This item is the archived peer-reviewed author-version of:

A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry

Reference:

Zhou Jianfeng, Reniers Genserik, Zhang Laobing.- A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry
Chemical engineering science - ISSN 0009-2509 - 174(2017), p. 136-145
Full text (Publisher's DOI): <https://doi.org/10.1016/J.CES.2017.09.002>
To cite this reference: <https://hdl.handle.net/10067/1455410151162165141>

A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry

Jianfeng Zhou ^a, Genserik Reniers ^{b, c, d, *}, Laobing Zhang ^b

a. School of Electromechanical Engineering, Guangdong University of Technology, Guangzhou 510006, China

b. Faculty of Technology, Policy and Management, Safety and Security Science Group (S3G), TU Delft, 2628 BX Delft, The Netherlands

c. Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000 Antwerp, Belgium

d. CEDON, KULeuven, 1000 Brussels, Belgium

Abstract: As large amounts of hazardous chemicals are handled in the petrochemical industries, the plants in these industries are attractive for terrorists because they can cause great losses and have important social impact. Security risk assessment is important to determine the risk level of a plant in order to take targeted measures to reduce the security risk. Based on Security Risk Factor Table (SRFT) which covers the essential elements for the security risk assessment, a weighted fuzzy Petri-net (WFPN) based security risk assessment approach is proposed in this paper. This approach can easily model different relationships between the risk factors as well as their importance, and use the analysis method of Petri-nets to perform the risk assessment. Two WFPN models of security risk assessment are established according to different relationships between the factors, and a matrix operation based security risk inference method is developed. An illustrative example is used to demonstrate the approach. The results show that correctly determining and modeling the relationships among the risk factors is important to assess the security risk.

Keywords: security; risk assessment; terrorism; weighted fuzzy Petri-net; chemical industry

*Corresponding author.

Nomenclature			
$P = \{p_1, p_2, \dots, p_n\}$	Place set	$T = \{t_1, t_2, \dots, t_m\}$	Transition set
M	Marking of Petri-net	M_0	Initial marking
$W = \{w_{ij}\}$	Weight matrix	w_{ij}	Weight of place p_i for transition t_j
$U = \{\mu_{ij}\}$	Certainty factor matrix of transitions	μ_{ij}	Certainty factor of transition t_j for the output place p_i .
$\alpha(p_i)$	Truth value in place p_i .	$D = \{d_1, d_2, \dots, d_n\}$	Proposition set
α_i	Truth value	CF	Certainty factor
μ_i	Certainty factor	μ'_i	Certainty factor
$A = \{a_{ij}\}$	Judgment matrix	a_{ij}	Importance of factor a_i on a_j
idx	Times of iteration	Γ_{idx}	Vector of equivalent fuzzy truth values of the transitions at iteration idx

29

30 1. Introduction

31 In the petrochemical industries, a large number of hazardous chemicals are handled in
32 production or storage activities. The corresponding production, storage, or transportation facilities
33 therefore may have a strong appeal to terrorists as large amounts of hazardous chemicals can be
34 used by the terrorist as weapons of mass destruction.

35 After the 9-11 events, intentional events/attacks that are likely to cause severe consequences
36 are getting more and more attention. These attacks can vary through a wide range from mundane
37 (e.g., thieving) to potentially highly damaging terrorist actions. Therefore risks related to
38 intentionally intruded activities within chemical plants need to be assessed.

39 The assessment of industrial security risk has been studied by some scholars. Bajpai and
40 Gupta (2005; 2007) discussed essential steps of security risk assessment which include threat

analysis, vulnerability analysis, security countermeasures, and emergency response. Depending on the threat likelihood and vulnerabilities, various security countermeasures were suggested to improve plant security. Reniers et al. (2008) provided a theoretical conceptualization on how to manage the prevention and the mitigation of intentionally induced domino effects in a possibly very complex industrial cluster. A software tool was developed to deal with taking preventive measures concerning domino effect-related security risks. Bajpai et al. (2010) modified the SRFT (Security Risk Factor Table) model using the concepts of fuzzy logic. In the modified fuzzy SRFT model, two linguistic fuzzy scales (three-point and four-point) are devised based on trapezoidal fuzzy numbers. Human subjectivity of different experts associated with the previous SRFT model is tackled by mapping the scores to the fuzzy scale. Finally, the fuzzy score obtained is defuzzified to get the results. Moore (2013) examined the key elements of the American National Standards Institute (ANSI)/American Petroleum Institute (API) Security Risk Assessment (SRA) process and discussed how forward-thinking organizations may use risk-based performance metrics to analyze plant security postures and identify cost effectively countermeasures based on current and projected threats. The ANSI/API SRA is a tool to assist management in making structured decisions regarding the need of threat-based countermeasures tied to risk-based performance measures. Reniers et al. (2015) proposed a security risk assessment and protection methodology that was developed for use in the chemical and process industries in Belgium. The model combines the rings-of-protection approach with generic security practices including management and procedures, security technology (e.g., CCTV, fences, and access control), and human interactions (proactive as well as reactive). Zhang and Reniers (2016) analyzed the general intrusion detection system in process plants, and proposed a game-theoretical model for security risk assessment in such plants.

