Threat modelling on nuclear and radioactive materials based on intelligent approach

Altab Hossain* and A.Z.M. Salahuddin
Department of Nuclear Science and Engineering,
Military Institute of Science and Technology,
Dhaka 1216, Bangladesh
Email: altab@nse.mist.ac.bd
Email: altab76@gmail.com
Email: opu_bka@yahoo.com
*Corresponding author

M.S. Akbar
Bangladesh Atomic Energy Commission,
Dhaka, Bangladesh
Email: shawkat_nped@yahoo.com

Abstract: Threat modelling and assessments are the processes of gathering, organising and analysing existing or potential threats and deemed to have the capabilities to commit a malicious act. Potential adversaries who may attempt unauthorised removal of nuclear materials (NM) or other radioactive materials (RM) for which a physical protection system (PPS) is designed, and therefore must be assessed and prevented. In case of an undesired condition, the authorities have to carry out analytic activities to detect risky circumstances. Hence, in spite of the various methods for threat modelling, it is essential to systematically analyse these threats. Therefore, in this paper, a threat modelling technique by using fuzzy logic based intelligent approach is designed. The technique involves linking the relationship between input parameters of capability, intent, material and vulnerability and output parameter of threat level for nuclear and radioactive materials and their adaptation for the early forecast of irregular behaviour. For inputs overall capabilities 70%, overall likelihood 60%, and impact 60%, the output threat level is estimated as 76.5% for the domestic group deploying an RDD at an annual celebration. Results obtained from the study show the good performance of the developed model as compared to results considering single fuzzy inference system (SFIS).

Keywords: nuclear materials; physical protection system; threat modelling; fuzzy logic.


Biographical notes: Altab Hossain, PhD, CEng (UK), FIEB, is an Associate Professor & Postgraduate Program Coordinator in Nuclear Science & Engineering (NSE) department at Military Institute of Science and Technology (MIST) and served earlier as a Head of NSE department from April 2015 to April 2016. He also served as an Assistant Professor in Mechanical Engineering.
1 Introduction

