ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 8, February 2015

Cyber Security Risk Assessment Using Multi Fuzzy Inference System

Hany Sallam

Abstract*— Digital instrumentation and control I&C systems are software based systems. These systems as information systems are vulnerable to cyber security attacks which impact the safety systems which are based on these digital I&C systems. Cyber security risk assessment is necessary to identify system vulnerabilities which could be exploited in malicious acts to determine actions to be taken in the form of risk management to avoid potential impacts of such malicious acts. Fuzzy logic is one of the major tools used for security analysis. Fuzzy systems are characterized by their capabilities to reasoning in case of incomplete or vague data which make it a good tool for evaluating the risk of a given system. Fuzzy logic techniques that are based on max-mini fuzzy inference engine are used to identify the potential threats to computer-based systems. In this paper a risk assessment method based on multi fuzzy systems is proposed for assessing cyber threats. This method evaluates cyber security risk as a function of risk factors which are the overall capabilities of an attacker, the overall likelihood of an attack success, and the impact of an attack. This system composed of three sub-fuzzy inference systems FISs, the first FIS1 evaluates the overall capabilities of an attacker, the second FIS2 evaluates the overall likelihood of an attack success, and the third evaluates the risk level based on the output of the attack impact and the output of FIS1 and FIS2.

***Index terms:* Risk Assessment, Cyber Security, and Fuzzy Inference Systems.**

I. INTRODUCTION

The techniques of risk analysis are powerful tools to help people manage uncertainty. Thorough risk analysis estimation and evaluation a valuable support for decision making can be provided [1]. There are many risk analysis techniques currently in use that attempt to evaluate and estimate risk. These techniques can be either qualitative, quantitative, or semi-quantitative depending on the information available and the level of detail that is required [2]. Qualitative techniques rely more on judgment than on statistical calculations such as scenario Analysis. This can be a very straightforward process based on informed judgment and reference to appropriate guidance. A qualitative risk assessment should be a systematic examination of what in the workplace could cause harm to assets, so that decisions can be made as to whether existing precautions or control measures are adequate or whether more needs to be done to prevent harm. This type of assessment supports communicating risk results to decision makers. Quantitative risk assessment involves obtaining a numerical estimate of the risk from a quantitative consideration of event probabilities and consequences. Quantitative techniques rely heavily on statistical approaches, which include Monte Carlo Simulation, Fault and Event Tree Analysis, Sensitivity Analysis, Annual Loss Expectancy, Risk Exposure, Failure Mode and Effects Analysis, etc; This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action [3]. Semi-quantitative is an intermediate technique where the hazards are neither few nor simple, nor numerous and complex, in such as a particular complex process or technique, it may be appropriate to supplement the simple qualitative approach with a semi-quantitative assessment. *Semi-quantitative* assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. This type of assessment can provide the benefits of quantitative and qualitative assessments [1]. A number of different techniques for carrying out semi-quantitative risk assessments exist, including risk matrix approaches and lines of defence/layers of protection analysis. Quantitative and qualitative techniques have their own advantages and disadvantages. Among these techniques, the application of Fuzzy Inference System FIS to risk analysis seems appropriate; as such analysis is highly subjective and related to inexact and vague information [4]. Since FIS was introduced by Lotfy Zadeh (1965) [5] to deal with problems in which vagueness was present, linguistic values have been widely used to approximate reasoning. The fuzzy logic approach has been used recently for the evaluation of risk in different situations. Numerous studies of FIS in risk assessment have appeared in different areas. Fuzzy logic is one of the major tools used for security analysis. A fuzzy logic technique that was based on Madiami-style inference engine was used to identify the potential threats to computer-based systems. The result showed an effective way of carrying out threat modeling. Also for software, a rule based fuzzy expert system is used to analyze the risk associated with software before it is finally deployed [6]. Another application for fuzzy risk assessment presented in [7] to support the assessment of risk management in network security field for government agencies. In this paper, a fuzzy risk assessment system is designed using Multi Fuzzy Inference System MFIS to determine the risk rate using factors associated with each risk. Fuzzy inference system is a computer paradigm implying a collection of fuzzy membership functions, rules and reasoning. There are three common inference systems known. These are Mamdani Fuzzy models, Sugeno Fuzzy Models, Tsukamoto Fuzzy models [8]. In our MFIS approach we are using Mamdani Fuzzy model as it is best suitable to adapt our approach. This fuzzy logic approach proceeds in several steps as will be shown in section 4. This paper is organized as follows, section 2 discusses assessment approaches, section 3 explains risk model, section 4 introduces the proposed multi fuzzy inference system, and finally conclusion.

