ISSN : 0974 - 7435 Volume 10 Issue 20

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(20), 2014 [11874-11882]

Review on information Security risk assessment

Ren Shuai [1]*, Lou Zong-Zong [1], Zhang Tao [2], Mu De-Jun [3]
[1]School of Information Engineering, Chang'an University, Xi'an, (CHINA)
[2]School of Electronic Control Engineering, Chang'an University, Xi'an, (CHINA)
[3]School of Automation, Northwestern Polytechnical University, Xi'an, (CHINA)
Email:maxwellren@qq.com

ABSTRACT

Risk assessment of information security is the important evaluation methods and decision mechanism for construction of information safety assurance system in kinds of fields. It is also an important component in research of information security. In this paper, the domestic and foreign general development situation of information security risk assessment will be introduced, and the related methods will be classified and summarized. Based on the discussion on some typical assessment methods, the advantages and disadvantages, emphasis and the applied characteristics in accessing process of them are analyzed. As a conclusion, issues urgently need to be addressed for recent information security assessment is proposed.

KEYWORDS

Information security; Risk assessment; Assessment methods.

INTRODUCTION

With the rapid development of computer and Internet technology, information technology is used more widely. More and more business systems become open Internet-based systems, in which data exchanging among the various departments is becoming more frequently by the information network. And along with the development of openness of system and freedom of data accessing, the information of those systems and themselves face a variety of new threats and risks. It is necessary to analyze and assess the security of those systems and the potential threats. In the processing of analysis and assessment, the existence of security weaknesses in various information systems is exploited by intruders, and suffered increasingly threat. Therefore, the information security risk assessment has a certain necessity and urgency, and it is the key to ensure the healthy operation of information systems, it provide the necessary basis for decision making for the establishment of information system security system, information security risk assessment in information systems was given full attention in the national strategy[l].

The overall network security threat situation is very serious in recent years. Hackers tamper site, Trojans, spam, DDoS incidents remained high, and the peak period occurs from time to time. New threats continue to worsen, particularly Zombie and phishing is still on the rise. Information security is a dynamic process, which runs through the entire life cycle of information systems. The world's commonly used risk management approach to address security issues, risk management including two aspects of risk assessment and risk analysis. Risk management is an acceptable cost of identification, control, reduce or eliminate the process that may affect system security. Risks are avoided, transferred or reduced to an acceptable level through risk assessment to identify the size, through the development of information security control measures, appropriate control objectives and control methods to control risks. Information security should be run through the entire life cycle of information systems. The common study on risk management includes two aspects, such as risk analysis and assessment. According to the related research, objective and accurate assessment is an issue of crucial importance to system management and avoidance.

THE CONCEPT AND RELATED WORK OF INFORMATION SECURITY RISK ASSESSMENT

Information security risk assessment (ISRA for short), which should be run through the entire life cycle of information systems, is an integrated estimation process for some complicate systems. It is necessary to consider the costs and benefits before the assessment, and to understand the risks through the assessment of confidentiality, integrity and availability for system[1, 2]. After that, measures such as transfer, avoidance and confrontation will be employed to reduce risks in order to achieve the security objective.

The primary functions of information security risk assessment[3, 4] are as follows: (1) to analyze the threats to information systems and the existing fragile points; (2) to estimate the damage degree resulted by risk events; (3) to put forward some targeted safeguard procedures and rectification measures; (4) to guard against and defuse the risks in order to control the risks at a relatively acceptable low level.

With more than 40 years for the emergence and development of information security risk assessment, it begins quite early abroad. The United States is the country with the most laws and regulations for information security[5-9], such as the Computer Operational Environment Security Strategy Research Group organized by The US Department of Defense in 1967, Rainbow Project in 1980s, the Common Criteria (six countries, seven parties) in 1990s, the Federal Information Security Management Act at the beginning of twenty-first century, and a set of guidelines taking SP 800-37 as the core[10]. These laws and regulations show the well-established legal system of the US and can play a key role in safeguard and guidance of information security order for both the US and other countries in the whole world. BS7799, which was established by British Standards Institution, is the most representative information security management system standard internationally at present. Approved by ISO in 2000, it became ISO17799 formally and was widely accepted by many countries. Related research by other countries in Europe also made great advances in recent years. Member countries of European Community have developed dozens of related laws and regulations such as The Multi-media Law by Germany, Information Technology Security Assessment Criterion (ITSEC) and Law of Participation in International Information Communication, which have greatly accelerated the integration of European. In Asia, information security is also a highly focused issue for countries. The Information Military Revolution Manual was published by Japan Defense Agency in 2000. With a rapid development of information security field in China, several laws and regulations have been established, such as the Law on Guarding State Secrets introduced in 1988, RPC Security Statutes for Computer Information System issued in 1994, the Measures for the Administration of the Computer Information Network and Internet Security and Protection in 1997, Regulations on the Commercial Passwords in 1999, Division Criterion of Classified Protection for Computer Information Security called as GB-17859 in 1999, Prevention and Management Measures of Computer Virus in 2000, the Assessment Standards for Information Technology, Security Technology and Security of Information Technology called as GB/T-18336 in 2001, Guides for Information Security Risk Assessment in 2006, and so on.

