International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Analytic Hierarchy Process (AHP) Based Modeling for the Nuclear Cyber Security Incorporated with Fuzzy set Algorithm

Tae Ho Woo

Abstract: ***The method of the nuclear cyber terrorism prevention is analyzed in which the cyber security is investigated in the aspect of the nuclear matters. In the method, the radiological detection sites are considered as the cyber terror incident points. Using the Analytic Hierarchy Process (AHP) method, the complex algorithm of the terrorism could be manipulated incorporated with the fuzzy set method in which the verbal uncertainty could be expressed by the matrix algorithm. In addition, by the dynamical analysis, the terror incident time could be estimated. In the work, during the period of 60 years, it is considered the reactor runs securely as the values between 0.0215112 in 7th year and 0.0202358 in 22nd year. This means that the securest one is 1.063 times higher comparing to the lowest one. Furthermore, the five sites are variable by the dynamical manner where the #1 sites are more than those of #5. Results show the estimations of nuclear cyber terrorism successfully. This method could be applicable to the industrial plants and facilities.***

Index Terms: ***Analytic Hierarchy Process (AHP), Cyber, Nuclear; Security, Terrorism.***

I. INTRODUCTION

The importance of the nuclear cyber terrorism prevention is one of critical issues in a nation where the incident could be variable without any notices, although the endeavors of the terrorism controls continue regarding the mutual matters among some countries. It is very interesting to investigate the quantitative analysis of treating the potential nuclear cyber terrorism. The proposed cyber terrorism process is incorporated with the nuclear detections in which the radiological detection ways are analyzed. In the previous incident on nuclear power plants (NPPs) in South Korea, the dangerous damages were not happened, fortunately [1]. The internet protocol (IP) address was searched and was founded out at a region in China. However, it was failed to arrest the terrorist. Considering the system of NPPs, there are many potential possibilities in nuclear cyber terrorism. The search of the terror incident could be one of the most important factors in this study. The Analytic Hierarchy Process (AHP) is applied to the quantified analysis.

It is very difficult to find out the cyber terror incident, especially in the case of the complex facilities like the NPPs. Conventional linear algorithm could not be used in the complicated cases, because the linear and objective processes are simply detected by the terrorist. Hence, the nonlinear and complex methods should be applied to the security solutions. In this work, the process of cyber terrorism is modified as the event flows where the sampling by Monte-Carlo method is used for the quantifications. Five different kinds of types in events are applied to AHP analysis. Each event is related to the detection site where the importance of the cyber terrorism in nuclear industry are reflected by the randomly selected numbers. So, the assessment of the terror incidents is performed by the matrix forms including the ambiguous trend in terrorism and fuzziness object of the incident in which the AHP combined fuzzy set algorithm could be realized in the estimations of terror forecasting. The goal of the academic studies could be the nonlinear and indirect analyses that solve the approximate incident happening using the dynamical interpretations. So, the directions of the work should be related with several kinds of the algorithm instead of the single method.

For literatures in AHP method, Cagno and et al. had worked for probabilistic process in the multiple bidding cases by the contractors [2]. In addition, there is a paper as the entropy information applied AHP method by Wang and et al. [3]. Suh and et al. [4] used the optimal weighting method for the comprehensive assessment result. This is analyzed as various ways like the paired comparison, asset dependency diagrams, and so on. Furthermore, there are some AHP papers applied to the nuclear security [5-7].

II. METHOD

The critical points of modeling are to find the terrorism factor. In this work, the consequences of the terror progressions are the basic event in the modeling. There is the modified process of cyber terrorism in Table 1 [8] where five factors are considered for the modeling of this study. Reconnaissance should be the 1st stage of the nuclear terrorism crisis and the Weapon Delivery could be supplied by several kinds of technological methods. Exploitation for nuclear stuffs are triggered by the terrorist. Command & Control is done by the keyboard access. Finally, the Attack is done. In another aspect, it is possible to think the crisis response regarding the cyber terrorism [9]. In each case of the process of cyber terrorism, the detection could be matched each other. Table 2 shows the detection strategy of Department of Homeland Security (DHS) in the United States [10] where the possible detection technologies are the strategies for the terror incidents.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Tae Ho Woo*, Department of Mechanical and Control Engineering, The Cyber University of Korea, 106 Bukchon-ro, Jongno-gu, Seoul 03051, Republic of Korea

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Hence these detection skills are related to the crisis response in Table 1, because there are the crisis sequences which are affected by the terror consequence incidents. In the graphical description, the modified process of cyber terrorism is seen in Fig. 1 [8]. Additionally, Fig. 2 is the outline of safeguard study which expresses the nuclear security in this work.

