CHEMICAL ENGINEERING TRANSACTIONS
VOL. 26, 2012
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Valerio Cozzani, Eddy De Rademaeker

ISBN 978-88-95608-17-4; **ISSN** 1974-9791
DOI: 10.3303/CET1226078

Security within the Chemical Process Industry: Survey Results from Flanders, Belgium

Genserik L.L. Reniers[a,b]

[a]Universiteit Antwerpen, Antwerp Research Group on Safety and Security (ARGoSS), Prinsstraat 13, 2000 Antwerp, Belgium
[b]Hogeschool-Universiteit Brussel, KULeuven, Research Group CEDON, Stormstraat 2, 1000 Brussels, Belgium
genserik.reniers@ua.ac.be

A survey on security was conducted in Flanders' Seveso industry. Prevention advisors of so-called Seveso companies were asked to fill in a questionnaire on current industrial practices and mindsets regarding security in the process industry. The survey investigated whether security is perceived and treated as an essential topic within Seveso companies and formulates an answer to this research question.

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 the company, as well as controlling such incidents and their adverse effects*'. A security risk thus suggests intentionality. It is essential to also have a thorough understanding of the existing difference between *safety* and *security*. The definition of a safety risk (e.g. CCPS, 2000) bears the suggestion of being accidental. Safety and security are thus different in the nature of incidents.
Both concepts may also differ in their proactive approach (Holtrop and Kretz, 2008). In case of safety assessments (often called 'risk analyses'), risks are detected and analyzed by using consequences and probabilities (or frequencies). In case of security assessments (also called 'threat assessments'), threats are detected and analyzed by using consequences, vulnerabilities and target attractiveness (Holtrop and Kretz, 2008). The different proactive approach sometimes leads to the need for different and complementary protection measures in case of safety and security. Despite the difference in proactive approach, safety and security also have a lot of important similarities. The way in which the consequences of a certain action, whether it is accidental or intentional, are treated the same for safety and security. However, it is important to take into account that criminals may deliberately search for the best manner to execute their plans and that their goal is to cause as much damage as possible.
Experts indicate that an integrated approach is required (Fontaine et al., 2007; Holtrop and Kretz, 2008), thereby employing early risk assessments and making proper arrangements in a pro-active stage. Only such an integrated approach inherently leads to a safe and secure situation, integrality and awareness. In this regard, it is interesting to verify to what extent a security culture is present within chemical corporations. We employ the definition of security culture for the chemical sector suggested by Reniers et al. (2011): *a security culture in a chemical plant is the extent to which workers within the organizational premises (e.g. plant employees, contractors) regard security as important and the beliefs about how (physical, electronic, organizational, etc.) security should be executed, bearing in mind that hazardous substances are being handled in large quantities in the plant. These values and beliefs will evolve into certain norms about how to handle chemical company security.*

Please cite this article as: Reniers G., 2012, Security within the chemical process industry: survey results from flanders, belgium, Chemical Engineering Transactions, 26, 465-470 DOI: 10.3303/CET1226078

Security practices, approaches and mindsets thus provide an idea of the security culture present in a chemical company. Building such a security culture within a chemical plant, besides the well-known safety culture, may be essential for preventing unwanted intentional events.
In the United States, ten years following the WTC 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. 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 Council Directive on the identification and designation of European Critical Infrastructures (EPCIP) and the assessment of the need to improve their protection (Council Directive, 2008) provides directives as how to enhance European prevention, preparedness and response to terrorist attacks involving critical 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. The legislation represents a vehicle for a bottom-up approach to regulate critical infrastructure protection offering great leeway (and also a lot of responsibility) to the private chemicals sector in Europe.
Besides the EPCIP 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. In Europe, this legislation is practically composed of two Commission Regulations (725/2004 and 884/2005) and a Council Directive (2005/65). 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.