II. ASSESSMENT APPROACHES

Risk assessment is the process of identifying, prioritizing, and estimating information security risks [9]. As shown in Fig. 1 assessing information security risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur [4], [10]. Risk assessment plays a critical role in the development and implementation of effective information security programs and help organizations address a range of security-related issues from advanced persistent threats to supply chain concerns. Risk, and its contributing factors, can be assessed in a variety of ways, including quantitatively, qualitatively, or semi-quantitatively and each approach has advantages and disadvantages [9]. The results of risk assessments are used by organizations to develop specific courses of action that can provide effective response measures to the identified risks as part of a broad-based risk management process. Any assessment of risk typically includes:

1. An explicit risk model, defining key terms and assessable risk factors and the relationships among the factors;
2. An assessment approach, specifying the range of values those risk factors can assume during the assessment; and
3. An analysis approach, specifying how values of those factors are functionally combined to evaluate risk.

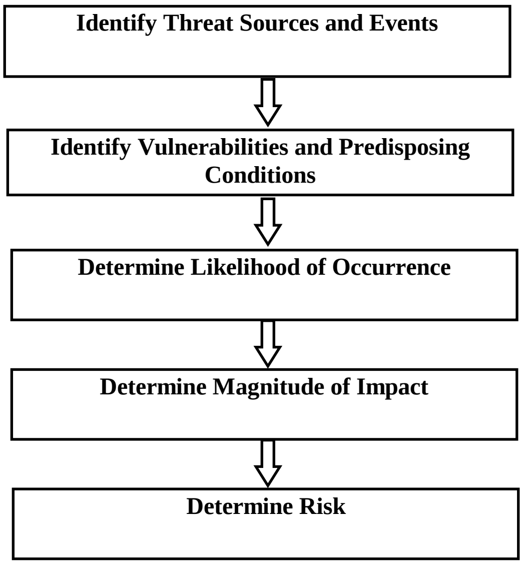

Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk

Fig. 1 Risk Assessment steps

Risk assessments address the potential adverse impacts to organizational operations and assets, individuals, other organizations, arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems. Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks. Rather, organizations employ risk assessments on an ongoing basis throughout the system development life cycle and across all of the tiers in the risk management hierarchy with the frequency of the risk assessments and the resources applied during the assessments, commensurate with the expressly defined purpose and scope of the assessments [2].

Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations.

III. RISK MODEL

There are several processes for identifying and prioritizing risk. One of the most effective is threat modeling. Threat modeling is the process of identifying, quantifying and analyzing potential threats of a computer-based system. It involves identifying the key assets of an application, decomposing the application, identifying and categorizing the threats to each assets or component, rating the threats based on a risk ranking, and then developing threat mitigation strategies that are then implemented in design. Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments [9]. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition as shown in Fig. 2. Risk factors can be decomposed into more detailed characteristics (e.g., threats decomposed into threat sources and threat events).

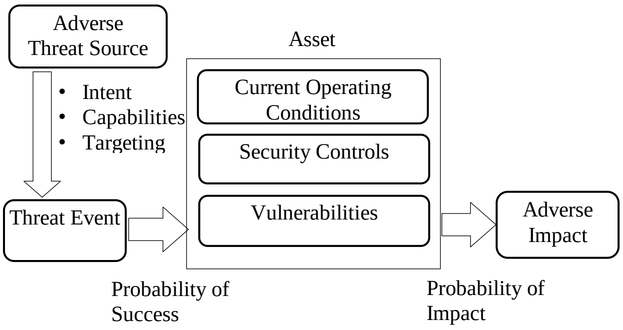


Fig. 2 Risk Model

A. Risk Factors

***1. Threat*:** A *threat* is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [3], [11]. Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders [12]. To protect against these threats, it is necessary to create a secure cyber-barrier around an asset. Adversarial threat characterized by, (i) adversary *intent*; (ii) adversary *capability*; and (iii) adversary *targeting*.