The risks originating from terrorists' attacks must be examined to determine if the existing security measures are adequate or need enhancement. The four essential elements for the security risk assessment of the chemical process industry are: threat analysis; vulnerability analysis; security countermeasures; and mitigation and emergency response. ACS (2002) has shown that the risk assessment can also be carried out by developing a Security Risk Factor Table (SRFT) for a given chemical plant. The factors influencing the overall security of a plant need to be identified

and rated on a scale from 0 to 5, with 0 being the ‘lowest risk’ and 5 the ‘highest risk’. The total score obtained from SRFT helps in assessing the current security risk status of the plant or the facility. Bajpai and Gupta (2005), Bajpai and Gupta (2007), and Bajpai et al. (2010) discussed and modified the SRFT method.

A Security Risk Factor Table (SRFT) is shown in Table 1.

Table 1 Security risk factors

Risk factors	Range of security points			
Location	Rural (1)	Urban (2,3,4)		High density (5)
Visibility	Not visible (0)	Low (1,2)	Medium (3,4)	High (5)
Inventory	Low (1)	Medium (2)	Large (3,4)	Very large (5)
Ownership	Private (1)	Public/co-operative(2,3)		Government(4,5)
Presence of chemicals which can be used as precursors for WMD (Weapons of Mass Destruction)	Absence (0)	Presence (5)		
Worst case impact on-site	Negligible (0)	Low (1)	Moderate(2,3,4)	Severe (5)
Worst case impact off-site	Negligible (0)	Low (1)	Moderate(2,3,4)	Severe (5)
History of security incidents	Nil (0)	Few (1,2,3)		Frequent (4,5)
Presence of terrorist groups in region	Absence (0)	Few (1,2,3)		Large no. (4,5)
Existing security measures	High level	Ordinary		Poor/none
Access control	1	2, 3		4, 5
Perimeter protection	1	2, 3		4, 5
Mitigation potential	1	2, 3		4, 5
Proper lighting	1	2, 3		4, 5
Use of metal detector/ X-ray/ CCTV (Closed-Circuit Television, at entrance and at all critical locations)	1	2, 3		4, 5
Personal preparedness and training	Well prepared(1)	Average (2,3)		Poor (4,5)

Although this approach is simple and easy to use, it has several deficiencies:

(i) It can't reflect the importance of the factors to the risk. As each factor is rated on a scale from 0 to 5, this means that all the factors are of the same importance. In most cases, this is not in conformity with the actual situation.

(ii) It can't reflect the relationship between the factors. This scoring approach implies that all factors have an "AND" relationship. However, in some conditions, an "OR" relationship may be considered between some factors. For example, if any factor for the security measures is not available, the security measures are considered to be invalid. This cannot be handled by traditional risk assessment approaches including this scoring method.

To solve these problems, the weighted fuzzy Petri-net is introduced based on the SRFT to assess the security risk in this study, because Petri-net is very suitable for modeling the relationship between the various parts of a system, such as sequential, parallel, conflict, etc, and the weights can reflect the importance of the parts of the system. In this study, the SRFT method is improved based on the weighted fuzzy Petri-net.

Petri-net (PN) was proposed by Dr. Petri in 1962 when he developed the information flow model of the computer operating system (David and Alla, 1994). It is a graphical modeling and analysis tool, including elements like places, transitions, arcs and tokens. Petri-nets are widely used to model and analyze discrete event systems such as communication, manufacturing, and transportation systems. Zisman (1978) pointed out that Petri-net transitions can be interpreted as rules in specific production rule systems. PN and artificial intelligence (AI) can be combined to achieve some goals difficult to fulfill by using only one of them. In order to deal with uncertainty, several authors from PN and AI communities have proposed different kinds of fuzzy Petri-net (FPN) based on different notions (Looney, 1988; Valette et al. 1989). After that, there had been a lot of research done on FPN and a number of their applications, including the weighted fuzzy Petri-net (WFPN) (Chen, 2002; Ha et al. 2007; Liu et al., 2013).

The scoring for the risk factors in a normal SRFT is uncertain in nature, so we put it together with fuzzy theory. In addition, the security risk assessment requires modeling the importance of factors and their relationships. Hence, WFPN is adopted as an analysis tool. WFPN has been efficiently used in many fields, such as fault diagnosis of power systems. (Cheng et al., 2015; Zhang et al., 2016) and esophageal cancer prediction (Hamed, 2015). It can also perform security

risk analysis according to the theory of fuzzy Petri-net, e.g. fuzzy reasoning.

This study discusses the security risk assessment approach based on WFPN. In Section 2, the definition of WFPN is provided. In Section 3, WFPN-based models of security risk assessment and the security risk inference process are proposed. An illustrative example is discussed in Section 4. Conclusions of this study are formulated in Section 5.

2. Weighted fuzzy Petri-net

(i) Petri-net

Petri-nets are mathematical modeling tools used to analyze and simulate concurrent systems (Murata, 1989). The system is modeled as a directed graph with two sets of nodes: the set of places that represent state or system objects and the set of events or transitions that determine the dynamics of the system. Usually, the places are denoted by circles, and the transitions are denoted by rectangles.

A Petri net is a 5-tuple:

$$PN = (P, T, I, O, M)$$

Where:

$P = \{p_1, p_2, \dots, p_n\}$ is a finite set of places.

$T = \{t_1, t_2, \dots, t_m\}$ is a finite set of transitions.

I : an input function, $(P \times T) \rightarrow \mathbb{N}$, where $\mathbb{N}$ is the set of non-negative integer numbers. The value $I(p, t)$ is the number of (directed) arcs from the place p to the transition t .

O : an output function, $(T \times P) \rightarrow \mathbb{N}$, where the value $O(t, p)$ is the number of arcs from the transition t to the place p .

