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

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 Section, Delft University of Technology, The Netherlands

* Corresponding author: n.khakzadrostami@tudelft.nl
Phone: +31 15 2784709
Address: Jaffalaan 5, Building 31, Delft 2628 BX, The Netherlands

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, thus based on expert judgment and 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 efficacy of security countermeasures. The methodology is applied to an illustrative gas pipeline in order to rank order the pipeline segments based upon their criticality.

Keywords: Security vulnerability assessment; Physical countermeasures; Relative attractiveness; Dynamic Bayesian network; Gas pipeline

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. [1]. 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 [2] and to chemical plants in France in June and July 2015 [3] have demonstrated the criticality of security risks in chemical industries.

[1] At the time of this research, the first author was with the Safety and Security Science Section at Delft University of Technology, The Netherlands.

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 [4]. 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.

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 [5]. Security risk variables, based on the API guideline [5] 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 [6]. 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) [7]. 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) [1, 8] 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. 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 [9]. 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 [10]. 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 [10].

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 [11, 12]. Khalil [13] 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. [14] 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.

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 [12, 13, 14] 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 [15, 16, 17] and vulnerability analysis of chemical plants [18, 19]. 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 [20]. A BN consist of [21]:

- 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 Figure 1.

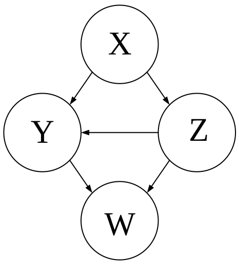


Figure 1. A simple example of a BN

In a BN, for a set of variables $U = \{A_1, \dots, A_n\}$, a unique joint probability distribution can be defined as in Equation 1.

$$P(U) = \prod_{i=1}^{n} P(A_i \mid pa(A_i)) \quad (1)$$

where pa(A$_i$) are the parents of A$_i$ in the BN. For instance, the joint probability distribution for random variables $U = \{X, Y, Z, W\}$ shown in Figure 1 can be calculated as:

$$P(U) = P(X, Y, Z, W) = P(X).P(Y|X, Z).P(Z|X).P(W|Y, Z)$$

Consequently, the probability of each node can be obtained as well, for example:

$$P(Y) = \sum_{X,Y,Z} P(X, Y, Z, W) = \sum_{X} (P(X)(\sum_{Z} P(Z|\, X)P(Y|X, Z)(\sum_{W} P(W|Y, Z)))$$

During the past decades, the BN approach has been extensively used in safety risk analysis due to its flexible structure and capability to consider spatial and temporal dependencies. The main advantage of BN over linear techniques such as AT and FT is in considering conditional dependencies and updating the probabilities in the light of new information (also known as “evidence”). Using Bayes theorem, the posterior probability can be calculated as [15, 16]:

$$P(U|E) = \frac{P(U,E)}{P(U)} = \frac{P(U,E)}{\sum_U P(U,E)} \quad (2)$$

where E is the evidence (new observation).

2.2. Discrete-time Bayesian network

Several formalisms of BNs have been developed for dynamic domains applications such as Temporal Bayesian Networks (TBN), Dynamic Bayesian Networks (DBN), network of dates and modifiable Temporal Belief Networks (MTBN) [20]. The main approach in all these methods is to discretize the time line and associate a node to each time interval. The Discrete Time Bayesian Network (DTBN) formalism was first developed by Boudali and Dugan [22].

In this approach, the time line is divided into n+1 intervals. Each node variable has a finite number, n+1, of states. The first n states divide the time interval]0,T] (T is the mission time) into n (possibly equal) intervals, and the last state n+1 represents the time intervals]T,+∞]. The last state means that the corresponding basic component or gate output does not fail during the mission time. The sum of probabilities associated to each time interval should be equal to one [22].

Khakzad et al. [23,24] applied DTBN to risk-based design of process vessels [23] and risk management of domino effects [24]. Using this novel type of dynamic Bayesian network, the dynamic gates in FTs (as well as ATs) such as the Priority AND gate (PAND) and Sequential failures gate (SEQ) can be mapped to a BN. For instance, for a PAND gate to occur, all the input events to the gate should be accomplished in a specific order – usually from left to right – whereas the order does not matter in a conventional AND gate. Figure 2(a) shows that if both events A and B are accomplished, the event C occurs. Whereas Figure 2(b) demonstrates that not only events A and B should both take place, but also A should occur before B.

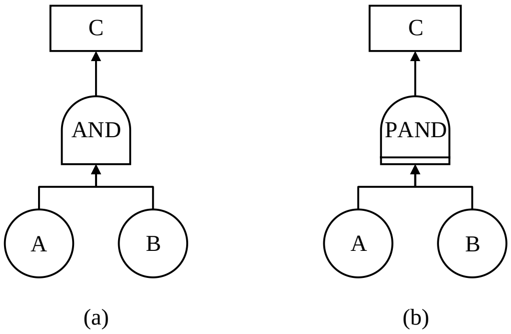


Figure 2. Example of a) AND gate and b) PAND gate in fault trees

3. Methodology

The security risk assessment approach that we elaborate includes three main factors, that is, attractiveness assessment, vulnerability assessment, and consequence analysis [5]. The threat is assumed a terrorist (or terrorist group) that has an intent to attack a specific pipeline. The terrorist capabilities and patterns of operation as well as the chance of executing a successful attack are included in a vulnerability assessment. Thus the threat analysis is included in vulnerability assessment by the basic nodes representing the probability of the success of the attacker considering both the attacker's ability, skills and equipment (threat) and the barriers' effectiveness. The only security factor left is the likelihood (chance of being targeted) which is 100% since it is assumed that there is a terrorist or terrorist group who plans to attack the pipeline.

Attractiveness, vulnerability, and consequences are quantified separately and the risk is obtained as a function of the three. As a first step, the pipeline should be divided into several segments, since a pipeline may pass through different geographical areas, and thus the respective security risk varies as well. Then the assessment should be carried out for all segments. By this procedure, not only the security risk could be obtained for each segment, but also the main sources of risk for each segment can be identified. The final outcome will be (i) to rank the most critical pipeline segments in terms of security risk, and (ii) to propose suggestions to reduce the security risk. The flowchart of the procedure is displayed in Figure 3.