Nuclear and radioactive materials have a wide range of civilian and military applications such as industry, medicine, agriculture, nuclear power, research reactor in education, and nuclear submarines. However, radioactive materials have unstable nuclei that decay by emitting ionising radiation which in turn damage living tissue and exposure to excess radiation can therefore be harmful to human health. Some radioactive materials can undergo nuclear fission, where heavy atomic nuclei fragment into smaller nuclei, releasing energy and neutrons in the process. These are known as fissile materials such as certain isotopes of uranium and plutonium. Similarly, nuclear material is a term used to describe both fissile materials and non-fissile materials which are suitable for transformation into fissile materials. It is noted that the threat from radiological and nuclear terrorism can be: (a) terrorists detonating nuclear weapons by stealing nuclear material and constructing their own device, (b) dispersing radioactive material by means of a ‘dirty bomb’ and (c) dispersing radioactive material by means of sabotage of a nuclear installation or a shipment of radioactive materials. Hence, nuclear security
system (NSS) of a nuclear installation and its associated facilities is an important part, in particular for safe and reliable operations of nuclear and radioactive materials. In establishing the NSS, it is important to consider factors that make the facility a target for adversarial acts (threats) as well as those that characterise the value or criticality of the facility (consequences). Consequently, the risks to a facility must first be identified and assessed in order to determine if the baseline level of protection is sufficient or if customisation is required (IAEA, 2011, 2013). Moreover, transport of nuclear material and nuclear waste, and also authorisation for the transport of nuclear material are important transients to be considered in nuclear security measures. This situation creates a demand and need for inspecting and assessing of threat level inside or outside the nuclear installation and its associated facilities. Therefore, various researches have been done on this matter to reduce the negative impact of nuclear security activities for the protection of nuclear and other radioactive materials (IAEA, 2009; IAEA, 2015; Hashim et al., 2014). The work on effective and efficient threat assessment is a process of gathering, organising and analysing existing or potential threats and deemed to have the capabilities to commit a malicious act. Hence, several organisations including research institutions with various areas of expertise are essential to work jointly and efficiently. In addition, severe investigation and policy making are crucial in order to establish performance needs for the design of threat analysis model on nuclear and other radioactive materials. However, in case of an undesired condition, commonly known as an introducing episode, the concerned authorities carry out analytic and remedial activities in order to detect possibly risky circumstances. Hence, many approaches have been practised to identify and assess threats and risks that are consistent with international guidance (Hashim et al., 2014; Barry et al., 2000; Rachid et al., 2016; Gowri and Posonia, 2016; Boc et al., 2012). However, risk informed approach is an iterative approach though it is essential for undesirable consequences resulting from a nuclear security event. When an event arises starting from the steady state operation of nuclear reactor, an extensive range of advanced nuclear accidents including those caused by system or structural failures could result in a core meltdown and dispersion of radiation, are essential to analyse by systematically according the threats. On the other hand, probabilistic risk analysis (PRA) or qualitative risk assessment (QRA) approaches have been practised for assessing terrorism risks and informing risk management decisions, in particular in areas such as environmental protection, industrial safety and so on (Barry et al., 2000; Rachid et al., 2016). They have their own advantages and disadvantages. However, there is a major challenge in risk analysis of terrorism due to the unlike nature of terrorist acts especially on nuclear and radioactive materials. To challenge this problem, a number of linear and nonlinear pattern recognition methods have been utilised (Gowri and Posonia, 2016). Artificial intelligence systems are extensively recognised as a technology donating a substitute to grab difficult and vague problems. They can acquire from examples, are intelligent to tackle noisy and imperfect data, and are capable to deal with non-linear problems such as nuclear reactors and their adaptation for the early prediction of irregular behaviour. However, it needs the identification of possible incidences of events and charting of the each event with the pertinent constraints. Compared with traditional methods, fuzzy expert system (FES) is more appropriate and proficient in relating the numerous inputs to a single output in a
non-linear domain, particularly in a convenient way to conduct risk analysis (Boc et al., 2012; Zlateva et al., 2015). Moreover, security risk assessment is growing gradually to identify threat level as well as system vulnerabilities using fuzzy based evaluation model or multi fuzzy inference system (Choudhary and Raghuvanshi, 2012; Sallam, 2015). Therefore, the aim of the present work is to study the application of FES model on a complex system such as nuclear and radioactive materials and their adaptation for the early forecast of irregular behaviour. The choice of fuzzy set theory as the main analytical tool is due to the good applicability of this approach to uncertain security conditions. Generally, fuzzy sets use the linguistic expressions instead of numerical values as compared to classical data sets.

The purpose of this study is to examine the relationship between threat parameters such as capability, intent, material and vulnerability for nuclear and radioactive materials and their impact of severity, and to illustrate how fuzzy expert systems might play an important role in assessment of threat. In order to deliver heuristics as well as intelligent support for NM and RM, the entire nuclear database is considered under one roof with the help of expert system. For implementation of fuzzy theory into the system, the fuzzy toolbox from MATLAB has been used. Four fundamental units such as fuzzification unit, the knowledge base (rule base), the inference engine and defuzzification unit are necessary for successful application of fuzzy modelling approach. The construction of fuzzy knowledge-based model using if-then rules for the threat assessment on nuclear materials is actually based on Mamdani approach (Mamdani and Assilian, 1975).

2 Threat assessment model

Threat assessment model is the process of identifying, quantifying and analysing existing or potential threats that are deemed to have the capabilities to commit a malicious act (IAEA, 2009; Sallam, 2015). An evaluation of the threat generally includes intelligence assessment that documents credible intents, motivations, and capabilities to cause undesirable consequences to nuclear materials (NM) or other radioactive materials (RM). The sabotage for which a physical protection system (PPS) is designed, can lead to unacceptable consequences and therefore must be assessed and prevented. The capabilities of adversaries are usually estimated by their composition, grouping, intent, explosive tools, level of skills, etc. Threat assessment is generally based on the evaluation of various factors. Some of them are: intent and capability of adversaries, nuclear material (NM) or other radioactive material (RM), and the vulnerability of the target (IAEA, 2015). Capability can be categorised as organisational, technical and financial. Similarly, intent of adversaries can be categorised as ideology and objective. Consequently, the possibility of creating a device can be distributed into the material, the effort of attaining material and the difficulty of constructing the device. Finally, the vulnerability of the target can be divided into the type of target and the timing of an attack. Assailants often break into systems and cause a lot of damage and hence, there is a demand to know the level of risk by using threat modelling. Generally, risk is calculated as to multiply the severity (Impact) of consequences by the likelihood of their occurrence (Sallam, 2015). Subsequently, 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). However, an important component known
as ‘capabilities of threat source’ is also to be included in risk level estimation since the
success of threat source in targeting a system is dependent on the capabilities. Therefore,
the risk level can be evaluated as a function of overall capabilities, overall likelihood, and
impact, as explained by the following equations (Sallam, 2015).