TYPICAL METHODS FOR ISRA

According to related national policies, technology criterion, management requirement, professional standard and so on, four properties such as controllability, integrity, minimal impact and confidentiality will be considered during the risk assessment process. Assets, threats, vulnerability, security measures and risks are the basic elements, and business strategy, asset value, security incident and residual risk will be the basic attributes for the these four elements, and all of them are shown in Figure 1.

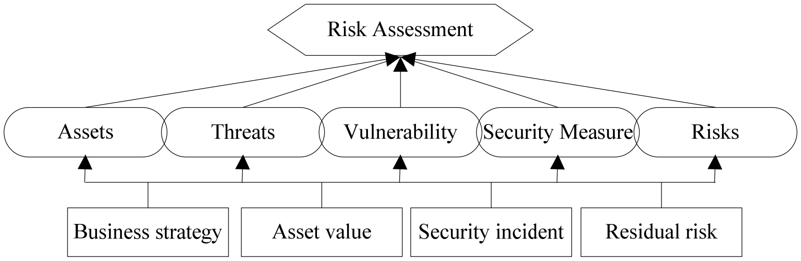

Figure 1 : Elements and attributes of ISRA

ISRA is a comprehensive evaluation process for complex system. It is necessary to carry out ISRA according to some commonly used technological process. The generally acknowledged process for several fields is shown in Figure 2.