Table 1. List of the modified process of cyber terrorism.

Rating	Meaning
A	Reconnaissance
B	Weapon Delivery
C	Exploitation
D	Command & Control
E	Attack

Table 2. List of the detection strategy (Department of Homeland Security (DHS)).

Rating of detection	List
D1	Air cargo
D2	Small maritime vessel
D3	Ports of entry
D4	Urban area
D5	Advanced detection technology

Fig. 1. Modified process of cyber terrorism

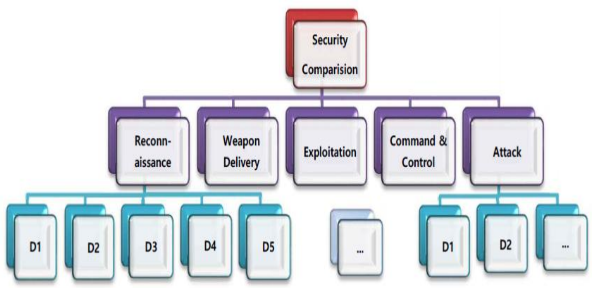


Fig. 2. Outline for the nuclear safeguard using AHP

In this study, the random number is used for the Saaty comparisons which are ranked from 1 to 9, which his in Table 3, even though usually the quantifications in the modeling are performed by the experts in AHP method [5,6]. This is made by the verbal definition incorporated with fuzzy set theory. The modified triangular fuzzy number (TFN) values are obtained [11,12] in Table 4. Fig. 3 shows the graphical shape of modified TFN where the numbers between 1.0 and 1.9 are written as 1.0. In the same way, the numbers between 2.0 and 2.9 are written as 2.0. Therefore, the left numbers of the peak point of the TFN are made as even numbers, which means the intermediate values in Table 3. Otherwise, the right numbers of the peak point of the TFN are made as odd numbers which are same to the peak point numbers. The fuzziness of the distribution is considered as the regions of the interested membership function in fuzzy set. Table 5 shows the random index for the *C.R.* that should be 0.1 for the consistency of hierarchy distributions [13,14].

Table 3. Scale of Saaty comparison

Numerical rating	Verbal definition
1	Two elements are equally important
3	One element is slightly more important than another
5	One element is strongly more important than another
7	One element is very strongly more important than another
9	One element is extremely more important than another
2, 4, 6, 8	Intermediate values

Table 4. List of modified triangular fuzzy numbers (TFN)

Meaning	TFN
Equal	(1,1,3)
Moderate	(1,3,5)
Strong	(3,5,7)
Very strong	(5,7,9)
Extreme strong	(7,9,9)

Table 5. Random index

Size	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

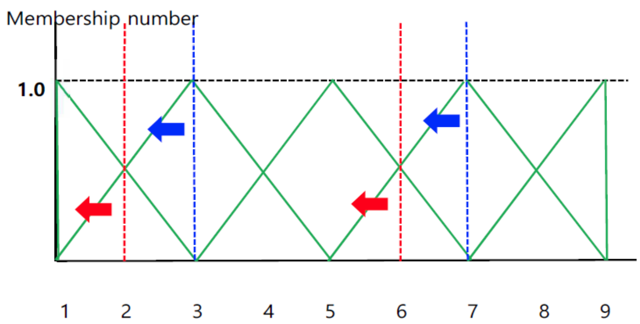


Fig. 3. Graphical shape of modified triangular fuzzy numbers (TFN)

Considering the historical review, the AHP was called as the Saaty method, which was created by Dr. Saaty [15]. This method has been used in many areas including the military purposes. In the early stage, it was used for his son where the travel planning was analyzed by transportations to Sudan, which means that there are many applications to our lives from the restricted matters to the basic human lives. Coyle [16] made the basic principle for the purchase of the equipment. For example, variables of expense (*E*), operability (*O*), reliability (*R*) and adaptability for other uses or flexibility (*F*) are mutually governed each other in which the AHP method could manage as the aspect of the multiple considerations that can show the complicated problem solutions. In addition, he also offered three case of *X*, *Y*, *Z* where the interested options like the price and operability are examined. Eventually, the company could be selected by the optimized best choice in the manufacturing.The cyber nuclear terrorism could be related each other in the interested conditions in which nuclear factors as well as cyber stuffs should be analyzed.

