# CPS Information Security Risk Evaluation System Based on Petri Net

Yonggui FU
School of Information Management
ShanXi University of Finance and Economics
Taiyuan, China
School of Information
Central University of Finance and Economics
Beijing, China
sxcdfyg@163.com

Jianming ZHU
School of Information
Central University of Finance and Economics
Beijing, China
zjm@cufe.edu.cn

Sheng GAO
School of Information
Central University of Finance and Economics
Beijing, China
sgao@cufe.edu.cn

***Abstract*—Cyber Physical Systems(CPS) have achieved attention, research and applications from the governments, academic circles, industry circles of domestic and foreign, so, CPS have become an important content of China's two modernizations' deeply integration in future. Using Petri net model to describe CPS information security risk evaluation process. Colligating Petri net model analysis results and CPS information security risk evaluation related big data analysis results, to confirm CPS information security risk evaluation element index system and index weight value, and further by using RBF neural network model construct evaluation model to realize CPS information security risk's quantitative evaluation. The Petri net model constructed in the paper can realize the correlation relation analysis among CPS information security risk evaluation elements, and the description for system risk has the characteristics of temporality, integrity, diversification etc. The constructed index system and its weights have the characteristic of dynamic adaptability with the diversification of CPS information security risk evaluation related big data, that are according with the complexity and dynamic structure of CPS. The paper research has guide function to CPS information security risk evaluation, and has important practical significance and application value.**

***Keywords- Cyber Physical Systems; Information Security; Risk Evaluation; System Construction***

## I. INTRODUCTION

With the gradually deepening of two modernization integration guiding ideology, and the development of intelligence sensing, pervasive computing, wireless communication technology, large-scale data processing technology etc, the traditional physical system gradually integrates computing, control, remote collaboration, communication etc functions, forming the Cyber Physical Systems (CPS) that integrate communication, computation, and control as a whole [1-3].

CPS was first proposed by the American scientist Helen Gill in 2006, since it had proposed, CPS has get high attention from each country's governments, academic circles, and industry circles. "American Competitiveness Initiative" that published by American in February 2006 had listed CPS as an important research project. In July 2007, American President's Council of Advisors on Science and Technology (PCAST) in the report "Leadership Under Challenge: Information Technology Research & Development in a Competitive World" had listed CPS as the top of eight key information technology. In 2007 European Union started the project "Advanced Research & Technology for Embedded Intelligence and Systems" (ARTEMIS), in the project CPS as an important research direction of intelligence system. In Japan and South Korea etc countries, CPS have also get high attention, such as since 2008 the Korea Institute of Science and Technology tried to set up the correlated courses on CPS content. In China, with the gradually deepening of the two modernization integration, the country has in succession issued a series of documents, such as, in December 2011 State Council issued "Industrial Transformation and Update Programming (2011-2015)", in August 2013 Ministry of Industry and Information Technology issued "Informatization and Industrialization Depth Integration Special Action Plan (2013-2018)", in January 2014 Ministry of Industry and Information Technology issued "Informatization and Industrialization Integration Management System, Requirement" (Trial), in May 2015 State Council issued "Made in China 2025", in August 2016 Ministry of Industry and Information Technology issued "Intelligence Manufacture Engineering Implementation Guidance (2016-2020)" etc., all these reflect the country's high attention on CPS, especially in the "industry 4.0" that is the fourth industry revolution based on

978-1-5386-1600-0/17 $31.00 © 2017 IEEE
DOI 10.1109/DSC.2017.65

intelligence manufacturing, the country has proposed new requirements on CPS application.

With the deepening of CPS research and application, CPS has formed different architectures in different fields, and then formed different definitions. Thereinto, CPS proposer Helen Gill think: Cyber-Physical Systems are physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is deeply embedded into every physical component, possibly even into materials. The computational core is an embedded system, usually demands real-time response, and is most often distributed[4]. The United States National Natural Science Foundation Committee (NSF) think: CPS are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components[5]. Basing on the existing CPS definitions, the paper think: CPS are an integrating human, systems and physical equipment as a whole network "human-systems-physical equipment" comprehensive systems that on the basis of computer technology, network technology, communication technology etc technology, at the same time integrating management science, control theory etc ideological system, CPS operation objects are realizing the intelligent dynamic and real-time interaction among information systems and physical equipment. Therefore, with the development of cloud computing, big data, artificial intelligence, mobile computing etc technologies, CPS are also developing constantly.