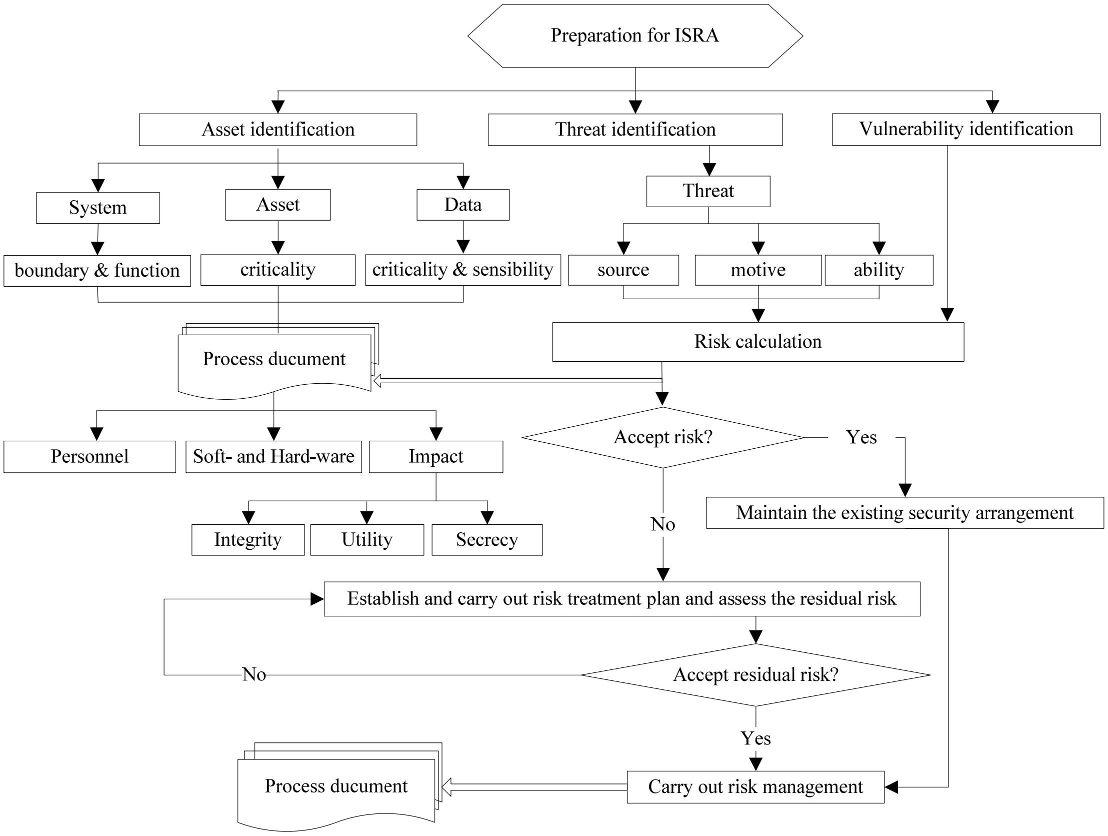

Figure 2 : Process of ISRA

There are many kinds of methods for ISRA. In general, these methods can be classified as qualitative-, quantitative-, and partial quantitative-based methods according to calculation method. Furthermore, they can be classified as tree- and dynamic system-based technologies according to implementation means. Some generalized and traditional risk assessment theories of international are listed in Figure 3.

Practically, ISRA should be realized by the combination of calculation methods and implementation means. The combination can be called as an integrated risk assessment method. Some typical risk assessment methods are introduced in the following sections.

FTA is a kind of effective Top-Down system analysis technology[11] based on the analysis result to hardware, software, environment and the human factor which can cause fault of system. And the logical relationship between the reason and result of fault event will be analyzed by deductive method and can be indicated by a hierarchical tree graph[12, 13]. Then the occurrence probability of these faults can be computed. The core processes[14, 15] and reference standards[16] are shown in Figure 4.

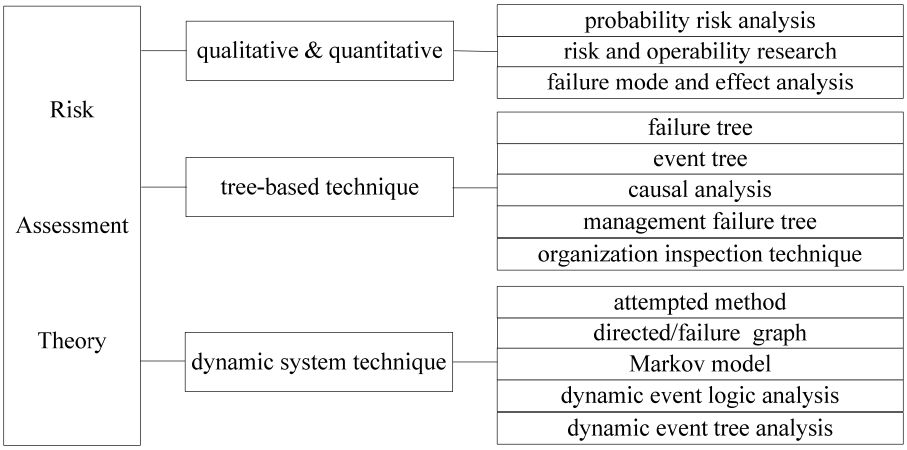
Risk
Assessment
Theory
qualitative & quantitative
probability risk analysis
risk and operability research
failure mode and effect analysis
tree-based technique
failure tree
event tree
causal analysis
management failure tree
organization inspection technique
dynamic system technique
attempted method
directed/failure graph
Markov model
dynamic event logic analysis
dynamic event tree analysis