M : $P \rightarrow \{0, 1, 2, 3, \dots\}$ is the initial marking assigning to place p a non-negative integer k , i.e., marking place p with k tokens.

Places are represented with circles, and transitions are represented with rectangles on PN graphs. The arcs (input and output functions) are represented with directed lines.

(ii) Fuzzy logic

Fuzzy logic networks are used to modify Petri-Nets, allowing rule-based fuzzy decision systems to be represented and executed.

To deal with vagueness in human thought, Zadeh (1965) first proposed fuzzy set theory which has the capability to deal with uncertain data and information possessing. Moreover, fuzzy set theory has been designed to mathematically represent uncertainty and vagueness and provide formalized tools for dealing with imprecision inherent to decision making problems.

A fuzzy subset A of set X, called a universe of discourse, can be defined as the set of ordered pairs $(x, \mu_A(x))$, where $\mu_A(x)$ is the membership function for fuzzy set A, defined as

$$\mu_A: X \rightarrow [0, 1]$$

This function can take on any value within the interval from 0 to 1. A value of 0 implies non-membership in set A and a value of 1 implies full membership in the set. When considering the statement “x is in A”, the membership will tell us whether the statement is true, false, or partially true, in which case x is said to belong to A with degree of membership $\mu_A(x)$. A fuzzy number is a specific case of a fuzzy set whose membership function is continuous, convex and defined over a closed interval of real numbers. Membership function can take on different shapes, triangular or trapezoidal, which are characterized by a reduced number of parameters, are the most typical ones, though Gaussian or generalized bell shapes are also common.

Fuzzy logic can be used to represent production rules (IF-THEN rules) with fuzziness or vagueness. A fuzzy rule of the if-then type has the following form:

If x is A then y is B

Where A and B are specific assessments of linguistic variables. The term “x is A” is called the antecedent, while the term “y is B” is the consequent. Both the antecedent and the consequent adopt memberships to express the truth values. In addition, a fuzzy rule usually has a certainty factor (CF) which is a value within the interval from 0 to 1 to indicate the confidence when applying the rule.

(iii) Weighted fuzzy Petri-net

A fuzzy Petri-net is an extension of Petri-net by using fuzzy logic rather than Boolean logic (Looney, 1998). The fuzziness concept can be incorporated in Petri-nets by applying a fuzzy

reasoning mechanism over the Petri-nets structure.

The fuzzy production rules of a rule-based system can be represented by a fuzzy Petri-net (FPN) model. Each place may or may not contain a token associated with a truth value between zero and one. Each transition is associated with a certainty factor value between zero and one. The relationships from places to transitions and from transitions to places are represented by directed arcs. Based on the fuzzy Petri-net definitions of Chen et al. (1990) and Gao et al. (2003), a generalized fuzzy Petri net can be defined as a 9-tuple:

$$FPN = (P, T, I, O, M, D, U, R, \alpha)$$

Where, (P, T, I, O, M) defines a Petri-net, and

$I: P \rightarrow T$ is the input function, a mapping from places to transitions.

$$I = \{\beta_{ij}\} = \begin{cases} \beta_{ij} = 1, p_i \text{ is input of } t_j \\ \beta_{ij} = 0, p_i \text{ is not input of } t_j \end{cases} \quad (1)$$

$O: T \rightarrow P$ is the output function, a mapping from transitions to places.

$$O = \{\beta_{ij}\} = \begin{cases} \beta_{ij} = 1, p_i \text{ is output of } t_j \\ \beta_{ij} = 0, p_i \text{ is not output of } t_j \end{cases} \quad (2)$$

$\alpha: P \rightarrow [0,1]$ is an association function, a mapping from places to real values between zero and one.

M is a marking of the FPN. $M = (\alpha(p_1), \alpha(p_2), \dots, \alpha(p_n))^T$. The initial marking is denoted by M_0 . $\alpha(p_i)$ is the truth value in place p_i .

$D = \{d_1, d_2, \dots, d_n\}$ is a finite set of propositions. $|P| = |D|$.

$U: T \rightarrow P$ is an association function, a mapping from transitions to real values between zero and one. $U = \{\mu_{ij}\}$, $j = 1, 2, \dots, m$; $i = 1, 2, \dots, n$, where, μ_{ij} is the certainty factor of transition t_j for output place p_i .

$R: P \rightarrow D$ is an association function, a bijective mapping from places to propositions.

In many cases of decision making, decision factors have impacts on the decision-making goal(s), and the importance of each factor is different. Accordingly, in a production rule, the propositions in an antecedent usually have different importance. Chen (2002) presented a weighted fuzzy Petri-net model to represent the fuzzy production rules of a rule-based system. On

this basis, a generalized weighted fuzzy Petri Net (WFPN) structure can be defined as a 10-tuple:

$$WFPN = (P, T, I, O, M, D, U, R, \alpha, W)$$

Where, $(P, T, I, O, M, D, U, R, \alpha)$ defines a fuzzy Petri-net, and

$W: P \rightarrow T$ is an importance function of places, a mapping from places to real values between 0 and 1, $W = \{w_{ij}\}$, $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$, where, w_{ij} is the weight of place p_i for transition t_j .

