Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080345

Risk Assessment Model of Information Security for Transportation Industry System Based on Risk Matrix

Zhao Xiangmo[1], *Dai Ming*[1,2], *Ren Shuai*[1,*], *Li Luyao*[1,2] *and Duan Zongtao*[1]

[1] School of Information Engineering, Chang'an University, Xi'an 710064, China
[2] China Transport Telecommunications and Information Center, Beijing 100011, China

Received: 16 Jun. 2013, Revised: 21 Oct. 2013, Accepted: 22 Oct. 2013
Published online: 1 May. 2014

Abstract: Risk assessment is a vital part of classification protection system for transportation industry system information security. In this paper, an information security risk assessment model based on risk matrix was put forward for heterogeneous-based transportation industry system. The risk matrix method was brought into assessment system. Then an accurate risk assessment model was constructed. In this model, there were three critical modules, such as expert 2-dimension matrix, Borda sequence and gray analytical hierarchy process. In this assessment system, qualitative analysis was firstly processed. Those three modules have quantitative feature, so the assessment results described by words before can be denoted by numbers. The final quantitative results were obtained by related equations. This model was put into practical application of transportation security decision support system for emergency response, and the application results indicate that this model can increase the objectivity of the assessment.

Keywords: heterogeneous-based system, transportation industry, risk assessment, risk matrix.

1 Introduction

Transportation industry system is a large-scale complex system with many sub-systems, such as marine traffic system, land traffic system, air traffic system and so on. Each sub-system , related with factors like persons, vehicles, enviroment and so on, includes large amount of data and should be estimated qualitatively for safety [1]. With the development of network informationization, there is an urgent need for transportation system information mangement risk assessment and classified protection. However, the transportation industry has suffered since its inception from a lack of accurate information safety management for its own diversification and heterogeneous structure. Recently years, there are many researchers having studied about security assessment for information and data management of transportation industry system or its sub-systems, but hardly anyone propose a classifiction assessment and protection model. Classification protection system for information security is an important aspect of national information security, and is also a political task for national security and social stability.With the rapid development of personal computer, mobile communicaton and internet technologies, information systems are widely used in all industries. Many industries have designed information security assessment systems according to their own characteristics. But information security classification protection system for transportation industry is still in the stage of exploration at present. There are many methods about the information security risk assessment nowadays. In general, it can be divided into qualitative analysis [2] and quantitative analysis [3, 4]. Qualitative analysis is the groundwork of assessment while it may influence the objectivity of the assessment. In order to increase objectivity of assessment, reasonable quantitative analysis methods based on qualitative analysis must be introduced. Working out a assessment model can play a key role in selecting a reasonable quantitative analysis. According to the reference retrieval, there are several assessment models, for instance, fuzzy reasoning, artificial neural network, Bayesian Network, and so on, but these methods emphasize qualitative assessment. In view of the shortages of transportation industry such as, heterogeneous, massive data and multistage interaction, an integrated information security risk assessment model was put forward based on risk matrix [5], Borda sequence [6] and gray analytical

* Corresponding author e-mail: maxwellren@qq.com

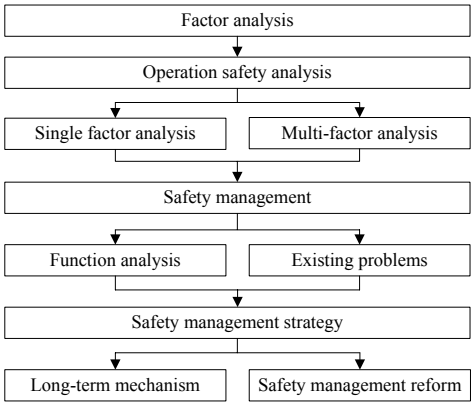

Fig. 1: The research technological route.

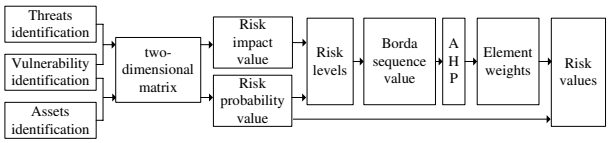

Fig. 2: Information security risk assessment model based on risk matrix.

