CHEMICAL ENGINEERING TRANSACTIONS
VOL. 67, 2018
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Valerio Cozzani, Bruno Fabiano, Davide Manca

ISBN 978-88-95608-64-8; **ISSN** 2283-9216
DOI: 10.3303/CET1867042

Security Management of Process Plants by a Bayesian Network Methodology

Alessio Misuri[a], Nima Khakzad[b], Genserik Reniers[b], Valerio Cozzani[a,*]

[a]Department of Civil, Chemical, Environmental, and Materials Engineering, University of Bologna, Bologna, Italy
[b]Faculty of Technology, Policy, and Management, Delft University of Technology, The Netherlands
valerio.cozzani@unibo.it

Before the tragedy of 9/11, the perception of risk in process plants was mainly focused on accidental events caused by technical failures, human errors or natural events. However, since then, the risk of deliberate actions against process facilities – also known as security risk – has also become a concern. Security risk assessment of engineering systems and infrastructures constitutes a complex task since a significant multitude of technical and socio-political information is needed to reasonably predict the risk of intentional malevolent acts. In the present study, a methodology based on Bayesian network (BN) has been applied to increase the security of critical infrastructures via cost-effective allocation of security measures. Using the probability updating feature of BN, the proposed methodology can be employed to investigate the effect of vulnerabilities on adversaries' preferences while planning security scenarios. Moreover, the proposed methodology is capable of efficiently identifying an optimal defensive strategy given a security scenario (i.e., an attack) through maximizing defenders' expected utility.

1. Introduction

Process plants are well known for storing and processing large quantities of hazardous substances, which can be targeted by malicious agents with the aim of causing fatalities, properties losses and business interruption. After the terrorist attacks to the World Trade Centre in 2001, deliberate acts of interference against chemical and process plants have become an issue of major concern (Baybutt et al., 2003). A number of methodologies have been developed for supporting plants' owners in the task of efficient resource allocation for prevention and mitigation of such security events. Examples of guidelines for carrying out security risk assessments (SRAs) have been provided by American Petroleum Institute for securing Oil & Gas (O&G) infrastructures (API, 2003), and for petrochemical industries (API, 2012); Bajpai and Gupta (2007) proposed semi-quantitative guidelines for O&G facilities. Common features of these methodologies is that they provide at best semi-quantitative outcomes, and that they are mainly based on sequential steps of parameters' scoring. According to API (2012), SRA has to be carried out starting from (i) identification of critical units, followed by (ii) threat assessment, (iii) attractiveness assessment, (iv) vulnerability assessment, (v) estimation of security risk, and finally (vi) evaluation of risk treatment options. As pointed out by Khakzad et al. (2017), such sequential scoring of security parameters may largely undermine the accuracy of the assessments. For example, the attractiveness is generally assessed before the vulnerability, and thus the influence of the latter cannot be fully accounted for when assessing the former. Another issue related to security is the complexity of the task: following API (2012), the team appointed to conduct SRA needs to gather a significant amount of information, from technical documentation about the plant (plant layout, operational procedure, etc.), to data about socio-political context where the facility operates (international tensions, armed conflict zones, etc.). It is clear that a holistic approach is required in conducting SRA. The present study focuses on the development of a novel probabilistic methodology based on Bayesian network (BN) to realize an overarching framework for dealing with the need to consider mutual interactions between parameters of various nature. BN is a widespread tool employed in reliability engineering and safety science, but only a few applications can be found in the field of security. Some examples can be found in Paté-Cornel and Guikema (2002), Argenti et al. (2016), van Staalduinen et al. (2017), and Misuri et al. (2018). In the next section BN and Limited Memory

Please cite this article as: Misuri A., Khakzad N., Reniers G., Cozzani V., 2018, Security management of process plants by a bayesian network methodology, Chemical Engineering Transactions, 67, 247-252 DOI: 10.3303/CET1867042

Influence Diagram (LIMID) as an extension of BN for decision making will be described. In Section 3 the application of the methodology will be outlined, while Section 4 is reserved for demonstrating the effectiveness of the methodology through the application to a notional case study. Section 5 reports the conclusions of the study.

