International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.73-84
http://dx.doi.org/10.14257/ijsia.2015.9.2.08

Information Systems Security Assessment Based on System Dynamics

Liu Wei, Cui Yong-feng* and Li Ya

College of Computer Science and Technology, Zhoukou Normal University, Zhoukou 466001, China
cuiyf@zknu.edu.cn

Abstract

With the rapid development of information technology, information systems security becomes more and more important for both national economics and people's everyday life. Therefore, in this paper, we study on the problem of information systems security assessment. However, existing traditional methods has two major issues. First, it is unclear that whether there remains severe potential risks unrecognized, and thus the reliability is limited. Second, the assessment results deviate from the real one due to the time and environmental restrictions, the subjective reasons of the researchers, or biased observed data, etc. To this end, we propose to leverage system dynamics (SD) for information systems security assessment. Specifically, based on the analysis of casual loops and positive and negative feedbacks among factors, we explore potential risks and capture those who are impossible to be measured using traditional methods.

Keywords*: Information systems security, System dynamics, Assessment model*

1. Introduction

With the rapid development of information technology, the dependence on information systems increases a lot in national economics and everyday life. For example, the publishment of national informatization leading group on strengthening information security work [1] shows the seriously attention of the government on the information systems security issues. Therefore, studying on the information systems security assessment is important for national construction and the development of information security strategy.

There are too many factors in information systems security assessment [2], and some of them is hard for quantitative description. There are some problems with existing methods for security assessment. First, since it is unclear that whether there remains severe potential risks unrecognized, the reliability is limited. Second, due to the time and environmental restrictions, or the subjective reasons of the researchers, there exist difference between the observed data and the real data, and therefore the results deviate.

To this end, we propose to leverage system dynamics (SD) for information systems security assessment. SD is a methodology and mathematical modeling technique for framing, understanding, and discussing complex issues and problems [3]. The behavior pattern of SD models is determined by the internal dynamic structure and positive and negative feedbacks. Compared to traditional methods, SD has the following advantages: (1) through the analysis of positive and negative feedbacks, SD can find potential risks; (2) the SD models can reveal

ISSN: 1738-9976 IJSIA

the important information of the current status of system, and capture risks that are impossible to be measured by traditional methods.

To remain of this paper is organized as follows. Section 2 discusses some related works, and Section 3 illustrates the concept of information systems security. In Section 4, we proposed our SD model for information systems security assessment. Then, we conduct a simple simulation to explore the effect of each subsystem of factors in Section 5. In the end, Section 6 concludes this paper.

2. Related Work

There are many methods for information security assessment. For example, Fault tree analysis (FTA) is a top down, deductive failure analysis for understanding system failure and reducing risks of a safety accident or a particular system level failure in safety engineering and reliability engineering [4]. Failure Mode and Effects Analysis (FMEA) [5] is a semantic technique for failure analysis by reviewing components, assemblies, and subsystems to identify failure modes, and their causes and effects. Hazard and operability study (HAZOP) [6] is a qualitative method by stimulating the imagination of participants to identify potential hazards and operability problems. Markov chain was also employed for quantitative system reliability modeling [7], where the overall failure process is described exactly and asymptotically for highly reliable sub-systems. Consultative Objective Risk Analysis System (CORAS) [8] is a tool-supported framework for precise, unambiguous, and efficient risk assessment of security critical systems, and has been applied successfully in telemedicine and telecommunications fields. Control objectives for information related technology (COBIT) [9] is a trusted open standard to help recognize the critical dependence of many business processes and manage risks effectively. Chorppath *et al.* [10] proposed a Risk-Rank algorithm for assessment of operational risk in the organization and a risk mitigation algorithm for finding the optimum set of measures under certain budget constraints. Liu *et al.* [11] designed an entropy based method to quantitatively assess the enterprise information system information risk. Based on existing research, we leverage SD to model information systems security risks, and analyze the casual relationships and feedbacks between factors.