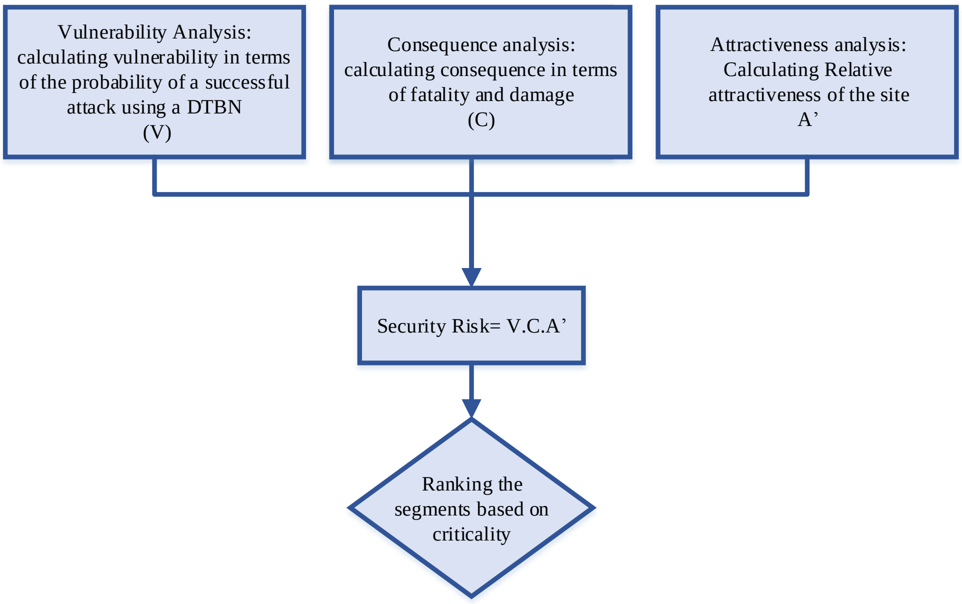

Vulnerability Analysis: calculating vulnerability in terms of the probability of a successful attack using a DTBN (V)
Consequence analysis: calculating consequence in terms of fatality and damage (C)
Attractiveness analysis: Calculating Relative attractiveness of the site A'
Security Risk= V.C.A'
Ranking the segments based on criticality

Figure 3. Schematic illustration of the security risk assessment methodology

The DTBN is applied in vulnerability assessment to take into account the time dependency of a successful attack, considering that the attacker has to disable the barriers, reach the pipeline, and damage it.

3.1 Vulnerability assessment

Vulnerability in the API [5] is defined as "any weakness that can be exploited by an adversary to gain success and damage or steal an asset or disrupt a critical function." In the present study, vulnerability is quantified and expressed in terms of the probability of a successful attack. It is assumed that there is a suspected adversary who wants to plan an attack to a pipeline. The vulnerability assessment can be carried out using the following steps:

1. Develop an attack scenario in form of a DAT;
2. Map the DAT to the DTBN;
3. Calculate the marginal probabilities as the input of parent nodes in the DTBN;
4. Develop the conditional probability tables based on the logic gates in the attack trees;
5. Run the DTBN using values obtained in Steps 3 and 4.

The steps of the procedure are illustrated in Figure 4.

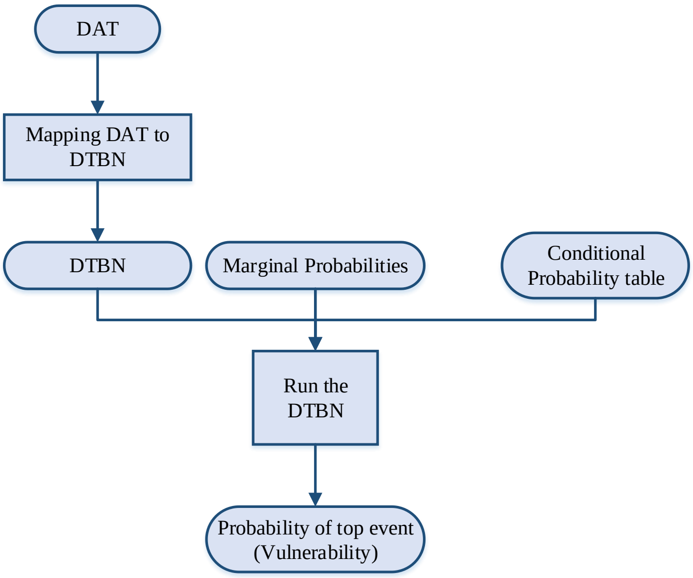

DAT
Mapping DAT to DTBN
DTBN
Marginal Probabilities
Conditional Probability table
Run the DTBN
Probability of top event (Vulnerability)

Figure 4. Schematic of vulnerability assessment procedure

3.2. Consequence analysis

In order to carry out consequence analysis, event trees (ETs) are created and quantified as in safety risk assessment. ETs identify the probable outcome scenarios in case of gas releases and the probability of occurrence of each. Then for each scenario, using ALOHA consequence analysis software [25] (or any other modelling tool), the impact area of the scenarios (in terms of heat radiation and overpressure) should be obtained. The final step is to calculate the effects of the scenarios on human and assets (probability of death and damage) using dose-effect functions. Different types of dose-effect relationships can be found in literature [26, 27]. Table 1 shows the dose-effect functions that were used in this study.

Table 1. Probit functions for heat radiation effects. Y: Probit value; ttf : time to failure (s); V: vessel volume (m3); I: radiation (kW/m2);D: dose value; teff: exposure time.

Effect	Target	Probit function	Reference
damage	Atmospheric vessel	$Y = 12.54 - 1.847.\ln(ttf)$	[27]
		$\ln(ttf) = -1.13.\ln(I) - 2.67 \times 10^{-5}V + 9.9$	
	Pressurized vessel	$Y = 12.54 - 1.847.\ln(ttf)$	[27]
		$\ln(ttf) = -0.95.\ln(I) + 8.845V^{0.032}$	
death	Human	$Pr = -36.38 + 2.56lnD$	[26]
		$D = t_{eff}(I)^{4/3}$	

3.3. Attractiveness

There are a few methodologies that quantify the attractiveness such as those proposed in API [5]. In this study, attractiveness is assessed using the method developed by Argenti et al. [28]. In their approach, an index is calculated as the overall attractiveness index (I_A). It is the product of a hazard-based index (I_H) and a site-specific induction index (ϕ). The main parameters and scoring ranges of the indexes and sub-indexes are briefly listed in Table 2. More details could be found in Argenti et al. [28].

