Process Safety and Environmental Protection xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Process Safety and Environmental Protection

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

Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects

Genserik L.L. Reniers[a,b,*], *Amaryllis Audenaert*[a,c]

[a] *Universiteit Antwerpen, Antwerp Research Group on Safety and Security (ARGoSS), Faculty of Applied Economics, Prinsstraat 13, 2000 Antwerp, Belgium*

[b] *Hogeschool-Universiteit Brussel, KULeuven, Research Group CEDON, Warmoesberg 26, 1000 Brussels, Belgium*

[c] *Faculty of Applied Engineering, Universiteit Antwerpen, Paardenmarkt 92, 2000 Antwerp, Belgium*

ABSTRACT

Chemical industrial areas or so-called chemical clusters consist of hundreds, and sometimes thousands, of chemical installations situated next to each other. Such areas can thus be seen as the summation of a large number of structures exhibiting danger to a certain degree for initiating or continuing accident domino effects or knock-on effects. In this article, an approach to investigate in a systemic way the vulnerability of each installation within the larger chemical cluster context, is developed. Our suggested method results in a prioritization of chemical installations with respect to their vulnerability for domino effects. The method can be used for intelligently designed protection of chemical industrial areas against terrorist attacks.

Keywords: Chemical cluster; Security; Process industries; Security management; Domino effects

1. Introduction

Following Reniers (2011), we define security as 'taking all preventive measures in order to avoid harmful incidents caused by unauthorized (internal or external) persons who intend to seriously damage an organization, as well as controlling such incidents and their adverse effects'. Security risks are composed of consequences, vulnerabilities, and threats. A security risk thus suggests intentionality. In CCPS (2000), a safety risk is defined as a measure of human injury, environmental damage, or economic loss in terms of both the incident likelihood and the magnitude of the loss or injury. The definition of a safety risk thus bears the suggestion of being accidental. Safety and security are thus different in the nature of incidents.

In the case of security an aggressor is present (Johnston, 2004; Randall, 2008; George, 2008) who is influenced by the physical environment and by personal factors (Randall, 2008). These parameters should thus be taken into account during security assessments. The aggressor may act from within the organization (internal) and from outside the organization (external) (Fontaine et al., 2007). Since probabilities in terms of security are very hard to determine (Johnston, 2004), the identification of threats and the development of measures in terms of security is a challenging task which is largely qualitative, as opposed to the case of safety measures where qualitative as well as quantitative techniques exist to determine preventive measures.

In case of safety risk assessments (or so-called 'risk analyses'), risks are detected and analyzed by using consequences and probabilities (or frequencies). In case of security risk assessments (or so-called 'Vulnerability Assessments'), threats are usually analyzed by using consequences, vulnerabilities and target attractiveness (Holtrop and Kretz, 2008) in some configuration. Occasionally, the intention to do harm is also considered in the Vulnerability Assessment.

It should be clear that the different proactive approach sometimes leads to the need for different and complementary protection measures in case of safety and security. Table 1

* Corresponding author at: Universiteit Antwerpen, Antwerp Research Group on Safety and Security (ARGoSS), Faculty of Applied Economics, Prinsstraat 13, 2000 Antwerp, Belgium.
E-mail address: genserik.reniers@ua.ac.be (G.L.L. Reniers).

Received 13 February 2013; Received in revised form 18 April 2013; Accepted 19 April 2013
0957-5820/$ – see front matter © 2013 The Institution of Chemical Engineers. Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.psep.2013.04.002

Table 1 – Non-exhaustive list of differences between safety and security.

Safety	Security
The nature of an incident is an inherent risk	The nature of an incident is caused by a human act
Non-intentional	Intentional
No human aggressor	Human aggressor
Quantitative probabilities and frequencies of safety-related risks are available	In case of less common security risks (e.g., terrorism), only qualitative (expert-opinion based) likelihood of security-related risks may be available
Risks are of rational nature	Threats may be of symbolic nature

Based on Reniers et al. (2011)

provides an overview of different characteristics attached to safety and to security.

Although the effects of accidental or intentional events are often comparable, terrorists deliberately searching for the best manner to execute their plans are aiming to cause as much damage as possible, and therefore, certain scenarios that would be labelled as extremely unlikely in case of safety thinking, might actually be likely in case of security thinking.