2. Research methodology

In Flanders, a region situated in the north of Belgium, 273 companies subject to the European Seveso legislation, are situated. In Europe, the basic guidelines for preventing major accidents are set out in the Seveso Directive (Council Directive, 1996). The so-called Seveso II Directive stipulates that any establishment storing or handling an amount of dangerous substances exceeding a predefined threshold, has to specify its safety policy in a safety report. The legislator has made a distinction between two types of enterprises with hazardous activities, so-called Seveso threshold 1 companies (or lower tier plants) and Seveso threshold 2 companies (or upper tier plants). A Seveso threshold 1 or 2 company is a company where the total amount of dangerous substances is larger than the first or the second threshold as defined in the application of the Directive. Seveso upper tier companies endure by far the largest risk potential and as a result, the regulation is a lot stricter.
In our study, 155 Seveso companies were contacted via e-mail with the question to respond to our survey on current safety and security practices in chemical plants. In total, 55 questionnaires were received, representing a response rate of 35.5 %. The respondents were asked to be people knowledgeable of safety and security practices and -management within the company. Out of the 55 participating companies, 37 belong to the upper tier group and 18 to the lower tier group.
In the questionnaire four different themes were spread over 13 questions. The survey was structured according to the themes, being (i) general company information, (ii) safety and industrial accidents, (iii) process security practices and vision for the future, and (iv) relationship between safety and security. It should be noted that we carried out a rather explorative study, not so much a study in depth, and that

the questionnaire was not conceived to allow for the identification of various discriminating factors, besides the Seveso categories. The interpretation of the results should be done baring this in mind.

3. Survey results

The answers of the practitioners will be discussed in relation to some important security topics related to security practices and organizational security cultures.

3.1. Relationship between safety and security in the Flemish process industries

In 78 % of the participating companies, the security policy is a part of the safety policy of the company, indicating that safety and security are indeed largely overlapping and often managed by one department. 67 % of the respondents believe that further security studies are needed in the process industries and recognize the importance of process security. According to 51 % of the respondents, safety and security are equally important domains and they should not compete with each other for budget allocation. In contrast, 49 % of the respondents think that safety is more important than security, and that security should always be a part of the health and safety department. As a reason for this opinion, these respondents explain safety to be a daily matter, and safety improvements, safety measures, safety equipment, etc. to be highly visible on the work floor and to have a direct impact on the employees. Moreover, the likelihood for a security-related incident is considered very low and if safety is well-managed (well organized and inherent), due to the overlapping, security is also well-managed, at least partially.

3.2. Security-related incidents in the Flemish process industries

Approximately one out of three of the respondents have already experienced security-related incidents. Mostly, these incidents concerned theft, representing high frequency - low impact security incidents, mostly committed by contractors or by employees. The reasons mentioned by the respondents for intentionally causing losses to a company, concern frustration, dissatisfaction at work, social disruption, resignation, etc. The notice period of an employee is often seen as a period of high possible security risk.

Other motives relate to ideologies, extremism, and religion. The respondents indicate that the possible impact and likelihood of these motives are very hard to assess, since useful information available on such high impact – low frequency security incidents, is extremely rare and incomplete.

Furthermore, the majority of respondents (60 %) indicated that they believe that the attractiveness of the chemical process industries for intentionally designed incidents by e.g. terrorists, would-be terrorists, or drug dealers is higher than that of other industrial sectors, due to the processing, storage, etc. of certain hazardous goods.

3.3. Security policy in the Flemish process industries

The majority of the respondents indicate that a security policy within their companies was implemented in a pro-active way and is actually part of the mission statement of the company. The prevention advisor or security manager identifies a need for security measures in the company and communicates this to the higher management, where after such measures are planned and implemented if the required budget is available.

The need for security countermeasures is sometimes driven by legislation (e.g. by the ISPS-code in case of harbor facilities), sometimes by internal company guidance or external benchmarking, based on for example a change in the amounts of hazardous goods within the company. Another important cause for the development of a security policy within a chemical facility, are the 9/11 terrorist attacks. For example, the headquarters of some chemical plants situated in Flanders are located in the United States, and these local plants are often pushed towards more security-driven policies. Organizations with European headquarters also understand and acknowledge the importance of security in today's business environment, but the pressure for security-improvements on local management seems to be less as that of US-headquartered organizations. Finally, some companies elaborated security measures only after incident investigations or external audits. Table 1 gives an overview of the different reasons for introducing a security policy within organizations, and their relative importance as indicated by the survey's respondents.