Table 1: Risk matrix column for information security

Risks (R)	Risk probability (RP)		Risk impact (RI)	Risk level (RL)		Risk weight (RW)
	Quantization value	level		quantization value	level	

Table 2: Description of risk impact

Risk impact level	Definition or description
Critical (5)	failure of the whole project
Serious (4)	the serious decline of index
Ordinary (3)	the medium affect and part of the goal can be achieved
Tiny (2)	the low-grade affect and the objectives can be achieved
Negligible (1)	nearly cannot affect the project

Table 3: 7 risk elements and specific properties

Risk elements	Properties
Network application	network equipment, structure, service, operating and database system
Personnel	resource, security awareness, training, information access control and maintenance
Physical security	environment, equipment, electric cable, media
Asset	internal asset management framework, rights and liabilities of assets responsible persons
Strategy risk control	system standard, the third-level blanket document and process record, institutional framework
Management	operation, change control, abandon, system technology, public administration, laws
Organizational system	decision, management, executing

hierarchy process [7]. In this model, experts two-dimensional matrix method was used to deal with massive expert data. The risk elements of evaluated object was calculated quantitatively, and the Borda method and Analytical Hierarchy Process (AHP) [8] were used to work out the weight of each risk element. At last, the risk matrix was introduced to figure the risk level value of the evaluated object. Model proposed in this paper quatilizes the expert qualitative process, so the objectivity of assessment process can be improved, and the assessment results will be clear intuitive.

2 Risk assessment model of information security risk matrix

Before the assessment of transportation system information management by risk matrix, the technology roadmap was proposed as shown in Figure 1 based on qualitative analysis. During this process, the safety factors were summarized and the safety current situation and development trend was obtained.

Referring to the assessment criteria of information security in China, the foundation elements of information security risk assessment include threats, vulnerability and assets identification. On the base of international information security management practice standards GB 17859: 1999 [9], advantages of the characteristics of the risk matrix method were taken to put forward the risk assessment model of information security risk matrix, as shown in Figure 2.

In the assessment model mentioned above, construction of the risk matrix is the foundation work of the model. And the construction steps are as follows:

Step1: Make the list of the risk matrix column. According to the risk assessment model in Figure 2, the risk matrix for information security risk assessment was figured out. The specific columns are shown in Table 1. And according to the levels division rules of GB/T 20984-2007, the risk probability and risk impact are divided into 5 levels respectively. And the description of risk impact levels is shown in Table 2.

Step2: Determine risk elements. On the base of international information security management practice standard ISO/IEC 17799 and assessment criteria of information security in China, these 7 risk elements of information security were summed up; the specific content of each element is shown in Table 3.

Step3: Introduce details of risk column and impact column. To identify risk ranks, the risk occurrence rate and the risk influence should be firstly determined. According to the classification rules in GB/T 20984-2007 [10], we respectfully grade the risk occurrence rate and the risk influence into 5 levels [11]. Concerning levels of risk occurrence rate, the probability increased from level 1 to level 5. With regard to levels of risk impact, the influence degree increased from level 1 to level 5.

Table 4: Mapping of risk levels

RP (level)	RI (level)									
	1		2		3		4		5	
1	0.5	L-	1.0	L-	1.5	L	2.5	M	3.0	M
2	1.0	L-	1.0	L	2.0	L	2.5	M	3.5	H
3	1.5	L	1.5	L	3.0	M	3.0	M	4.0	H
4	2.5	M	3.0	M	3.0	M	3.5	H	4.5	H+
5	3.0	M	3.5	H	4.0	H	4.0	H+	5.0	H+