Figure 3 : Some traditional ISRA theories

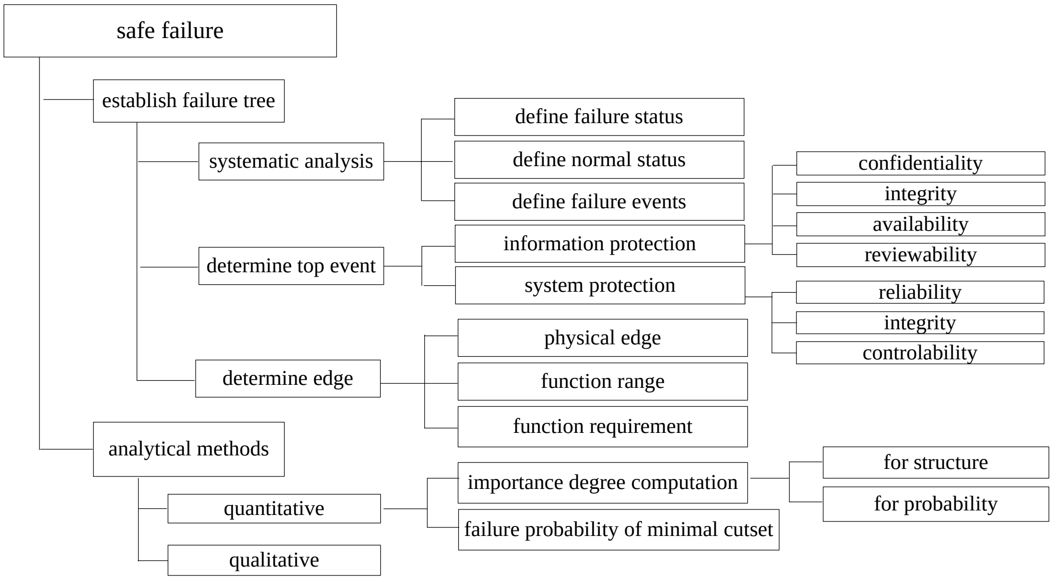

Figure 4 : Core contents of FTA

FTA can be classified as qualitative-, quantitative-based methods. It is the key content of qualitative-based methods to obtain all of the fault modes of the top event from the acquisition of minimal cutset. And the minimal cutset can be get through logical simplifying of the original fault tree by boolean algebra method.

In quantitative analysis process, the probability of top event can be obtained by logical relationship and given minimal cutset. Failure probability of bottom event x_i can be represented as $q_i(i=1,2,\cdots,n)$, in which n is the number of bottom events. And the probability of minimal cutset and top events can be respectively expressed as $P_1 = P(x_1 \cap x_2 \cap \cdots \cap x_m) = \prod_{i=1}^{m} q_i$ and $P(Top) = P(y_1 \cup y_2 \cup \cdots \cup y_k)$, in which y_i is one of the minimal cutsets and k is the number of minimal cutsets.

ETA, which is evolved from decision tree, is a kind of logical inductive method. It can track the developments of event and analyse the casual relationship among events over time from the original events. ETA can reflect the operating process dynamically and analyse information security system in order to give risk assessment.

Logically, event tree of information security can be classified as the contents in the first column of TABLE 1. In which, the original condition is used to describe the system status which can effect kinds of events; the original events can trigger failure; intermediate event is after the original event logically and cannot represent any failure; recovery act represents the response to prevent or reduce damage of failure; terminal event represents the different types and severity of failures.

During the process of ETA, security events will be put on the upper branch and treat events will be put on the under branch. Take policy changes as the example, the indication for the expression of event tree.

The total probability of system failure is the sum of probabilities for every event sequence, and probability of every sequence is the product of condition probabilities which are used to define the events of the sequence.

CCA[17] is the synthesis of FTA and ETA, which takes the failing initiating events and link events from ET as the top event of

FT to achieve FTA. The root of failure tree in CCA is the failure, and the leaves are the reasons for failure. By microanalysis to mechanism of the accident causes, safety arrangements to control the accidents can be found. But the root of event tree in CCA is the initiating event and leaves are the possible consequences. Dynamic analysis to dangerous events of system can be helpful to predict kinds of accidental results. Qualitative results of CCA are the true representation of information security accidents and can reflect the basic process of accidents.

TABLE 1 : The classification and description of ET

Classification	**Details**			
Original condition	institutional type	business strategy	technology platform	standards
Original event	Hardware	personnel	policy	natural disaster
Intermediate event	Repetition	redundancy	tardiness	fragility
Recovery act	Simplification	strengthen	prohibition	redefinition
Terminal event	data disaster	employee turnover	business collapse	institution invalidation

In CCA, failure tree and event tree can develop according to their own nature characteristics, and they can also be interrelated with each other by dangers.

By analysis to all of the possible risk modes of the system, risk mode and effect analysis can determine the potential effect to system and information security. After that, the risk points should be found out and the criticality can be sure according to the probabilities and impact degree[18].

REMCA is composed by RMEA and CA. RMEA, by analysing the impact of every impossible failure mode to system, can classify those modes into different type according to their severity[19].

