of security operation and maintenance and the efficiency of security equipment. The specific security RBS risk breakdown structure is shown in Figure 2.

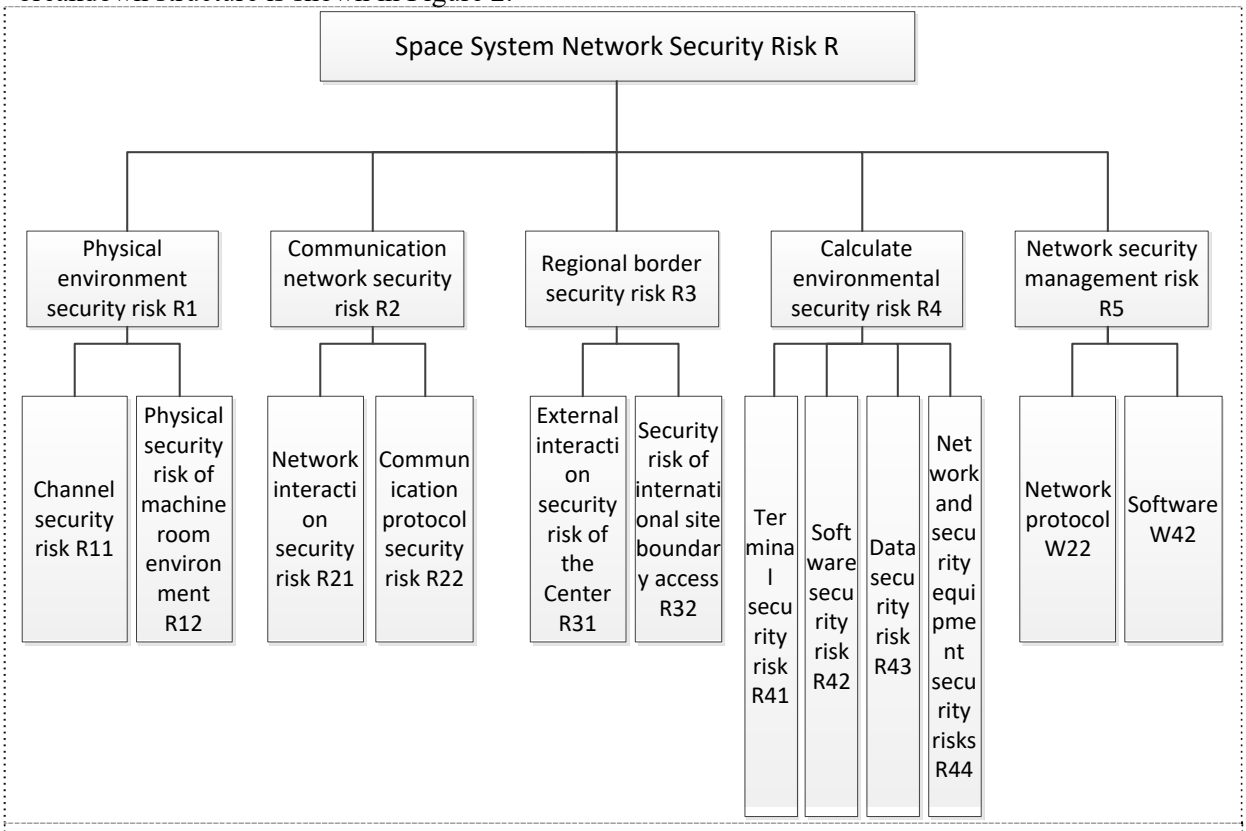

Figure 2 Risk decomposition structure of private network security RBS in the aerospace field

2.3. Build WBS-RBS safety risk index coupling matrix

The WBS work breakdown structure and RBS risk breakdown structure of the special network security are coupled in the aerospace field, whether the coupled basic element elements have security risks is judged, the risk sources and representative risk points are determined through analysis, and the WBS-RBS security risk index coupling matrix of the special network is constructed in the aerospace field, as shown in Table 1.

Table 1 WBS-RBS security risk index coupling matrix of the special network in the aerospace field

Elements of work / Risk Factor		W1		W2		W3	W4		W5
		W11	W12	W21	W22	W3	W41	W42	W5
R1	R11	1	1	0	0	0	1	0	0
	R12	1	1	1	0	1	0	0	0
R2	R21	0	0	1	0	1	0	0	0
	R22	0	1	0	1	0	0	0	0
R3	R31	0	0	0	0	0	0	0	0
	R32	0	0	1	0	0	0	0	0
R4	R41	0	0	0	0	1	0	1	0
	R42	0	0	0	0	0	0	1	0
	R43	0	0	0	0	1	0	1	0
	R44	0	0	0	0	0	0	0	0
R5	R51	0	0	0	0	0	0	0	1
	R52	0	0	0	0	0	0	0	1

By summarizing and sorting out the identified security risk indicators, since the risks faced by various computer room environments are the same, W11/R12, W12/R12, W21/R12, and W3/R12 can be unified into the security risk indicators of the computer room environment; The security risk indicators of W3/R41 computer terminals and W42/R41 software operation terminals can be unified into the security risk indicators of computer terminals; The security risk indicators of W5/R51 network security operation and maintenance management and W5/R52 security protection equipment management can be consolidated into the security risk indicators of operation and maintenance management. After consolidation, there are 14 safety risk indicator elements, as shown in Table 2.