Indeed, SD method has been applied in many fields. For example, Cheng *et al.* [12] presented the application of SD simulation into capturing the operation processes of the berth and yard. Hassan *et al.* [13] applied SD analysis on important energy policy issues. Suryani *et al.* [14] developed a SD model to forecast air passenger demand and to evaluate some policy scenarios related with runway and passenger terminal capacity expansion to meet the future demand. Stave *et al.* [15] introduced SD for sustainable environmental management. Fan *et al.* [16] studied the bullwhip effect caused in a military weapons maintenance supply system using SD approach. Melse *et al.* [17] employed SD for accounting system. Campuzano *et al.* [18] developed a SD model for supply chain simulation. Haase *et al.* [19] introduced SD simulation method for modeling urban systems. In this study, we use SD for information systems security assessment.

3. Concept of Information Systems Security

Information technology has brought dramatic changes, and play important roles in everyday life. The development of information industries has been a significant indicator of the national strength and international competitiveness of a country. However, the damages of information systems security issues are increasingly growing as well. Therefore, more and more attentions have been paid to the information systems security.

Specifically, the concept of information systems security has the following meanings.

(1) Confidentiality. After encrypted, information or data is transformed into cipher text, so that only authorized users with secret keys can decode the data. In this way, the confidentiality of information is ensured.

(2) Integrity. Attach specific information to the original data, so that the data integrity can be evaluated by the system. Only authorized users can commit add, delete and modify actions upon the data. Any illegal changes would be prevented to preserve the integrity.

(3) Availability. The system can provide services to authorized users for resources utilization. The goal is to avoid illegal rejections of accessing system resources and services.

(4) Authenticity. In order to prevent information from infected, anti-virus technologies are employed to monitor the internal system and data files.

According to Min *et al.* [20], information systems security risks are composed of five parts: origin, manner, channel, receptor and consequence. Origin is the source of threaten; manner is how the origin affects, typically represented as a series of threatening behaviors; channel is vulnerability threatens utilized to produce influences, such as leaks; receptor is the target of threatens, such as assets; and consequence is the influence and damage of risks. As illustrated in Figure 1, the origin of risks attacks the vulnerability of assets though some threaten behavior, and produces negative influence.

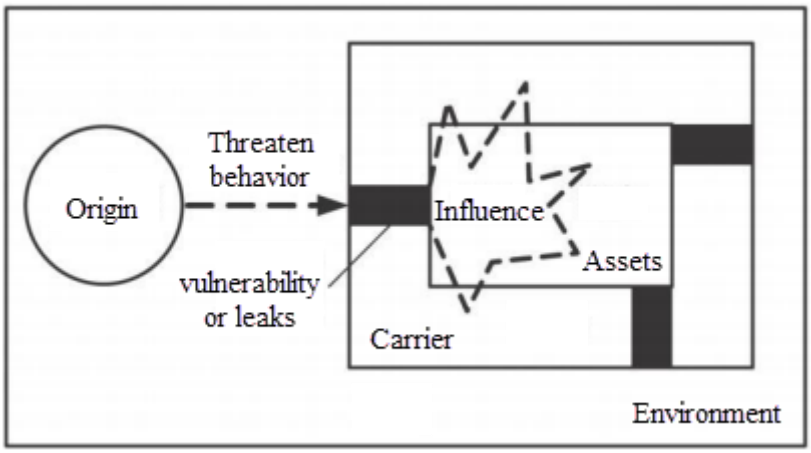

Figure 1. The Formation Mechanism of Information Systems Security Risks

Generally, information system security is a complex system engineering process. Other than technology issues, it also needs coordination of law and management factors. Therefore, the model of information systems security is a multi-layered structure, as shown in Figure 2. The lower layers provide support for upper layers, and upper layers rely on lower layers.

Typically, threatens of information systems security could be caused by deliberate or accidental factors, including:

(1) Human threaten: including deliberate destroy, such as network attacks, malicious code spread, mail bomb and unauthorized access; and unintentional mistakes, such as incorrect operation and carelessness maintenance error.

(2) System threatens: including failures of system, network and service, such as software and hardware failures, and database corruption.

(3) Environmental threaten: fire, vibration, electromagnetic interference, dust, floods, earthquakes, lightning, etc.

(4) Manage mental threaten: including defects in strategy, programming, principles, consciousness of staff, and organizational structure.