The qualitative analysis of RMECA will be achieved by a matrix shown in Figure 7, in which the horizontal and vertical axes represent the severity classes and the dangerous levels of system respectively. There are four levels of severity, which are respectively represented by I, II, III and IV to describe the increasing trend loss of system and economic. In this matrix, the more distance between shadow of risk mode localities on diagonal and the original point, the greater the damage produced by them. And in the quantitative analysis, the damage degree C_{mj} of the *j*th risk mode can be worked out by $C_{mj} = \beta_j \alpha_j \lambda_e t$, in which β_j is the risk impact probability, α_j is the frequency ratio, λ_e is the incurrence probability of top event e and t is the working time. So the sum of the risk is $C_r = \sum_{i=1}^{n} C_{mj}$

PRA[5,6,20] can be called as quantitative risk analysis (QRA) or probability security analysis (PSA), which works by the combination of Bottom-Up (such as FMECA and ETA) and Top-Down (such as FTA). PRA can achieve analysis process by using experts and assessment the data, and the steps are as following: (1) to establish the top event; (2) to determine the original event by MLD analysis; (3) to obtain the set of risk accidents sequences by FTA analysis; (4) to establish the minimal cutset by FMECA and ETA analysis.

In the process of PRA analysis, the comprehensive application of function events sequence diagram (FESD) and the computing of multi-probabilities. The computing formula is $Risk_{(v,i,c)}(t) = p_{v,c}(t) \times loss_{(i,c)}$, in which c is the event result and $c \in C$. C is a collection of results produced by events, v represents the event approach and is the lose result after the failure of some given linkages. And $i \in I$, $I = \{i \mid 1, 2, \ldots n\}$, $p_{(v,c)}(t)$ represents the probability of result c via v . From the tree shape structure, it is known that $p_{(v,c)}(t)$ depends on the being used probability of some system fragility construction, $p_{(v,c)}(t) = 1 - \prod_{h \in H_{c,k}} \left[1 - q_h(t)\right]$. $q_h(t)$ is the being used probability of risk h at time t , in which $q_h(t) = pro_1 + pro_2 + \cdots + pro_m$, $pro_i \ (i = 1, 2, \ldots, m)$ is the attack proportion by using the fragility reason of system. And the final risk probability is $Risk = \sum_{i=1}^{n} Risk_i = \sum_{i=1}^{n} \sum_{c \in C} Risk_{(i,c)}$.

HAZOP (HAZard and Operability study)[21] is a kind of analysis based on the proposing of expert group problems and together discussion of assessment group and the being assessed organization (in another word, brain storming). There are three frequently-used types of HAZOP techniques, such as Guide Word Approach[22], Knowledge-based HAZOP and Checklist. The Guide Word Approach is the mostly used method. In Figure 8, the expert group can propose problems after the combination of the guide word and security elements. The team, which is responsible for these problems, will report the summary of security status and order the related team to solve the problems.

According to some related standards, there are seven elements of ISRA, such as the network application security, personnel security, physical security, asset security, policy and risk control mechanism, management security and organization system.

The basic idea of expert group in the assessment is that any phenomenon with operating condition value which is deviated from the default can cause dangers and finally lead to accident and loss[23].

AHP[24], proposed by a U.S. operational research expert named Saaty, is a kind of famous decision-making method. It can establish a multi-layered structure model by using all elements of complicated system, and the steps are in following:
Hierarchy structure establishment: According to the principle of AHP, there are three layers such as the object, criterion and indicator. Three layers of information security layered assessment are respectively information system security (as the object), seven elements of information security (as the criterion) and three assessment standards (as the indicators), shown in Figure 5.

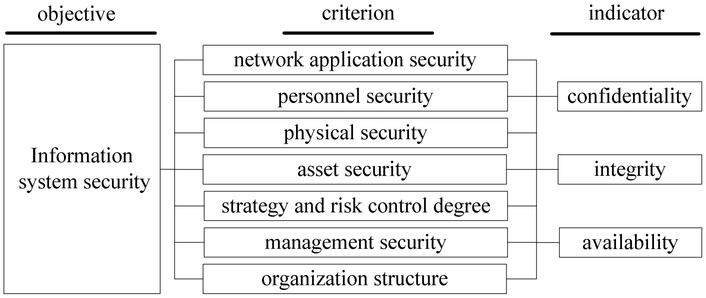

Figure 5 : Hierarchy structure of information security

Judgment matrix building: Based on the judgment from the experts, the assessment matrix can be built. Contents in the row are the assessment elements on the same layer, and contents in the column are the relative importance ranks of elements.