Compared with the other network system or embedded system, CPS pay more attention to the whole systems' intelligent integration collaborative automation, each physical component of CPS has stronger communication ability and information processing ability [3], CPS are the combination of modern computer management system with artificial intelligence and network communication, focusing on resources' efficient dynamic organization and real-time coordinate allocation [3]. Compared with Internet of things, the "things" in Internet of things only communicate with the servers, while the "things" in CPS can communicate with each other, so, CPS own stronger intelligence, control ability and automation ability, and pay attention to human's participation. Therefore, CPS reflect the massive data computing power of things in system, are the fat C/S mode, and the Internet of things can be regarded as the thin C/S mode.

Therefore, CPS' architecture include application layer (application entity environment, user terminal, human, etc.), collaborative processing layer (cloud computing platform, network processing platform, etc.), network layer (Internet, industry private network, the third party network, etc.) and physical layer (control center, perceiving center, physical world, etc.) [6]. From CPS own intelligent control and data interaction perspective, CPS have closeness, from the system inclusion perspective, CPS have the extendibility of function and architecture. The architecture of CPS is shown in Figure 1.

At present, the application research on CPS include CPS application research in the concrete fields, CPS data management, CPS virtual simulation system construction, CPS and cloud platform combination, CPS information security, etc.

CPS research in the concrete fields involve industrial control (such as ref [7-9]), aerospace (such as ref [10-12]), health care (such as ref [13,14]), intelligent life (such as ref [15, 16]) etc extensive fields. The existing research results mainly from the concrete fields' physical topology structure construction, data interaction relation analysis, simulation etc aspects to start, at the same time analyzing the concrete fields' CPS application value. Some research are on analyzing CPS data management, these research mainly illustrate CPS will generate big data, the effective management for these big data will help to improve the concrete CPS management and decision level [17-19].

In the construction of CPS virtual simulation system, the researchers intended to construct a simulation system on CPS, explained the operation principle of CPS, helped the other researchers have an image cognition on CPS, and promoted the real CPS construction (such as ref [20-22]). In combining cloud platform to research CPS, the researchers focused on analyzing the application promotion and value realization's upgrading function of cloud computing technology to CPS, emphasizing the cloud platform is an indispensable component part in the application of CPS (such as ref [23,24]). In CPS information security, some research are on CPS vulnerability analysis (such as ref [25-27]), some research are on CPS attack identification, evaluation analysis (such as ref [28-30]), and also some research are on CPS information security risk evaluation research (such as ref [1, 31,32]).

In addition, still some research are on the algorithm design in CPS environment, CPS value analysis, etc., here no longer enumerate one by one.

As a complex network system, data communication is an important component part of CPS, we can't simply use physical isolation method to realize CPS information security protection, so, compared with the other information systems, CPS information security problem is more prominent, in fact in the operation process CPS exactly encountered bigger security threats than traditional information system, and have get high attention from experts and users. In China, in "Informatization and Industrialization Integration Management System, Requirement" (Trial), data, technology, organization structure, business process as the four basic elements of informatization era two modernization integration to promote enterprise innovation, in the four elements, data become the enterprise's core element, at the same time, capital investment, talent guarantee, equipment and facilities, information resources and information security as the basic guarantee of two modernization integration. So, data and information security become the core content of "Informatization and Industrialization Integration Management System, Requirement" (Trial). Therefore, information security is the key for the great development of CPS, basing on CPS architecture and businesses, data stream characteristics to construct CPS information security risk evaluation system is very necessary.