Therefore, the Monte-Carlo method including random sampling is quite practical to solve the complicated and fuzzy circumstances. Even though the quantification of AHP is usually performed by the survey of the chosen group by the experts. For the verbal interpretations, the Table 3 shows the rating scale of Saaty which is used in the numerical rating for the process of cyber terrorism. There is the consistency (λ) calculation obtained by the following weighting multiplication where elements of a_{ii} are in the matrix form of equation (1).

$$Weighting\ multiplication = \begin{bmatrix} a_{11}a_{11}a_{11}a_{11}a_{11} \\ a_{21}a_{22}a_{23}a_{24}a_{25} \\ a_{31}a_{32}a_{33}a_{34}a_{35} \\ a_{41}a_{42}a_{43}a_{44}a_{45} \\ a_{51}a_{52}a_{53}a_{54}a_{55} \end{bmatrix} \begin{bmatrix} W_1 \\ W_2 \\ W_3 \\ W_4 \\ W_5 \end{bmatrix} \quad (1)$$

$$Consistency(\lambda) = \frac{Weighting\ Mult.}{Weighting} \quad (2)$$

Furthermore, the C.I. (Consistency Index) and C.R. (Consistency Ratio) are calculated for the weighting value and consistence. In Table 5, the random index is shown for the *C.R.* which should be below 0.1 for the consistency of hierarchy distribution [13,14]. There is the equation with the weighting multiplication and weighting, which means the consistency. Hence, *C.I.* and *C.R.* are found out by maximum value of λ as,

$$C.I. = \frac{\lambda_{\max} - n}{n-1} \quad (3)$$

$$C.R. = \frac{C.I.}{Random\,Consistency\,Index} \quad (4)$$

In simulations, the Vensim code system is used, which has been applied for quite qualified dynamic modeling where the designs include the dynamic functions, optimization, Monte-Carlo sensitivity analysis, and more [17].

III. RESULTS

The dynamical analysis shows the cyber security in the interested area which is expressed by the detection sites. There are 60 years' runs as one time per year. Fig. 4 has the exampled matrix of comparisons from *A* to *E* where there are five detections in each case. According to AHP method, the reverser numbers are arrayed from the diagonal line. The mean and standard deviation values are obtained by the experts' judgments. In the matrix, the diagonal lines are made by the inversed numbers. For the matrix comparisons, the 1st column is found as for detection #1 in equation (5) with the maximum value and the minimum value as the dotted circles in Fig. 5.

$$0.4566 \times 0.021 + 0.3545 \times 0.014 + 0.4768 \times 0.015 + 0.5009 \times 0.019 + 0.2988 \times 0.014 = 0.035404 \quad (5)$$

D#	1	2	3	4	5	1	2	3	4	5	Relative Rate
1	1	7	7	3	7	0.567568	0.812155	0.457944	0.165354	0.280000	0.4566
2	1/7	1	7	7	3	0.081081	0.116022	0.457944	0.385827	0.120000	0.2322
3	1/7	1/7	1	7	7	0.081081	0.016575	0.065421	0.385827	0.280000	0.1658
4	1/3	1/7	1/7	1	7	0.189189	0.016575	0.009346	0.055118	0.280000	0.1100
5	1/7	1/3	1/7	1/7	1	0.081081	0.038674	0.009346	0.007874	0.040000	0.0354
Total	1.833333	9.708333	13.375	16.125	24	1	1	1	1	1	1

(a)