Table 2. Attractiveness indexes and sub-indexes

Index	Sub-indexes	range of sub-indexes	affecting factors
$I_H= I_{PFH} + I_P + I_{vc}$ (Hazard index)	I_{PFH} (Process facility hazard index)	1-6	Hazardous substances inventories
	I_P (Population hazard index)	1-4	Population in impact area
	I_{vc} (Vulnerability center index)	0-4	Number of vulnerability centers
$\Phi=1+(F_A+F_T)$ (Site-specific induction index)	F_A (Attractiveness increase sub-index)	0-0.24	Socio-economic issues; strategic issue.
	F_T (Threat worsening sub-index)	0-0.36	Malicious act encouraging factor; public perception.

4. Application to a demonstrative case-study

In order to provide a comprehensive understanding of the methodology, its application is demonstrated using a case study. The case study consists of four segments of a buried natural gas pipeline. Three segments are parts of the pipeline crossing: a rural area, an urban area, and near a chemical plant, whereas the fourth segment is a compression station. These segments were chosen because they may be representative for any pipeline network. Table 3 shows the characteristics of the segments.

Table 3. Segments specification.

Segment	Population density (person/km2)	Security countermeasure	Equipment
Station	100*	Patrol**, surveillance, 2 layer of fence, acoustic detection system	two compressors and two filters
Near a chemical plant	110***	Patrol**, 2 surveillance (one for the chemical plant and one for the pipeline), 1 layer of fence, acoustic detection system	4 storage tanks containing gasoline
Rural area	100*	Patrol**, 1 layer of fence, acoustic detection system	-
Densely	7000*	Patrol**, surveillance, 1 layer	-

populated urban area	of fence, acoustic detection system

* Population density is reported in green book (TNO) [29]
** patrolling schedule are different in each segment.
*** Number of staff was also considered in population densities near the chemical plant.

As shown in Table 3, the compression station and the nearby chemical plant have some facilities that need to be considered in attractiveness assessment and consequence analysis. More details about the inventory and the location of the equipment with respect to the attack point in the pipeline are shown in Table 4.

Table 4. Equipment type, distance from the pipeline and volume

Site	Equipment	Distance (m)	Volume (m^3)
Station	Compressor 1	50	100
	Compressor 2	100	100
	Filter 1	50	100
	Filter 2	100	100
Chemical plant	Tank 1&2	50	12,560
	Tank 3&4	100	12,560

4.1. Vulnerability assessment

As it was explained before, vulnerability is the probability of a successful attack given that an attack has already been launched at the facility. For a successful attack the attacker first needs to pass the barriers, places the explosive material on the buried pipeline, and regresses, all before the arrival of the patrol; it is assumed that the bomb can be detonated remotely. This scenario is qualitatively modelled in form of DATs for each segment (Figure 5).

The root nodes shown in Figure 5 are:

- S: representing the failure of the surveillance system by the attacker. S_1 and S_2 in the DAT of the segment near the chemical plant indicate the surveillance system of the plant and the pipeline, respectively;
- F: representing the failure of the fences by the attacker. F_1 and F_2 in the DAT of the compression station indicate the two layers of fences;
- D: representing the state of the acoustic detection system. It has two modes of work and fail;
- R: representing the success of the attacker to regress;
- EXP: representing the success of the attacker to damage the pipelines by means of an explosion.