3. Security risk assessment based on WFPN

(1) WFPN models for security risk assessment

WFPN can be used to establish an intuitive graphical production rule model. In security risk assessment, the logical relationships among risk factors can be transformed into the relationships of transitions and places of WFPN. There are two basic relationships of the production rules, namely, "AND" and "OR", in the hierarchical risk assessment:

“AND” rule: If $d_1(\alpha_1, w_1)$ AND $d_2(\alpha_2, w_2)$ AND ... AND $d_k(\alpha_k, w_k)$ Then d_g (CF = μ) (3)

“OR” rule: If $d_1(\alpha_1)$ OR $d_2(\alpha_2)$ OR ... OR $d_k(\alpha_k)$ Then d_g (CF = $\mu_1, \mu_2, \dots, \mu_k$) (4)

Where, $\mu, \mu_1, \mu_2, \dots, \mu_k$ are fuzzy numbers defined in the universe of discourse $[0, 1]$, indicating the certainty factor (CF) of the rule.

Fig. 1 shows how the “AND” rule is converted to WFPN, and Fig. 2 shows the conversion of the “OR” rule.

Fig. 1 WFPN model of “AND” fuzzy production rule

In the “AND” WFPN model,

$$\alpha_g = (\alpha_1 \times w_1 + \alpha_2 \times w_2 + \dots + \alpha_k \times w_k) \times \mu \quad (5)$$

Fig. 2 WFPN model of “OR” fuzzy production

In the “OR” WFPN model,

$$\alpha_g = \max(\alpha_1 \times \mu_1, \alpha_2 \times \mu_2, \dots, \alpha_k \times \mu_k) \quad (6)$$

The risk factors of SRFT shown in Table 1 are adopted to establish the hierarchical security risk assessment index system, and based on the security risk assessment index system, the corresponding WFPN model is established according to the conversion approaches shown in Fig. 1 and Fig. 2. Thus, the security risk assessment can be converted to evaluate the truth value of the target proposition (d_{17} in this work).

The propositions/places of the WFPN model relating to the indices are listed in Table 2, where, d_i ($i=1, 2, \dots, 17$) indicates the propositions in the production rules for security risk assessment, and p_i ($i=1, 2, \dots, 17$) indicates the corresponding places in the WFPN model. The proposition d_{17} and corresponding place p_{17} reflect the assessment objective, that is, whether the security risk is very high.

Table 2 Propositions/Places of the WFPN model for security risk assessment

Name	Proposition/Place	Name	Proposition/Place
d_1/p_1	Access control is poor	d_{10}/p_{10}	Chemicals which can be used as precursors for WMD exist
d_2/p_2	Perimeter protection is poor	d_{11}/p_{11}	Worst case impact on-site is severe
d_3/p_3	Mitigation potential is poor	d_{12}/p_{12}	Worst case impact off-site is severe

d ₄ /p ₄	Proper lighting is poor	d ₁₃ /p ₁₃	History of security incidents is frequent
d ₅ /p ₅	Use of metal detector/ X-ray/ CCTV is poor	d ₁₄ /p ₁₄	Large number of terrorist groups exist in region
d ₆ /p ₆	Location has a high density of population	d ₁₅ /p ₁₅	Existing security measures are poor
d ₇ /p ₇	The processing area is visible	d ₁₆ /p ₁₆	Personal preparedness and training is poor
d ₈ /p ₈	Inventory is very large	d ₁₇ /p ₁₇	Security risk is very high
d ₉ /p ₉	Ownership is not private		

According to different requirements of security management, propositions d₁ to d₅ may have different relationships. If they are thought to play a synthetic role in d₁₅ (the security measures are poor), they have an “AND” relationship; if all the measures are considered necessary, they have an “OR” relationship, that is, if any of the propositions d₁ to d₅ is true, the proposition of d₁₅ is true.

Thus, the “AND” relationship risk assessment rules can be obtained:

Rule 1: If d₁ AND d₂ AND d₃ AND d₄ AND d₅ Then d₁₅ (CF = μ_1)

Rule 2: If d₆ AND d₇ AND d₈ AND d₉ AND d₁₀ AND d₁₁ AND d₁₂ AND d₁₃ AND d₁₄ AND d₁₅ AND d₁₆ Then d₁₇ (CF = μ_2)

The “OR” relationship risk assessment rules are:

Rule 3: If d₁ OR d₂ OR d₃ OR d₄ OR d₅ Then d₁₅ (CF = $\mu'_1, \mu'_2, \mu'_3, \mu'_4, \mu'_5$)

Rule 2 is still applicable.

According to different relationships of propositions d₁ to d₅, two WFPN models for security risk assessment are established. Model 1 which is based on Rule 1 and Rule 2 is shown in Fig. 3. Model 2 which is based on Rule 3 and Rule 2 is shown in Fig. 4.

Besides, because there is not enough information or data to determine the value of certainty factors μ_1, μ_2 and μ'_i (i=1, 2, ..., 5), they are assumed to be 1 in this study.

Fig. 3 WFPN model 1 of security risk assessment

Fig. 4 WFPN model 2 of security risk assessment

In a fuzzy Petri-net, the truth value is used to indicate the degree of truth of a proposition. In the SRFT security risk assessment method, all factors that influence the overall security of the plant are linearly (or approximately linearly) rated on a scale from 0 to 5. To avoid the re-grading of risk factors, this study's constructed truth functions (corresponding to the $\alpha()$ function in the definition of FPN) for all propositions are categorized as monotonically increasing linear functions from 0 to 5. This indicates the greater the function value is, the greater truth of the proposition there will be. The truth function is shown in Fig. 5.

Fig. 5 Truth function for all propositions

(2) Weights of the risk indices

In the WFPN models, the “AND” relationship of risk factors determined by formula (3) needs the weights of the factors to clarify their importance. While the “OR” relationship determined by formula (4) does not need the weights of the factors.

