Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network

Donya Fakhravar[a,1], *Nima Khakzad*[b,*], *Genserik Reniers*[b], *Valerio Cozzani*[a]

[a] *Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum—Università di Bologna, Bologna, Italy*
[b] *Safety and Security Science Group, Faculty of Technology, Policy, and Management, Delft University of Technology, The Netherlands*

ARTICLE INFO

Article history:
Received 19 April 2017
Received in revised form 21 August 2017
Accepted 24 August 2017

Keywords:
Security vulnerability assessment
Physical countermeasures
Relative attractiveness
Attack tree
Discrete-time Bayesian network
Gas pipeline

ABSTRACT

Security of chemical and oil & gas facilities became a pressing issue after the terrorist attacks of 9/11, due to relevant quantities of hazardous substances that may be present in these sites. Oil & gas pipelines, connecting such facilities, might be potential targets for intentional attacks. The majority of methods addressing pipeline security are mostly qualitative or semi-quantitative, based on expert judgment and thus potentially subjective. In the present study, an innovative security vulnerability assessment methodology is developed, based on Discrete-time Bayesian network (DTBN) technique to investigate the vulnerability of a hazardous facility (pipeline in this study) considering the performance of security countermeasures in place. The methodology is applied to an illustrative gas pipeline in order to rank order the pipeline segments based upon their criticality.

1. Introduction

Before 9/11 terrorist attacks, risk assessment of chemical plants mostly included safety issues related to accidental events mainly due to human errors, technical failures, natural disasters, etc. (Bajpai and Gupta, 2005). However, the tragedy of 9/11 demonstrated how unexpected and costly a terrorist attack could be. The risk of terrorism is not limited to the borders of countries and is a worldwide issue that endangers human lives, societies, industries, economies and even the environment worldwide. Therefore, security risk assessment started to be investigated and applied in all sectors including the chemical and process industries. An intentional incident could result in more severe damages compared to an unintentional accident because in the former, and especially in a terrorist attack, an attacker intelligently plans and acts to cause as much losses as possible. Recent terrorist attacks to Iraq's largest refinery in 2015 (AFP, 2015) and to chemical plants in France in June and July 2015 (Scott, 2015) have demonstrated the criticality of security risks in chemical industries.

The security risks of a pipeline may be even more critical than those of fixed plants since pipelines run thousands of kilometres in different areas whose population density, natural surroundings, assets and nearby vulnerable centres might be totally different. Gas pipelines transport highly flammable gases at high pressure on long distances. A survey on gas pipeline incidents evidences that the most frequent causes of damage are intentional acts (Gas Pipeline Incidents, 2015). The flammability of gas can be an attractive property for a terrorist group seeking mass casualties. Additionally, as a great share of the energy supply of the world is gas, a disturbance on gas transporting pipelines can be a goal for the attackers in order to affect the global economy and supply chains.

[*] *Corresponding author at*: Jaffalaan 5, Building 31, Delft 2628 BX, The Netherlands.
E-mail address: n.khakzadrostami@tudelft.nl (N. Khakzad).
[1] At the time of this research, the first author was with Safety and Security Science Group at Delft University of Technology, The Netherlands.

http://dx.doi.org/10.1016/j.psep.2017.08.036
0957-5820/© 2017 Institution of Chemical Engineers. Published by Elsevier B.V. All rights reserved.

The American Petroleum Institute (API) and the National Petrochemicals & Refiners Association (NPRA) have developed a guideline for conducting Security Vulnerability Assessment (SVA) in May 2003. Later, in October 2004, they enhanced their methodology to be applicable to transportation security risk (i.e. pipeline, truck and rail). This methodology specifically focuses on petroleum and petrochemical industrial facilities. The last version of the API methodology was published in 2013 entitled ANSI/API Standard 780 (ANSI/API STD 780). Security risk variables, based on the API guideline (ANSI/API STD 780) include:

- Consequence: "potential adverse impact of an attack";
- Likelihood: "the chance of being targeted by an adversary";
- Attractiveness: "perceived value of a target to an adversary";
- Threat: "an adversary's intent, motivation, capabilities and known pattern of operation";
- Vulnerability: "any weaknesses that can be exploited by an adversary to gain access and damage".

Another methodology was developed by Air Product and Chemicals Inc. (APCI) for SVA in 2004 (Dunbobbin et al., 2004). This methodology is consistent with the Centre for Chemical Process Safety (CCPS) guidelines and is used for the evaluation of a large number of facilities. The APCI methodology includes evaluating potential consequences, attack scenarios and the attractiveness of the facility to a terrorist attacker, all in terms of vulnerability. The assessment is done by a team of experts from process safety, security and site operations. Transportation is out of the scope of this methodology even though the developers claim that it is robust enough to be applied to this sector as well.