Table 2. Summary of Network Security Risk Indicator Elements

NO.	Elements of safety risk indicators
one	Safety risk indicators of ground circuit intrusion
two	Security risk indicators of satellite communication link being intercepted and counterfeited by electromagnetism
three	Safety risk indicators of various computer room environments
four	Security risk indicators without internal network isolation
five	Security risk indicators of network boundary not isolated
six	Security risk indicators of network protocols
seven	Security risk indicators of wireless channel protocols
eight	Security risk indicators of uncontrolled network access
nine	Security risk indicators of computer terminal security
ten	Safety risk indicators of software
eleven	Safety risk indicators for data transmission over the ground
twelve	Security risk indicators of data transmission through SATCOM
thirteen	Safety risk indicators of software data
fourteen	Security risk indicators of operation and maintenance management

3. The idea of building the security evaluation index system of the special network in the aerospace field

3.1. The idea of index system construction

To make the evaluation results objectively and truly reflect the security situation of the information system, the selection of evaluation indicators should, on the one hand, be based on the relevant national and industrial standards, and be subdivided into relevant inspection and evaluation items according to the standards, so that the evaluation indicators can effectively measure the compliance of the information system and judge whether it meets the basic standards. On the other hand, the selection of evaluation indicators should also consider the actual situation of the information system, which can objectively and truly reflect the key points and risk points in the network security work, so that the indicators can accurately judge whether the special network security system in the aerospace field can control the threats and hidden dangers and whether the business system, risk hidden dangers, and vulnerabilities can be protected.

1. Scientific principle. On the construction of the indicator system, it should be able to reflect the objective laws of the assessment object, scientifically reflect the level of network security of the assessed object and the potential risks, and objectively and comprehensively reflect the true relationship between the indicators.

2. Principle of typicality. The selection of evaluation indicators should reflect the comprehensive situation of the evaluation object and be representative. Especially in some cases, if the number of indicators needs to be reduced, it can also be easy to carry out data calculation, so that the credibility of the evaluation results will not be reduced [10].

3. Principle of practicality. In the design of evaluation indicators, special attention should be paid to the operability of the follow-up in practice. In particular, the indicator design needs to be able to quantify and compare, and unify the measurement unit and calculation method of indicators, so that it is very practical in the specific evaluation process.

In the systematic analysis and carding of this paper, there are many network-security factors and corresponding evaluation indicators. Therefore, to improve the efficiency of detection and evaluation and highlight key factors, this paper has summarized and combed the indicator content in combination with the OSM model, and referred to relevant theories and actual situations, to form a more objective and scientific detection and evaluation indicator system.

3.2. OSM model

The OSM model is an abbreviation for Object, Strategy, and Measure. By defining the research goal, understanding the target behavior path and indicator hierarchy, establishing the corresponding strategy, and disassembling the strategy tasks, we can obtain the required evaluation indicators. This model is usually used for the evaluation of enterprise management.

The traditional indicator system construction method is not targeted and is mainly oriented to compliance indicators. The construction of the special network security evaluation indicator system in the aerospace field can use the OSM model to map the risk points and indicator measures one by one, making the construction of the indicator system more targeted and the evaluation indicators more objective.

Based on the OSM model, the Object is the network security protection capability, and then the strategy and measure are layered for the research objectives. The bottom-up approach is adopted. First, the identified risk problems are used to determine the evaluation indicators from the risk perspective, and then the evaluation indicators are summarized to form strategies, and finally, the network security evaluation indicator system is formed [11].

3.3. Design of security evaluation index system for the special network in the aerospace field

Based on the above analysis results of special network security risk indicators in the aerospace field, combined with the OSM model, the bottom-up approach is adopted to start with the risk points and

formulate targeted evaluation indicators for different risk points. Then, according to the categories of evaluation indicators, the evaluation strategy is formed and the evaluation objectives are finally formed.

According to the security characteristics of the space TT&C system and the potential risks it faces, the security assessment system indicators and specific assessment items are sorted out. The content of the security indicators of the special network in the space field is preliminarily selected as shown in Table 3.