If the importance of the risk indices are different, their weights have great impacts on the result of risk assessment. There are many approaches that can be used to determine the weights. The Analytic Hierarchy Process (AHP) is a structured technique for organizing and analyzing complex decisions. It quantifies expert empirical judgments by combining quantitative and qualitative analyses. The decision makers systematically evaluate the importance of various elements of the hierarchical system by comparing them to each other two at a time, with respect to their impact on an element above them in the hierarchy (Saaty, 1987). It has considerable practical value in situations with multiple objectives or complicated structures when there is a lack of necessary or sufficient data, and therefore the technique is widely applied in the theory of fuzzy mathematics (Vargas, 1990; Zhou, 2010; Shi et al. 2012; Stefanovi et al. 2016).

The steps of determining the weights of the security risk indices are as follows:

(i) Establish the judgement matrix

The factors under the same element in the hierarchy (“AND” relationship), can be prioritized

by making pairwise comparisons against their related criteria specified at the adjacent higher level element using the AHP scale which is shown in Table 3. The comparison results are filled in the judgement matrix A:

$$A = (a_{ij})_{n \times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad (7)$$

Where, a_{ij} indicates the importance of risk factor a_i on a_j , $a_{ij} > 0$; $a_{ij} = 1/a_{ji}$; $i, j = 1, 2, \dots, n$.

Table 3 The fundamental AHP scale

Intensity of importance on an absolute scale	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective
3	Moderate importance of one over another	Experience and judgment strongly favor one activity over another
5	Essential or strong importance	Experience and judgment strongly favor one activity over another
7	Very strong importance	An activity is strongly favored and its dominance demonstrated in practice
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation
2, 4, 6, 8	Intermediate values between the two adjacent judgments	When compromise is needed
Reciprocals	If activity i has one of the above numbers assigned to it when compared with activity j, then j	

	has the reciprocal value when	
	compared with i	
Rationals	Ratios arising from the scale	If consistency were to be forced by obtaining n numerical values to span the matrix

(ii) Calculate the weights

Calculate the weights of the risk factors according to formulas (8) and (9).

$$m_i = (a_{i1}a_{i2} \cdots a_{in})^{\frac{1}{n}} \quad (8)$$

$$w_i = \frac{m_i}{\sum_{i=1}^n m_i} \quad (9)$$

(iii) Consistency examination

In a general decision-making environment, we cannot give the precise values of the w_i/w_j , but only estimates of them. The estimates of these values given by an expert may have (small) errors in the judgment. It is known from eigenvalue theory, that a small perturbation around a simple eigenvalue, as we have in n when A is consistent, leads to an eigenvalue problem of the form $Aw = \lambda_{\max} W$, where $\lambda_{\max}$ is the largest or principal eigenvalue of A . If we obtain w by solving this problem, and then form a matrix with the entries (w_i/w_j) , we obtain an approximation to A by a consistent matrix. The inconsistency throughout the matrix can be captured by a single number $\lambda_{\max} - n$, which measures the deviation of the judgments from the consistent approximation.

Consistency ratio:

$$CR = CI / RI \quad (10)$$

Where,

$$CI = (\lambda_{\max} - n) / (n - 1) \quad (11)$$

If the ratio (called the consistency ratio CR) of CI to that from random matrices is significantly small (carefully specified to be about 10% or less), we accept the estimate of w . Otherwise, we attempt to improve consistency. The consistency index RI is shown in Table 4.

Table 4 Consistency index

Matrix dimension	3	4	5	6	7	8	9	10	11
RI	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

(3) Security risk inference process

The security risk can be deduced according to formulas (5) and (6) transition by transition. However, in the process of fuzzy inference, using the ability of parallel computing and matrix operation of the WFPN model, we can make an inference for the security risk based on the initial matrix M_0 (Liu et al., 2013). Before the inference, to express the matrix operation more clearly, accurately and succinctly, we define two special operators:

(a) $\oplus : X \oplus Y = Z$, where, X , Y and Z are all $n \times m$ matrices, x_{ij} , y_{ij} , z_{ij} are their elements, respectively, such that

$$z_{ij} = \max\{x_{ij}, y_{ij}\}, i = 1, 2, \dots, n; j = 1, 2, \dots, m$$

(b) $\otimes : X \otimes Y = Z$, where, X is a $n \times p$ matrix, Y is a $p \times m$ matrix, and Z is a $n \times m$ matrix. x_{ik} , y_{kj} , z_{ij} denote their elements, respectively, such that

$$z_{ij} = \max_{1 \leq k \leq p} (x_{ik} \times y_{kj}), i = 1, 2, \dots, n; j = 1, 2, \dots, m$$

As defined aforementioned, W and U are $n \times m$ -dimensional matrices; M_0 which is the initial marking of the WFPN model is an $n \times 1$ -dimensional matrix. $W = \{w_{ij}\}$ is the weight matrix of places for transitions, where, w_{ij} is the weight of place p_i for transition t_j if place p_i is the input place of transition t_j . If place p_i is not the input place of transition t_j , $w_{ij} = 0$.

U is the certainty matrix of the transitions for their outputs:

$$U = \{\mu_{ij}\}$$

Where, μ_{ij} is the certainty factor of transition t_j for the output place p_i . If place p_i is not the output place of transition t_j , $\mu_{ij} = 0$.