D#	1	2	3	4	5	Relative Rate
1	1	2	2	4	4	0.3545
2	1/2	1	4	2	4	0.2814
3	1/2	1/4	1	4	2	0.1745
4	1/4	1/2	1/4	1	4	0.1222
5	1/4	1/4	1/2	1/2	1	0.0674
Total	2.5	4.0	7.75	11.5	15	1

(b)

D#	1	2	3	4	5	Relative Rate
1	1	4	4	9	4	0.4768
2	1/4	1	4	2	9	0.2577
3	1/4	1/4	1	4	2	0.1251
4	1/9	1/2	1/4	1	4	0.0864
5	1/4	1/9	1/2	1/4	1	0.0540
Total	1.861111	5.861111	9.75	16.25	20	1

(c)

D#	1	2	3	4	5	Relative Rate
1	1	7	9	5	9	0.5009
2	1/7	1	7	9	5	0.2366
3	1/9	1/7	1	7	9	0.1505
4	1/5	1/9	1/7	1	7	0.0840
5	1/9	1/5	1/9	1/7	1	0.0280
Total	1.565079	8.453968	17.25397	22.14286	31	1

(d)

D#	1	2	3	4	5	Relative Rate
1	1	1	7	7	1	0.2988
2	1	1	1	7	4	0.2711
3	1/7	1	1	1	7	0.1912
4	1/7	1/7	1	1	1	0.0549
5	1	1/4	7	1	1	0.1840
Total	3.3922857	3.393857	17	17	14	1

(e)

Fig. 4. Exampled matrix of comparisons (a) A (b) B (c) C (d) D and (e) E

D#	A	B	C	D	E	Weighting	Value
1	0.4566	0.3545	0.4768	0.5009	0.2988	0.021	0.035404
2	0.2322	0.2814	0.2577	0.2366	0.2711	0.014	0.020972
3	0.1658	0.1745	0.1251	0.1505	0.1912	0.015	0.013338
4	0.1100	0.1222	0.0864	0.0840	0.0549	0.019	0.007681
5	0.0354	0.0674	0.0540	0.0280	0.1840	0.014	0.005605

Fig. 5. Matrix of comparisons

There are the pairwise comparison for the process of cyber terrorism which is obtained for *C.I.* (Consistency Index), *C.R.* (Consistency Ratio) and consistency (λ) calculation in Fig. 6. As it is done in Fig. 5, Fig. 6 has the maximum consistency (λ_{max}) and subsequently, the *C.I.* and *C.R.* are found out. In this simulations, since the value is higher than 0.1, there is not consistent very highly considering the *C.R.* Hence, the dynamical calculations make the most important analysis in this work, because the *C.R.* could be variable. The *C.I.* and *C.R.* are,

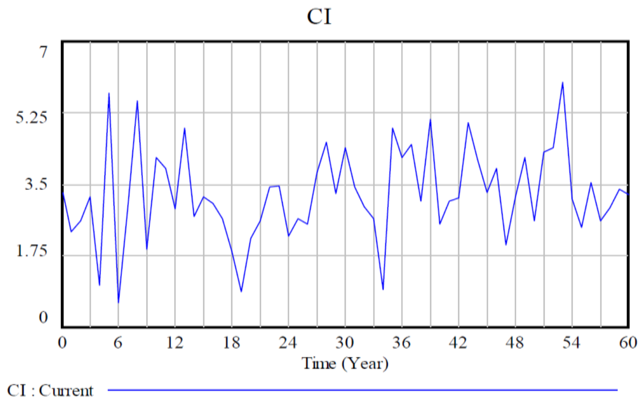
$$C.I. = \frac{\lambda_{max} - 1}{n-1} = \frac{18.1875-1}{5-1} = 4.296875 \quad (6)$$

$$C.R. = \frac{C.I.}{Radom\ Con.\ Ind.} = \frac{4.296875}{1.12} = 3.836496 \quad (7)$$

