Reliability Engineering and System Safety 169 (2018) 515–530

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network

Francesca Argenti[a], Gabriele Landucci[b], Genserik Reniers[c,d], Valerio Cozzani[a,*]

[a] LISES - Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum - Università di Bologna, via Terracini n.28, Bologna 40131, Italy
[b] Dipartimento di Ingegneria Civile e Industriale, Università di Pisa Largo Lucio Lazzarino 1, Pisa 56126, Italy
[c] Safety Science Group, TU Delft, Jaffalaan 5, Delft, The Netherlands
[d] Engineering Management Department, Research Groups ARGoSS and ANT/OR, University of Antwerp, Prinsstraat 13, Antwerp 2000, Belgium

ARTICLE INFO

Keywords:
Security risk
Physical protection systems
Vulnerability
Probabilistic assessment
Bayesian Networks

ABSTRACT

Chemical facilities may be targets of deliberate acts of interference triggering major accidents (fires, explosion, toxic dispersions) in process and storage units. Standard methodologies for vulnerability assessment are based on qualitative or semi-quantitative tools, currently not tailored for this type of facilities and not accounting for the role of physical protection systems. In the present study, a quantitative approach to the probabilistic assessment of vulnerability to external attacks is presented, based on the application of a dedicated Bayesian Network (BN). BN allowed the representation of interactions among attack impact vectors and resistance of process units, which determine the final outcomes of an attack. A specific assessment of protection systems, based on experts' elicitation of performance data, allowed providing a knowledge support to the evaluation of probabilities. The application to an industrial case study allowed the assessment of the potentialities of the approach, which may support both the evaluation of the vulnerability of a given facility, and the performance assessment of the security physical protection system in place.

1. Introduction

Industrial facilities storing and processing relevant quantities of hazardous chemicals have an inherent hazard potential that may be exploited by malevolent agents, causing a major accident [1–3]. The attack perpetrated in France against the production site of a chemical company in June 2015 [4] demonstrated that this type of threat for industrial facilities located in western countries is credible. At the same time, it was shown that the security of industrial sites must be addressed, both from the legislative and the technical point of view, as an issue of the greatest urgency.

Actually, after the events of "9/11", the security of sites where relevant quantities of hazardous chemicals are stored or processed became a concern [5], and security risks started to be included in formal risk assessment [6]. According to the prescriptions of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 ("the CFATS Act of 2014") [7], the U.S. Department of Homeland Security (DHS) is required to analyze vulnerabilities and establish risk-based security performance standards for critical infrastructures, which include chemical facilities as one of the highest priority sectors; facility owners and operators are required to prepare a security vulnerability assessment and a facility security plan, identifying specific assets of concern.

The "European Programme for Critical Infrastructure Protection (EPCIP)" [8] promotes the prevention, preparedness and response to terrorist attacks involving installations of the energy (electricity, oil and gas) and the transport (road, rail, air, inland waterways and ocean and short-sea shipping and ports) sectors. On the other hand, European Seveso-III Directive [9] concerning major accident hazards focuses on safety-related issues and does not addresses the need for a security analysis or for security countermeasures in industrial installations that may be considered attractive or vulnerable targets of terrorist attacks. Hence, no detailed guidelines are yet available for the security of chemical and process plants in the EU.

In the last 15 years, the development of security risk assessment methodologies was promoted to guide and support industrial operators in assessing and managing security risks. Among others, it is worth recalling the security risk assessment methodologies proposed by American Petroleum Institute – API [10], American Institute of Chemical Engineering [11], Sandia National Laboratories [12] and U.S. National Institute of Justice [13]. These methodologies allow for a qualitative or a semi-quantitative (e.g. in the case of API methodology) assessment of security risk, while only general guidance for security risk mitigation and lists of possible solutions in terms of security countermeasures depending on the existing security alert level are provided in the litera-

* Corresponding author.
E-mail address: valerio.cozzani@unibo.it (V. Cozzani).

https://doi.org/10.1016/j.ress.2017.09.023
Received 19 September 2016; Received in revised form 24 September 2017; Accepted 30 September 2017
Available online 3 October 2017
0951-8320/

ture [14]. However, as the credibility of the threat against chemical and process industry facilities increases, the assessment of security-related and terrorism-related risks should be dealt with using more systematic approaches at a quantitative level, in order to provide a metric of existing vulnerability and of the available level of protection with respect to external attack scenarios.

In this study, an approach based on probabilistic risk analysis, supported by Bayesian Networks (BN), was developed for the analysis of outsiders' threat against chemical facilities. The approach focuses on the vulnerability of high-consequence loss of physical assets within the facility, i.e. process and storage equipment that are critical in terms of potential of causing major accidents [11,13]. A dedicated approach was developed in order to include the contribution of physical security elements in the determination of vulnerability. The approach and the BN presented herein are aimed at supporting the analysis of existing installations by security managers and risk analysts, as they provide a quantitative tool to conduct scenario-based vulnerability assessment.

The paper is structured as follows: in Section 2, the background on security and vulnerability studies dedicated to the process industry is presented; in Section 3, the methodological approach and the Bayesian Network tool are described; in Section 4 a case study is presented, whose results are discussed in Section 5; Section 6 discusses potentialities and limitations of the present approach and in Section 7 conclusions are drawn.