\[
\text{Risk} = (\text{overall capabilities, overall likelihood, impact}) \tag{1}
\]

\[
\text{Overall capabilities} = (\text{capability, intent, target}) \tag{2}
\]

\[
\text{Overall likelihood} = (v, a, s) \tag{3}
\]

where \(v\) is the vulnerability, \(a\) is the action likelihood, and \(s\) is the success likelihood.

### 3 Use of intelligent approach

The prospective consequences of any nuclear security events, in particular for nuclear
and radioactive material, could be catastrophic. There are various types of threat
assessment and several methodologies suitable for a diversity of situations. One of the
important features of any sabotage threat assessment is the intelligent approach used to
characterise and model terrorist adversaries. An intelligent approach based on fuzzy
expert system (FES) can be used to assist threat modelling in evaluating various options
and accordingly prioritising the nuclear security measures.

#### 3.1 Development of fuzzy expert system

The term of fuzzy logic has been acquired from fuzzy set theory and it is a branch of
mathematics developed by Zadeh at the University of California in 1965 (Mamdani and
Assilian, 1975). The basic structure of the fuzzy expert system is divided into four major
parts shown in Figure 1 (Hossain et al., 2012). They are: (1) Fuzzification – which
takes the crisp numeric inputs and converts them into information of fuzzy form, (2)
Knowledge base – which holds a set of linguistic terms, if-then rules that quantify the
knowledge like human experts about solving problems, (3) Decision making logic –
which creates the control actions according to the information provided by the
fuzzification module by applying knowledge about how best to control the plant, and (4)
Defuzzification – which creates the actual output, i.e. converts fuzzy output into precise
numerical values (crisp values) and then sends them to the physical system (plant or
process), so as to execute the control of the system.

![Figure 1 Structure of fuzzy expert system (FES)](image-url)
3.2 Implementation of fuzzy expert system

The system is designed using multi fuzzy inference system (MFIS) in a form of ‘IF and THEN’ rules which relate input and output variables mentioned in equations (1) to (3). The multi fuzzy inference system for threat modelling consists of three fuzzy inference systems (FIS) as shown in Figure 2. The first fuzzy inference system (FIS 1) determines the overall capabilities based on equation (2). The second fuzzy inference system (FIS 2) determines the overall likelihood based on equation 3. Finally, the third fuzzy inference system (FIS 3) determines the risk level to make threat model based on the output from FIS 1 and FIS 2 and the adversary impact (equation 1).

![Figure 2: Fuzzy threat assessment model](image)

For fuzzification, three possible linguistic variables, namely, low (L), medium (M), and high (H) were chosen for all the variables except the final output variable ‘Threat Level’, where five linguistic variables, namely very low (VL), low (L), medium (M), high (H) and very high (VH) were considered. The sample membership functions of input variable ‘Capability’ and output variable ‘Threat level’ are shown in Figures 3 and 4. In this study, the membership functions for input and output variables have been selected based on system knowledge, and expert’s appraisals. The membership functions of the linguistic terms are characterised by trapezoidal membership functions for ‘Low’ and ‘High’, and triangular shaped membership functions have been used for the input variables due to their wide applications, well suited for modelling, designing and accuracy (Sallam, 2015; Hossain et al., 2012). A similar pattern has been selected for the membership functions of ‘Very Low’ and ‘Very High’ in case of the final output variable. An important benefit of providing threat ratings is that they may be transformed or interpreted as likelihood estimates, and such estimates can support quantitative risk assessment methodologies. However, threat sources such as terrorists have different capabilities of the adversary, intent, material amount and type of device, and targeting a system. In this study, a domestic adversary group that has advocated the overthrow of any government has been considered in determining the threat level for their violent acts. Table 1, Table 2, Table 3, and Table 4 show the meaning of membership functions for the variables, overall capabilities, overall likelihood, impact, and threat level, respectively.
Figure 3  Membership functions of input variable ‘Capability’