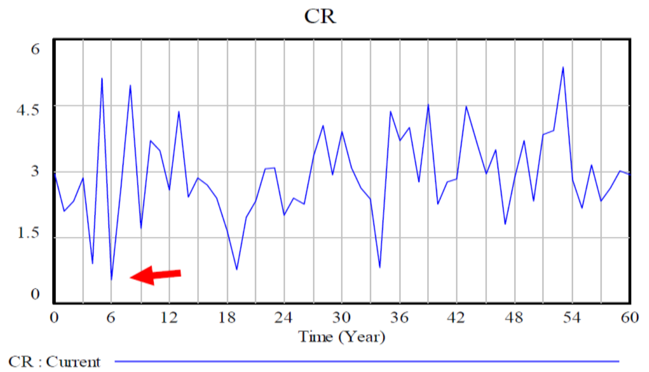
Total *C.I.* and *C.R.* are in Fig. 7. There is the minimum value of *C.R.* that is very consistent in 6th year. Furthermore, there are maximum pair values with multiplications in Fig. 8 (a). These are accompanied by detection number in Fig. 8 (b). In the work, during the period of 60 years, it is considered the reactor runs securely as the values between 0.0215112 in 7th year and 0.0202358 in 22nd year. This means that the securest one is 1.063 times higher comparing to the lowest one. For the graphics, there are dotted circles for the highest and lowest values in detection #1. The five sites are variable by the dynamical manner where the #1 sites are more than those of #5 during 60 years, which means 'Air cargo' region has more vulnerable than 'Advanced detection technology' equipped region. That is, the air cargo could be attacked by the cyber terrorist comparatively in this simulation. Considering the applications of AHP, there is the nuclear safeguard protocol to be promoted in the aspect of the nuclear industry.

	A	B	C	D	E	Weighting	Weighting Mult.	Consist. (λ)
A	1	8	4	3	8	0.021	0.362	17.2381
B	1/8	1	8	4	3	0.014	0.254625	18.1875
C	1/4	1/8	1	8	4	0.015	0.23	15.33333
D	1/3	1/4	1/8	1	8	0.019	0.143375	7.546053
E	1/8	1/3	1/4	1/8	1	0.014	0.027417	1.958333

Fig. 6. Maximum Consistency (λ)

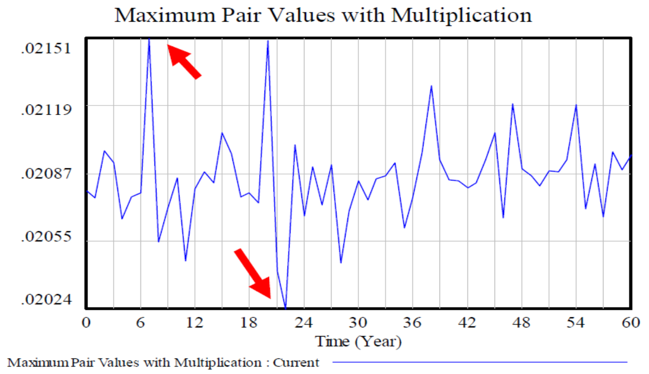


(a)

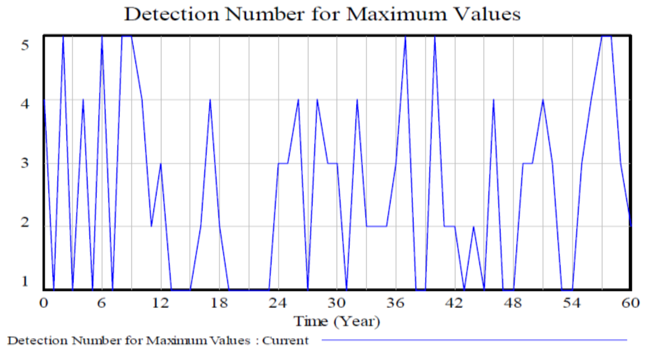


(b)

Fig. 7. Graphs for (a) the consistency index (C.I.) and (b) the consistency ratio (C.R.).



(a)



(b)

Fig. 8. Graphs for (a) Maximum pair values with the multiplications and (b) Detection numbers for the maximum values.

IV. CONCLUSIONS

The cyber security is investigated in the aspect of the nuclear matters where the radiological detection sites are considered as the cyber terror incident points. Using the AHP method, the complex algorithm of the terrorism could be manipulated incorporated with the fuzzy set method in which the verbal uncertainty could be expressed by the matrix algorithm. Several critical points are proposed as follows,

- The cyber security is studied for the nuclear matters.
- The AHP method could be applied to the terror incident.
- Dynamical analysis is performed for the practical purposes.

