Safety Science 77 (2015) 169–181

Contents lists available at ScienceDirect

Safety Science

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

The assessment of the attractiveness of process facilities to terrorist attacks

Francesca Argenti [a], Gabriele Landucci [a,*], Gigliola Spadoni [b], Valerio Cozzani [b,*]

[a] Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Largo Lucio Lazzarino 2, 56126 Pisa, Italy
[b] LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, via Terracini n.28, 40131 Bologna, Italy

ARTICLE INFO

Article history:
Received 17 November 2014
Received in revised form 17 February 2015
Accepted 20 February 2015

Keywords:
Terrorist attack
Process industry
Attractiveness
Security vulnerability assessment
Major accident hazard

ABSTRACT

Acts of interference against facilities of the process industry might result in severe consequences in case of a successful attack (major explosions, fires, toxic dispersions or environmental contamination). Although protection measures are usually in place to resist intrusion and process industry sites are mostly well equipped to meet emergencies, the security of industrial sites, and in particular of chemical and petro-chemical facilities, has become a matter of increasing concern in recent years. In the present study, a semi-quantitative methodology for the assessment of industrial facilities attractiveness with respect to malicious acts of interference was presented. The methodology considers two main aspects as targeting incentives. The first is related to the plant hazard potential, i.e. the potential of causing severe damage to population in case of successful attack leading to a major accident in the facility. The second aspect is the perceived value that a target may have for a specific threat. A set of relevant specification elements influencing the targeting logic were identified, considering socio-political and strategic elements, and scoring criteria were established to estimate the attractiveness increase due to the perceived value of the target to the threat. A set of case studies, drawn on the features of existing installations, was used to exemplify the procedure for attractiveness assessment. The methodology demonstrated the importance of considering both technical and socio-political aspects, as well as ideological and strategic incentives to an attack, for a holistic determination of plant attractiveness.

1. Introduction

A number of severe events caused by domino effect and natural events impacting on industrial sites has raised the issue of the assessment and prevention of external hazard factors (Antonioni et al., 2009a, 2009b; Baesi et al., 2013; Cozzani et al., 2009; Nolan, 2008; Reniers et al., 2005; Salzano et al., 2003; Zio and Ferrario, 2013). Actually, standards and regulations addressing the safety of industrial facilities and the prevention of major accident hazard as the Seveso Directives in Europe (European Commission, 1997, 2003, 2012) mostly refer to the prevention, control and mitigation of accident scenarios caused by internal failures (e.g. component failures, human error, etc.). However, external threats may also trigger major accident scenarios in industrial facilities where relevant quantities of hazardous substances are stored or processed (Antonioni et al., 2007; Cozzani et al., 2013; Landucci et al., 2012a, 2014; Necci et al., 2013, 2014a, 2014b; Rasmussen, 1995; Showalter and Myers, 1994; Salzano et al., 2003; Young et al., 2004).

The analysis of all possible threats faced by the process industry shall include intentional interferences. These are defined by CCPS (Chemical Center of Process Safety (CCPS), 2003) as security risks: "the likelihood that a defined threat will exploit a specific vulnerability of a particular attractive target to cause a given set of consequences". Although the assessment and control of security risks is quite different with respect to that of "conventional" accidents having internal causes, some conceptual and operative links may be identified. Actually, the hazards posed by security threats to industrial installations, and in particular to chemical and petrochemical facilities, in terms of disruption of operations, destruction of property, injury or loss of life and potential of cascading effects are somehow comparable to those coming from major accidents due to internal causes (Nolan, 2008). Management of external threats is a natural corollary to the chemical industry's safety culture (American Chemistry Council (ACC), 2001) as it aims at reducing a wide range of risks and mitigating the effects of associated incidents. Efforts to improve security, as those aimed at improving

* Corresponding authors. Tel.: +39 050 2217907; fax: +39 050 2217866 (G. Landucci). Tel.: +39 051 2090240; fax: +39 051 2090247 (V. Cozzani).
E-mail addresses: gabriele.landucci@unipi.it (G. Landucci), valerio.cozzani@unibo.it (V. Cozzani).

http://dx.doi.org/10.1016/j.ssci.2015.02.013
0925-7535/

safety, serve the goals of risk control and management, as they are aimed at protecting the community and the company employees while maintaining operational standards.

Prior to September 11th 2001 deliberate acts of interference were not included in the formal risk assessment of process industries handling hazardous chemicals (Bajpai and Gupta, 2005; Baybutt and Reddy, 2003). In fact, industrial sites were believed to be extremely unlikely targets of malicious acts when compared to public malls, railway stations, and other crowded locations. The events of "9/11" have changed the scene dramatically, making the security of sites where relevant quantities of hazardous chemicals are stored or processed a major concern (Baybutt and Reddy, 2003).

Although major industrial sites have efficient barriers to resist intrusions and are mostly well equipped for meeting emergencies, threats from deliberate terrorist acts are high due to the severe potential consequences in case of a successful attack. Undoubtedly, external attacks to facilities storing and/or processing large amounts of potentially hazardous chemicals might result in high impact explosion, fire, toxic dispersion or environmental contamination scenarios (Lou et al., 2003).