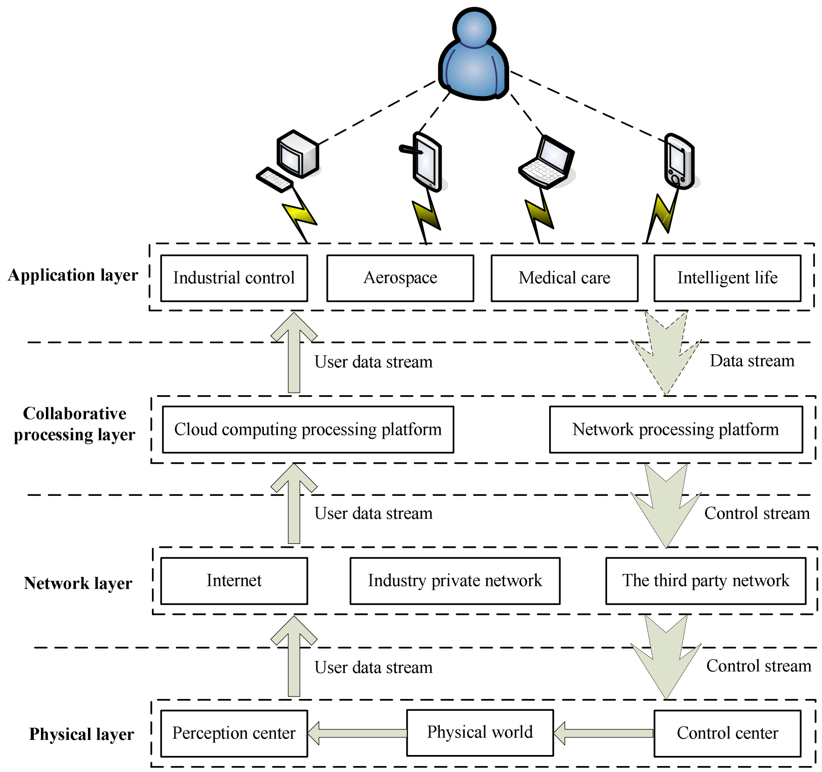


Figure 1. The system architecture of CPS

## II. THE SYSTEM FOR CPS INFORMATION SECURITY RISK EVALUATION

In the light of the characteristics of CPS information security risk evaluation, we can't use simple qualitative analysis method to achieve CPS information security risk evaluation, because the description of qualitative analysis to CPS information security risks is not accurate and meticulous enough. At the same time we also can't use simple quantitative analysis method to achieve CPS information security risk evaluation, because quantitative analysis can't vividly describe the characteristics and the casual relationships of CPS information security risks.

Basing on this, the paper proposed the method of combining qualitative analysis and quantitative analysis to construct CPS information security risk evaluation technology system. Using Petri net model to describe the process of CPS information security risk evaluation, combining CPS information security risk evaluation related big data analysis results, by experts providing risk evaluation index system and each index's weight. By the Petri net model analysis results and information security risk evaluation related big data analysis results to achieve the sample CPS' risk value and each index value, using RBF neural network model to construct evaluation model to achieve the quantitative evaluation of the evaluated CPS information security risk. CPS information security risk evaluation technology architecture is shown in Figure 2.

In Figure 2, after filtering and arranging, each risk evaluation element of each subsystem's each asset in each sample CPS will constitute the initial index system of CPS information security risk evaluation (achieved by evaluation experts evaluating CPS (reflected in the Petri net model)), while the corresponding weight value (provided by evaluation experts by who colligating the results for evaluation experts evaluating CPS information security risk, the results for data analysis experts analyzing CPS information security risk evaluation related big data, the results for evaluation experts implementing fuzzy comprehensive evaluation), the final index system (provided by evaluation experts by who colligating the initial index system, and the results for data analysis experts analyzing CPS information security risk evaluation related big data), and the evaluation results (provided by evaluation experts by who colligating the results for evaluation experts evaluating CPS information security risk, the results for data analysis experts analyzing CPS information security risk evaluation related big data) will become the basis of constructing quantitative model for calculating other CPS information security risk evaluation results.