As thresholds of transitions are not considered in this study, based on the algorithms given by Liu et al. (2013), we put forward our security risk assessment process as follows:

Step 1: Initialization. Establish the matrixes M_0 , W and U .

Step 2: Let $idx = 1$, where idx represents the times of iteration.

Step 3: Compute the vector of equivalent fuzzy truth values of the transitions.

$$\Gamma_{idx} = W^T \times M_{idx-1}$$

Step 4: Compute new marking M_{idx} .

$$M_{idx} = M_{idx-1} \oplus (U \otimes \Gamma_{idx})$$

If $M_{idx} = M_{idx-1}$ then go to Step 5; otherwise, let $idx = idx + 1$, go back to Step 3.

Step 5: End assessing.

After the assessment process ends, the marking of place p_{17} in M_{idx} is the security risk value.

It is worth noting that this inference process can handle both “AND” and “OR” rules with the same algorithm. Different rules only affect the structure of corresponding WFPN model, and thus affect the initial matrices W and U .

(4) Security risk rankings

Based on the rankings of Bajpai (2007), the fuzzy security risk rankings are determined in Table 5.

Table 5 Security risk rankings

Security risk status	Risk values obtained	Recommendations
Low	[0, 0.25)	Maintain security awareness without excessive concern
Moderate	[0.25, 0.5)	Review and update existing security procedures in light of possible threats
High	[0.5, 0.75)	Identify threat-drivers that can be reduced with reasonable controls. Conduct threat and vulnerability analysis and work with law enforcement agencies to enhance security.

Extreme	[0.75, 1]	Initiate aggressive risk-reducing activity, in conjunction with consultation with law enforcement agencies. Conduct threat and vulnerability analysis.
---------	-----------	--

4. An illustrative example

In the paper of Bajpai and Gupta (2007), a refinery is considered as a possible target for terrorist attacks. This case is taken as an illustrative example in this study. The values of the risk factors are shown in Table 6.

Table 6 Factor values of the refinery

Risk factors	Actual points	Risk factors	Actual points
Location	1	Presence of terrorist groups in region	3
Visibility	1	Access control	2
Inventory	5	Perimeter protection	2
Ownership	5	Mitigation potential	2
Presence of chemicals which can be used as precursors for WMD	0	Proper lighting	3
Worst case impact on-site	5	Use of metal detector/ X-ray/ CCTV (at entrance and at all critical locations)	3
Worst case impact off-site	3	Personal preparedness and training	2
History of security incidents	3		

Thus, according to the truth function shown in Fig. 5, the truth values of the places of the WFPN model can be obtained, which are listed in Table 7.

Table 7 Truth values of the places

$\alpha(p_i)$	Values	$\alpha(p_i)$	Values	$\alpha(p_i)$	Values
---------------	--------	---------------	--------	---------------	--------

$\alpha(p_1)$	0.4	$\alpha(p_2)$	0.4	$\alpha(p_3)$	0.4
$\alpha(p_4)$	0.6	$\alpha(p_5)$	0.6	$\alpha(p_6)$	0.2
$\alpha(p_7)$	0.2	$\alpha(p_8)$	1	$\alpha(p_9)$	1
$\alpha(p_{10})$	0	$\alpha(p_{11})$	1	$\alpha(p_{12})$	0.6
$\alpha(p_{13})$	0.6	$\alpha(p_{14})$	0.6	$\alpha(p_{16})$	0.6

Based on the AHP, the weights of the places p_1 to p_5 for p_{15} in Model 1 are determined as listed in Table 8. The weights of places p_6 to p_{16} against p_{17} are shown in Table 9.

Table 8 Weights of places p_1 to p_5

p_1	p_2	p_3	p_4	p_5
0.2601	0.2601	0.1378	0.0819	0.2601

Table 9 Weights of places p_6 to p_{16}

p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}
0.0684	0.0684	0.0857	0.0298	0.0857	0.0856	0.0856	0.0684	0.1060	0.2104	0.1060

For Model 1, we obtain

$$\begin{aligned}
W = & \begin{pmatrix} 0.2601 & 0 \\ 0.2601 & 0 \\ 0.1378 & 0 \\ 0.0819 & 0 \\ 0.2601 & 0 \\ 0 & 0.0684 \\ 0 & 0.0684 \\ 0 & 0.0857 \\ 0 & 0.0298 \\ 0 & 0.0857 \\ 0 & 0.0856 \\ 0 & 0.0856 \\ 0 & 0.0648 \\ 0 & 0.1060 \\ 0 & 0.2104 \\ 0 & 0.1060 \\ 0 & 0 \end{pmatrix} & U = & \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} & M_0 = & \begin{pmatrix} 0.4 \\ 0.4 \\ 0.4 \\ 0.6 \\ 0.6 \\ 0.2 \\ 0.2 \\ 1.0 \\ 1.0 \\ 0.0 \\ 1.0 \\ 0.6 \\ 0.6 \\ 0.6 \\ 0.47 \\ 0.6 \\ 0.45 \end{pmatrix}
\end{aligned}$$