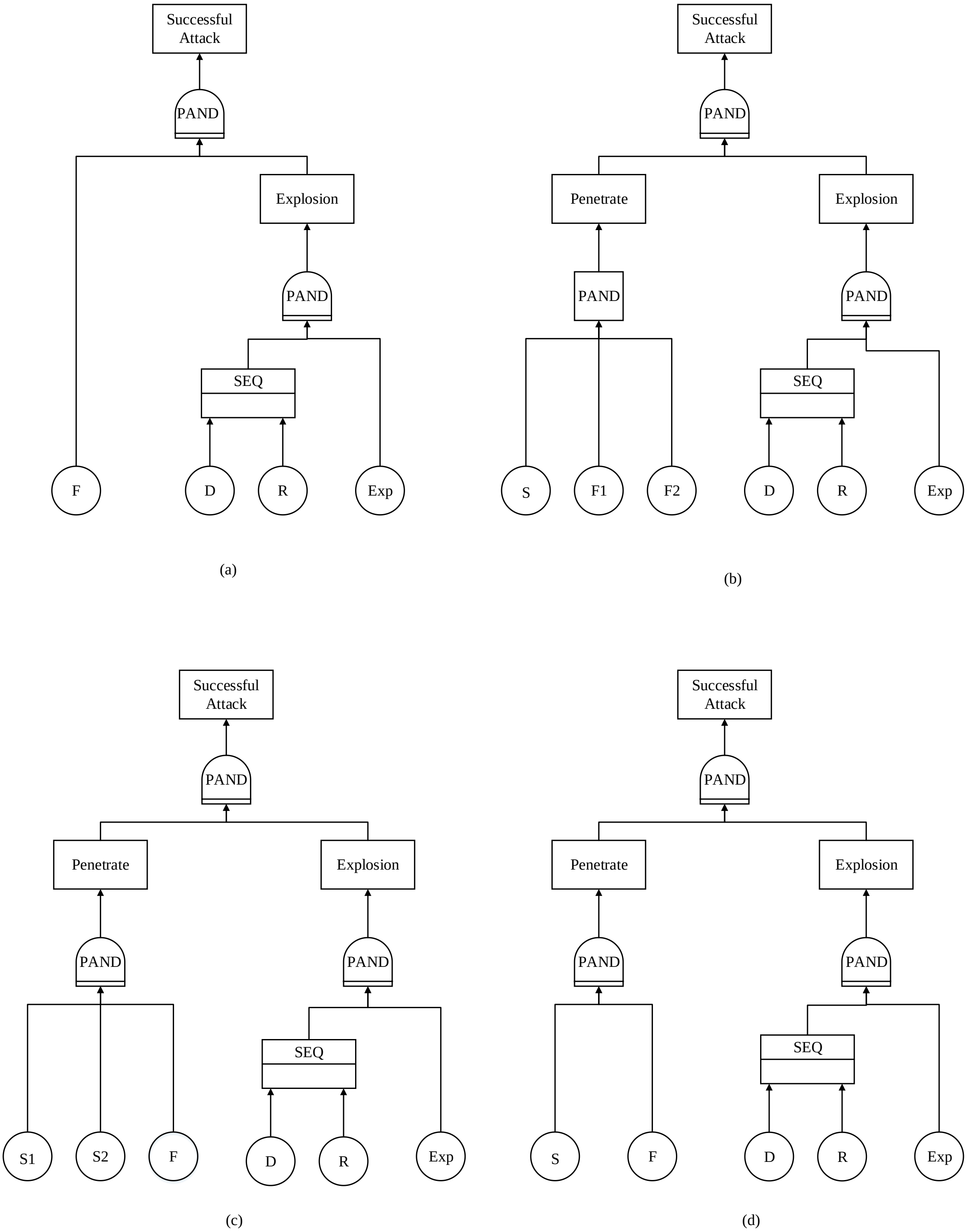


Figure 5. Dynamic Attack Trees developed for the four segments of the pipeline in the case study. a) DAT for the segment in rural area; b) DAT for the compression station; c) DAT for the segment near the chemical plant; d) DAT for the segment in urban area.

Two types of dynamic gates in these DATs are used. The first one is the Priority AND (PAND) gate to indicate that the connected actions should take place in a specific order, from the left to the right. For example, the penetration into the station (Figure 5.b) will occur when first the surveillance system (S), second the first fence (F1), and finally the second fence (F2) are disabled, all three and not in any other order. The failure of one action would lead to the failure of penetration. The second type of dynamic gate is the Sequential gate (SEQ) which demonstrates that the nodes connected to the gate will fail sequentially. The SEQ gates shown in Figure 5 relates the acoustic detection system to the regress of the attacker. In other words, the working or failure of the detection system is followed by the attempt of the attacker to regress. Each state of the detection node (failure or work) affects the failure probability of the regression.

Patrolling is not explicitly shown in the DAT as a security barrier though its schedule directly affects the marginal probability values corresponding to the success of the adversary to disable the barriers. The schematic of the DTBNs formed based on the DATs in Figure 5 are shown in Figure 6.

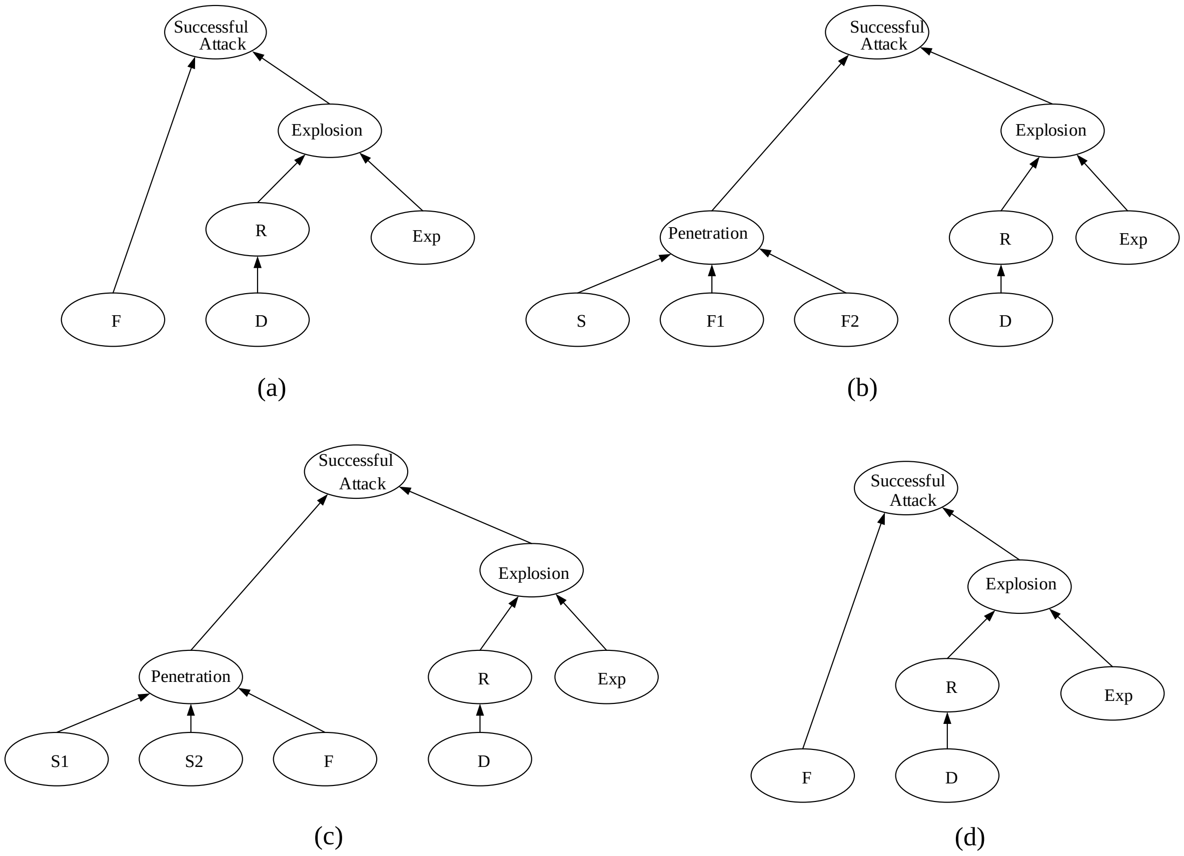


Figure 6. The schematic of DTBNs of the attack scenarios for all pipelines segments: a) the segment in a rural area; b) Compression station; c) the segment near the chemical plant; d) the segment in an urban area

To calculate the probability of the successful attack, the marginal and conditional probabilities should be calculated and assigned to the nodes. To construct the DTBNs, the mission time was considered as 1.0 hr and divided into four equal intervals, 15 min. The fifth interval, t > 1.0 hr, indicates the attacker cannot pass the barriers within an hour, and thus the attack fails.