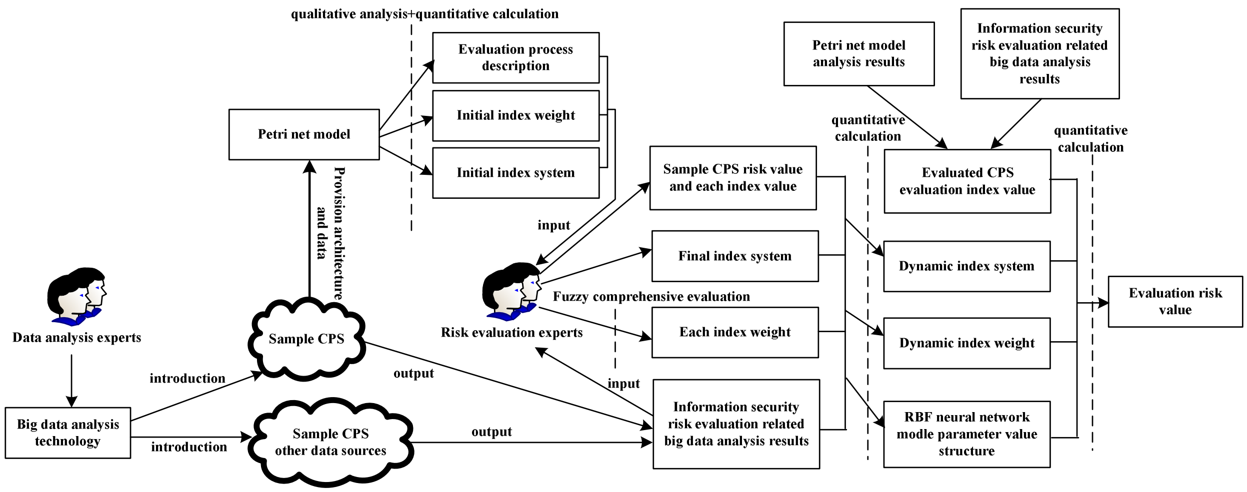


Figure 2. The technology architecture diagram for CPS information security risk evaluation

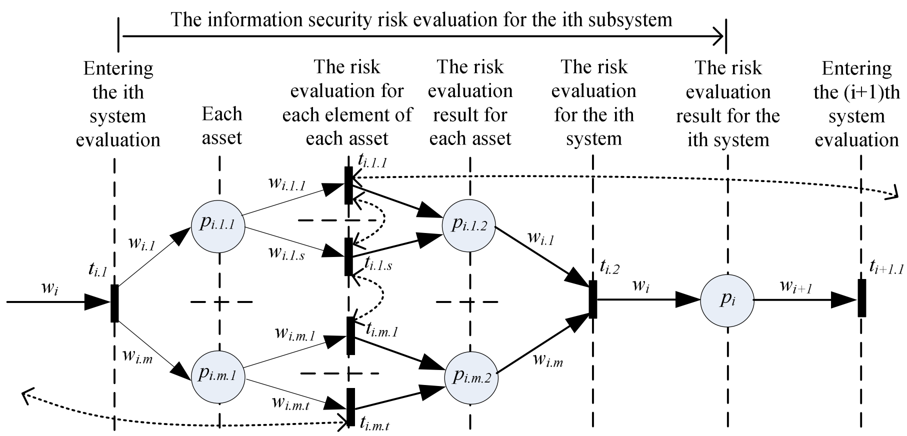


Figure 3. Petri net model for CPS information security risk evaluation process

*A. Petri net model for CPS information security risk evaluation*

Generally, fault tree and fault graph methods are used to describe the simple information security events of information system, while the two methods have serious deficiencies in describing the information security events of CPS complex information systems. Specific performance in:

- The fault tree can't describe the temporal logic multi-stage information security risk events, and can't describe the information security risk events with circular characteristics [33].
- The fault tree and fault graph are only the description for the fault events, and can't describe the structure of CPS risk assets and the correlation relations among different risk elements.
- The structure and the reflected information in fault tree and fault graph are more monotonous and rigid, can't well reflect the characteristics of risk assets and the severity of risk.
- The fault tree and fault graph can't well reflect the data stream and control stream of CPS, is not conducive to collect complete CPS risk information for analyzing.

Basing on the characteristics of CPS information security risk evaluation, the paper proposed using Petri net model for analyzing the process of CPS information security risk evaluation.

Petri net was proposed by Dr. Carl A. Petri in 1962, is a data method for describing the causality among computer system events [34]. Petri net has simulation function to system, can describe the data stream process, control stream process, and the data stream and control stream's trigger conditions in the system, in a Petri net model, we can describe multiple risk factors and their correlation relations for CPS information security risk evaluation. Petri net model has the characteristics of flexibility, refinement, extendibility and dynamicity etc., by using Petri net model we can comprehensively and systematically analyze the process, risk elements, evaluation results of CPS dynamic and real-time information security risk evaluation, and also can analyze the other information security risk management processes and element relations of CPS, at the same time, due to mathematics theory as the foundation, the description has high tightness and logicality.