In order to determine the risk occurrence rate and the risk influence, threaten, vulnerability and assets should be respectfully identified. According to GB/T 20984-2007, threaten, vulnerability and assets were set into 5 levels, and defines them as: 5-very high, 4-high, 3-medium, 2-low, 1-very low. The risk occurrence rate P is determined by the threaten frequency T and the vulnerability severity V:

$$P = f_1(V,T) \tag{1}$$

The risk influence value I is determined by the fragility severity V and the asset value A:

$$I = f_2(V,A) \tag{2}$$

In Equation (1), $T = (t_1, t_2, ..., t_i, ...t_m)$ is positive integer. $V = (v_1, v_2, ..., v_j, ..., v_n)$, $1 \leq j \leq n$, and v_j is positive integer. In this paper, f_1 and f_2 symbolize expert two-dimensional matrix, in which data in the row represent vulnerability degree. In f_1, data in the column represents the occurrence frequency of threaten, while in f_2 means level of asset importance. Use these lines and rows to establish matrix, the values in the matrix are respectfully risk occurrence rate P and risk impact value I.

Because of the randomness of risk rate or risk impact based on the combination of different vulnerability and different threatens or asset value, the calculation of the data in the matrix does not have to follow a uniform formula. The calculation method is decided by experts, which is the first quantitative valuation link with qualitative characteristics.

In order to put risk rate P and risk impact I into risk matrix effectively, we divide the risk occurrence rate and the impact value into different levels specially. This is the second step in the assessment model and also the last quantitative valuation link with qualitative characteristics. The specific operation processes can be referred to the example part below.

Step4: Determine the risk level. According to GB/T 20984-2007, literature [12] and the determination of the risk probability and risk impact level in step3, we make a mapping table showed as Table 3, in which the numbers represent level quantification value, words mean level description. Put the risk probability and the risk impact level into Table 4, the risk level can be determined.

Step5: Determine the risk weight. The determination of weight is a key step to transform qualitative analysis to quantitative analysis. Because in the risk matrix there will be a risk tie (the risk elements which on the same risk level), we should firstly utilize Borda sequence method to rank risks in order of importance to remove the risk tie. Then we use Borda sequence value and AHP to work out the weight of each risk element.

1) The determination of Borda sequence value. Borda sequence value will give quantitative order according to the importance of evaluated elements. The specific method is: set N symbolizes total number of risk elements; i represent a particular risk, and k as a criterion. If r_{ik} stands for the risk level of i under criterion k, then the Borda value of risk i could be expressed by Equation (3)

$$b_i = \sum_{k=1}^{n} (N - r_{ik}) \tag{3}$$

2) The determination of weight based on AHP. As a relative value sequence, it is easy to establish an AHP estimation matrix using Borda sequence. And finally we calculate the weight of each risk element expressed as RW_i, the specific calculation steps are shown in the practical application below. So far, the construction of risk matrix is finished.

Step6: The comprehensive evaluation of information security. According to the final risk matrix, figure out the comprehensive information security risk level of the evaluated system by Equation (4), K is the number of risks.

$$RRT = \sum_{i=1}^{k} RR_i \times RW_i \tag{4}$$

3 Application of risk matrix in transportation industry system

According to the situation of the transportation industry system, the overall structure of transportation industry data and information management system can be constructed as Figure 3.

According to the information security risk assessment model based on risk matrix, we design a model for a sub-system in transportation industry system. This sub-system has undertaken mass data processing. The business of this sub-system relies heavily on the IT technology and computer network, and it has plenty of confidential data. The structure of the lab is shown in Figure 2. There are 8 steps of risk classification for this sub-system [13]:

Step1: Determine the risk matrix column (shown as Table 1) and risk elements (shown as Table 2).

Step2: According to the judgment of the specific business in this sub-system, evaluate its risk probability and impact. We should construct of expert two-dimension matrix f_1 and f_2 according to the rules as follows:

$$f_1 = \alpha t + \beta v \tag{5}$$

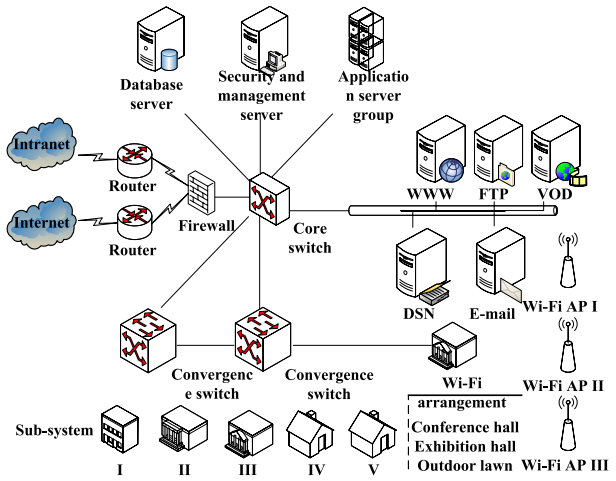

Fig. 3: Structure chart of transportation industry data and information management system.

Table 5: Risk probability calculation based on 2-dimensional matrix

$P=f_1(T,V)$		Vulnerability identifier V				
		1	2	3	4	5
Threaten identifier T	1	3	4	5	10	12
	2	5	6	7	12	14
	3	7	8	9	14	16
	4	13	14	15	20	22
	5	16	17	18	23	25

In Equation (5), $\alpha = \begin{cases} 2, & t \le 3 \\ 3, & 3 < t \le 5 \end{cases}$,
$\beta = \begin{cases} 1, & v \le 3 \\ 2, & 3 < v \le 5 \end{cases}$.

$$f_2 = \phi a + \varphi v \tag{6}$$

In Equation (6), $\phi = \begin{cases} 1, & a \le 2 \\ 2.5 & 2 < a \le 5 \end{cases}$,
$\varphi = \begin{cases} 2, & v \le 2 \\ 3, & 2 < v \le 5 \end{cases}$.

We express the risk matrix f_1 and f_2 as Table 4 and Table 5. According to the judgment of the specific business in lab, experts make an assessment for this sub-system. Taking one of seven risk elements, for example network application, the assessment result are vulnerability level is 2, threaten level is 4, asset identification level is 5. According to Table 5 and Table 6, we determine the risk occurrence rate of network application is 14; the value of risk impact is 16.5.

Step3: According to the above assessment standard of expert two-dimension matrix, the expert term create a specifically for compare table for the value in matrix, as shown in Table 7 and Table 8. The risk rate of network application belongs to level 3, the occurrence rate is 56%

Table 6: Risk impact calculation based on 2-dimensional matrix

$I=f_2(V,A)$		Vulnerability identifier V				
		1	2	3	4	5
Asset identifier A	1	3	5	10	13	16
	2	4	6	11	14	17
	3	9.5	11.5	16.5	19.5	22.5
	4	12	14	19	22	25
	5	14.5	16.5	21.5	24.5	27.5

Table 7: Classification of risk probability

Risk probability P	1~5	6~11	12~16	17~21	22~25
Risk probability levels	1	2	3	4	5

Table 8: Classification of risk impact

Risk impact I	1~5.5	6~11	12~15.5	16~22.5	23~27.5
Risk impact levels	1	2	3	4	5

Table 9: Information security risk matrix

Risks(R)	Risk probability(P)		Risk	Risk ranks(RR)		Risk
	quantization value	level	impact(I)	quantization value	level	weight(RW)
network	56	3	4	3.0	M	0.3877
personnel	16	1	4	2.5	M	0.1543
physica	80	4	2	3.0	M	0.0936
asset	4	1	3	1.5	L	0.0351
strategy control	20	1	4	2.5	M	0.2498
management	16	1	3	1.5	L	0.0568
organization	12	1	2	1.0	L-	0.0226

(the calculation should be followed Equation (7)). The risk impact belongs to level 4.

$$\Gamma = \frac{RP}{25} = \frac{14}{25} = 0.56 = 56\% \tag{7}$$

Step4: According to the qualitative analysis and quantitative calculation above, we get the risk probability level and risk impact level of network application, check table 3, and get final risk level of network application is 3, belongs to medium level.

For the same reason, the risk probability and impact level of other 6 risk elements in this sub-system can be obtained, and finally determine final risk level of each element. As the final risk matrix, Table 9 shows the related evaluation data.