For each barrier a probability distribution function was assumed. An important assumption that was made in the probability calculation of the present study is that, the attacker will be stopped if the patrol arrives. In relation to this matter, load-resistance reliability models are used in the present study to derive a failure probability for each barrier.

The patrolling schedule is assumed to follow an exponential distribution as Equation 3, where λ (1/hr) is the arrival rate of patrol within an hour:

$$f(t) = \lambda e^{-\lambda t} \tag{3}$$

The assumed values of λ for each segment are reported in Table 5.

Table 5. Patrol arrival rate (λ) for different segments.

Segment	λ (1/hr)
Rural are	0.5
Station	3
Near the chemical plant	3
Urban area	6
After receiving signals from detectors (all segments)	9.21*

*This value is calculated by the assumption that the patrolling arrival probability is 0.9 in 15 min in the case that the acoustic detection system works.

For the surveillance system and the fence, a lognormal failure distribution function was considered as in Equation 4.

$$f(t) = \frac{1}{\sqrt{2\pi}st} \exp[-\frac{1}{2s^2}\left(Ln\frac{t}{t_{med}}\right)^2] \tag{4}$$

where s is the shape parameter, and t_{med} is the median time to failure

The values for s and t_{med} are reported in Table 6. To calculate the shape parameter, the failure probability of the barrier (the success probability of the attacker in disabling the barrier) were assumed to be 0.9 in 45 min and 0.9 in 30 min for the surveillance and the fence, respectively.

Table 6. Shaping factor and median time to failure of surveillance system and fence

Security counter measure	t_{med} (min)	s
Surveillance system	20	0.63
Fence	10	0.85

For the acoustic detection system, an exponential failure probability distribution with a constant failure rate λ=0.1 was assumed. The acoustic detection system is installed inside the pipelines and sends signals to control rooms. Thus, the attacker does not have access to it and cannot disable it himself. The probability distribution function is used to calculate the probability of failure or work state of the detection systems since it directly affects the paroling schedule after the penetration. The probability distribution of regress of the attacker was also considered to be as exponential. It was assumed that the probability of regress in 15 min is 0.9, leading to λ=9.21 (Table 5).

Another probability to consider is the probability whether the explosion damages the pipeline or not. Using the TM-5 empirical equations [30], the upper and lower boundaries for peak pressure of every point in the soil with respect to the explosion point can be obtained.

Upper boundary of pp= $41.4 f_c (\frac{R}{W^{\frac{1}{3}}})^{-1.5}$ (5)

Lower boundary of pp= $5.26 f_c (\frac{R}{W^{\frac{1}{3}}})^{-2.5}$ (6)

where pp is the peak pressure in MPa, f_c is the coupling factor, R (m) is the distance from the charge centre, and W (kg) is the charge mass (TNT). In this case the TNT mass was assumed 0.5 kg and the depth of the buried pipeline was assumed to be 1m. Using these values, the upper and lower peak pressure boundaries were obtained as 27.8 and 2.80 MPa respectively. The median pressure was assumed as the average of the boundaries (15.30 MPa) and variance was calculated as twice the deviation of the boundaries to the average (6.25 MPa) to develop a log-normal distribution function for the pressure peak caused by the explosion.

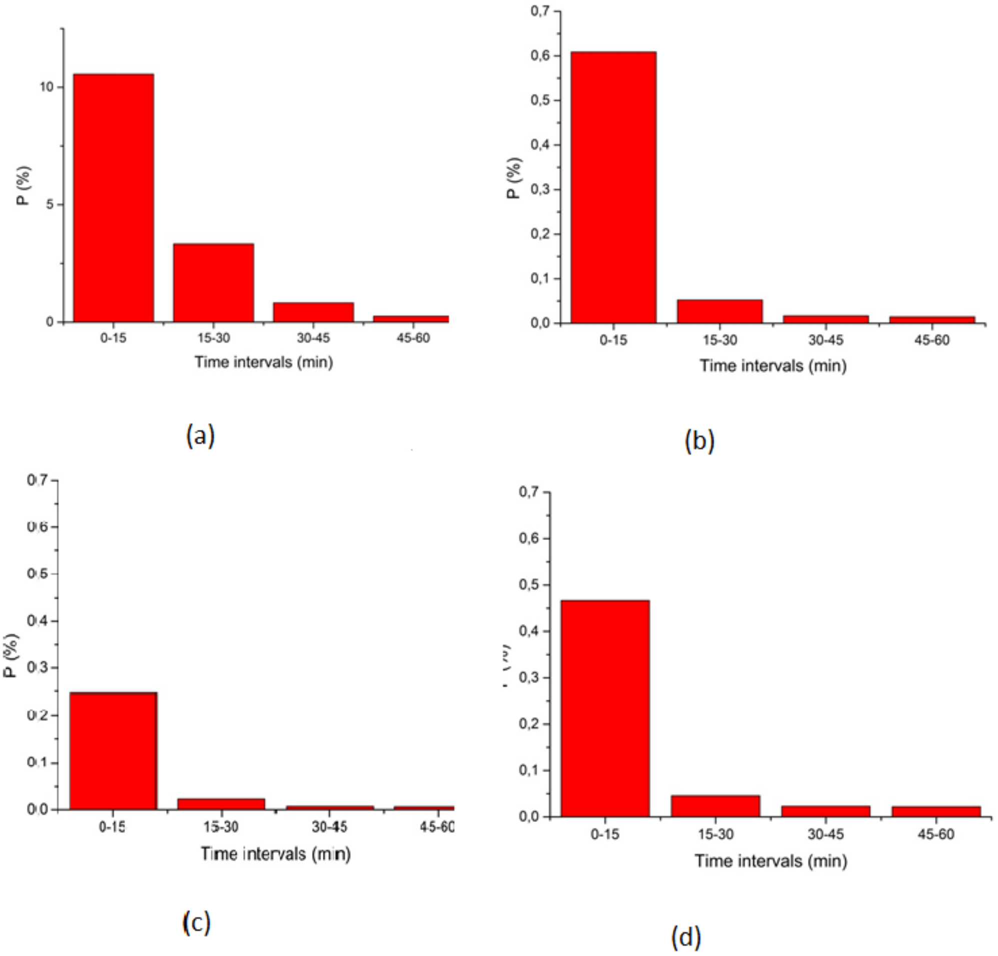
The attacker succeeds if he/she can disable the countermeasures and regress before the arrival of the patrol. Using the load-capacity model, we can consider the time needed to disable the barrier as the load and the patrol arrival time as the capacity. Both the barrier failure time and the patrol arrival time are random variables. In this case the success probability of the attacker can be obtained using Equation (7) [31]:

P= $\Pr\{Y \geq X\} = \int_0^{\infty} [\int_x^{\infty} f_y(y)dy] f_x(x)dx$ (7)

In Equation (7), X is the random variable representing the load with the probability density function of $f_x(x)$, and Y is the random variable representing the capacity of the system with the probability density function of $f_y(y)$. In the case of security countermeasures, the patrol arrival time (the amount of time the attacker has to disable the countermeasures) can be considered as the capacity (from the attacker's perspective) whereas the time needed to disable the security countermeasure (the amount of time during which the attacker has to penetrate the countermeasures) can be considered as the load (from the attacker's perspective); that is, the longer the patrol arrival time the higher the probability that the countermeasure fails (success of the attacker). Equation (7) can be rewritten as in Equation (8) in which P represents the probability of success from the attacker's point of view.

$$P = \Pr\{T_p \geq t_s\} = \int_0^{\infty} [\int_{t_s}^{\infty} f_p(t_p) dt_p] f_s(t) dt_s \quad (8)$$

where T_p is the patrol arrival time, and t_s is the time needed to disable the security countermeasure. Since we are using the DTBN, the success probability of the attacker should be calculated in each time interval, i.e., for every 15 min, considering the whole mission time of 1 hr. So the integral in Equation (8) was calculated separately in each interval.



(a)

(b)

(c)

(d)

Figure 7. Probability distribution of a successful attack in 1 hour: a) rural area segment; b) compression station; c) segment near the chemical plant; d) urban area.

To calculate the probability of the explosion damaging the buried pipeline, a similar load-capacity relationship was used with constant design pressure of the pipelines (10 MPa):

$$P = \Pr\{P_{design} = 10MPa < pp\} = 1 - \Phi(\frac{1}{s} ln \frac{10}{15.5}) = 0.7549$$

Using the probability functions, the probability of success of the attacker in each interval was calculated and used to run the DTBN. To run the network, the academic version of GeNIe software was used [32]. The final results of the vulnerability assessment are shown in terms of the probabilities of successful attack in Figures 7(a)-(d) for each time interval.

4.2. Consequence analysis

The first step in the consequence analysis is to develop an event tree for the top event which is a release of natural gas from the pipeline after the successful attack. The possible scenarios for the release of a flammable gas like methane are jet fire, vapour cloud explosion (VCE) and flash fire. Dispersion of the methane in atmosphere is also a scenario, but since methane is not much toxic it does not have a major consequence if there is no ignition. The event tree used for consequence analysis in all segments is shown in Figure 8. The next step is to calculate the probability of each scenario using this event tree. Since each segment has its own specifications, the probabilities may be different.

Having the release rate values from ALOHA [25] and the probabilities of ignition [33] and probabilities of VCE [34], the event tree analysis has been carried out. The barrier probabilities are shown in Figure 8 and the final results are reported in Table 7.

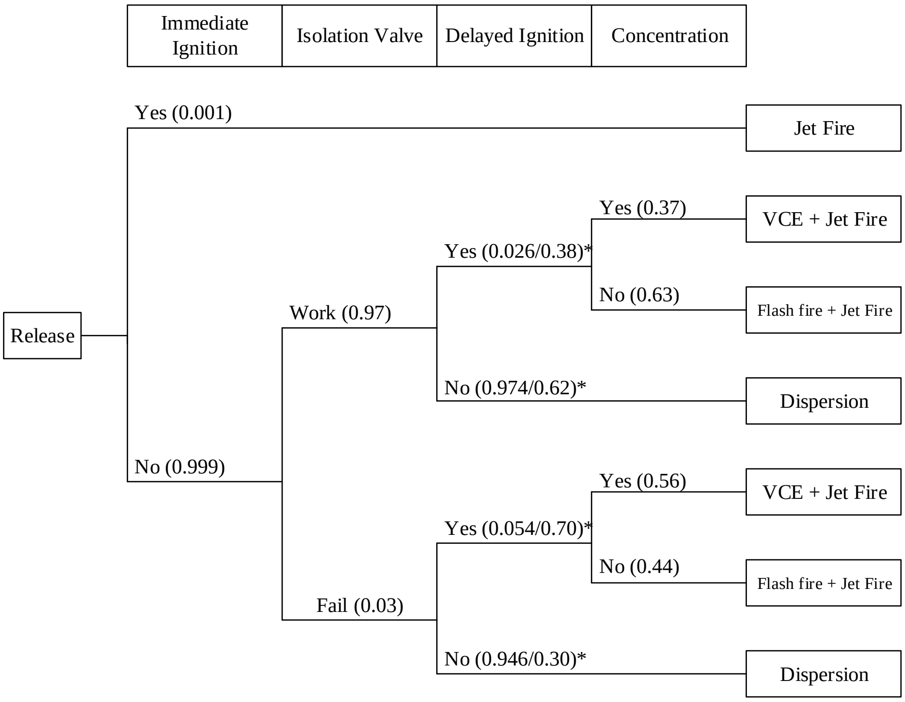


Figure 8. Event tree.
*First values refer to rural area and second values to the other segments

Table 7. Probability of consequence in the event tree

Consequence	Probability	
	Rural area	Urban and industrial are

Jet fire (immediate ignition)	1.00E-03	1.00 E-03
VCE (delayed ignition, IV work) followed by jet fire	9.35E-03	1.36 E-01
flash fire (delayed ignition, IV works) followed by jet fire	1.58E-02	2.31 E-01
VCE (delayed ignition, IV fails) followed by jet fire	9.00E-04	4.22 E-03
flash fire (delayed ignition, IV fails) followed by jet fire	4.90E-04	3.00 E-01

To calculate the consequences of each scenario in terms of losses of lives and assets, the ALOHA was used to obtain the impact areas. In the software, a pipeline was defined as the release source. A pressure of 70 bar and distance of the isolation valve distance of 30 Km were assumed. Heat radiation and overpressure obtained from ALOHA are used to calculate probit values and the probabilities of damage and death (Table 1). The economic loss is defined as the product of probability of damage and the cost of the equipment. For human loss, the number of fatalities is obtained by integrating the product of population densities and probability of death over the distance in the threat zone [26] as in Equation (9).

$$N = (N_0 \pi R^2) + \int_R^{\infty} P N_0 2\pi r dr \tag{9}$$

It is assumed that the probability of death of the individuals inside the fires (Radius R) is 100%. To be able to compare the losses, the loss of lives was monetized using the Value of Statistic Life (VSL). An average value of 3,500,000 € was assumed for VSL. The detailed results of consequence analysis can be found in a previous study [35]. The total loss values are reported in Table 8.