For analyzing the process of CPS information security risk evaluation, defining a ten tuple as $ISRE = (P, T, F, D, I, O, M, \beta, \lambda, \omega)$. Thereinto, $P = (\cdots, P_1, \cdots, P_2, \cdots, P_k)$ represents "Place", $T = (t_{1.1}, \cdots, t_{1.2}, t_{2.1}, \cdots, t_{2.2}, \cdots, t_{n.2})$ represents "Transition", $F$ represents "Connection", $D = (\cdots, d_1, \cdots, d_2, \cdots, d_k)$ represents "a Finite Set of Propositions", $I(O)$ represents "Input(Output) Functions", $M(P_j)$ $(1 \leq j \leq k)$ represents "the Value of Place $P_j$ under $M$ Identification". $\beta$ represents "the Correlation Function between $P$ and $D$", and represents the "One-to-One Mapping between $P$ and $D$", that is, $\beta(P_j) = d_j$. $\lambda = (\lambda_{1.1}, \cdots, \lambda_{1.2}, \lambda_{2.1}, \cdots, \lambda_{2.2}, \cdots, \lambda_{n.2})$ represents the "Threshold (Trigger Condition) of Transition $t$". $\omega = (\cdots, \omega_1, \cdots, \omega_2, \cdots, \omega_k)$ represents "Weight Value", that is the importance of risk at all levels.

Basing on CPS information security risk evaluation process Petri net ten tuple definition, giving CPS information security risk evaluation process Petri net model structure is shown in Figure 3.

In Figure 3 the implications of "Transition" and "Place" are marked, in Figure 3, CPS are divided into different subsystems according to CPS' business process and physical structure, for each subsystem the risk evaluation is implemented one by one, the risk evaluation of each element of each subsystem's each asset include asset identification (availability, integrity, confidentiality), vulnerability identification (each vulnerability element), threat identification (each threat element), the element constitute for each asset risk evaluation is different, so the Petri net model structure of each subsystem is also different. In Figure 3, the risk elements of each subsystem's different assets may mutually have a certain risk correlation relations, the different assets of a same subsystem or the different elements of a same asset may also mutually have a certain risk correlation relations (marked with dashed lines in Figure 3).

For the risk evaluation result of each element of each subsystem's each asset, by its threshold deciding if the element should be implemented the corresponding security measures, so after CPS information security risk evaluation finishing, we will enter into the security rectification stage, and this stage can also be described with Petri net model. The definition for CPS security rectification process Petri net model can be constructed refer to the definition for CPS information security risk evaluation process Petri net model $ISRE = (P, T, F, D, I, O, M, \beta, \lambda, \omega)$, CPS security rectification process Petri net model is shown in Figure 4.

From Figure 4 we can see, if the evaluation result for some a risk element of some a subsystem's some an asset is greater than or equal to the threshold (that is the acceptable risk value) (in Figure 3 and in Figure 4, the implications of some symbols are different), we will implement the security measures, then enter into the next evaluated object (compared with the previous evaluated object, the next evaluated object may be the different risk element for the same asset, or the risk element for the same subsystem's different assets, or another subsystem's risk element), if the evaluation result is less than the threshold, we will directly enter into the next evaluated object.

In Figure 4, there implied a game relation on CPS having been implemented security measures and the attacker implement threats, and the result of CPS having been implemented security measures reflect in the expected utility of having been implemented security measures caused economic investment and not having been implemented security measures caused risk loss, and the result of the attacker implementing threats reflect in the expected utility of threat success caused profit and threat captured caused loss, so the process of the game reflect in CPS' and the attacker's respective expected utility game process.

In addition, the other information security risk management process for CPS can also be defined by the corresponding Petri net model, and there are some risks or data stream correlation relations among these Petri net models.

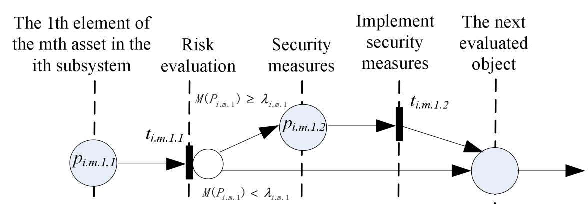


Figure 4. The security measure rectification process diagram for CPS

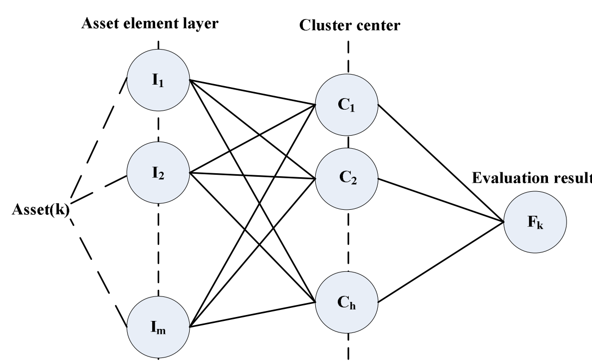


Figure 5. The structure of RBF neural network model

## B. Index system construction

By analyzing the information security risk evaluation process which described by Petri net model to construct CPS information security risk evaluation initial index system, the indexes are constructed according to the layered structure of "subsystem → asset → element", after the initial index system having been constructed, experts will analyze, check and revise the original index system, forming the revised index system, then with CPS information security risk evaluation related big data analysis results to further confirm the revised index system , in the end forming the final index system.