- Enhanced terrorism estimations are achieved.

Overall, this research could give the terror incident time as well as site using the nonlinear algorithms of AHP and fuzzy method as the combinational way. The dynamical analysis could give some hints to the other kinds of industries. For example, the oil and chemical plant could be damaged by the computer virus which could attack on the automatic system that control the oil or equipment delivery system in the plants. The industrial plants are usually operated by the automatic system. Hence, the cyber terrorism is one of critical disaster causes, which give another kind of threatening to the operators, because the on-line based terrorism couldn't be detected easily due to the unseen invasions to the goal as the plant or facility. So, this study gives many applicable strategies to the general industries. Including the nuclear industry, the industrial plants are able to be protected by the computer viruses by the complex based algorithms like the AHP incorporated with fuzzy set method.

REFERENCES

1. H. S. Cho And T. H. Woo, "Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs)," Annals of Nuclear Energy, Vol. 99, 2017, pp. 47-53.
2. E. Cagno, F. Caron And A. Perego, "Multi-criteria assessment of the probability of winning in the competitive bidding process," International Journal of Project Management, Vol. 19, 2001, pp. 313-324.
3. J. J. Wang, Y. Y. Jing, C. F. Zhang, And G. H. Shi, Integrated evaluation of distributed triple-generation systems using improved grey incidence approach. Energy, Vol. 33, 2008, pp. 1427-1437.
4. B. Suh, And I. Han, The IS risk analysis based on a business model. Information & Management, Vol. 41, 2003, pp. 149-158.
5. T. Woo, "Nuclear safeguard protocol construction for nuclear power plants using analytic hierarchy process with zero-sum method," International Journal of Nuclear Governance, Economy and Ecology, Vol. 3, No. 3, 2011, p. 2011.
6. T. H. Woo, "Dynamical nuclear safeguard investigations in nuclear materials using analytic pair values," Annals of Nuclear Energy, Vol. 38, No. 9, 2011, pp. 1916-1923.
7. T. H. Woo, And U. C. Lee, "Safeguard assessment in nuclear power plants (NPPs) operations using analytic hierarchy process (AHP) and production function," Energy Exploration & Exploitation, Vol. 29, No. 3, 2011, pp. 337-356.
8. US Senate, A "Kill Chain" Analysis of the 2013 Target Data Breach, Majority staff report for chairman Rockefeller, Committee on commerce, science, and transportation, US Senate, Washington DC, USA, 2014.
9. NNSA, Prevent, Counter, and Respond - A Strategic Plan to Reduce Global Nuclear Threats (FY 2016–FY 2020), National Nuclear Security Administration (NNSA), United States Department of Energy Washington, DC, USA, 2015
10. PNNL, Preventing Nuclear Terrorism: Does DHS have an Effective and Efficient Nuclear Detection Strategy? Pacific Northwest National Laboratory (PNNL), United States Department of Energy Washington, DC, USA, 2012.
11. E. Tolga, M. L. Demircan, And C. Kahraman, "Operating System Selection Using Fuzzy Replacement Analysis and Analytic Hierarchy Process," International Journal of Production Economics, Vol. 97, 2005, pp. 89-117.
12. D. H. Kim, And S. Y. Sohn, "Fuzzy analytic hierarchy process applied to technology credit scorecard considering entrepreneurs' psychological and behavioral attributes," Journal of Intelligent & Fuzzy Systems, Vol. 30, No. 4, 2016, pp. 2349-2364.
13. R. D. Holder, "Some comment on the analytic hierarchy process," Journal of the Operational Research Society, Vol. 41, 1990, pp. 1073-1076.
14. P. R. Drake, "Using the analytic hierarchy process in engineering education," Int. J. Eng. Edu. Vol. 14, 1998, pp. 191-196.
15. T. L. Saaty, 1980. The Analytic Hierarchy Process, McGraw Hill International.
16. G. Coyle, The Hierarchy Process (AHP), Pearson Education Ltd., 2004.
17. Vensim, Vensim Simulation Software, Vantana, Inc., Harvard, USA, 2016.