***2. Vulnerability*:** A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness [12]. For an asset there are three general categories [13]:

i. Vulnerabilities inherent in the asset manufacturing.
ii. Vulnerabilities caused during the installation, configuration, and maintenance of the asset.
iii. The lack of adequate protection because of poor network design or configuration.

***3. Likelihood*:** The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities) [11]. The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts) [13].

4. Impact: The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. Impact could be physical, economic, or social impacts [12].

B. Risk Evaluation

Attackers frequently break into systems and cause a lot of destruction as shown in Fig. 3 and as a result, systems users are now interested in expecting how much will be the risk. A simpler approach that is followed by many risk experts is to multiply the severity (Impact) of consequences by the likelihood of their occurrence. Risk level is defined as the product of the probability of an unsatisfactory outcome (Likelihood) and the loss to the parties affected when the outcome is unsatisfactory (Impact) [14]. Consequently, two linguistic variables, ''Likelihood'' and ''Impact'', are defined to calculate the overall risk level. But this approach neglects a vital component of risk calculations; it is the capabilities of threat source. The success of threat source in targeting a system using such system vulnerabilities depending on his capabilities. Threat sources such as extremists or terrorists have different capabilities, intent, and targeting for the same system [9]. Also, the likelihood of targeting a system depend on its vulnerabilities, likelihood of exploiting these vulnerabilities, and finally likelihood of success. So we propose to evaluate the risk level as a function of overall capabilities, overall likelihood, and impact, as explained by (1), (2), and (3).

$$Risk = (overall\ capabilities, overall\ likelihood, impact) \quad (1),$$

$$overall\ capabilities = (capabilities, intent, targeting) \quad (2)$$

$$overall\ likelihood = (v, a, s) \quad (3)$$

Where v is the vulnerability, a is the action likelihood, and s is success likelihood.

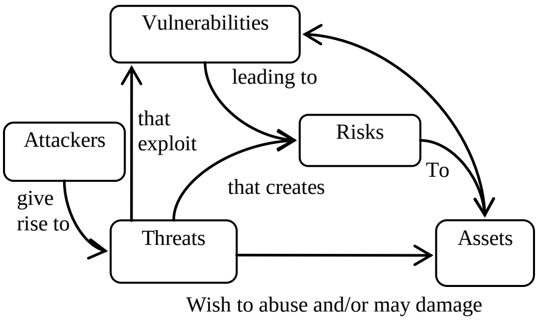


Fig. 3 Malicious Act Scenario

IV. PROPOSED MULTI FUZZY INFERENCE SYSTEM (MFIS)

Based on the risk model represented by Equations (1, 2, and 3), we propose multi fuzzy inference systems MFIS that consists of three fuzzy inference systems for risk assessment as shown in Fig. 4. The first fuzzy inference system (FIS1) calculates the overall capabilities of a threat source such as an extremist group or a terrorist group to target an asset based on its (capabilities, intent, and targeting). The second fuzzy inference system (FIS2) calculates the overall likelihood of a threat event resulting adversary impact based on the risk factors (vulnerabilities, action likelihood, and success likelihood). The third fuzzy inference system (FIS3) calculates the risk scale based on the output of FIS1, FIS3, and the adversary impact. All fuzzy variables (Capabilities, Intent, Targeting, Vulnerabilities, Action likelihood, Success Likelihood, Impact, and Risk Level) are expressed linguistically in terms of fuzzy sets, ''Very low'', ''low'', ''Moderate'', ''High'', and ''Very High'' as shown in Fig. 5. In this study, the membership functions of the linguistic terms are characterized by trapezoidal membership functions for "Very Low" and "Very High", and triangular membership functions for "Low", "Moderate", and "High" as these are very often used in applications such as fuzzy controllers, and in managerial decision making. Triangular membership function is a special case of trapezoidal membership function and they are well suited for modeling and designing [14]. Table I, Table II, Table III, and Table IV show the meaning of membership functions for the variables, overall Capabilities, overall likelihood, Impact, and Risk level respectively. *IF-THEN* rules are formed to reflect the relationship between the input variables taken as antecedents and the output variable taken as consequent of the fuzzy rules. Given input variables specified as 'IF' part of a rule and output variable (fuzzy risk level) is taken as 'THEN' part of a rule. As there are multiple input variables, AND operator is used to map inputs to one output. Rules designed in the rule base of FISs can be represented in general as [8], [15]:

IF (V_1 is A_i) AND (V_2 is B_i) AND …THEN (O is Z_i).

Where V_1 and V_2, represents the input variables, A_i and B_i are their linguistic values. O is the output variable and Z_i is its linguistics value.

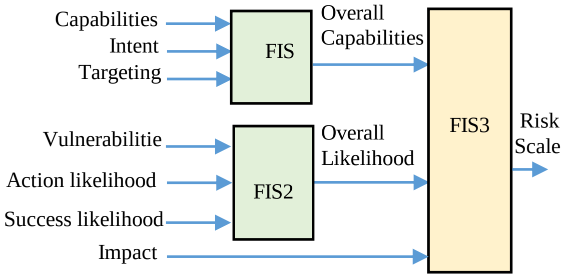


Fig. 4, Proposed Multi Fuzzy Inference System MFIS

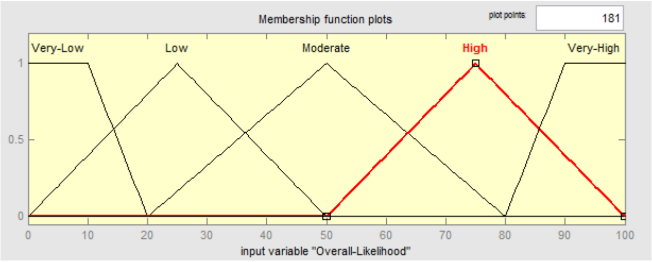


Fig. 5, Fuzzy Sets

TABLE I: Adversary Capability (adapted from [9])

Fuzzy Sets	Meaning
Very High	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

TABLE II: Likelihood of Threat Event Initiation [9]

Fuzzy Sets	Meaning
Very High	Adversary is almost certain to initiate the threat event.
High	Adversary is highly likely to initiate the threat event.
Moderate	Adversary is somewhat likely to initiate the treat event.
Low	Adversary is unlikely to initiate the threat event.
Very Low	Adversary is highly unlikely to initiate the threat event.

TABLE III: Impact of Threat Events (adapted from [9])

Fuzzy Sets	Meaning
Very High	The threat event could be expected to have multiple severe or catastrophic adverse effects.
High	The threat event could be expected to have a severe or catastrophic adverse effect.
Moderate	The threat event could be expected to have a serious adverse effect.
Low	The threat event could be expected to have a limited adverse.
Very Low	The threat event could be expected to have a negligible adverse effect.

Table IV: Level of Risk (adapted from [9])

Fuzzy Sets	Meaning
Very high	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effect.
High	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect.
Moderate	Moderate risk means that a threat event could be expected to have a serious adverse effect.
Low	Moderate risk means that a threat event could be expected to have a serious adverse effect.
Very low	Very low risk means that a threat event could be expected to have a negligible adverse effect.

A. Implementation of MFIS

In this section we briefly describe the implementation of our proposed method by applying it to the risk model explained in section 3. We have implemented our method using Matlab fuzzy toolbox. The FIS editor of fuzzy toolbox is used to define input, output names for FIS1, FIS2, and FIS3 as shown in Fig. 6, Fig. 7, and Fig. 8 respectively. Also to specify, the fuzzy operations such as AND (*min*), and OR (*Max*), and methods used to define Implication (*min*), Aggregation (*max*), and Defuzzification (*centroid*). After that the rule editor of FIS is used to edit, add, delete or change a rule. FIS editor can also be used to change the connection type (AND, OR) and the weight (importance) of a rule, the default value is 1. The rule editor for FIS3 is shown Fig. 9 where all the rules have the same importance (*i.e. weight=1*).