Layers' sequencing and synthetic judgment finishing: Based on AHP, weight matrix of all elements can be obtained by the processing to assessment matrix and then the relative weights of upper and lower layers can be got. According to the maximum membership principle, the layered elements should be sequenced after the normalization of weights.

DISCUSSION ON SEVERAL RISK ASSESSMENT METHODS

Qualitative-, quantitative- and the combination of both-based are three kinds of assessment attributes

Qualitative-based assessment is just a fuzzy evaluation, so it is quite subjective and strong assessment ability is required. Based on the qualitative assessment, quantitative analysis can quantify the elements and increase the operability, reliability and comparability. Incomplete understanding and misunderstanding are resulted by the simplicity of quantitative analysis, which are the disadvantages. Sometimes, qualitative and quantitative analyses are both used.
Some assessment methods will be discussed in the following, and the criterions are shown in TABLE 2.

TABLE 2 : Risk assessment criterions

Criterions	Descriptions
Integrity	full-scale assessment range
Controllability	assessor, methods and process are controllable
Minimal impact	produce minimal impact to the normal operation of system
Confidentiality	intermediate and results can be only obtained by related staff

FTA and ETA are all based on tree assessment, and CCA is the combination of FTA and ETA. All of them have the advantages and disadvantages of tree shape methods

Advantages: (1) be applicable to analysis to reliability and security of large-sized complicated system; (2) can easily master the accidental regulation and avoid the happening; (3) obvious events sequence, qualitative description of system characteristics; (4) can definite the relationship between the failure events and results brought by events; (5) be easily documented; (6) can provide a visual guide using graphical technical material.
Disadvantages: (1) too large to understand of failure tree; (2) very complicated logical relationship; (3) requirement of many reliable data for probability computing[25]; (4) limited to analysis for unparalleled events; (5) very easy to become more complicated.

Solutions: conventional tree shape analysis do not count for the probability uncertainty of basic events, so the fuzzy sets[26] are introduced to fuzzy the occurrence probability of basic events and fuzzy probability can be obtained by related algorithms[27]. These solutions are helpful to understand the distribution regulation of information security occurrence probability and to provide the theoretical foundation for risk management.

RMECA is a kind of systematic risk prediction technology and is applicable to the whole system

Advantages: (1) simple analysis process, only need the determination of the requirement of contents and the analysis process; (2) using tables, easily to be implemented, without complicated mathematic computation, be widely used (3) analytical results can be the basis of FTA and RCMA; (4) can be operated with inadequate experiences.

Disadvantages: (1) the consideration is limited to danger failure; (2) single factor analysis, insufficient common factor effect; (3) involve less human factor, environment effect and software error; (4) in adaptable to complicated system; (5) can only do systematic induce; (6) beginning from the failure mode of single factor, with too much working, hard to achieve.

Solutions: catching the main contradiction of system, to find out the key elements using FTA before RMECA[28]. Take the key elements as the joint points and combine FTA and RMECA, shown in Figure 6.

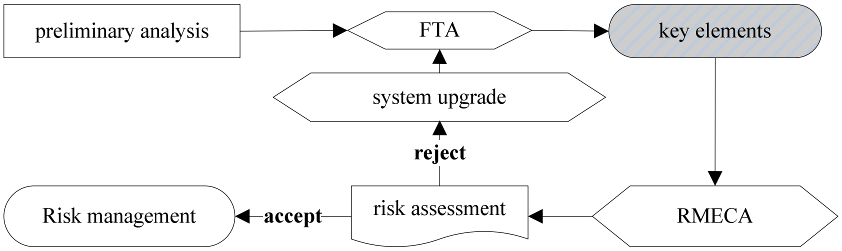

Figure 6 : Assessment process based on RMECA and FTA

Danger and operability analyses are relatively independent compared with other methods

Advantages: (1) can fully analyze the system design; (2) can analyze the operating mistakes and the consequences resulted by them, and adopt some measures to avoid[29]; (3) can discover the potential dangers and eliminate them by some measures; (4) can help designers and operators know the full details of system performance[21]; (5) good pertinence; (6) can appoint the executive of suggested by action, with good operability.

Disadvantages: (1) need too much manpower, material resource and time consumption; (2) dependent much on the accuracy of diagram paper and information examined; (3) high demand for the specialized knowledge and abundant experiences of the experts.

Solutions: define responsibilities before the assessment[30].

Obtain the hierarchical structure of system, and operate the weighted disposal. Sort the elements and provide the quantitative data for the decision maker

Advantages: (1) fully research on hierarchical structure of system design; (2) define the relative security status of bottom elements and know the vulnerable spot; (3) provide the risk management basis for the decision maker.