The American Society of Mechanical Engineers Innovative Technology Institute developed a guideline on Risk Analysis and Management for Critical Asset Protection (RAMCAP) for the US Department of Homeland Security (DHS) (Moore et al., 2007). RAMCAP is a framework for analysing and managing the risks associated with terrorist attacks against critical infrastructure assets in the United States. It is a methodology for analysing the consequences of attack, identifying security vulnerabilities, and developing threat information based on both asset owner and government information. Additionally, it provides methods for DHS to analyse risk, and to evaluate countermeasures and mitigation procedures. The abovementioned methodologies are qualitative assessments.

There are some semi-quantitative assessments such as the Security Risk Factor Table (SRFT) (Bajpai and Gupta, 2005; Bajpai and Gupta, 2007) which identifies and ranks from 0 to 5 (0 is the lowest while 5 is the highest risk) the factors influencing overall security. Vulnerability and threat analysis in such methodologies are, however, very general and do not follow a concrete structure and order. While the SRFT deals with the effects of individual threats, the Step Matrix Procedure deals with domino effects (Srivastava and Gupta, 2010). A stepped matrix model orders the independent threat events which lead to a catastrophic damage due to the failure of the respective security barriers in form of a matrix. Using this matrix also a character-state tree can be developed showing the path from primary events to catastrophic ones. Although the mentioned methodologies are semi-quantitative, they are still subject to the knowledge, judgement, values, opinions, and needs of the analyst.

Fault Tree (FT) analysis is a conventional method in safety risk analysis investigating risks, related to safety events both qualitative and quantitatively. The same concept is used in the Attack Tree (AT) approach in security risk assessments. AT was first used in the computer security domain, but it is applicable for security risk analysis in any other field (Gribaudo et al., 2015). AT is an excellent tool for brainstorming and evaluating threats and can be applied to analyse the risk that is generated by some action chains or combinations of them. AT also allows playing "what-if" games with potential countermeasures. In addition, its hierarchical structure is easy to follow and enable multiple experts to work on different branches in parallel (Edge et al., 2006). Besides all mentioned advantages of AT, there are some drawbacks. AT analysis has a static nature and is unable to include time dependencies. This shortcoming has to a large extent been alleviated through dynamic attack trees (DAT). ATs are difficult to be used in large scale analyses since they contain many probabilities and factors that need a huge amount of time and effort to carry out the assessment (Edge et al., 2006).

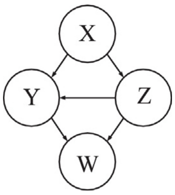

Fig. 1 – A simple example of a BN.

Game theory is a concept originating from mathematical and economic sciences. Methods based on Game theory focus on modelling how intelligent attackers can best exploit opportunities to cause losses and how defenders can optimize the allocation of resources to minimize the damage (Talarico et al., 2015; Zhang and Reniers, 2016). Khalil (2016) developed a model to calculate the probability of a successful attack based on the corresponding mission time of the attack and the time needed to deactivate/penetrate the security barriers in place. van Staalduinen et al. (2017) developed a methodology based on Bayesian network (BN). An advantage of their approach is the application of BN to a holistic security risk assessment. However, since their methodology is based on conventional BN, it cannot be applied to modelling complicated time-dependent relationships between attackers and countermeasures (or defenders) in place.

Table 1 shows a summary of different security risk assessments were discussed. Security risk assessment is a dynamic process and is fully dependent on factors that vary both spatially and temporally. A robust and reliable quantitative tool to carry out a security risk assessment should be able to model such dynamics taking into account new information and data. Moreover, the current quantitative methodologies are mostly developed for fixed plants (Zhang and Reniers, 2016; Khalil, 2016; van Staalduinen et al., 2017) and do not consider the characteristics of transportation systems, and specifically of pipelines.

The present study is aimed at developing a methodology based on Discrete-time BN (DTBN) – a type of dynamic BN – for dynamic security vulnerability assessment of gas pipelines. Due to their flexible structure and capability to consider dependencies, BN has been widely used in safety assessment (Khakzad et al., 2011, 2013a; Yuan et al., 2015) and vulnerability analysis of chemical plants (Khakzad and Reniers, 2015; Khakzad et al., 2016). Although security risk assessment can take advantage of BN, to the best knowledge of the authors, the applications of BN to security risk assessment have been very limited. The fundamentals of BN and DTBN and their application to safety and security are briefly explained in Section 2. The methodology is developed in Section 3. In Section 4, the application of the methodology is demonstrated on an illustrative gas pipeline. The paper concludes in Section 5.

2. Bayesian network

2.1. *Conventional Bayesian network*

A BN (G, P), by definition, is a directed acyclic graph G to factorize a joint probability distribution P that together satisfy the Markov condition (Neapolitan, 2004). A BN consist of (Jensen and Nilson, 2007):

- A set of variables and a set of directed edges between variables;
- Each variable has a finite set of states (except in continuous nodes);
- To each variable and its parents, a conditional probability table is attached.

A simple example of a BN has been depicted in Fig. 1.