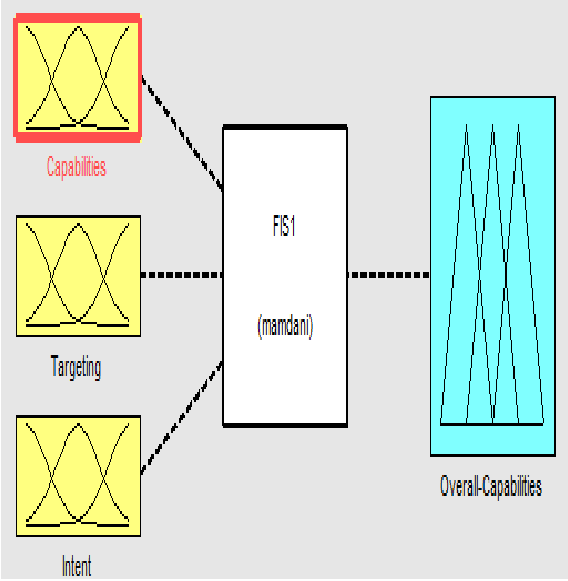


Fig. 6. Overall Capabilities FIS1

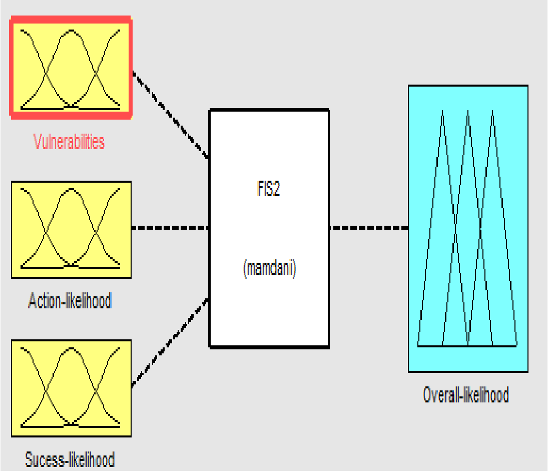
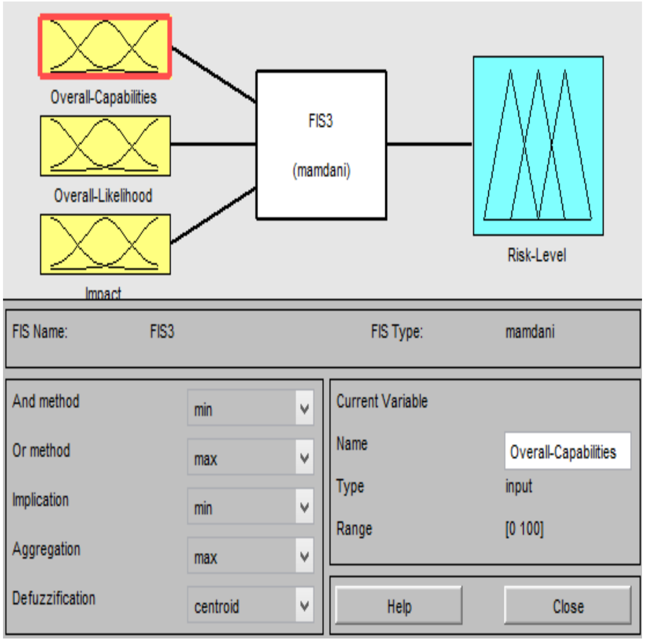