Table 3. Summary of network security indicators

NO.	Risk point	Corresponding evaluation index	Corresponding indicator category
1	Risk of ground circuit intrusion	Physical Access Control	Physical security
2		Ground circuit encryption	
3	Risk of electromagnetic interception and counterfeiting of SATCOM link	Electromagnetic protection of SATCOM circuit	
4		SATCOM link encryption	
5	Risks of various computer room environments	Machine room environment security	
6	Risk of no internal network isolation	Internal network isolation (VLAN division, ACL setting)	network security
7	Risk that the network boundary is not isolated	Boundary isolation (firewall, gateway)	
8	Risks of network protocols	Intrusion detection	
9	Risk of wireless channel protocol	Flow monitoring	
10	Risk of uncontrolled terminal network access	Terminal Access Control	Host security
11	Risk of computer terminal security	Localization rate of terminal	
12		Bug fix	
13		Virus killing	
14		Host control	
15	Software risks	Software code audit	Application security
16		Software Access Control	
17		Software vulnerability repair	
18	Risk of data transmission over the ground	Apply Encryption	
19	Risk of data transmission through SATCOM		
20	Risk of software data	Application Access Control	data security
21		Static data encryption	
22		Data operation audit	
23	Risks of network security operation and maintenance management	Personnel capacity	Mocha ITOM
24		Rules and regulations	

4. Instance application

The research results in this paper are applied to the security detection and evaluation of aerospace private networks. Based on the identified risk points and the corresponding evaluation indexes, the fuzzy comprehensive evaluation method and analytic hierarchy process are used to construct the

detection and evaluation model, and the network security detection and evaluation work is carried out. According to the analysis of the situation of detection and evaluation, the risk identified by the WBS-RBS method and the index system built on this basis can better evaluate the existing problems of network security, for the subsequent development of targeted reinforcement to provide a certain follow-up.

5. Conclusion

In this paper, the WBS-RBS method is used to decompose and identify the security risks existing in the special network in the aerospace field, and the identified multi-dimensional network security risk indicators are coupled into concrete indicator elements. Using the OSM hierarchical structure model, corresponding evaluation indicators are obtained by comparison one by one. Finally, a WBS-RBS-oriented approach to building the security risk analysis and evaluation indicator system for the special network in the aerospace field is proposed, It provides a reference for the subsequent construction of a complete network security detection and evaluation model and the development of risk assessment.

Acknowledgments:

First, I would like to thank my tutor Professor Xu Jihui for his painstaking efforts and frequent use of personal rest time on holidays to guide my thesis so that I can complete the thesis writing. Secondly, I would like to thank Yuan Shuai for his academic help. It is through the discussion with him that the paper is closer to the reality of the unit.

References:

[1] Zhang Xugao Research on information system security situation assessment based on interval matrix correction method [D]. Civil Aviation University of China, 2020. DOI: 10.27627/d.cnki.gzmhy.2020.000383

[2] Zhou Chao, Pan Ping, Huang Liang. Information Security Risk Assessment Based on Quantum Gate Circuit Neural Network [J]. Computer Engineering, 2018, 44 (12): 39-45. DOI: 10.19678/j.issn.1000-3428.0051383

[3] Cai Yue Research on the Construction and Application of Maritime Information System Security Assessment Model [D]. Beijing Jiaotong University, 2020. DOI: 10.26944/d.cnki.gbfju.2020.002771

[4] Xin Qian Research on Security Assessment of Civil Aviation Information System for Classification Protection [D]. Civil Aviation University of China, 2018

[5] Chen Zheyu, Lin Mingwei Hesitant fuzzy language envelope analysis model based on analytic hierarchy process and its application in edge node network security assessment [J]. Computer Application Research, 2021,38 (01): 209-214. DOI: 10.19734/j.issn.1001-3695.2019.09.0589

[6] Gao Yunyun Research on the Application of Data Mining Technology in the Evaluation and Decision of Network Security Classification Protection [D]. Beijing Jiaotong University, 2021. DOI: 10.26944/d.cnki.gbfju.2021.003167

[7] Zhang Chunjie Research on information security risk assessment technology of industrial control system based on game theory [D]. Changchun University of Technology, 2021. DOI: 10.27805/d. CNKI. GCC.2021.000610

[8] Zhao Chen Evaluation on Information Security System Construction of China Southern Airlines Dalian Branch Based on Fuzzy Comprehensive Evaluation [D]. East China Jiaotong University, 2020. DOI: 10.27147/d.cnki.ghdju.2020.000106

[9] Wang Yuhe Research on Industrial Control Network Security Assessment Method [D]. Harbin University of Technology, 2019

[10] Yao Yongzhang Research on the Evaluation Method and Application of the Standardized Construction of the Communist Youth League of an Enterprise [D]. Hunan University, 2014

[11] Li Ning, Wang Xiao, Yang Yu. Research on the Evaluation Method of Technical Standards for Electric Power Enterprises Based on Analytic Hierarchy Process [J]. China Standardization, 2017 (20): 32-34+38