![Membership function plots for Capability](image1.png)

Figure 4  Membership functions of output variable ‘Threat-Level’

![Membership function plots for Threat-Level](image2.png)

Table 1  Adversary capabilities (adapted from Sallam, 2015)

<table>
<thead>
<tr>
<th>Fuzzy Sets</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>The adversary has limited resources, expertise, and opportunities to support a successful attack.</td>
</tr>
<tr>
<td>Medium</td>
<td>The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.</td>
</tr>
<tr>
<td>High</td>
<td>The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.</td>
</tr>
</tbody>
</table>
Table 2  Likelihood of threat event initiation (adapted from Sallam, 2015)

<table>
<thead>
<tr>
<th>Fuzzy Sets</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>The adversary is unlikely to initiate the threat event.</td>
</tr>
<tr>
<td>Medium</td>
<td>The adversary is somewhat likely to initiate the threat event.</td>
</tr>
<tr>
<td>High</td>
<td>The adversary is highly likely to initiate the threat event.</td>
</tr>
</tbody>
</table>

Table 3  Impact of threat events (adapted from Sallam, 2015)

<table>
<thead>
<tr>
<th>Fuzzy Sets</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>The threat event could be expected to have a limited adverse effect.</td>
</tr>
<tr>
<td>Medium</td>
<td>The threat event could be expected to have a serious adverse effect.</td>
</tr>
<tr>
<td>High</td>
<td>The threat event could be expected to have a severe or catastrophic adverse effect.</td>
</tr>
</tbody>
</table>

Table 4  Level of threat (adapted from Sallam, 2015)

<table>
<thead>
<tr>
<th>Fuzzy Sets</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>Very low threat means that a threat event could be expected to have a negligible adverse effect.</td>
</tr>
<tr>
<td>Low</td>
<td>Moderate threat means that a threat event could be expected to have a serious adverse effect.</td>
</tr>
<tr>
<td>Medium</td>
<td>Moderate threat means that a threat event could be expected to have a serious adverse effect.</td>
</tr>
<tr>
<td>High</td>
<td>High threat means that a threat event could be expected to have a severe or catastrophic adverse effect.</td>
</tr>
<tr>
<td>Very High</td>
<td>Very high threat means that a threat event could be expected to have multiple severe or catastrophic adverse effect.</td>
</tr>
</tbody>
</table>

It is noted that if there is minimal information for a particular variable and this variable is a responsive indicator, the range of values is divided into numerous identical triangular membership functions (Gopal, 2009).

\[
\mu_{\text{triangle}}(x,c_1,c_2,c_3) = \begin{cases} 
0; & x < c_1 \\
\frac{x - c_1}{c_2 - c_1}; & c_1 \leq x \leq c_2 \\
\frac{c_3 - x}{c_3 - c_2}; & c_2 \leq x \leq c_3 \\
0; & x > c_3 
\end{cases} \quad (4)
\]

In this case, the edge of the variable’s interval may be represented with linear Z- and S-shaped functions described respectively as

\[
\mu_z(x,c_1,c_2) = \begin{cases} 
1; & x \leq c_1 \\
\frac{c_2 - x}{c_2 - c_1}; & c_1 < x < c_2 \\
0; & x \geq c_2 
\end{cases} \quad (5)
\]
In equations (4–6), $x$ is the input and output variable, $c_1$, $c_2$, and $c_3$ are the coefficients of membership functions for the described input and output variables. In this study, a Mamdani max-min inference approach and the centre of gravity defuzzification method have been used since these operators assure a linear interpolation of the output between the rules. After that the rule editor of FIS is developed to alter the rules when necessary. A sample rule editor for FIS 3 is shown in Figure 5. For the input and output parameters, a fuzzy associated memory was created as regulation rules based on expert knowledge.