2. Bayesian network

Within the field of security risk assessment, tools able to catch the inherent uncertainty of influential parameters and variables are needed. In this regard, probabilistic techniques such as Bayesian network (BN) offer not only a flexible framework to model security scenarios, but to capture the underlying uncertainties. BN is a probabilistic tool for knowledge elicitation and reasoning under uncertainty (Pearl, 1988). BN is a directed acyclic graph made of arcs and nodes. It allows the description of complex systems comprising variables of various nature through local specification of their dependencies. Thus, this tool allows merging together knowledges from various sources and provides a holistic framework for summarizing information in a concise and clear structure. BN makes it possible to compute the joint probability distribution of a set of random variables X = {X1, X2, ..., Xn} as multiplication of local conditional probabilities. Employing the Bayes' theorem, it is possible to use new information, called evidence *E*, to compute updated probabilities $P(X|E)$ as in Eq(1):

$$P(X|E) = \frac{P(X) \cdot P(E|X)}{\sum_{X/E} P(X) \cdot P(E|X)} \quad (1)$$

In this study, we employ Limited Memory Influence Diagram (LIMID) – an extension of BN by adding decision and utility nodes – for decision making. This tool is a sophistication of BN which can also account for decision nodes and utility nodes, and which has been specifically developed for decision making (Lauritzen and Nilsson, 2001).

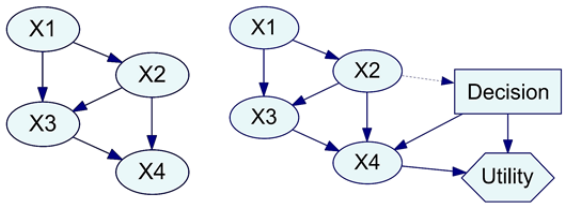

Figure 1: A simple BN on the left; Extension of BN to LIMID on the right.

LIMID takes the advantages of BN properties, with the additional possibility to evaluate the optimal strategy (i.e., the optimal temporally-ordered sequence of decisions), according to the expected utility theory (Pearl, 1988). For example, considering the LIMID in Figure 1, the expected utility of the j-th decision alternative $EU(d_j)$ can be computed according to Eq(2):

$$EU(d_j) = \sum_{X_2,X_3,X_4} P(X_4|X_2, X_3, d_j) \cdot U(d_j, X_4) \quad (2)$$

The optimal decision alternative d_k is the one which satisfies Eq(3):

$$EU(d_k) \geq EU(d_j) \text{ for each } j \neq k \quad (3)$$

3. Application of LIMID to security assessment

The methodology developed for SRA is specifically based on the LIMID presented in Figure 2. This network is realized to overarch knowledge and to deal with the task of determining the optimal strategy for allocating resources for securing a critical infrastructure through a systemic approach.

The network is made of thirteen chance nodes describing variables to be accounted for, two sequential decision (rectangle shaped) nodes for describing proactive ("Security_Countermeasures") and reactive ("Security_Response") security measures, three utility (diamond shaped) nodes to quantify decisions' cost and damages resulting from the attack. The "Total_Utility" node is a node which sums the values of its parents. It has been provided to summarize the expected utility of each scenario. The upper part of the network is aimed at the description of adversary and its features, together with a node for description of the level of awareness of each adversary (i.e., "Intelligence_Level_Alert"). The middle section is intended for description of the features of attack scenario, that is, the means of delivery, the target, and the threat (e.g., an explosive attack,

or a sabotage). The bottom part is provided for probabilistic description of consequences of the attack, including the life losses, the damages to assets, to production and to reputation.