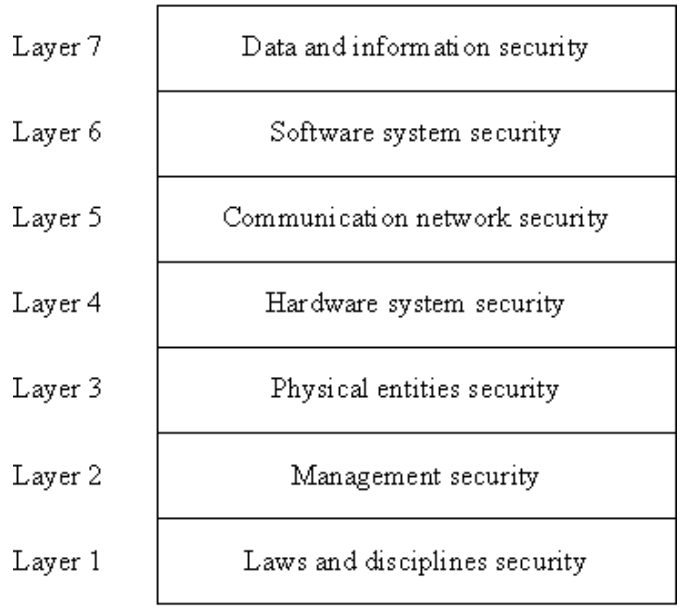

Figure 2. Multi-layer Model of Information Systems Security

Therefore, we divide the information system security into five components: hardware system security, software system security, environment security, data security and human security. Specifically, hardware system security factors include device failures, upgrade, design, settings and functions; software systems security factors include vulnerability of network system, databased system and TCP/IP protocol; environment security factors include fire, vibration, electromagnetic interference, dust and natural disasters; data security factors include data transmission, transmission media, and data sharing; human security factors include incorrect operations, personal capability and responsibility, artificial damage and software failure.

4. SD Analysis for Information Systems Security

System dynamics (SD) is a method for studying and analyzing the system in a quantitative way through causal loop diagrams. A system is composed of interrelated and interactive

elements, and the connections and relationship between elements can be described as causality. Therefore, the core of SD model is to identify a set of elements and determine the causal relationship between them.

Based on the previous analysis, we have five subsystems for information systems security risk: hardware system risk subsystem, software system risk subsystem, environment risk subsystem, data risk subsystem and human risk subsystem. Each subsystem has its own structure, and they have connections between each other. The key factors of each subsystem are described through a set of indicators, as shown in Table 1.

Table 1. Indicators of Information Systems Security

Level 1	**Level 2**	**Level 3**
Information systems security risk	Environment risk	Fire
		Vibration
		Dust
		Electromagnetic interference
		Natural disasters
	Hardware system risk	System device failure
		Equipment performance
		Equipment upgrade
		Inappropriate design or settings
	Software system risk	TCP/IP flaw
		Network system vulnerability
		Database system security
	Human risk	Artificial damage
		Software failure
		Incorrect operation
		Carelessness
		Personal ability
		Responsibility
	Data risk	Transmission media
		Data transmission
		Resource sharing
		TCP/IP flaw

Along with the relationship between subsystems and the feedback principles of SD, we build a causal loop diagram for information system security risks in Figure 3.

The causal loops for hardware system risk are listed as follows.

Loop 1: Hardware system risk → + network system vulnerability → + software system risk

Loop 2: Hardware system risk → + network system vulnerability → + software system risk → + data risk → + software failure → + intentional human risk → + human risk

Loop 3: Hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + intentional human risk → + human risk

Loop 4: Hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + TCP/IP flaw → + software system risk

Loop 5: Hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + network system vulnerability → + software system risk

Loop 6: Hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + database system security → + software system risk

Loop 7: Hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + intentional human risk → + human risk→ + software system risk

Loop 8: Hardware system risk → + network system vulnerability → + software system risk → + data risk → + software failure → + intentional human risk → + human risk → + environment risk

Loop 9: Hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + intentional human risk → + human risk → + environment risk