Table 8. Total loss of scenarios

Segment	Total loss (million €)
Rural area	92
Station	2,239
Near the chemical plant	2,556
Urban area	156,726

4.3. Attractiveness analysis

An attractiveness analysis was carried out using the methodology developed by Argenti et al. (2015) which was summarized in Section 3.3. To quantify the attractiveness, the overall attractiveness index was calculated for each segment using Equation (10) [28]:

$$I_A = I_H \times \phi \tag{10}$$

where I_A is the overall attractiveness index, I_H is the hazard-based index, and ϕ is the induction index. The detail of the calculation steps are reported elsewhere [35]. The following assumptions were made:

- Private ownership
- Absence of military targets, institution buildings, embassies, monuments of high symbolic value, critical infrastructure in the site proximity
- Chemicals that can be used as weapons of mass destruction are not stored/ handled/ processed/ produced in significant quantities in the site
- Threat history provides no records of attack to similar facilities. Suspect of terrorist calls or active groups presence in the area
- A context of political stability and democracy exist. Governing authorities are legitimated and supported by populace
- Strict legislation concerning the transport, selling and detention of weapons of any nature. Effective and diffuse implantation of controls by police forces
- Company activities are accepted by local community. Few aversion motives of minor importance
- Medium level of engagement of local stakeholders. Company activities are accepted by local community, few aversion motives of minor importance
- No significant negative interactions with culture/ historical, archaeological, religious heritage. Sporadic demonstrations of aversion by local activities

In order to compare the attractiveness scores and use them to evaluate the security risk, the attractiveness scores were converted to a relative attractiveness index which is the attractive index of each segment divided to the sum of all the indexes, as in Table 9.

Table 9. Attractiveness index and relative attractiveness index

	Rural area	Station	Near chemical plant	Urban area
I H	2	4	4	20
ϕ	1.177	1.177	1.177	1.177
I A	2.4	4.7	4.7	23.5
A' (relative attractiveness index)	0.07	0.13	0.13	0.67

As shown in the results, the segment in the urban area is the most attractive one due to the presence of a higher population exposed to risk.

4.4. Security Risk

Assuming that an attack would happen to the pipeline (likelihood of attack = 1.0), the conditional security risk (SR) can be defined as:

$$SR = A' \times V \times C \tag{11}$$

Table 10 summarizes the results of the vulnerability assessment, the consequence analysis, and the attractiveness assessment along with the values of security risk for each segment; obviously, the higher the SR the more critical the segment.

Table 10. The final results of the security risk assessment

Segment	Vulnerability	Consequence	Relative Attractiveness	Security Risk (€)
Urban are	0.006	156,726	0.67	582.17
Station	0.007	2,239	0.13	2.07
Rural area	0.149	92	0.07	0.98
Near chemical plant	0.003	2,556	0.13	0.89

As shown in Table 10, the security risk of the pipeline segment in the urban area is much higher than those of the other segments due to the large value of loss because of a high population density (consequence). Also the relative attractiveness, which is affected as well by the population density, is higher for this segment. Based on the results obtained, the owners should allocate more security countermeasures to protect the pipelines in the urban area to reduce the security risk in this segment to values as low as reasonably practicable.

4.5. Discussion

The present study was aimed at demonstrating the application of DTBN to SVA of chemical facilities. As such, for illustrative purposes only, some simplifying assumptions were made. To develop an attack scenario, it was assumed that the attacker would regress before detonating the explosive materials. However, in case of either suicide bombers or car bombs the situation becomes more challenging even with the intervention of patrols. The ATs approach is suitable to be extended to account for a variety of attack scenarios, including suicide bomber and car bombs. Moreover, in consequence analysis, only human casualties and direct economic losses were considered. However, for a more precise and comprehensive consequence analysis, indirect economic costs such as the losses due to the ruined reputation of the company, business discontinuity, and disruption in supply chain should be taken into account.

To further improve the developed methodology, the incorporation of attractiveness assessment and of consequence analysis in a single dynamic BN should be considered. This should allow updating the security risk including any relevant information and precursor data that becomes available, such as failure in the surveillance system due to internal failures, breaches in the fences, and even accidental release of hazardous chemicals.

5. Conclusion

In this study, an innovative methodology was introduced for security vulnerability assessment of hazardous pipelines. The developed methodology uses a discrete-time Bayesian network to quantify the vulnerability as an indication of the conditional probability of success given an attack. The methodology takes into account the proficiency of the attacker, the attack plane and the barriers' efficiency as well as the dynamic behaviour and time dependencies existing in executing a successful attack. The security risk of a pipeline was evaluated and quantified as the product of (i) the pipeline relative attractiveness, as an indication of the attack likelihood, (ii) pipeline vulnerability, as an indication of the conditional probability of a successful attack given that an attack has taken place, and (iii) the consequences of a successful attack in terms of human casualties and damage to the assets while considering potential domino effects. Such quantitative methodology enables the owner/operators of the pipeline to rank order the pipeline segments based on security risk and decide about the optimal allocation of budget and security barriers to reduce risks.

References

[1] Bajpai S, Gupta JP, "Site security for chemical process industries," *Journal of Loss Prevention in the Process Industries ,* vol. 18, pp. 301-309, 2005.

[2] "AFP, ISIS launches attacks at Iraq's largest oil refinery. 2015, Alarabia: Kirkuk, Iraq.," Alarabia, Kirkuk, Iraq, 2015.

[3] Scott A, "Terrorist Attack Hits U.S.-Owned Chemical Plant In France," Chemical and Engineering News, 2015.