Fig. 7. Overall Likelihood FIS2



FIS Name: FIS3
FIS Type: mamdani

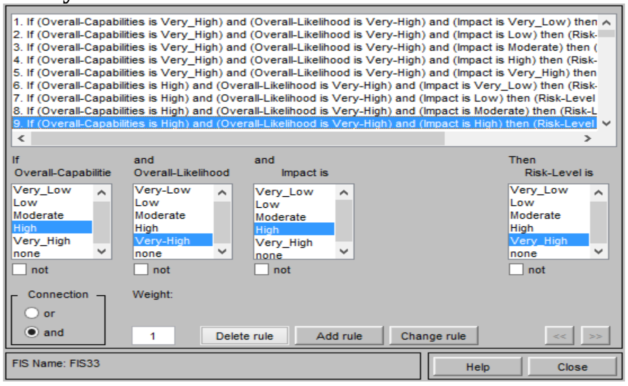
And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: Overall-Capabilities
Type: input
Range: [0 100]

Fig. 8. FIS3 Inputs, Output, and Setting Parameters

B. Rule Viewer

The rule viewer shows a graphical representation of each of the variables through all the rules, a representation of the combination of the rules, and a representation of the output from the defuzzification. It also shows the crisp value output of the system. Data are entered for analysis through the Rule Viewer at the Input text field. Also rule viewer shows the fired rules and fuzzy sets evaluated according to given input. For example as shown in Fig. 10 for inputs overall capabilities 65.66, overall likelihood 83.73, and impact 63, the output risk level is 62.3. The surface viewer of the FIS editor displays a 3-D graph that shows the relationship between the inputs and the output. The output, Risk Level is represented on the *z*-axis while 2 of the inputs, Impact on *x*-axe and overall capability on *y*-axe as shown in Fig. 11, and Impact on *x*-axe and overall Likelihood on *y*-axe as shown in Fig. 12. The surface viewer shows a plot of the possible ranges of the input variables against the possible ranges of the output.



1. If (Overall-Capabilities is Very_High) and (Overall-Likelihood is Very-High) and (Impact is Very_Low) then
2. If (Overall-Capabilities is Very_High) and (Overall-Likelihood is Very-High) and (Impact is Low) then (Risk-
3. If (Overall-Capabilities is Very_High) and (Overall-Likelihood is Very-High) and (Impact is Moderate) then (
4. If (Overall-Capabilities is Very_High) and (Overall-Likelihood is Very-High) and (Impact is High) then (Risk-
5. If (Overall-Capabilities is Very_High) and (Overall-Likelihood is Very-High) and (Impact is Very_High) then
6. If (Overall-Capabilities is High) and (Overall-Likelihood is Very-High) and (Impact is Very_Low) then (Risk-
7. If (Overall-Capabilities is High) and (Overall-Likelihood is Very-High) and (Impact is Low) then (Risk-Level
8. If (Overall-Capabilities is High) and (Overall-Likelihood is Very-High) and (Impact is Moderate) then (Risk-L
9. If (Overall-Capabilities is High) and (Overall-Likelihood is Very-High) and (Impact is High) then (Risk-Level

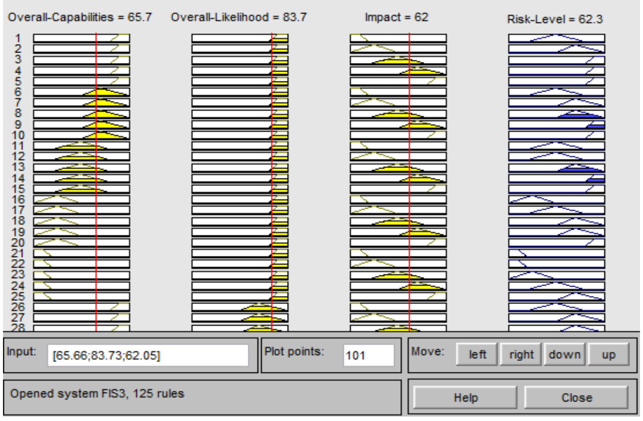
If Overall-Capabilitie	and Overall-Likelihood	and Impact is	Then Risk-Level is
Very_Low	Very-Low	Very_Low	Very_Low
Low	Low	Low	Low
Moderate	Moderate	Moderate	Moderate
High	High	High	High
Very_High	Very-High	Very_High	Very_High
none	none	none	none
□ not	□ not	□ not	□ not