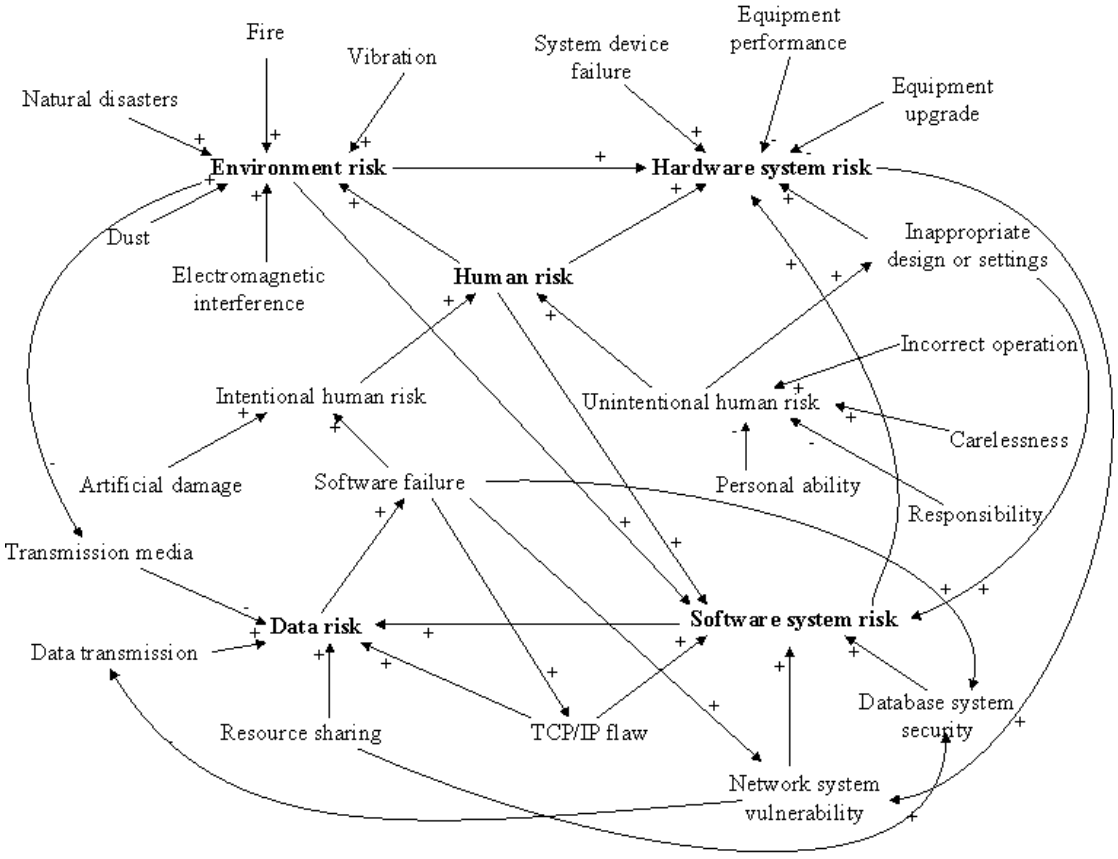

Figure 3. Casual Loop Diagram of Information Systems Security Risks

The causal loops for software system risk are as follows.

Loop 1: Software system risk → + hardware system risk → + network system vulnerability

Loop 2: Software system risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + TCP/IP flaw

Loop 3: Software system risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + network system vulnerability

Loop 4: Software system risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + database system security

Loop 5: Software system risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + intentional human risk → + human risk

Loop 6: Software system risk → + data risk → + software failure → + database system security

Loop 7: Software system risk → + data risk → + software failure → + intentional human risk → + human risk

Loop 8: Software system risk → + data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability

Loop 9: Software system risk → + data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + TCP/IP flaw

Loop 10: Software system risk → + data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + network system vulnerability

Loop 11: Software system risk → + data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + database system security

Loop 12: Software system risk → + data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability → - data transmission → + data risk → + software failure → + intentional human risk → + human risk

The causal loops for data risk are as follows.

Loop 1: Data risk → + software failure → + database system security → + software system risk

Loop 2: Data risk → + software failure → + TCP/IP flaw

Loop 3: Data risk → + software failure → + network system vulnerability → + software system risk

Loop 4: Data risk → + software failure → + network system vulnerability → - data transmission

Loop 5: Data risk → + software failure → + intentional human risk → + human risk → + software system risk

Loop 6: Data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability → - data transmission

Loop 7: Data risk → + software failure → + intentional human risk → + human risk → + hardware system risk → + network system vulnerability → + software system risk

Loop 8: Data risk → + software failure → + intentional human risk → + human risk → + environment risk → - transmission media

Loop 9: Data risk → + software failure → + intentional human risk → + human risk → + environment risk → + hardware system risk → + network system vulnerability → - data transmission

Loop 10: Data risk → + software failure → + intentional human risk → + human risk → + environment risk → + hardware system risk → + network system vulnerability → + software system risk

Loop 11: Data risk → + software failure → + database system security → + software system risk → + hardware system risk → + network system vulnerability → - data transmission

Loop 12: Data risk → + software failure → + intentional human risk → + human risk → + software system risk → + hardware system risk → + network system vulnerability → - data transmission

The causal loops for environment risk are as follows.