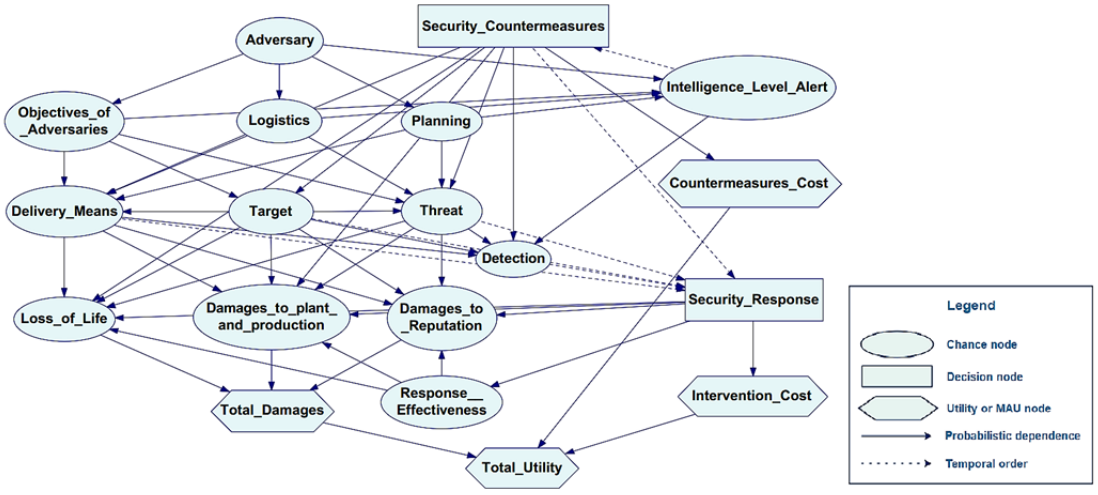

Figure 2: The LIMID for optimal security management. (Misuri et al., 2018).

The LIMID model has to be completely specified before it can be used for optimal strategy computation. To do that, the behaviour of the attacker should be described according to a bounded rationality system (Rubinstein, 1998): each adversary is supposed to act as a rational decision-maker with a finite set of alternatives. As a result, the conditional probability of each scenario, given a specific adversary, can be identified as the ratio of the expected utility of the scenario to the sum of the expected utilities of all scenarios estimated by the defender from adversary's perspective.

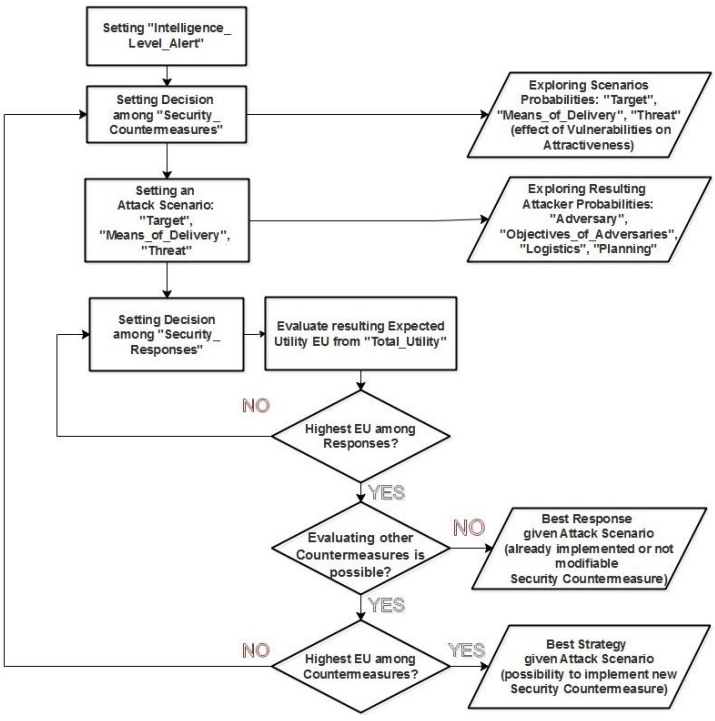

Figure 3: Flowchart to be followed for running the LIMID model (EU: expected utility) (Misuri et al., 2018).