In any case, an integrated approach (Fontaine et al., 2007; Holtrop and Kretz, 2008; Hessami, 2004; Neven, 2005) is required, thereby employing early risk analyses and Vulnerability Assessments and making proper arrangements in a pro-active stage. Therefore, to deter potential terrorists and to decrease the possible consequences of an attack, it is essential that a quantitative methodology is developed to identify those chemical installations that are most vulnerable for initiating or continuing escalating events. If such installations would be intelligently protected against malicious acts, the industrial area's security – and safety – would be truly increased from a systemic viewpoint.

1.1. *Security legislation regarding terrorism aimed at chemical facilities*

In the United States, ten years following the World Trade Centre terrorist attacks on "9/11" in New York, security at the nation's chemical facilities remains a key focus. In 2007, the so-called CFATS regulations (Chemical Facility Anti-Terrorism Standards) came into effect, regulating the security of high-risk chemical facilities in the US. Information is collected and the US Department of Homeland Security (DHS) determines whether a facility is "high risk" or not. Subsequently, if a plant is considered "high risk", the Department assigns a facility to a tier, whereafter it is required to prepare and submit a Security Vulnerability Assessment, identifying specific assets of concern to DHS.

In Europe, the situation is quite different. Following the well-known (safety-related) European Seveso II Directive (Council Directive 96/82/EC, 1997) security analyses are not required, nor does the Directive impose additional security measures for installations that are either particularly vulnerable to terrorist attacks or that are potential targets of attacks. It should, nevertheless, be noted that all Seveso Directive requirements related to the mitigation of the consequences of accidents, and in particular the formulation in advance of emergency plans, will be of equal help with the consequences of a terrorist attack targeting a Seveso facility.

The Council Directive on the identification and designation of European Critical Infrastructures[1] (ECI) and the assessment of the need to improve their protection (Council Directive, 2008/114/EC, 2008) provides directives as how to enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures. The goal is to ensure there are adequate and equal levels of protective security for critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the European Union. However, harmonized European legislation on the issue of chemical plant security has yet largely to be determined. There are no detailed regulations at European level which could act as concrete guidelines for security management of chemical enterprises.

In addition to this European Directive, national legislation derived from current prevailing international security legislation (i.e., the International Ship and Port Facility Security Code or ISPS) (IMO, 2004) exists within the European Member States. The ISPS code is a comprehensive set of obligatory measures to enhance the security of ships and port facilities, developed in response to the "9/11" attacks in the United States. The measures under the Code were brought into force worldwide on July 1, 2004 (Bailleul, 2005). In Europe, this legislation is practically composed of two regulations (Commission Regulation No 725/2004, 2004; Commission Regulation No 884/2005, 2005) and a directive (Council Directive, 2005/65/EC, 2005). It should be remarked and stressed that implementing the ISPS code has strongly influenced security-related issues in enterprises of any kind situated within European ports. More specific, since the ISPS code's initiation, many chemical companies to a greater or lesser extent made changes in their physical and organizational security measures.

Security-related legislation is aimed at single facilities and how to control and if necessary, increase their preventive and protective measures against terrorist acts. However, none of these security-related regulations deal with escalation events between different chemical companies situated in each other's neighbourhood. Indeed, deliberately induced domino effects within chemical clusters has not been the concern of the legislator as yet, neither in the US, nor in Europe.

Nonetheless, practitioners as well as regulators should realize that chemical industrial activities are considered and known to be prone to terrorist threats, with possibly devastating human and financial consequences if an attack would be intelligently organized.

1.2. *Chemical clusters and terrorism*

As Fortis and Maggioni (Curzio and Fortis, 2002) state, firms decide to settle in a cluster on the basis of the expected profitability of being located there. This profitability depends on geographical and agglomeration benefits, obtained as the difference between gross location-related benefits and costs. As the number of corporations located in an industrial cluster increases, gross benefits increase due to productive

[1] There are a certain number of European critical infrastructures, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies among interconnected infrastructures. The sectors envisioned by the Directive are the energy (electricity, oil and gas) and the transport (road, rail, air, inland waterways and ocean and short-sea shipping and ports) sectors.

Please cite this article in press as: Reniers, G.L.L., Audenaert, A., Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Safety and Environmental Protection (2013), http://dx.doi.org/10.1016/j.psep.2013.04.002