The index weight for CPS information security risk evaluation can achieve by colligating the information security risk evaluation process results described with Petri net model, and the importance score for each subsystem, each risk asset, each element index that provided by experts using fuzzy comprehensive evaluation method, on this basis further with the reflection of CPS information security risk evaluation related big data to each element information security risk importance, to verify and adjust each asset information security risk evaluation index element weight. Because the information content that reflected in big data are dynamically varied, so CPS' index system structure and the index weight are also real-time dynamically varied, this is suitable to the different requirements for the different periods of CPS information security risk evaluation.

In the construction of each asset information security risk element index system, with Petri net model analyzing the correlation of each element index, we can also carry out correlation analysis for the same profession's same type's several CPS' information security risk evaluation related big data, to achieve the element index information security risks' correlation degree (generally, the difference of information security risk evaluation related big data for different CPS is large, so this method need take care in the use), as the basis of adjusting the weight value.

## C. Evaluation model

Due to the complex of CPS' physical structure and business process, and the data stream and control stream are intertwined, so in computing CPS information security risk evaluation value using simple linear model is not suitable, therefore, the paper proposed using the current popular evaluation model-RBF neural network model to realize CPS information security risk's quantitative calculation, in the light of the weighted RBF neural network model is easier for approaching the true value of the evaluated object in evaluation calculation[35,36], the paper introduced risk element weight value in model construction. The structure of RBF neural network model is shown in Figure 5.

For explaining CPS information security risk evaluation RBF neural network model quantification calculation model, we define as following: $F(A_k) = \sum_{i=1}^{m}[\delta_i \exp(-\frac{1}{2\sigma_i^2}\|A_k - C_i\|^2) + b_i]$. Thereinto, $F(A_k)$ represents the result value for CPS information security risk evaluation. $\delta_i (i = 1,2,\cdots m)$ represents the connection weight value from the hidden layer to output layer. $A_k = [I_{k1}, I_{k2}, \cdots, I_{km}]$ represents each index constituted value vector for the kth asset's information security risk element index system, $C_i = [C_{i1}, C_{i2}, \cdots, C_{im}] (i = 1,2,\cdots h)$ represents cluster center. $\|A_k - C_i\| = \sqrt{w_1^2(I_{k1} - C_{i1})^2 + w_2^2(I_{k2} - C_{i2})^2 + \cdots + w_m^2(I_{km} - C_{im})^2}$ represents the Euclidean weighted distance between the asset element index value vector and cluster center. $w_t (1 \le t \le m)$ represents asset element index weight value. $\exp(-\frac{1}{2\sigma^2}\|A_k - C_i\|^2)$ represents RBF-kernel function, $\sigma_i$ represents the radius of kernel function, $b_i$ represents the adjustment parameter value of the output results.

For computing CPS information security risk evaluation value by using RBF neural network model, it need use multiple same physical structure and functional structure CPS' history same a period information security risk evaluation element index value and system risk evaluation result value as the training data (or use some a CPS multiple periods' information security risk evaluation element index value and system risk evaluation result value as the training data, we suggest this method try not to use), to achieve the parameter value structure for using RBF neural network model to calculate CPS information security risk evaluation result. Because of the complexity of CPS structure, sometimes we need construct different RBF neural network evaluation model for different subsystems, even we also need construct different RBF neural network evaluation model for different assets, then further summary calculating these evaluation result values.

# III. CONCLUSION

Due to the characteristics of complex, dynamic, risk correlation etc., CPS information security risk evaluation reflect more complex than the traditional system, which makes the simple qualitative model or quantitative model can't perfectly describe CPS information security risk evaluation process, evaluation results, and security measure implementation process. Basing on this, the paper used Petri net model realize the description of CPS information security risk evaluation process and security measure rectification process, proposed putting CPS information security risk evaluation into big data environment, combined big data analysis results and experts analysis results to construct the dynamic index system and index weight, and used the RBF neural network model construct the weighted evaluation model to realize CPS information security risk's quantitative evaluation.