Loop 1: Environment risk → + hardware system risk → + network system vulnerability → + software system risk → + data risk → + software failure → + intentional human risk → + human risk

Loop 2: Environment risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk → + human risk

Loop 3: Environment risk → + software system risk → + data risk → + software failure → + intentional human risk → + human risk

Loop 4: Environment risk → + software system risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk → + human risk

Loop 5: Environment risk → - transmission media → - data risk → + software failure → + intentional human risk → + human risk

The causal loops for human risk are as follows.

Loop 1: Human risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk

Loop 2: Human risk → + hardware system risk → + network system vulnerability →+ software system risk → + data risk → + software failure → + intentional human risk

Loop 3: Human risk → + software system risk → + data risk → + software failure → + intentional human risk

Loop 4: Human risk → + software system risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk

Loop 5: Human risk → + environment risk → - transmission media → - data risk → + software failure → + intentional human risk

Loop 6: Human risk → + environment risk → - transmission media → - data risk → + software failure → + TCP/IP flaw → + software system risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk

Loop 7: Human risk → + environment risk → - transmission media → - data risk → + software failure → + network vulnerability → + software system risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk

Loop 8: Human risk → + environment risk → - transmission media → - data risk → + software failure → + database system security → + software system risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk

Loop 9: Human risk → + environment risk → + software system risk → + data risk → + software failure → + intentional human risk

Loop 10: Human risk → + environment risk → + software system risk → + hardware system risk → + network system vulnerability → - data transmission + data risk → + software failure → + intentional human risk