Disadvantages: (1) to quantify the uncertainty in the process is necessary; (2) it is hard to ensure the connected reasonability of real elements; (3) high demand for the specialized knowledge and abundant experiences of the experts; (4) existing some problems of the reference value for weight and feasibility of system update.

Solutions: introduce fuzzy clustering and gray system theories to facilitate the achievement of weighted value and judgment matrix; reduce the uncertainty resulted by human factor; give some reference values to refine the membership principle in order to improvement the integrity and operability of assessment, shown in Figure 7.

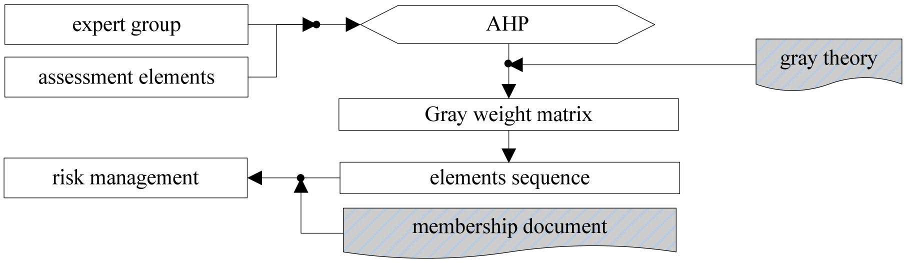

Figure 7 : AHP base on Gray theory

The logical relationship among those methods is shown in Figure 8. Numbers in Figure 8 are represented for some different situations: (1) If the assessment system cannot describe the event occurrence probability using the exact numbers by statistical methodology, Delphic can be brought into and assess the occurrence probability of given events by fuzzy language based on knowledge of the experts. (2) Considering that the ambiguity can express the fuzzy uncertainty to some extent, the uncertainty of fuzzy numbers can be analysed. (3) To fuzzy the generation of weight values by fuzzy theory and gray theory. (4) To overcome the inherent defect that AHP cannot find new problems, and simplify the complicated problems. (5) Being existing because CCA is the integration of failure tree and event tree analysis. (6) To establish minimal cutest by RMECA and ETA. (7) To determine the risk accidents sequence set by FTA. (8) To analyse the original events by MLD. (9) To find out key elements of FTA, and combine it with RMECA.

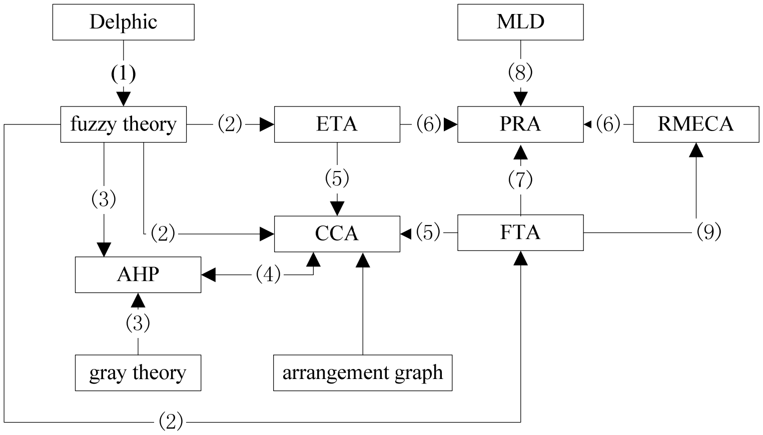

Figure 8 : Relationship among those methods

THE EXISTING PROBLEMS

In the future, the related researchers should pay more attentions on the following contents: (1) to determine the assessment roles and responsibilities exactly; (2) to issue standards as soon as possible; (3) to consider the risk of assessment process itself; (4) to accumulate as much research experiences as they can; (5) to improve the specialized techniques and staff structure.

ACKNOWLEDGEMENT

Our research was funded by several Projects, and the names and numbers of these Projects are as follows: 1. The National Natural Science Foundation of China (Grant No. 61402052). 2. Basic Research Project of Shaanxi Province Natural Science Foundation (Grant No. 2013JM8018). 3. The Special Fund for Basic Scientific Research of Central Colleges of Chang'an University (Grant No. 2013G1241118 and 2013G2241020).

REFERENCES

[1] ISO/IES TR 17799:2000.Information Security Management-Code of Practice for Information Security Management **(2000)**.