[4] "9th Report of the European Gas Pipeline Incident Data Group," 2015.

[5] "API recommended practice 780: Security Risk Assessment for the Petroleum and Petrochemical Industries," American Petroleum Istitute , Wanshington DC, 2013.

[6] Brian R. Dunbobbin T.J.M., Murphy M, Ramsey A, "Security Vulnerability Assessment for Chemical Industry," *Wiley InterScience,* 2004.

[7] RAMCAP™ EXECUTIVE SUMMARY. Available at: http://files.asme.org/ASMEITI/RAMCAP/12604.pdf

[8] Bajpai S, Gupta JP, "Securing oil and gas infrastructure," *Journal of Petroleum Science and Engineering,* vol. 55, pp. 174-186, 2007.

[9] Gribaudo M, Iacono M, and Marrone S, “Exploiting Bayesian Networks for the Analysis of Combined Attack Trees,” *Electronic Notes in Theoretical Computer Science,* vol. 310, pp. 91-111, 2015.

[10] Kenneth S. Edge, G.C.D.I., Richard A.Raines, Robert F.Mills, “Using attack and protection trees to analyze threats and defense to homeland security .,” *Air Force Institute of Technology.*

[11] Talarico L, Reniers G, Sörensen K, Springael J, “MISTRAL:A game-theoretical model toallocate security measures,” *Reliability Engineering and System Safety ,* vol. 138, pp. 105-114, 2015.

[12] Zhang L, Reniers G, “A Game-Theoritical Model to Improve Process Plant Protection from Terrorist Attacks,” *Risk Anal,* 2016.

[13] Khalil Y, “A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures,” *Process Safety and Environmental Protection,* vol. 102, pp. 473-484, 2016.

[14] van Staalduinen MA, Khan F, Gadag V, Reniers G, “Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure,” *Reliability Engineering & System Safety,* vol. 157, pp. 23-34, 2017.

[15] Khakzad, N., F. Khan, and P. Amyotte, “ Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches,” *Reliability Engineering & System Safety,* vol. 96, no. 8, pp. 925-932, 2011.

[16] Khakzad, N., F. Khan, and P. Amyotte, “Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network,” *Process Safety and Environmental Protection,* vol. 91, no. 1-2, pp. 46-53, 2013.

[17] Yuan Z, Khakzad N, Khan F, Amyotte P, “Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks,” *Risk Analysis,* vol. 35, no. 2, pp. 278-291, 2015.

[18] Khakzad N, Reniers G, “ Using graph theory to analyze the vulnerability of process plants in the context of cascading effects,” *Reliability Engineering and System Safety ,* vol. 143, pp. 63-73, 2015.

[19] Khakzad N, Reniers G, Abbassi R, Khan F, “ Vulnerability analysis of process plants subject to domino effects,” *Reliability Engineering and System Safety ,* vol. 154, pp. 63-73, 2016.

[20] Neapolitan R, “Probabilistic Methods for Bioinformatics with an introduction to Bayesian Networks,” in *Chapter: 5: Foundation of Bayesian Networks*, United States, 2009.

[21] Jensen FV, Nilson TD, “Bayesian Networks and Decision Graph,” in *Causal and Bayesian Networks*, 2007.

[22] Boudali H, Dugan JB, “A discrete-time Bayesian network reliability modeling,” *Reliability Engineering and System Safety ,* vol. 87, pp. 337-349, 2005.

[23] Khakzad N, Khan F, Amyotte P, “Risk-based design of process systems using discrete-time Bayesian networks,” *Reliability Engineering & System Safety,* vol. 109, pp. 5-17, 2013.

[24] Khakzad N, Khan F, Amyotte P, Cozzani V, “ Risk Management of Domino Effects Considering Dynamic Consequence Analysis,” *Risk Analysis,* vol. 34, no. 6, pp. 1128-1138, 2014.

[25] “ALOHA Computer Code Application Guidance for Documented Safety Analysis,” Department of Energy, Safety and Health, 2004.

[26] Marc J, Assael K, Fires, Explosions, and toxic Gas Dispersion, CRC Press, 2010.

[27] Antonioni G, Spadoni G, Cozzani V, “Application of domino effect quantitative risk assessment to an extended industrial area,” *Journal of Loss Prevention in the Process Industries,* vol. 22, no. 5, pp. 614-624, 2009.

[28] Argenti F, Landucci G, Spadoni G, Cozzani V, “The assessment of the attractiveness of process facilities to terrorist attacks,” *Safety Science ,* vol. 77, pp. 169-181, 2015.

[29] J. Blom-Bruggman, “Chapter 7,” in *Methods for determination of possible damages to people and objects resulting from release of hazardous materials* , TNO (the Netherlands Organization of Applied Science Research), 1992.

[30] Mokhtari M, Alavi Nia A, “The application of CFRP to strengthen buried steel pipelines against subsurface explosion,” *Soil Dynamics and Earthquake Engineering ,* vol. 87, pp. 52-62, 2016.

[31] Ebeling C, Reliability and Maintainability Engineering, MacGraw Hill, 1997.

[32] “Data Analytics, Mathematical modeling, Decision Support,” [Online]. Available: www.bayefusion.com.

[33] “Risk Assessment Data Directory, Ignition probabilities,” International Association of Oil and

Gad Producer, 2010.

[34] Lees F, Hazard indentification, Assessment and Control, UK: Butterworth-Heinemann: Oxford, 1996.

[35] Fakhravar D, “Security Risk Assessment of Gas Pipeline Using Bayesian Networks,” University of Bologna, Bologna, Italy, 2016.

[36] Khakzad N, Reniers G, “Protecting Chemical Plants against Terrorist Attacks: A Review,” *Socialomics,* 2015.

[37] Moore DA, Fuller B, Hazzan M, Jones JW, “Development of a security vulnerability assessment process for the RAMCAP chemical sector,” *J Hazard Mater,* vol. 143, pp. 689-94, 2007.

[38] Srivastava A, Gupta JP, “New methodologies for security risk assessment of oil and gas indusrty,” *Process SAfety and Environmental Protection ,* vol. 88, pp. 407-412, 2010.

[39] Tambe M, Security and Game Theory: Algorithms, Deployed systems, Lessons Learned, New York: Cabridge University Press, 2011.