As an example, Eq(4) reports the corresponding equation for the choice of a weapon W_i (i.e., the probability $P_{def}(W_i|I_{adv})$) within a finite set of alternatives. In Eq(4), the subscripts "*adv*" and "*def*" refer, respectively, to

from an adversary or defender perspective, U is the utility, W is the weapon, and I is the intention of the adversary.

$$P_{def}(W_i|I_{adv}) = \frac{EU_{adv}(U_{adv}|W_i,I_{adv})}{\sum_i EU_{adv}(U_{adv}|W_i,I_{adv})} \quad (4)$$

This approach has been applied by Paté-Cornell and Guikema (2002) in their work and was extended by Misuri et al. (2018).
The specification of utility nodes should be carried out via utility functions which convert monetary values into utilities based on decision maker's attitude toward risk and costs. Once the utility functions and values are specified, the model has to be run following the flowchart presented in Figure 3. On the right-hand side of the figure the four outcomes are reported as parallelograms: from the top, (i) the probability of each scenario, given a set of security countermeasures, describing the effect of process plant's vulnerabilities on the plant's attractiveness, (ii) the probability of different adversaries, given the attack scenario and the proactive measures, (iii) the best response, given an attack and the proactive measures, and (iv) the best strategy to deal with a defined attack scenario, intended as the collection of both proactive and reactive measures.

4. Illustrative case-study

In order to show the effectiveness of the methodology, it has been applied to a hypothetical refinery in Figure 4 adapted from API RP-780 (API, 2012). The dock has been considered as a possible path of entrance rather than a possible target. Target set is thus composed of the tank farm area, the production facility and the offices. Attacks via ground and via water are considered, as shown by black arrows in Figure 4. The threats considered are attack with explosive, and sabotage. Thus, 12 scenarios are accounted for as combination of targets, means of entrance, and threats. For example, "Scenario 1" is an explosive attack via ground against the tank farm area. For a complete list, refer to the legend in Figure 5.

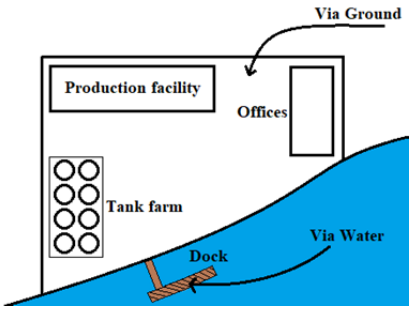

Figure 4: Simplified layout of a hypothetical refinery adapted from API RP-780 (2012).

The set of possible adversaries is composed of terrorists, disgruntled employees, and environmental activists. In either case, the aim, most probably, would be to cause the maximum damage in form of fatality (losses) or damage to the assets (symbolism).
An available budget of $B_{Max} = 0.5\ M\$$ for enhancing the security has been considered. Table 1 reports three possibilities for each decision, together with cost (C_i) and relative utilities ($U(C_i)$) using the utility function (Blank, 1980), provided in Eq(5).

$$U(C_i) = 1 - \frac{C_i - B_{Max}}{B_{Max}} \quad (5)$$

Table 1: Policies for security countermeasures and responses with respective costs and utility values

Node (in Figure 2)	Decision	C_i (M$)	Utility ($B_{Max} = 0.5M\$$)
Security_Countermeasure	No additional countermeasures	0.0	2.0
Security_Countermeasure	CCTV (Closed Circuit Television)	0.4	1.2
Security_Countermeasure	Patrol	0.3	1.4
Security_Response	Do nothing	0.0	2.0
Security_Response	ESD (Emergency Shut Down)	0.3	1.4
Security_Response	ESD + Evacuation Plan	0.5	1.0

The total attack consequences have been evaluated as the sum of monetary quantification of loss of lives, assuming a value of statistical life of 3.5 M$ (Reniers and Van Erp, 2016) and of physical damages and business interruption costs multiplied by a factor to account for the loss of reputation as well. The utility table of the node "Total_Damage" has been fulfilled for each possible consequences' combination after converting the monetary values through Eq(5), considering a risk tolerance $B_{Max} = 1\ M\$$. Table 2 shows part of the utility table for total damage quantification.