Table 1: ntroducing a security policy: different reasons mentioned by respondents

Reason for introducing a security policy within the organisation	*Percentage*
1. Security is part of the company's mission statement and objectives and is introduced accordingly	55 %
2. Security results from legislation, inspection, and controls from authorities	20 %
3. A security policy was introduced in the company after 9/11	14.5 %
4. A security policy results from incident investigations or external audits	10.5 %

Table 1 indicates that security within chemical corporations has approximately equally been the result of pro-active (55 %) as well as reactive (45 %) handling.

3.4. Security management systems implemented in the Flemish process industries

In total, 53 % of the respondents point out that they have a security management system elaborated and implemented within the company. The reasons for having such a management system are various: sometimes the ISPS-code obliges the company, or global headquarters oblige the local plant to have such a system, some companies share a joint security policy with other companies on the same industrial site, etc.

Those companies not disposing of a security management system point out that implementing such a system would be financially very difficult to achieve. Respondents from these companies also question the usefulness of having a security management system. They see security as a domain subordinating to safety, and hence, security matters should be dealt with within a company's health and safety department. In such plants, the prevention advisor is often responsible for security. Table 2 illustrates the difference between Seveso upper tier companies and Seveso lower tier companies in having a security management system.

Table 2: Difference between Seveso companies in disposing of a security management system

Seveso lower tier company		Seveso upper tier company	
Yes	No	Yes	No
(security MS available)	(no security MS available)	(security MS available)	(no security MS available)
28 %	72 %	66 %	33 %

Table 2 shows that, of the companies participating to the survey, a distinction can be made between Seveso lower tier companies and Seveso upper tier companies. Upper tier plants more often manage security issues according to a specific management system, whereas lower tier plants more often handle security matters – seen as a cost and as a part of safety – via the company's prevention department and via a safety management system.

3.5. Security measures within the Flemish process industries

The respondents could make a choice out of 12 security measures to indicate which security measures are implemented in their companies. Each security measure can be categorized into one of four classes: prevention, detection, control, and mitigation. Table 3 shows an overview of the responses.

Table 3 shows that the security measures implemented are quite diverse. 20 % of the participating companies use buffer zones between the fences and the public domain as a preventive measure to deter intrusion of unwanted persons. In 82 % of the cases, fences surround the company premises. Vehicles entering the company are controlled in 58 % of the responding plants, and in 52 % of the cases, a guard is present at the entrance for pedestrians. Before entering the site, a (badge or ID) check is carried out in 64 % of the companies. In case of entrance to storage of hazardous goods, 36 % of the respondents indicate that access controls (such as codes, fingerprints, etc.) are implemented. In case of 72 % of the companies participating to the study, systems with cameras are used for intrusion detection, and 60 % of the companies have guards patrolling at night. Detection systems for cyber-crimes are less popular: only 18 % of the responding enterprises have software to detect software intrusion. Security measures for optimal control of site activities include lay-out of the site and good housekeeping, applied in 40 % and 56 % of the companies, respectively. In the event of a major incident, police and fire departments have to respond quickly and arrangements can be made

to ensure this. In 42 % of the companies, emergency plans take into account security issues and agreements are made between the company and law enforcement.

Table 3: Security measures implemented within the participating companies

Category	Security measure	Percentage of companies implementing the security measure
Prevention	- using buffer zones	20 %
	- fences surrounding the company premises	82 %
	- Entrance control while driving a car (barriers, looking into the car, etc.)	58 %
	- Guard at entrance	52 %
	- Identification control at entrance (ID, screening, badges)	64 %
	- Access control for storage locations of hazardous materials and for vulnerable locations	36 %
Detection	- System for intrusion detection and cameras on site	72 %
	- Guards on patrol at night	60 %
	- Cyber intrusion detection	18 %
Control	- Lay-out/design of site	40 %
	- Good housekeeping	56 %
Mitigation	- Emergency management (fast response of fire departments, police, etc.)	42 %

4. Discussion

A difference between Seveso lower tier companies and Seveso upper tier companies can be observed concerning dealing with security issues. Seveso lower tier plants believe to be less prone to terrorist attacks or to security incidents in general. Lower tier companies are usually much smaller (in size and in numbers of employees) than upper tier companies, and safety-related accident figures in these lower tier companies are often higher than in their upper tier counterparts. If costs are to be divided between safety and security, safety gets priority in these lower tier plants, since the likelihood of a security incident is (at least in the perception of the decision-makers) much lower. However, decision-makers should realize that since upper tier Seveso companies are subject to much more stringent legislation (such as e.g. regulations stipulated in the Seveso legislation, and, if applicable, ISPS and/or EPCIP), and since they are usually more concerned with security measures, lower tier plants can be more vulnerable than upper tier plants and may thus be more attractive to terrorists.