### 3.3 Rule viewer

The rule viewer actually displays a graphical depiction of each of the variables through all the rules, an illustration of the combination of the rules, and a demonstration of the output from the defuzzification. The operation of the fuzzy expert system is shown schematically in Figure 6. An example for the assessment of a certain domestic insurgent group deploying an RDD (radiological dispersal device) at an annual celebration (IAEA, 2015) is shown in the Figure 6. It is noted that the domestic group has a strong organisation and is well funded but has less knowledge of nuclear material or other radioactive material. On the other hand they have good motivation to carry out an act that increases their profile. Consequently, the desired radioactive material is available in average but access to it is tightly controlled. Lastly, the target is civilian and highly
vulnerable, but timing is very limited to ensure maximum impact. For example as shown in Figure 6 for inputs overall capabilities 70%, overall likelihood 60%, and impact 60%, the output threat level is estimated as 76.5% for the domestic group deploying an RDD at an annual celebration of an example place. Results obtained from the study shows the good performance of the developed model as compared to results considering single fuzzy inference system (SFIS) and published by the authors elsewhere (Salahuddin et al., 2016). However, the rating of input variables is dependent on the methodology used for the assessment of overall threat level rating. Moreover, the threat model can be improved with better accuracy by adding more factors and rules.

Figure 6  Rule evaluation viewer

Using MATLAB the fuzzy control surface was developed as shown in Figure 7. These can serve as a visual depiction of how the fuzzy expert system operates dynamically over time. The images show the mesh plots for the above example case, showing the relationships between overall capabilities, and overall likelihood on the input side and threat level on the output side. The plots are used to verify the rules and membership functions and to see if they are appropriate or whether modifications are necessary to improve the output. The plot shows that when overall capabilities and overall likelihood increases, the threat will be higher.
Figure 7  Graphically surface viewer for threat matrix

3.4 Evaluation

The rule viewer displays a graphical depiction of each of the variables through the evaluation of the proposed model and shows a system that can be effectively used for threat assessment on nuclear and radioactive materials. The fuzzy based expert systems were used to analyse using different assumed values and the output shows that the system is robust enough for the evaluation of the threat level. A good correlation (‘High’ and ‘Very High’) has been found for the results of both methods (risk informed approach, Ref. (IAEA, 2015), and proposed intelligent approach). However, the result from proposed intelligent model using fuzzy expert system is more precise and defined in details with their final score. A terrorist with deep experience or interest to attack the target depending on different vulnerabilities, his intent is to steal information related to nuclear material transportation to cause civilian causalities, so the possibility of the terrorist success is very high, the possibility of stealing nuclear material by a terrorist group is very high, the threat of using such nuclear material in dirty pomp by terrorists is very high. Through this way the proposed intelligent approach for threat assessment on nuclear and radioactive materials can be used to evaluate different scenarios of nuclear security threats. Consequently, this model will assist nuclear security persons or policy makers to categorise the threat levels.

4 Conclusion

In this paper, a fuzzy logic-based intelligent approach has been proposed for threat modelling on nuclear and radioactive materials to categorise the threat level. The main advantage of this approach is the practical modelling to systems atmosphere in contrast to the common threat model such as risk informed approach. The proposed method is based on multi fuzzy inference system MFIS. The third (final) fuzzy inference system (FIS 3) calculates the threat scale from the combinations of three input variables (two obtained from first and second fuzzy inference system, respectively and combined with new input variable known as ‘Impact’). The implementation of the proposed method can be used as
a tool for threat assessment of nuclear security threats targeting any system in more detailed and decisive way. As compared with the existing ranking method, this approach is more precise and accurate and will also assist to reduce the threat ties wherever possible. However, the specific conclusions can be drawn from this study as follows:

1. For inputs overall capabilities 70%, overall likelihood 60%, and impact 60%, the output threat level is estimated as 76.5% which shows the good performance of the developed model.

2. This model can integrate the opinions of experts in a more accurate way and can rank the threat level quantitatively with the early forecast of irregular behaviour.

The model gives better results as compared to the results obtained with considering single fuzzy inference system (SFIS) (Salahuddin et al., 2016).

5 Future studies

The rating of input variables is dependent on the methodology used for the assessment of overall threat level rating. Moreover, the threat model can be improved with better accuracy by adding more factors and rules. A state should allocate its resources more effectively and efficiently by systematically future studying with human verification for the threats and risks to avoid unauthorised removal of nuclear materials (NM) or other radioactive materials (RM) and sabotage for which a physical protection system (PPS) is designed.

Acknowledgement

The authors are grateful for the support provided by Military Institute of Science & Technology (MIST) for this project.

References