Table 2: Part of the utility table for the node "Total_Damage".

Loss of lives	[M$]	Physical & Business Damages	[M$]	Reputation Loss (factor)	Total [M$]	Utility ($B_{Max} = 1M\$$)
No injuries	0	Short period damages	1	Low (1.25)	1.25	0.75
From 1 to 3 deaths	10.5	Medium period damages	5	High (1.5)	23.25	-21.25
From 3 to 5 deaths	17.5	Long period damages	35	High (1.5)	78.75	-76.25

Conditional probability tables have been fulfilled using illustrative values, since the aim of the study is to demonstrate how the methodology works rather than to provide results from a real case study.
The network has then been solved using GeNIe software (Bayes Fusion, LCC). Through the application of Bayes' Theorem (see Eq(1)) posterior probabilities of scenarios have been calculated, given the implementation of a CCTV, which is a modification to the plant's vulnerability. The first outcome of the model is presented in Figure 5. The horizontal axis reports the allowed scenarios. The figure shows how modification to the plant's vulnerability affects attractiveness of different scenarios to the attackers. For example, probability of scenario 1 decreases significantly, while probability of scenario 10 increases as adversaries' reaction to security system's strengthening (adversaries are supposed not to renounce to attack).

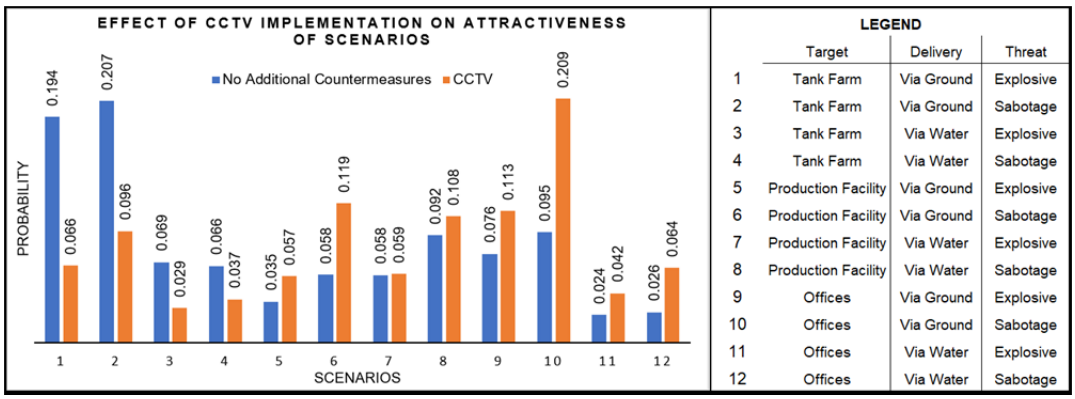

Figure 5: Effect of change in vulnerabilities on attractiveness of scenarios for the illustrative case study.

The second outcome of the model is the set of posterior probabilities of adversaries, given scenario of interest and implementation of security countermeasure.

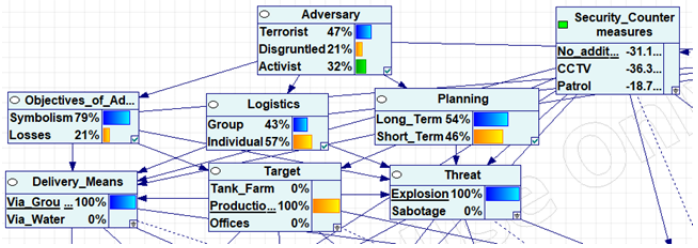

Figure 6: Adversaries' features ranking, given no additional countermeasures, and a certain scenario (target: Production facility, delivery means: via ground, threat: explosion).