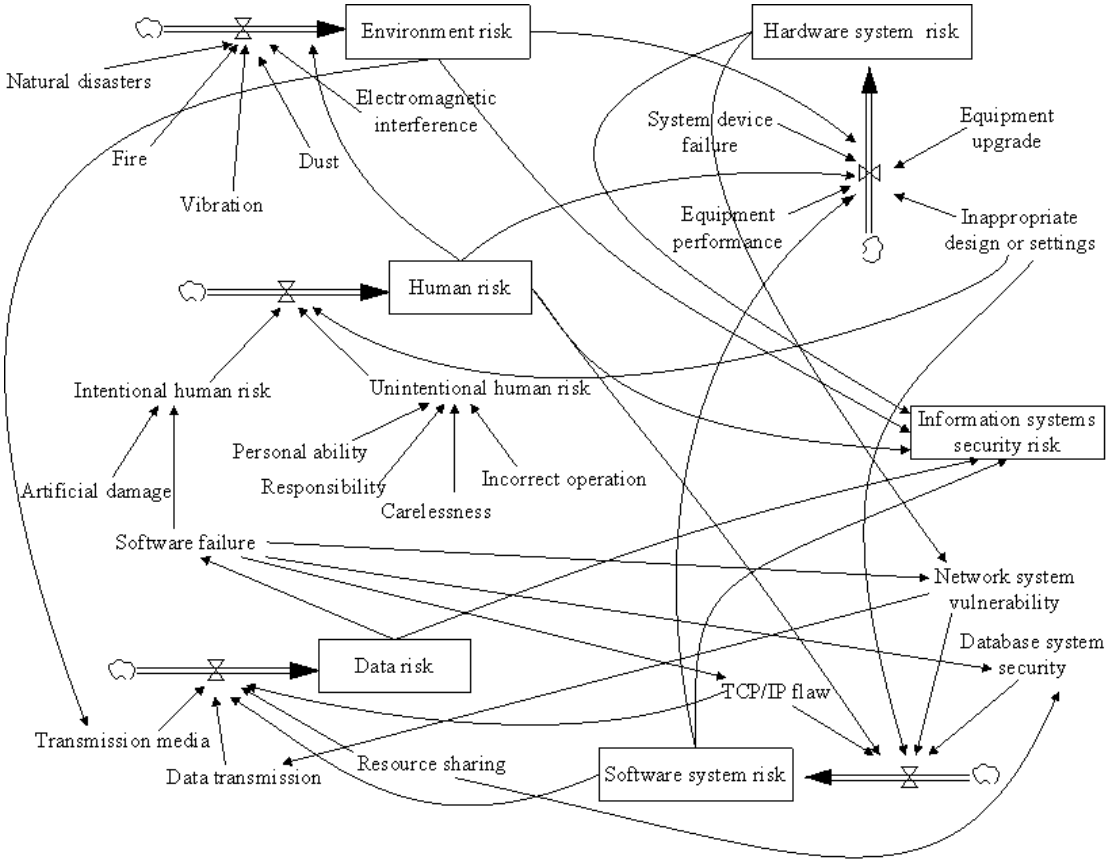

Figure 4. SD Model of Information Systems Security Risks

Moreover, based on above causal analysis, we construct the SD model in Figure 4. Let the security status of the system be $S = \{s_1, s_2, s_3, s_4\}$, where s_i denotes the security status of the systems, *i.e.*, excellent, good, normal, poor. The security status is determined by the grades given by domain experts.

The equation for system status is:

$$s = \sum v_i * w_i \quad (1)$$

Where v_i is the i-th indicators, and w_i is the weight, $\sum w_i = 1$. In our model, we have 23 indicators.

5. Simulation

We implement the SD model in VENSIM software based on Figure 3 and 4. We build a simple system with 2 PCs, 1 database server and 1 switch, as shown in Figure 5.

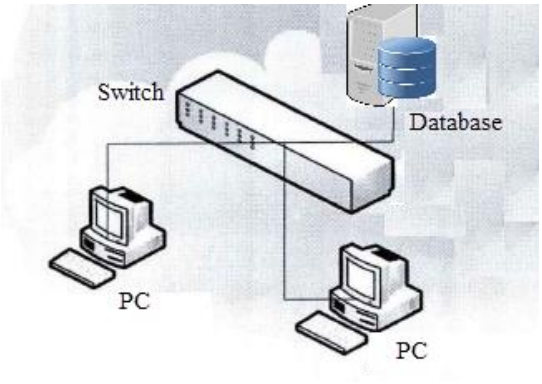

Figure 5. Simulation Environment

We monitor the system for 200 days, and simulate the security value from five aspects in Figure 6. We can observe that as the days pass by, the risk level of the system increases. Specifically, human risk is the most unstable one, while environment risk is relative stable. The reason is that human interference is unpredictable, and the external environment remains basically unchanged. Besides, hardware system risk, software system risk and data risk are increasing almost linearly with time.

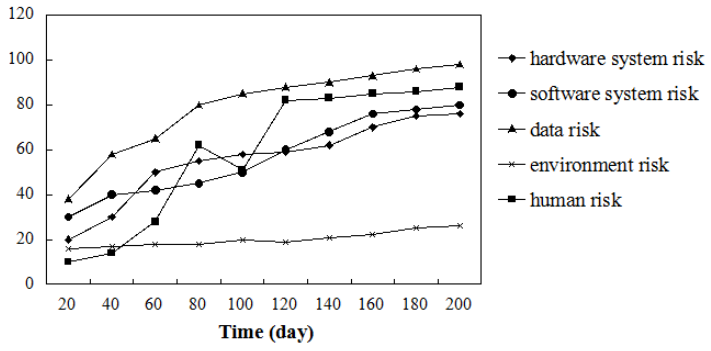

Figure 6. Simulation Results of Five Types of Risks

6. Conclusion

In this study, we employ system dynamics to analyze the information systems security assessment. Specifically, we build the casual loop diagram with a set of identified factors, and then construct the SD model to reveal the risk assessment model. However, the factors

identified in this paper are based upon existing efforts of information systems security assessment, which means the factors identification could be limited. In future works, we would explore comprehensive factors analysis and then extend our SD model.

References

[1] National Informatization Leading Group on strengthening information security work, (**2013**), http://www.hnsf.gov.cn/Item/8409.aspx

[2] T. R. Peltier, "Information security risk analysis", CRC press, (**2005**).