Hence, the specific identification and management of security threats in the framework of risk analysis represents nowadays an important component in the control of major accident hazards, especially if it is considered that terrorists are aiming to cause as much damage as possible, and therefore, certain scenarios that would be considered extremely unlikely in case of safety thinking, might actually be likely in case of security thinking (Reniers and Audenaert, 2014).

The World Trade Centre terrorist attacks on "9/11" signed a dramatic change also in the level of attention devoted to terrorist threats by the legislation. In the US, prior to "9/11", the assessment of chemical plant site security as proposed by the US Agency for Toxic Substances and Disease Registry (Joseph et al., 1999) was considered as the most comprehensive analysis that was publicly available (Schierow, 2006). In the published work derived from ATSDR report (Joseph et al., 1999), plants manufacturing chemicals or pesticides, compressed gases in tanks, pipelines, pumping and fuels refueling stations were categorized among the 'soft targets' (Schierow, 2006). After "9/11", the US Congress enacted legislation that requires the Department of Homeland Security (DHS) to analyze vulnerabilities and establish risk-based security performance standards for critical infrastructure and facilities, and requires facility owners and operators to prepare a Security Vulnerability Assessment (SVA) and a facility security plan, identifying specific assets of concern (Schierow, 2006). The DHS identified chemical facilities as one of the highest priority critical infrastructure sectors (Shea, 2006), and suggested the key aspects to be weighted for assessing security, including the facility industrial classification, known or theoretical terrorist threat faced by a particular facility, the chemical hazards present, the quantities and location of the hazardous chemicals with respect to the surrounding population.

The European Seveso Directives (European Commission, 1997; European Commission, 2003; European Commission, 2012) concerning major accident hazards mainly addresses safety-related issues: not even in the Seveso-III Directive, issued in 2012 (European Commission, 2012), security analysis or additional security measures are mentioned as requirements for installations that may be considered attractive or vulnerable targets of terrorist attacks. On the other hand, the Council Directive 2008/114/EC (European Commission, 2008a) presents the "European Programme for Critical Infrastructure Protection (EPCIP)", which is based on a multiple risk approach that gives priority to the prevention, preparedness and response to terrorist attacks involving Critical Infrastructures (CIs) at European level. The sectors envisioned by the Directive as falling into the CI category are the energy (electricity, oil and gas) and the transport (road, rail, air, inland waterways and ocean and short-sea shipping and ports (IMO, 2004)) sectors. However, no detailed guidelines are yet available for the security of chemical and process plants in the EU.

The backdrop given above clearly evidences a context where growing requirements are posed to the assessment of security issues and external threats to sites where relevant quantities of hazardous substances are stored or processed. The state of the art of methods and tools available for the identification and management of security issues was carried out in the present study, and results are discussed in Section 2 of the present paper. What emerges from the literature survey carried out is that most of the tools are focused on the management of the security-related issues and on threat motives characterization. On the other hand, only few tools, mostly qualitative, are available to assess the attractiveness of industrial installations with respect to malicious acts of interference. The present study was thus aimed to develop a method for the semi-quantitative evaluation of the attractiveness of a process installation to external attacks. The procedure developed is based on the quantification of the hazards related to the industrial site and of the assessment of relevant features of the area around the site. Several deterrence factors as well as incentives to deliberate acts of interference were considered. The methodology was applied to a set of case studies in order to exemplify the calculation procedure, to assess the relevance of the results obtained and to understand the potential application of the technique.

2. State of the art of Security Risk Assessment (SRA) methods

Systematic methodologies were developed in the last four decades to support the enhancement of industrial safety, which have been translated into consolidate practices as QRA (Quantitative Risk Assessment) and QARA (Quantitative Area Risk Assessment) studies (CCPS, 2000; Cozzani et al., 2014; Mannan, 2005; Uijt de Haag and Ale, 1999). In contrast, the risk of terrorist activity is not yet effectively considered and may vary significantly over time, depending on rather unpredictable social and political phenomena (European Commission, 2008b). Assessing the risk of terrorist acts targeting industrial facilities is a challenging task for at least three reasons:

- there are few prior examples of terrorist acts targeting chemical or process facilities;
- numerous external factors may increase or decrease risks;
- interactions among factors influencing risks are dynamic and change over time (European Commission, 2008b).

In part, these difficulties stem from the fact that terrorism is a phenomenon of multi-causal factors and from the terrorists' deliberate efforts to defy prediction. The complexity of terrorism combined with the unique attributes of individual groups make it nearly impossible to capture the explanatory characteristics of the phenomenon in a single model (European Commission, 2008b).

For the above-mentioned reasons, contributions available in the open literature are mostly speculative and qualitative. Early work on the topic started after 9/11, with the development of the so-called security vulnerability assessment methods (API, 2003; Jochum, 2005; Störfallkommission (SFK), 2002; Uth, 2005). In parallel, a number of scholars focused on the psychology of individual terrorists or group processes (Post, 2002). Gupta (2004) started addressing terrorism's nature as a collective action and thus presented arguments rooted in economic and socio-psychological dimensions of human motivations. Few semi-quantitative methodologies have been proposed or adopted in practice for the Security