Step5: According to the definition from Borda, there are 7 risk elements (N=7). Borda value of risk element i (i=1,2,7) is represented as b_i. There only two criterions related to risk matrix of information security risk: k=1 stands for the risk impact criterion I and k=2 stands for the risk probability criterion P.

Take network application for example, the risk impact level of network application is the highest, so $r_{11} = 0$, and

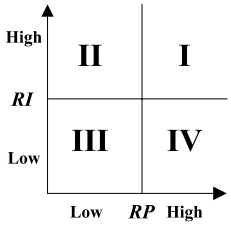

Fig. 4: Two-dimensional quadrant relation of seven risks.

the risk probability is only larger than one risk element called physics, so $r_{12} = 1$. The value of b_1 is:

$$b_1 = \sum_{k=1}^{2} (N - r_{ik}) = (7 - r_{11}) + (7 - r_{12}) \\ = (7-0) + (7-1) = 13 \quad (8)$$

With the same method, we get the Borda values of other 6 risk elements. At last, the Borda value of 7 risk elements are respectfully 13, 11, 9, 5, 12, 8, 4. Get the relative number through Borda value to determine the Borda sequence value, so they are: 0, 2, 3, 5, 1, 4, and 6.

At last, the two-dimensional quadrant method was used to show the quantitative relation between the seven risks. And the risk order of severity can be visualized as Figure 4.

The risks in quadrant I should be paid close attention from the management officers. Once these risks occur, the data management project could be paralyzed. The risks in quadrant II are of low probability, but once these risks occur, the project will be destroyed seriously. The risks in quadrant III are of both low probability and seriousness, and are not required of immediate measures. The risks in quadrant IV are of high probability and low seriousness, so the improvement or some control methods could be proposed to reduce the occurrence frequency of these risks.

4 Conclusion

We put forward the information security risk assessment model based on the risk matrix. And illustrate the procedure of risk assessment by the risk matrix for transportation industry system. In assessment process, we use Borda sequence method of two-dimensional matrix, and AHP to obtain risk levels. Based on the traditional evaluation process, we greatly adopt quantitative calculation to reduce the loss brought by the human error. This algorithm is of clear steps and good practicability. The simulation experiments show that our assessment model can effectively evaluate the most common risks of transportation industry system. Security investigation experts are full of praise for the results of our models.

Acknowledgments

Our research was funded by many Projects, and the names and numbers of these Projects are as follows: 1. The National Natural Science Foundation of China (Grant No. 51278058). 2. The Program for Changjiang Scholars and Innovative Research Team (Grant No. IRT0951). 3. National IOT Project Major Demonstration Projects (Grant No. 2012-364-208-205 and 2012-364-812-105). 4. The State 863 Project (Grant No. 2012AA112312). 5. The Ministry of Transport of the People?s Republic of China Project (Grant No. 2012-364-208-600, 2012-364-208-200 and 201231849A70). 6. Jilin Province Association for International Exchange of Personnel Project (Grant No. 2012-7-102-2). 7. The Special Fund for Basic Scientific Research of Central Colleges of Chang?an University (Grant No. 2013G1241118 and 2013G2241020). 8. Xi?an Science and Technology Project (Grant No. CXY1318). 9. The Fund from Xi?an Red Sun Company (Grant No. XARESUN2013090101). 10. Basic Research Project of Shaanxi Province Natural Science Foundation (Grant No. 2013JM8018). 10. The National Natural Science Foundation of China (Grant No. 61303041).

References

[1] Jacobs, I.M.; Salmasi, A.; Bernard, T.J. The application of a novel two-way mobile satellite communications and vehicle tracking system to the transportation industry, IEEE Transactions on Vehicular Technology, **40**, 57-63 (1991).

[2] Andersen, S.; Mostue, B.A.. "Risk analysis and risk management approaches applied to the petroleum industry and their applicability to IO concepts", SAFETY SCIENCE, **50**, 2010-2019 (2012).