Figure 6 shows a section of the model in case of scenario 9, indicating that if no countermeasures are implemented, the most probable attacker is an individual terrorist carrying out long-term planned actions, for objectives related to symbolism (highest probabilities expressed as percentages in the nodes of Figure 6). However, it should be noted that such results have been obtained under specific assumptions and thus cannot be considered viable or generalized to other case studies.
Last two outcomes from the model can directly be read from expected utility tables provided by the software solving the LIMID. Table 3 shows the expected utility table related to scenario 1. The optimal strategy is associated with the highest value in table: implementing a patrol surveillance, and in case of attack activating ESD. The underlined values represent the best response for the same scenario, in case the first decision cannot be modified. For example, in case a no additional countermeasures were going to be implemented, the best policy would be to activate ESD and alert authorities.

Table 3: Expected utility table for scenario 1, that is, explosive attack against tank farm via ground.

Security Countermeasure → Security Response ↓	No additional countermeasures	CCTV	Patrol
Do nothing	-43.5	-39.8	-18.5
ESD (Emergency Shut Down)	-37.1	-35.1	-15.7
ESD + Evacuation Plan	-36.9	-36.5	-31.4

5. Conclusions

A novel methodology for optimal security management has been presented in this study. The employed model is based on a limited memory influence diagram (LIMID) able to incorporate probabilistically and systematically a multitude of information including the type of threats, adversary types, delivery means, attack objectives, available countermeasures, and emergency response actions. The methodology takes the advantage of the Bayes' Theorem to evaluate the effect of countermeasures on adversaries' choice of attack scenarios. Furthermore, the model can be used to rank strategies and to define cost-effectively the best response to an attack scenario, given the already implemented security countermeasure. We demonstrated the application of the methodology to a hypothetical process plant; yet the methodology can be tailored for security risk assessment and management of a variety of critical infrastructures.

References

American Petroleum Institute (API), 2003, API RP-70: Security for offshore oil and natural gas operations. American Petroleum Institute, Washington, DC.

American Petroleum Institute (API), 2012, API RP-780: Security risk assessment methodology for the petroleum and petrochemical industries. American Petroleum Institute, Washington, DC.

Argenti F., Landucci G., Reniers G., 2016, Probabilistic vulnerability assessment of chemical plants subjected to external acts of interference, Chemical Engineering Transactions, 48, 691-696.

Bajpai S., Gupta J.P., 2007a, Securing oil and gas infrastructures. J. of Petroleum Sci Eng. 55, 174-186.

Baybutt P., Reddy V., 2003, Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defence Journal, 2, 1.

Bayes Fusion, LCC, GeNIe Modeler, <www.bayesfusion.com> accessed 20.06.2018.

Blank L., 1980, Statistical procedures for engineering, management and science. McGraw Hill, New York.

Khakzad N., Reniers G., van Gelder P., 2017, A multi-criteria decision making approach to security assessment of hazardous facilities. J Loss Prev Process Ind, 48, 234-243.

Lauritzen S.L., Nilsson D., 2001, Representing and solving decision problems with limited information. Manag Sci, 47(9), 1235-51.

Misuri A., Khakzad N., Reniers G., Cozzani V., 2018, A Bayesian network methodology for optimal security management of critical infrastructures. Rel Eng Sys Saf, DOI:10.1016/j.ress.2018.03.028.

Paté-Cornell E., Guikema S., 2002, Probabilistic modelling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Mil Oper Res, 7(4).

Pearl J., 1988, Probabilistic reasoning in intelligent systems. CA: Morgan Kaufmann, San Francisco.

Reniers G, Van Erp H.R.N., 2016, Economic foundation in operational safety economics: a practical approach focused on the chemical and process industries. John Wiley & Sons, Chichester, UK.

Rubinstein A., 1998, Modeling bounded rationality. Mass: MIT Press, Cambridge.

van Staalduinen M.A., Khan F., Gadag V., Reniers G., 2017, Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructures. Reliab Eng Syst Saf, 157, 23-34.