Moreover, the hypothetical benefits of security measures (that is, having no costs from a terrorist attack), are very hard to calculate due to lack of information about attack probabilities. Nonetheless, although characterized with extremely low probabilities, a terror-related incident may have major human as well as huge financial consequences. These hypothetical security benefits may thus be huge for companies, but they are very often taken for granted (especially by the lower tier companies).

A need for standardization of security practices can be derived from the results of this research. Security guidelines, checklists, codes of best practice, policy rules, etc. should be provided for advancing security management in the Flemish chemical industry, especially within Seveso lower tier chemical plants. Nevertheless, respondents indicate that some kind of equilibrium should always be strived for, and that cost-benefits analyses should be taken into account regarding security requirements in chemical facilities.

5. Conclusions and recommendations

Safety and security are two related concepts. Similarities as well as differences exist between the two domains. Process safety has a long tradition, based on major accidents, legislation (in Europe mainly the Seveso Directive and in the US the OSHA legislation) and pro-active management. A lot of

knowledge and know-how has been built up in the chemical industry as regards safety practices and to create adequate safety cultures within chemical corporations.
Process security is a rather new domain, which largely gained interest from regulators, practitioners and academics after the 9/11 attacks in New York. At present, security in the process industries seems largely to be legislation-driven, in the US by CFATS and ISPS, and in Europe by EPCIP and ISPS.
Prevention advisors are divided on the importance of security management in the process industries: half of them consider security as an independent management domain, and the others think of security as a sub-domain of safety. No uniformity or harmonization as regards the use of security measures and –practices could be noticed in the study. Moreover, the mindset of prevention advisors regarding the subject of security requirements and -needs within chemical plants, was quite divergent.
As a recommendation, codes of good practice for managing security within chemical industrial areas should be elaborated. Chemical organizations, especially Seveso lower tier companies, should be able to dispose of generally accepted and widely-used guidelines. Such codes would allow security managers to develop well-accepted and effective security management systems and sound security cultures within their companies.

Acknowledgements

The author would like to thank Laura Heuninck for her active support in the empirical survey and three anonymous referees for helpful comments and suggestions.

References

CCPS, Center for Chemical Process Safety, 2000, Evaluating Process Safety in the Chemical Industry: a user's guide to quantitative risk analysis, American Institute of Chemical Engineers, New York, United States.

Commission Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security, Official Journal of the European Union, L129, 6-9.

Commission Regulation (EC) No. 884/2005 of 10 June 2005 laying down procedures for conducting Commission inspections in the field of maritime security. Official Journal of the European Union, L148, 25-29.

Council Directive, 2005. 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security. Official Journal of the European Union , L310, 28-39.

Council Directive, 2008. 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345, 75-82.

Council Directive, 1996. 96/82/EC on the control of major-accident hazards involving dangerous substances, Official Journal of the European Union, L010/97, 1-38.

Fontaine F., Debray, B., Salvi O., 2007, Protection of hazardous installations and critical infrastructures – complementarity of safety and security approaches. In Linkov I. et al. Managing Critical infrastructure Risks, 65-78, Springer, London, UK.

Holtrop D., Kretz D., 2008, Research security & safety: an inventory of policy, legislation and regulations (in Dutch). Research Report 141223/EA8/043/000603/sfo. The Netherlands: Arcadis.

IMO (International Maritime Organization), 2004, The Ship and Port Facility Security Regulations, HMSO, London, UK.

Reniers G., 2011, Terrorism security in the chemical industry: results of a qualitative investigation, Security journal, 24(1), 69-84.

Reniers G., Cremer K., Buytaert J., 2011, Continuously and simultaneously optimizing an organisation's safety and security culture and climate : the improvement diamond for excellence achievement and leadership in safety and security (IDEAL S&S), Journal of Cleaner Production, 19(11), 1239-1249.