2. State of the art

2.1. Literature dealing with security risks evaluation

Literature studies concerning security-related issues faced by the process industry were mostly devoted to the evaluation of the severity of impacts due to external attacks on process plants [15–17], to the analysis and characterization of terrorist threats [18], or were focused on the determination of process facilities attractiveness to potential malevolent adversaries [19,3].

Beside the characterization of attacks and the assessment of attack tactics, several literature studies were also devoted to the analysis of the defense strategy adopted in complex systems. According to the review carried out by Hausken and Levitin [20], defense measures are divided into separation of system elements, redundancy, protection, multilevel or multilayered defense, deployment of false targets and preventive strike.

Few contributions investigated the potential of deliberate attacks to trigger domino effects [15,17,21,22], leading to extensive damages due to consequence escalation and to the involvement of multiple units.

The scientific Community was however divided in the selection of the most suitable approach to be adopted to address the assessment of the likelihood of security risks: in particular, several authors (e.g. see [23–25]) discussed if probabilistic risk analysis (PRA) or intelligent adversary methods would be preferable for counterterrorism risk management. An extended discussion on the strengths and drawbacks of the two approaches can be found in the Special Issue dedicated to "Advances in Terrorism Risk Analysis" of the Risk Analysis journal [26]. Among others, Garrick et al. [27] and Paté-Cornell and Guikema [28] used a PRA approach to assess quantitatively the risk posed by terrorist-initiated events. Apostolakis and Lemon [29] applied PRA in the analysis of the risk posed to different types of infrastructures at Massachusetts Institute of Technology University campus by malevolent attackers with limited capability (minor threat). In the latter case, the whole analysis is conditional to the presence of the threat. Hausken applied game theory [30] to assess the role of human behavior and conflicts in resource allocation for the defense, thus providing a quantitative tool to incorporate the defender's perspective into PRA.

Concerning the assessment of attacks against sophisticated networks and complex systems and infrastructures, several examples of modeling approaches are available in the literature. Hausken [31] proposed an integrated method for the optimization of protection investments and resources for complex infrastructures considering one strategical defender protecting an entire system of multiple targets potentially affected by multiple strategic attackers. In the approach, operations research, reliability theory, and game theory are merged to support the optimization.

Chopra and Khanna [32] combined an empirical economic input–output model with graph theory based techniques for understanding interdependencies and resilience in the United States economic system due to interdependencies among critical infrastructures; in particular, a comparison among the effect of random failures and targeted attacks on key nodes of the critical infrastructures network was carried out, evidencing critical system vulnerabilities.

Wu et al. [33] developed an attack strength degradation model able to capture the interdependencies among infrastructures and to model cascading failures based on the application of graph theory. The problem of interdependency, with particular reference to transportation networks, was also addressed by Zhang et al. [34], that investigated overloads and cascading failures possibly leading to catastrophic events.

However, according to the literature survey and in light of the qualitative or semi-quantitative nature of existing security risk assessment methodologies [11,13], the need to develop a quantitative evaluation approach tailored to the chemical industry clearly emerges. For this purpose, a PRA approach was selected in the present study, since it allows to structure the analysis of external attack scenarios from the point of view of the system under attack, more easily accounting for the measures in place to protect it. Actually, as pointed out by Garrick et al. [27], in the case of external attacks to chemical industry or, more in general, to industrial facilities, the initiating events triggered by external threats are tied to the design and operations of the facility under attack, which are fixed and well defined, as well as the protection systems.

In order to illustrate the framework in which the present study set its basis, the security risk formulation is firstly presented to support the PRA approach considered (Section 2.2). Then, since the focus of the study is the vulnerability assessment of chemical facilities, the concept of vulnerability and some key definitions are briefly discussed (Section 2.3).

2.2. Security risk formulation

The necessary basis to support the quantitative assessment of vulnerability adopted in the present study is to define a sound scientific risk framework aimed at conceptualizing the relevant terms object of the present investigation. The commonly adopted risk framework in process safety domain defines risk as a combination of consequences and associated probabilities or associated uncertainties [35]. In this framework, probability is normally interpreted as a "frequentist probability", thus interpreted as the fraction of time in which the event occurs and continuously repeats over time [36].

Differently, within security framework, e.g. dealing with the assessment of intentional acts of interference, risk is commonly defined as the triplet asset/value, threat and vulnerability [23,26], without any explicit reference to a probabilistic component.

However, in a recent study, Amundrud et al. [36] provided indications on how safety and security risk frameworks are compatible and traced a blue line in which also security risk may be defined through events-consequences and uncertainties. To express the uncertainties, it is recommended to use probability or interval probabilities, together with judgments of the strength of knowledge supporting the probabilities [37,38]. In the review provided by [39] it is indicated that a way to express the uncertainties is to refer to probability. Moreover, a necessary element needed to strengthen this kind of approach is the support of a strong knowledge judgment, which, however is not systematically adopted in security analyses and may constitute an element of novelty [38].

Based on the aforementioned considerations, the following expression is adopted to describe the risk in the present work:

$$R = (P(A),\ P(L|A),\ K) \tag{1}$$