376

377 and

$$378 \quad M_1 = [0.4 \ 0.4 \ 0.4 \ 0.6 \ 0.6 \ 0.2 \ 0.2 \ 1.0 \ 1.0 \ 0.0 \ 1.0 \ 0.6 \ 0.6 \ 0.6 \ 0.47 \ 0.6 \ 0.45]^T$$

$$379 \quad M_2 = [0.4 \ 0.4 \ 0.4 \ 0.6 \ 0.6 \ 0.2 \ 0.2 \ 1.0 \ 1.0 \ 0.0 \ 1.0 \ 0.6 \ 0.6 \ 0.6 \ 0.47 \ 0.6 \ 0.55]^T$$

$$380 \quad M_3 = [0.4 \ 0.4 \ 0.4 \ 0.6 \ 0.6 \ 0.2 \ 0.2 \ 1.0 \ 1.0 \ 0.0 \ 1.0 \ 0.6 \ 0.6 \ 0.6 \ 0.47 \ 0.6 \ 0.55]^T$$

381 When idx equals 3, M_3 equals M_2 . This means that no transition in the WFPN system can be
 382 executed, and the system has reached a stable state. In M_3 , the marking of place p_{17} is 0.55, which
 383 is the final security risk value and the security risk status is high. The plant should identify
 384 threat-drivers that can be reduced with reasonable controls and conduct threat and vulnerability
 385 analysis to enhance security.

386 For Model 2, we obtain (M_0 is the same as that of Model 1):

387

$$W = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.0684 \\ 0 & 0 & 0 & 0 & 0 & 0.0684 \\ 0 & 0 & 0 & 0 & 0 & 0.0857 \\ 0 & 0 & 0 & 0 & 0 & 0.0298 \\ 0 & 0 & 0 & 0 & 0 & 0.0857 \\ 0 & 0 & 0 & 0 & 0 & 0.0856 \\ 0 & 0 & 0 & 0 & 0 & 0.0856 \\ 0 & 0 & 0 & 0 & 0 & 0.0684 \\ 0 & 0 & 0 & 0 & 0 & 0.1060 \\ 0 & 0 & 0 & 0 & 0 & 0.2104 \\ 0 & 0 & 0 & 0 & 0 & 0.1060 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad U = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$M_1 = [0.4 \ 0.4 \ 0.4 \ 0.6 \ 0.6 \ 0.2 \ 0.2 \ 1.0 \ 1.0 \ 0.0 \ 1.0 \ 0.6 \ 0.6 \ 0.6 \ 0.6 \ 0.6 \ 0.45]^T$$

$$M_2 = [0.4 \ 0.4 \ 0.4 \ 0.6 \ 0.6 \ 0.2 \ 0.2 \ 1.0 \ 1.0 \ 0.0 \ 1.0 \ 0.6 \ 0.6 \ 0.6 \ 0.6 \ 0.6 \ 0.57]^T$$

$$M_3 = [0.4 \ 0.4 \ 0.4 \ 0.6 \ 0.6 \ 0.2 \ 0.2 \ 1.0 \ 1.0 \ 0.0 \ 1.0 \ 0.6 \ 0.6 \ 0.6 \ 0.6 \ 0.6 \ 0.57]^T$$

When idx equals 3, M_3 equals M_2 . Thus, the assessment process ends. In M_3 , the marking of place p_{17} is 0.57, which is the final security risk value and the security risk status is also high.

It can be seen from the results that the security risk value of Model 2 is different from (higher than) that of Model 1. However, the difference of the risk values between the two models is not significant in this illustrative example, because the actual points of the factors for *existing security measures* are not quite different (they are two or three). The security risk ranks of the two models are both high. But in some conditions, the assessment results of the two models may be quite different. For example, assume that a plant has good security measures in access control, perimeter protection, mitigation potential, and use of metal detector/X-ray/CCTV (Closed-Circuit Television) at entrance and at all critical locations, but it has no proper lighting, the corresponding scores of d_1 to d_5 are 0, 0, 0, 5, and 0, respectively. Suppose the scores of other factors remain the same as

those in the example illustrated above. According to Model 1, the marking of place p_{17} is 0.47 in this circumstance, and the security risk status is moderate; according to Model 2, the marking of place p_{17} is 0.66, and the security risk status is high.

In a more complex or detailed indices system, there may be more complex relationships among the factors. So, to assess the security risk, correctly determining and modeling the relationships between the factors is important to obtain reasonable results. For the security risk indices system discussed in this study, if we focus on the combined effects of the factors for *existing security measures*, we should use Model 1; if each of the factors for *existing security measures* is considered necessary, we should use Model 2. This mainly depends on the requirements of security management.

5. Conclusions

Currently the threat of terrorist attacks has raised serious security concerns for the petrochemical industries. The threat of terrorists striking petrochemical plants is now considered both real and credible as these plants handle large amounts of flammable, explosive or toxic hazardous materials that can cause great loss and social impact.

Through a security risk assessment, we can determine the risk level of the plants in the face of terrorist attacks, and then take targeted measures to reduce the risk. It is considered that the security risk status of a chemical plant can be assessed by developing a Security Risk Factor Table (SRFT), which synthesizes the main parts of the security risk assessment: threat analysis, vulnerability analysis, security countermeasures, and mitigation and emergency response. Based on the SRFT, a weighted fuzzy Petri-net approach for security risk assessment is proposed in this paper. It can easily model the importance of risk factors and the relationship among them, and use the Petri-net analysis method to carry out the risk assessment.

Although the proposed method is more complicated than the one based on the SRFT, it is more complete and powerful, and can obtain somewhat more reasonable results. Determining the weights of the factors and modeling using Petri-net may be a bit complicated, but they are one-time jobs. Once the weights are determined and the model is established, the data for SRFT can be easily used for the analysis of the WFPN approach.

