Chemical Engineering Science 174 (2017) 136–145

Contents lists available at ScienceDirect

Chemical Engineering Science

journal homepage: www.elsevier.com/locate/ces

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, KU Leuven, 1000 Brussels, Belgium

HIGHLIGHTS

- A weighted fuzzy Petri-net (WFPN) based security risk assessment approach is proposed in this paper.
- This approach can model the importance of risk factors and their different relationships.
- The analysis method of Petri-nets can be used to perform the security risk assessment.
- Two WFPN models of security risk assessment are established according to different relationships between the factors.
- A matrix operation based security risk inference method is developed.

ARTICLE INFO

Article history:
Received 30 November 2016
Received in revised form 24 June 2017
Accepted 1 September 2017
Available online 7 September 2017

Keywords:
Security
Risk assessment
Terrorism
Weighted fuzzy Petri-net
Chemical industry

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.

1. Introduction

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

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

The assessment of industrial security risk has been studied by some scholars. Bajpai and 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

* Corresponding author at: Faculty of Technology, Policy and Management, Safety and Security Science Group (S3G), TU Delft, 2628 BX Delft, The Netherlands.
E-mail address: genserik.reniers@uantwerpen.be (G. Reniers).

http://dx.doi.org/10.1016/j.ces.2017.09.002
0009-2509/

Nomenclature

$P = \{p_1, p_2, \ldots, p_n\}$	place set
M	marking of Petri-net
$W = \{w_{ij}\}$	weight matrix
$U = \{\mu_{ij}\}$	certainty factor matrix of transitions
$\alpha(p_i)$	truth value in place p_i
α_i	truth value
μ_i	certainty factor
$A = \{a_{ij}\}$	judgment matrix
idx	times of iteration
$T = \{t_1, t_2, \ldots, t_m\}$	transition set
M_0	initial marking
w_{ij}	weight of place p_i for transition t_j
μ_{ij}	certainty factor of transition t_j for the output place p_i
$D = \{d_1, d_2, \ldots, d_n\}$	proposition set
CF	certainty factor
μ'_i	certainty factor
a_{ij}	importance of factor a_i on a_j
Γ_{idx}	vector of equivalent fuzzy truth values of the transitions at iteration idx

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 defuzzyfied 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, 2007) and Bajpai et al. (2010) discussed and modified the SRFT method.

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

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, 1998; 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

2.1. 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 tran-