The paper research are the construction of CPS information security risk evaluation system, and hasn't furthermore discussed the evaluation's implementation. In the implementation process, CPS information security risk evaluation will mainly face the following difficulties:

- Using Petri net model to describe the process of information security risk evaluation. Only by constructing objective and perfectly risk evaluation process guidance model can form the effective guidance for information security risk evaluation, although Petri net model can realize the dynamicity, correlation description to CPS information security risk evaluation, but because of the structure complexity of Petri net model, and need experts effectively mine the data relations and accurately grasp CPS information security risk, so the realization is difficult.

- The definition, collection, and analysis for CPS information security risk evaluation related big data. Because of the complexity, dynamicity, and extendibility of CPS structure, and the characteristics of big data structure alienation, data source much, etc, making how to define the range of CPS information security risk evaluation related big data becomes a difficulty, and the difficulty for data's collection and analysis also greatly increased.

In the future, we will realize CPS information security risk evaluation system, including the construction of cloud computing environment, the construction of evaluation process model and evaluation model.

## ACKNOWLEDGMENT

This work was supported by the Joint Founds of the National Natural Science Foundation of China under Grant U1509214, the National Natural Science Foundation of China under Grant 61602537, Beijing Municipal Philosophy and Social Science Foundation under Grant 16XCC023.

## REFERENCES

[1] Charalambos Konstantinou, Michail Maniatakos, Fareena Saqib, Shiyan Hu, Jim Plusquellic and Yier Jin. Cyber-Physical Systems: A Security Perspective. 2015 20th IEEE European Test Symposium (ETS),2015

[2] Teodora Sanislav, George Mois, Liviu Miclea. An approach to model dependability of cyber-physical systems. Microprocessors and Microsystems, 2016(41),pp. 67–76

[3] Zhongjie WANG , Lulu XIE. Cyber-physical Systems: A Survey. Acta Automatica Sinica,2011,37(10):1157-1165

[4] http://www.ima-zlw-ifu.rwth-aachen.de/fileadmin/user_upload/INSTITUTSCLUSTER/Publikation_Medien/Vortraege/download//CPS_27Feb2013.pdf

[5] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286

[6] Kan Zhang, Guangquan Zhang, Mingtai Zhang. A Preliminary Framework for Designing the Trusted Cyber-Physical Systems. Journal of Computer Research and Development, 2010,48(Z):242-246

[7] Xuefeng LEI.Research on Coal Washery and Production Scheduling of the System. Beijing: China Mining University Master Degree Candidate Dissertation, 2015

[8] Kleanthis Thramboulidis, Foivos Christoulak. UML4IoT—A UML-based approach to exploit IoT in cyber-physical manufacturing systems. Computers in Industry, 2016(82),pp. 259–272

[9] Andrea Bonci, Massimiliano Pirani, Sauro Longhi. A database-centric approach for the modeling, simulation and control of cyber-physical systems in the factory of the future. IFAC-Papers OnLine, 2016, 49(12), pp.249-254

[10] K. Sampigethaya, R. Poovendran, Cyber-physical integration in future aviation information systems. Digital Avionics Systems Conference, 2012.10, pp.7C2-1-7C2-12.

[11] K Sampigethaya, R Poovendran. Aviation cyber-physical systems: Foundations for future aircraft and air transport. Proceedings of the IEEE, 2013, 101(8),pp.1834-1855.

[12] Kyungmin Bae, Joshua Krisiloff, José Meseguer, Peter Csaba Ölveczky. Designing and verifying distributed cyber-physical systems using Multirate PALS: An airplane turning control system case study. Science of Computer Programming, 2015.6,pp.13–50

[13] C. Sankavaram, A. Kodali, K. Pattipati, An integrated health management process for automotive cyber-physical systems. IEEE Icnc International Workshop on Cyber-physical Systems, 2013, 12(9),pp.82-86

[14] G. Hackmann, W. Guo, G. Yan, Z. Sun, C. Lu, S. Dyke, Cyber-physical co-design of distributed structural health monitoring with wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1),pp.119-128

[15] Alexander Smirnov, Alexey Kashevnik, Andrew Ponomarev. Multi-level self-organization in cyber-physical-social systems: smart home cleaning scenario. Procedia CIRP, 2015(30),pp.329-334