For the factors that affect the *existing security measures* in the SRFT, two kinds of WFPN models are established according to their "AND" or "OR" relationship. The weights of the factors with "AND" relationship are calculated according to AHP method. A method of the security risk deduction based on matrix operation is provided.

Finally, an illustrative example is presented to demonstrate the proposed approach, and the calculation of the two models is compared. The difference between the results reflects the different modeling of the relationships among the risk factors. To assess the security risk, correctly determining and modeling the relationships among the factors is important to obtain reasonable results.

Acknowledgments

This work is supported by National Natural Science Foundation of China (No. 71673060).

References

- ACS, (2002). Advanced Chemical Safety Inc., San Diego, available at: <http://www.chemical-safety.com/documents/pdf/SECURITY%20RAT.pdf>.
- Bajpai S., Gupta J.P., (2005). Site security for Chemical Process Industry. Journal of Loss Prevention in the Process Industries 18 (4-6), 301-309.
- Bajpai S., Gupta J. P., (2007). Securing oil and gas infrastructure. Journal of Petroleum Science and Engineering 55, 174-186.
- Bajpai S., Sachdeva A., Gupta J.P., (2010). Security risk assessment: Applying the concepts of fuzzy logic. Journal of Hazardous Materials 173, 258-264.
- Chen S.-M., (2002). Weighted fuzzy reasoning using weighted fuzzy Petri nets. IEEE Transactions on knowledge and data engineering 14(2): 386-397.
- Chen S.-M., Ke J.-S., Chang J.-F., (1990). Knowledge Representation Using Fuzzy Petri Nets. IEEE transactions on knowledge and data engineering 2(3), 311-319.
- Cheng H., He Z., Wang Q., Yang J., Lin S., (2015). Fault diagnosis method based on Petri nets considering service feature of information source devices. Computers and Electrical Engineering 46, 1-13.

David R., Alla H., (1994). Petri nets for modeling of dynamic systems – a survey. *Automatica*, 30 (2), 175-202.

Gao M., Zhou M., Huang X., Wu Z., (2003). Fuzzy Reasoning Petri Nets. *IEEE transactions on systems, man, and cybernetics-part A: systems and humans* 33(3), 314-324.

Ha M-H., Li Y., Wang X-F., (2007). Fuzzy knowledge representation and reasoning using a generalized fuzzy Petri net and a similarity measure. *Soft Comput*, 11: 323-327.

Hamed R. I., (2015). Esophageal cancer prediction based on qualitative features using adaptive fuzzy reasoning method. *Journal of King Saud University - Computer and Information Sciences* 27, 129-139.

Liu H.-C., Liu L., Lin Q.-L., Liu N., (2013). Knowledge Acquisition and Representation Using Fuzzy Evidential Reasoning and Dynamic Adaptive Fuzzy Petri Nets. *IEEE Transactions on Cybernetics* 43(3), 1059-1072.

Looney C. G., (1998). Fuzzy Petri nets for rule-based decision making. *IEEE Trans Syst, Man, Cybern* 18(1), 178-183.

Moore D. A., (2013). Security Risk Assessment Methodology for the petroleum and petrochemical industries. *Journal of Loss Prevention in the Process Industries* 26, 1685-1689.

Murata T., (1989). Petri nets: properties, analysis and applications, *Proceedings of the IEEE* 77 541-580.

Reniers G., Lerberghe P. V., Gulijk C. V., (2015). Security Risk Assessment and Protection in the Chemical and Process Industry. *Process Safety Progress* 34 (1), 72-83.

Reniers G.L.L., Dullaerta W., Audenaert A., Ale B.J.M., Soudan K., (2008). Managing domino effect-related security of industrial areas. *Journal of Loss Prevention in the Process Industries* 21, 336-343.

Saaty R. W., (1987). The Analytic Hierarchy Process-What It Is and How It Is Used. *Mathematical Modelling* 9 (3-5), 161-176.

Shi S., Jiang M., Liu Y., Li R., (2012). Risk assessment on falling from height based on AHP-fuzzy. *Procedia Engineering* 45, 112-118.

Stefanovi G., Milutinovi B., Vucicevic B., Dencic-Mihajlov K., Turanjanin V., (2016). A comparison of the Analytic Hierarchy Process and the Analysis and Synthesis of Parameters

- under Information Deficiency method for assessing the sustainability of waste management scenarios. *Journal of Cleaner Production* 130, 155-165.
- Valette R., Cardoso J., Dubois D., (1989). Monitoring manufacturing systems by means of Petri nets with imprecise markings. *Proc. IEEE Int. Symp. Intelligent Control*, 233-238.
- Vargas L. G., (1990). An overview of the Analytic Hierarchy Process and its applications. *European Journal of Operational Research* 48, 2-8.
- Zadeh, L. A. (1965). Fuzzy sets. *Information and Control* 8, 338-353.
- Zhang L., Reniers G., (2016). A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. *Risk Analysis*, DOI: 10.1111/risa.12569.
- Zhang Y, Zhang Y, Wen F., Chung C. Y., et al., (2016). A fuzzy Petri net based approach for fault diagnosis in power systems considering temporal constraints. *Electrical Power and Energy Systems* 78, 215-224.
- Zisman M. D., (1978). Use of production systems for modeling asynchronous, concurrent processes. In *Pattern Directed Inference Systems*, Watterman D. A. and Hayes-Roth F. (Eds), Academic Press, London, 53-68.
- Zhou J., (2010). SPA–fuzzy method based real-time risk assessment for major hazard installations storing flammable gas. *Safety Science* 48, 819-822.