[3] Feali, M.;Pinczewski, W. V.; Cinar, Y., et al. Qualitative and Quantitative Analyses of the Three-Phase Distribution of Oil, Water, and Gas in Bentheimer Sandstone by Use of Micro-CT Imaging, SPE RESERVOIR EVALUATION and ENGINEERING, **15**, 706-711 (2013).

[4] S. W. Yoona,; J. D. Velasqueza; B. K. Partridgeb; S.Y. Nofa. Transportation security decision support system for emergency response: A training prototype, Decision Support Systems, **46**, 139-148 (2008).

[5] Larrosa, D.; Casaravilla, G.; Chaer, R.. Evaluation of contractual arrangement of new energy sources for generation expansion in Uruguay and its impact on the risk matrix of the utility costs, 6th IEEE/PES Transmission and Distribution - Latin America Conference and Exposition (TandD-LA), Montevideo, URUGUAY, (2012)

[6] Zhang T.; MU D.J.; REN S.. Risk assessment model of information security based on risk matrix, ,Computer Engineering and Applications, **46**, 93-95 (2010).

[7] Yang, H. J.; Meng, J.; Liu, Y.X. Effectiveness Evaluation on Material Modularity Storage and Transportation by Grey-Analytical Hierarchy Process. International Conference on Multimedia, Software Engineering and Computing, **129**, 9-13 (2011).

[8] Maitra, S.; Dominic, P.D.D.. IT Vendor Selection Model by Using Structural Equation Model and Analytical Hierarchy Process, PROCEEDINGS OF THE SIXTH GLOBAL CONFERENCE ON POWER CONTROL AND OPTIMIZATION, **1499**, 287-293 (2012).
[9] GB 17859: 1999, Classified criteria for security protection of computer information system [S].
[10] GB/T 20984-2007, Information security technology-Risk assessment specification for information security [S].
[11] Ji G.. Research on the Five-class Classification of Loans in China, Shandong University Masters Thesis, 23-32 (2008).
[12] Krause M., Tipton H. F. Information Security Management Handbook, Fifth Edition. Auerbach Publications, 223-252 (2003).
[13] Stephan M. Wagner. Innovation Management in the German Transportation Industry, Journal of Business Logistics, **29**, 215-231 (2008).

Zhao Xiangmo, was born on August, 1966 in Chongqing, China. He is professor and Doctoral tutor in Changan University. His research is focus on intelligent detection and fusion technology of traffic information, theory and application of intelligent transportation system. He has published 97 papers, including 66 SCI, EI and ISTP articles.

Dai Ming was born in Huangshan, Anhui Province in 1979.He received the B.Sc. degree in Applied Electronic Technology from Changan University, Shanxi, China in 1998 and the M.Sc. degree in Traffic Information Engineering and Control there in 2002. Dai has been serving Internationalisation Department of China Transport Telecommunications and Information Center ever since his graduation from college, and now works as Senior Telecommunication Engineer. His research interests include Intelligent Transportation and Information Security of Transportation Industry.

Ren Shuai obtained his PhD from Northwestern Polytechnical University of China in 2009. He is a lecture in School of Information Engineering in Chang'an University. He has been engaged in Information hiding and Network security for 7 years. He published 23 scientific research articles in international publications and 2 are cited by SCI, 7 are cited by EI. He has carried out 5 tasks to study a plan in all, won patent 2. During the last yearhe has written or co-edited for 5 textbooks.

Li Luyao was born in Harbin, Heilongjiang Province in 1965.She received the M.Sc. degree in Management of Engineering and Science from Harbin Institute of Technology, Heilongjiang, China in 2005. She supervised the Science and Technology Department of Heilongjiang Provincial Ministry of Transportation from 2005 to 2009 and worked as the deputy chief engineer in China Academy of Transportation Science. In year 2010, she was appointed as the director of Informationization Department of China Transport Telecommunications and Information Center. Her research interests include Informationization of Transportation Industry, Information Security and Intelligent Transportation.

Duan Zongtao received his Ph.D. from Northwestern Polytechnical University in 2006. He is currently an associate professor in the School of Information Engineering at Changan University. His research interests include intelligent transportation system, cloud computing and big data processing.