[3] M. J. Radzicki and R. A. Taylor, "Origin of system dynamics: Jay W. Forrester and the history of system dynamics", US Department of Energy's Introduction to System Dynamics, (**2008**).

[4] W.-S. Lee, "Fault Tree Analysis, Methods, and Applications: A Review", Reliability, IEEE Transactions on vol. 34, no. 3, (**1985**), pp. 194-203.

[5] D. H. Stamatis, "Failure mode and effect analysis: FMEA from theory to execution", Asq Press, (**2003**).

[6] J. Dunjó, "Hazard and operability (HAZOP) analysis, A literature review", Journal of hazardous materials vol. 173, no. 1, (**2010**), pp. 19-32.

[7] B. Littlewood, "A reliability model for systems with Markov structure", Applied Statistics, (**1975**), pp. 172-177.

[8] T. Dimitrakos, "Model-based security risk analysis for Web applications: The CORAS approach", Proceedings of the EuroWeb 2002 (**2002**).

[9] G. Ridley, J. Young and P. Carroll, "COBIT and its Utilization: A framework from the literature", System Sciences, 2004, Proceedings of the 37th Annual Hawaii International Conference on. IEEE, (**2004**).

[10] Chorppath, A. Kumar and T. Alpcan, "isk management for it security: When theory meets practice", New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on. IEEE, (**2012**).

[11] L. Yong, L. Qi and M. Kun, "A quantitative risk assessment of the safety of the enterprise information system information based on entropy", Computer Science, vol. 37, no. 5, (**2010**), pp. 45-48,56 (In Chinese)

[12] Cheng, J. Kie, R. M. Tahar and C.-L. Ang, "Understanding the complexity of container terminal operation through the development of system dynamics model", International Journal of Shipping and Transport Logistics, vol. 2, no. 4, (**2010**), pp. 429-443.

[13] Q.-U. Hassan and B. S. Seong, "How to do structural validity of a system dynamics type simulation model: the case of an energy policy model", Energy Policy, vol. 38, no. 5, (**2010**), pp. 2216-2224.

[14] E. Suryani, S.-Y. Chou and C.-H. Chen, "Air passenger demand forecasting and passenger terminal capacity expansion: A system dynamics framework", Expert Systems with Applications, vol. 37, no. 3, (**2010**), pp. 2324-2339.

[15] K. Stave, "Participatory system dynamics modeling for sustainable environmental management: Observations from four cases", Sustainability, vol. 2, no. 9, (**2010**), pp. 2762-2784.

[16] C.-Y. Fan, P.-S. Fan and P.-C. Chang, "A system dynamics modeling approach for a military weapon maintenance supply system", International Journal of Production Economics, vol. 128, no. 2, (**2010**), pp. 457-469.

[17] E. Melse, "The Financial Accounting Model from a System Dynamics' Perspective", (**2006**).

[18] F. Campuzano, J. Mula and D. Peidro, "Fuzzy estimations and system dynamics for improving supply chains", Fuzzy Sets and Systems, vol. 161, no. 11, (**2010**), pp. 1530-1542.

[19] D. Haase and N. Schwarz, "Simulation models on human-nature interactions in urban landscapes: a review including spatial economics, system dynamics, cellular automata and agentbased approaches", Living Reviews in Landscape Research, vol. 3, no. 2, (**2009**), pp. 1-45.

[20] J. Min, "Conceptual model of information system security and risk assessment models", Information Security and Communications Privacy, vol. 8, (**2004**), pp. 26-28. (In Chinese)

Authors

Wei Liu, He received the BS degree in computer science and technology from Henan Normal University and the MS degree in Computer Technology from The PLA Information Engineering University, China in 1996 and 2006 respectively. He is currently researching on Network Technology (NT) and Computer Application Technology (CAT).

Yongfeng Cui, He received the BS degree in Computer Science and Technology from Henan Normal University and the MS degree in Computer Application Technology from Huazhong University of Science and Technology, China in 2000 and 2007 respectively. He is currently researching on Computer Application Technology (CAT).

Ya Li, He received the BS degree in Computer Science and Technology from Northeast Normal University and the MS degree in Computer Technology from Beijing Jiaotong University, China in 1995 and 2005 respectively. He is currently researching on Computer Application Technology (CAT) and Mobile Internet Technology (MIT).