[2] GB/T 18336-2001, Information technology security technology **(2013)**.

[3] Thomas R.Peltier; Information Security Risk Analysis [M], Auerbach Publications **(2012)**.

[4] T.Bedford, R.Cooke; Probabilistic Risk Analysis [M], Cambridge University Press **(2001)**.

[5] United States General Accounting Office, Accounting and Information Management Division, Information Security Risk Assessment [Z], **(1999)**.

[6] S.A.Butler, P.Fischbeck; Multi-Attribute Risk Assessment, Technical Report CMD-CS-01-169 [R], **(2001)**.

[7] S.A. Butler; Security Attribute Evaluation Method: A Cost-Benefit Approach [Z], Computer Science **(2014)**.

[8] Thomas R.Peltier; Information Security Risk Analysis [Z], Rothstein Associates Inc, **(2001)**.

[9] National Institute of Standards and Technology (NIST), ICAT Metabase [Z], http://icat.nist.gov **(2012)**.

[10] National Institute of Standards and Technology, Special Publications 800-30, Risk Management Guide [Z], **(2011)**.

[11] K.S.Hong, Y.P.Chi; An integrated system theory of information security management [J], Information Management & Computer Security, **11(5)**, 243-248 **(2003)**.

[12] P.Camarda, F.Corsi; Trentadue A.An efficient simple algorithm for fault tree automatic synthesis from the reliability graph [J], IEEE Transactions on Reliability, **27(3)**, 215-221 **(1978)**.

[13] T.Kohda; Finding Modules in Fault Tree [J], IEEE Transactions on Reliability, **38(3)**, 165-176 **(1989)**.

[14] G.Sindre, A.L.Opdahl; Eliciting security requirements with misuse cases [J], Requirements Engineering, January, **10(1)**, 34-44 **(2005)**.

[15] Fault Tree Diagrams and System Analysis [Z], http://www.chinarel.com/systemrelweb/ **(2003)**.

[16] A.Anand; Hierarchical Analysis of Fault Trees with Dependencies, Using Decomposition [C], RAMS Proceedings, 169-75 **(1998)**.

[17] J.Wang; An approach to designing an expert system through know ledge organization in expert system application [J], **21(8),** 34-39 **(1988)**.

[18] J.B.Bowles; The new SAE FM ECA standard [A], Proceedings Annual Reliability and Maintainability Symposium [C], Atlanta Georgia USA: IEEE, 48-53 **(1998)**.

[19] J.Barkai; Automatic generation of a diagnostic expert system from failure mode and effects analysis (FMEA) information [M], SAE Technical Paper Series **(1999)**.

[20] National Institute of Standards and Technology (NIST), ICAT Metabase [Z], http://icat.nist.gov **(2012)**.

[21] D.W.Jones; Lessons From HAZOP Experiences **(1992)**.

[22] Nigel Hyatt, Guidelines for Process Hazards Analysis (PHA,HAZOP) Hazards Identification and Risk Analysis, CRC Press, **(2003)**.

[23] T.Kletz; Hazard And Hazan-Identifying and Assessing Process Industry Hazards[M], IchemE **(1992)**.

[24] T.L.Saaty; The Analytic Hierarchy Process [M], New York: McGraw-Hill **(2012)**.

[25] D.P.Weber; Fuzzy Fault Analysis [J], Fuzzy system, **(3)**, 1899-1904 **(1994)**.

[26] D.Singer; Fuzzy set approach to fault tree and reliability analysis [J], Fuzzy Set and Systems, **(34)**, 145-155 **(1990)**.

[27] H.Song, H.Y.Zhang, X.R.Wang; Fuzzy Fault Tree Analysis Based on T-S Model [J], Control and Decision(China), **20(8)**, 854-859 **(2005)**.

[28] S.Amari, G.Dill, E.Howald; A New Approach to Solve Dynamic Fault Trees [A], 2003 Proceedings of Annual Reliability and Maintainability Symposium [C], 374-379 **(2013)**.

[29] M.Cocchiara, V.Bartolozzi, A.Picciotto, et al.; Integration of interlock system analysis with automated HAZOP analysis [J]. Reliability Engineering and System Safety, **74(1)**, 99-105 **(2001)**.

[30] R.T.Clemen, R.L.Winkler; Combining probability distributions from expert in risk analysis [J], Risk Analysis, **19(2), (1999)**.