[16] Christos G. Cassandras Smart Cities as Cyber-Physical Social Systems. Engineering, 2016,2 (2) ,pp.156–158

[17] Jeungeun Song, Yin Zhang, Kui Duan, M. Shamim Hossain,Sk Md Mizanur Rahman.TOLA: Topic-oriented learning assistance based on cyber-physical system and big data. Future Generation Computer Systems,2016.6,pp.1-5

[18] Zhiting Song, Yanming Sun, Jiafu Wan, Peipei Liang.Data quality management for service-oriented manufacturing cyber-physical systems. Computers and Electrical Engineering,2016.8, pp.1-11

[19] Radu F.Babiceanu, Remzi Seker.Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in Industry, 2016(81),pp.128–137

[20] Alessandro Beghi, Fabio Marcuzzi, Mirco Rampazzo.A Virtual Laboratory for the Prototyping of Cyber-Physical Systems. IFAC-PapersOnLine, 2016,49 (6) ,pp.63-68

[21] P. Hehenberger, B. Vogel-Heuser, D. Bradley, B. Eynard, T. Tomiyama, S. Achiche.Design, modelling, simulation and integration of cyber physical systems: Methods and applications. Computers in Industry,2016(82),pp.273–289

[22] Yuying WANG, Xingshe ZHOU, Dongfang LIANG. Heterogeneous model translation method for cyber physical system. Journal of Xidian University (Natural Science Edition), 2015,42(2):109-115

[23] Xuejun Yue, Hu Cai, Hehua Yan, Caifeng Zou, Keliang Zhou.Cloud-assisted industrial cyber-physical systems: An insight. Microprocessors and Microsystems, 2015, 39 (8),pp.1262-1270

[24] Rihab Chaari, Fatma Ellouze, Anis Kouböaa, Basit Qureshi,Nuno Pereira, Habib Youssef, Eduardo Tovar. Cyber-Physical Systems Clouds: A Survey. Computer Networks, 2016(108),pp.260–278

[25] Marina Krotofil etc al. Vulnerabilities of cyber-physical systems to stale data-Determining the optimal time to launch attacks. International Journal of Critical Infrastructure Protection,2014,7(4),pp.213-232

[26] S.Conti, A.La Corte, R.Nicolosi, S.A.Rizzo. Impact of cyber-physical system vulnerability, telecontrol system availability and islanding on distribution network reliability. Sustainable Energy, Grids and Networks, 2016 (6) ,pp.143-151

[27] Stefano Marrone, Ricardo J. Rodríguez, Roberto Nardone, Francesco Flammini,Valeria Vittorini. On synergies of cyber and physical security modelling in vulnerability assessment of railway systems. Computers and Electrical Engineering,2015(47),pp.275-285

[28] Hamed Orojloo, Mohammad Abdollahi Azgomi. A method for evaluating the consequence propagation of security attacks in cyber-physical systems. Future Generation Computer Systems, 2017(57),pp.57-71

[29] Stavros Ntalampiras. Automatic identification of integrity attacks in cyber-physical systems. Expert Systems With Applications, 2016 (58),pp.164–173

[30] Xin XU, Huiqun YU, Junhu HUANG. Petri net based security quantitative analysis model for cyber-physical system. Computer Engineering and Applications, 2014,50(3):82-88

[31] Yong Peng,Tianbo Lu,Jingli Liu. Cyber-Physical System Risk Assessment.2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013:442-447

[32] Hamed Orojloo , Mohammad Abdollahi Azgomi. A Method for Modeling and Evaluation of the Security of Cyber-Physical Systems. International Isc Conference on Information Security and Cryptology, 2014, 138(5):35-44

[33] Niandong LIAO. Research on the Dynamic Risk Assessment Model of Information Security. Beijing: Beijing Jiaotong University Doctoral Dissertation, 2009

[34] Zhibin JIANG. Petri net and its application in modeling and control of manufacturing system. Beijing: Machinery Industry Press,2004.5:21

[35] Yonggui FU. Jianming ZHU. Network Supplier Credit Evaluation Model Based on Big Data. Journal of Central University of Finance and Economics, 2016,(348):74-83

[36] Xiaoyan GUO, Ming ZHANG. Method of Personal Credit Evaluation of Bank Based on RBF Neural Network with Weight. Computer Engineering and Applications,2013,49(5):258-262