Connection
○ or
● and

Weight: 1

FIS Name: FIS33

Fig. 9. Rule Editor



Input: [65.66;83.73;62.05]
Plot points: 101
Move:
Opened system FIS3, 125 rules

Fig. 10. Rule Evaluation Viewer

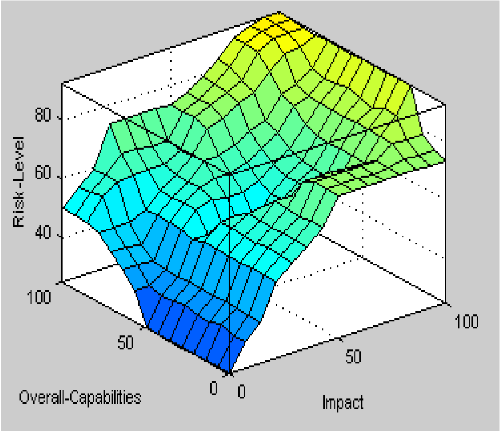


Fig. 11 Surface Viewer for (capabilities, impact, and risk level)

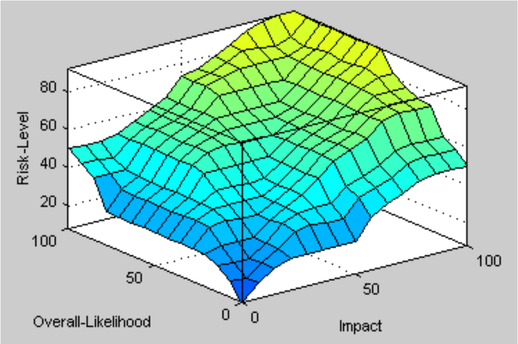


Fig. 12, Surface Viewer for (likelihood, impact, and risk level)

C. Evaluation

The proposed method for risk assessment can be used to evaluate different scenarios of cyber threats and consequently redesigns or modifies or use more security controls to diminish system vulnerabilities. The proposed method can be used model different threat sources such as terrorist, extremist, disgruntled employee, covert agent, and criminal organization with different capabilities, intent, and targeting. As a case study, accessing sensitive information about the transportation of nuclear material from the transportation company information system by hackers, such information can be used by terrorists to steal nuclear material to be used in a dirty pomp. The assessment of such case is explained in Fig.13, the company vulnerabilities are brittle security controls, and employees have shallow security culture, internet connection, and weak physical security. On the other hand, a hacker with deep experience in hacking the servers of information system depending on different vulnerabilities, his intent is to steal information related to nuclear material transportation and buy it to terrorist to get money, so the chance of the hacker success is very high, the chance of stealing nuclear material by a terrorist group is very high, the risk of using such nuclear material in dirty pomp by terrorists is very high. Risk assessment summary for this case is shown in Table V.

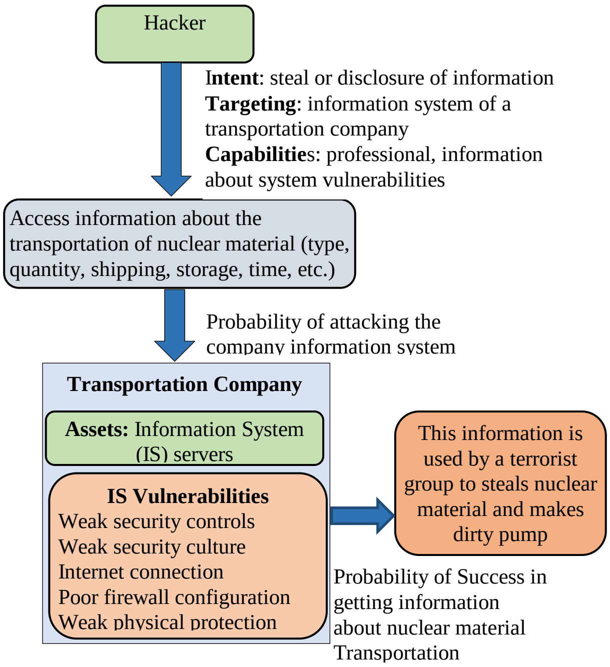

Hacker
Intent: steal or disclosure of information
Targeting: information system of a transportation company
Capabilities: professional, information about system vulnerabilities
Access information about the transportation of nuclear material (type, quantity, shipping, storage, time, etc.)
Probability of attacking the company information system
Transportation Company
Assets: Information System (IS) servers
IS Vulnerabilities
Weak security controls
Weak security culture
Internet connection
Poor firewall configuration
Weak physical protection
This information is used by a terrorist group to steals nuclear material and makes dirty pump
Probability of Success in getting information about nuclear material Transportation

Fig. 13 Risk Assessment for hypothetical Transportation Company

Table V: Risk Assessment Results

Overall Capabilities of hacker	90
Overall likelihood of success	92
Impact	91
Risk level	90

V. CONCLUSION

Fuzzy logic approach had been known as powerful tool for risk assessment due to the fact that most approaches from classical statistics assume that they deal with exact measurements. But in most, if not all real scenarios, there is no precise measurements. Based on that fact, in this paper new method for assessing cyber security risk is introduced. The proposed method is based on a new risk model which takes into account many risk factors such as system vulnerabilities, the likelihood of exploiting such vulnerabilities, and the likelihood of success. Also, the characteristics of a threat source such as his capabilities, intent, and targeting. The principal advantage of this method is the realistic modeling to systems environment in contrast to the common risk model which takes only into account the likelihood of an event and the impact of that event. The proposed method is based on multiple fuzzy inference system MFIS. The first fuzzy inference system FIS1caluclates the overall capabilities of threat source such as extremist group or terrorist group for targeting an asset based on (capabilities, intent, and targeting). The second fuzzy inference system FIS2 calculates the overall likelihood of threat event resulting adversary impact based on risk factors (vulnerabilities, action likelihood, and success likelihood). The third fuzzy inference system FIS3 calculates the risk scale based on the output of FIS1, FIS3 and the impact of adversary action. The implementation of the proposed method can be used as tool for risk assessment of cyber threats targeting any system.

REFERENCES

[1] National Institute of Standards and Technology NIST (Feb. 2012), Framework for Improving Critical Infrastructure Cyber security, Version 1.0

[2] National Institute of Standards and Technology NIST Special Publication 800-39, March 2011, Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View.

[3] U.S. Department of Energy, Electricity Subsector Cyber security Risk Management Process, DOE/OE-0003, May 2012.

[4] M.H. Zirakja, R. Samizadeh, “Risk Analysis in E-commerce via Fuzzy Logic,” Int. J. Manag. Bus. Res., 1 (3), 99-112, summer 2011.

[5] Zadeh, L. A. “Fuzzy sets. Information and Control,” 1965

[6] Sodiya, A.S., Longe, H.O.D. and Fasan, O.M., “Software Security Risk Analysis using Fuzzy Expert System,” In Journal of INFOCOMP: Journal of Computer Science, Brazil, Vol. 7, No. 3, 70—77, 2007.

[7] Rahul Choudhary and Abhishek Raghuvanshi, “Fuzzy Based Evaluation Model of a Systems Security,” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.

[8] Sonia, A. Singhal, H. Banati, “Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD model,”. In IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No. 1, July 2011, Mauritius.

[9] National Institute of Standards and Technology NIST Special Publication 800-30 rev. 1 (Sep. 2012), Guide for Conducting Risk Assessments.

[10] ISO/IEC 27005: 2011 Information Technology- Security techniques - Information security risk management (second edition).

[11] National Institute of Standards and Technology NIST (Feb. 2006), Guide for Developing Security Plans for Federal Information Systems.

[12] Wonderware Invensys Systems, Inc Revision 1.4, (2007), Securing Industrial Control Systems, A guide for properly securing Industrial Control Systems operating in a Microsoft Windows environment.

[13] Homeland, Report, (2011), Common Cyber security Vulnerabilities in Industrial Control Systems.

[14] Ming-Chang Lee, "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method", International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No1, pages 29-45, February 2014

[15] E.W.T. Ngai, and F.K.T. Wat,"Fuzzy decision support system for risk analysis in e-commerce development," Elsevier, Decision Support Systems 40 (2005) 235–255.