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/CET1226069

Harmonization of Safety and Security Aspects in Critical Installations of "Seveso"-Type

Roberta V. Gagliardi[a]

[a]INAIL ex-ISPESL, Via Urbana 167, 00184 Rome
r.gagliardi@inail.it

After terrorist acts committed in the United States and then in Europe, Seveso sites have been identified among critical infrastructures, which can led, in case of deliberate attacks, not only to human and material damage but also to fear and loss of confidence within the public with regard to chemical industry. For the identification and designation of European critical infrastructures, as well as for the assessment of the need to improve their protection, the Directive 2008/114/EC has been issued. At national level, this Directive has been recently implemented by the Legislative Decree 61/2011. Some provisions contained in this Decree establishes a direct link between safety and security issues for Seveso sites, and implies, as a consequence, the need to harmonize converging aspects or conciliate potential conflicting elements. Objective of this paper is, therefore, to propose a reflection on which aspects could be successfully integrated between safety and security for Seveso sites, as well as which opportunities exist to fill existing gap by research improvements.

1. Introduction

Terrorist acts committed in the United States (2001) and then in Europe (Madrid, 2004; London, 2005, 2007), determined the need to cope with the security issues related to critical infrastructures (CI): these are defined as an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have significant impact as a result of the failure to maintain those function. To deal with this emerging risk, the European Commission proposed a European Program for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN) in 2004 (EUROPA, 2011). Subsequently, the specific objectives of security and protection of critical infrastructures have been transposed in a new Directive on the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection (EC, 2008). An European critical infrastructure is defined as a critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on a least two Member States. In this context, Seveso sites have been identified among potential critical infrastructures as hazardous substances are stored, produced and handled, which can led to not only human and material damage but also to fear and loss of confidence within the public with regard to chemical industry. Seveso establishments are, therefore, of particular concern in the European security strategy as potential targets of external terrorist acts, due to the hazardous nature and quantity of chemicals being handled in these facilities, extreme process conditions of temperature and pressure, and importance of the products to the economy. Terrorist having sufficient information about the location of hazardous chemicals, inventory, chemical operations and other sensitive data, may exploit this knowledge, leading to toxic release, fire and explosion. This would result in serious impact on

Please cite this article as: Gagliardi R.V., 2012, Harmonization of safety and security aspects in critical installations of "seveso"-type, Chemical Engineering Transactions, 26, 411-416 DOI: 10.3303/CET1226069

economy, environmental contamination and casualties both on-side and off-site. Even worse consequences, moreover, could occur in complex areas, as industrial parks or port areas, in which the coexistence of a multiplicity of risk source and vulnerable targets could aggravate the effects of terrorist attacks. In Italy, Directive 2008/114/EC (EC, 2008) has been recently implemented by a Legislative Decree establishing the procedures for the identification and designation of European Critical Infrastructure in the energy and transport sectors, the procedures for the security assessment of such infrastructures, as well as the relevant minimum prescriptions for their protection from human and technological threats, and from natural disasters (Legislative Decree, 2011). One of the tasks assigned by new law to the operator of a critical infrastructure is the redaction of the Operator Security Plan (OSP), in cooperation with the security competent authorities. Among minimum requirements established by the new law, OPS must apply the art. 11, 12 and 20 of the Legislative Decree (Legislative Decree, 1999) implementing the Directive 96/82/EC "Seveso II" (EC, 1996) concerning the internal and external emergency plan, and the domino effect in Seveso establishments. This provision gives rise to a direct link between safety and security issues for Seveso sites, and implies, as a consequence, the need to harmonize converging aspects. Objective of this paper is, therefore, to begin consideration on potential elements of integration between two sectors, possible conflicting elements, and existing gaps which should be overcame by research activities.

2. Legislative framework

Directive 2008/114/EC (EC, 2008) establishes a procedure for the identification and designation of an ECI and a common approach to the assessment of the need to improve its protection in order to contribute to the people safeguard. Since has been recognized that various sectors have a particular experience, expertise and requirements concerning critical infrastructure protection, the Directive is based on a sectoral basis and is put into effect according to a list of main sectors. Two of them have the right of priority for the purpose of implementing the Directive, respectively the energy and transport sectors; subsectors of each one are identified in the Annex I. In order to assess the significance of the impact of the disruption or destruction of a particular infrastructure, cross-cutting criteria, i.e. criteria which satisfy a common and homogeneous criterion of criticalities among sectors, are introduced. They comprises casualties criterion (assessed in terms of the potential number of fatalities or injuries), economic effects criterion (assessed in terms of the significance of economic loss and/ or degradation of products or services; including potential environmental effects), public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services). It is worth mention that, the Directive, a review of which shall begin on January 2012, recognizes the need to extend in the future the list of sectors, assigning the priority to the Information and Communications Technologies sector. The Directive provides a step-by-step-approach to identify potential ECIs which both satisfy the cross cutting and sectoral criteria and meet the definitions of ECI. Once a potential ECI has passed through this procedure, it is duty of each Member State the final decision concerning the official designation of such infrastructure as ECI. Besides the identification and designation of ECI, the implementation of the directive also implies other procedures for Member States: the appointment of a protection contact point for the coordination of ECI protection issues within the Member State, with other Member States and with the Commission, and the risk, threat and vulnerability assessment, with specific reference to subsectors where belongs the designated ECI. Duty of the operator is the redaction of the operator security plant (OSP), identifying the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The operator has also the responsibility to designate a Security Liaison Officer working as a contact point for security related issues between the owner/operator of the ECI and the relevant Member State authority. It is worth noting that the Directive recognizes that methodological guidelines for carrying out risk analysis in respect of an ECI may be developed by the Commission in cooperation with Member States. Directive 2008/114/EC (EC, 2008) has been recently transposed in the national legislation by Lgs. Decree 61/2011 (Legislative Decree, 2011); it maintains the same structure, mainly based on the sectoral criteria for the identification of an ECI trough a step-by-step approach, and several procedures to be applied by the competent authorities. However, some points need to be pointed out in order to highlight specificities of the Italian context with respect to the

European Directive. While the Directive takes into consideration the potential impact of a hazard independently of its nature, the Italian Decree details the nature of the threats for an ECI as human (accidental or deliberate), technological, or due to natural disasters. As far as the competent authorities involved at national level in concerned, the head of Government designates an inter ministerial team on state and planning (NISP) which is responsible for the individuation and designation of an ECI, in cooperation with the representatives of the ministry involved (Economic Development, Infrastructure and Transportation, Interior, Foreign Affairs, and Civil Protection Department); the NISP also acts as contact point with the other Member States and the European Commission. The head of Government also individuates the "responsible structure" which must support NIPS, with technical and scientific activities, for the individuation of an ECI, for cooperation with the European commission and with similar structures existing in other Member States. This structure is also in charge for the definition of the sectoral criteria thresholds trough which establishes the criticality of a structure. Responsible for the protection of an ECI are, at national level, the Ministries involved together with the Civil Protection Department, and, at local level, the prefect with territorial jurisdiction. A classification of secrecy is also attributed to the sensitive information related to CI according to in force legislation. From an operating point of view, the infrastructure's operator, with the support of representatives of the Ministries involved and the "responsible structure", draws up the Operator Security Plan, on the basis of the minimum requirements stated by Annex B of the Decree. The OSP identifies critical infrastructure assets and which security solutions exist or are being implemented for their protection; at procedural level it covers at least: the identification of important asset; the risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; the identification, selection and prioritisation of counter-measures and procedures with a distinction between permanent security measures and graduated security measures. According to the last provisions of Annex B, OSP must apply, inasmuch compatible, the art. 11, 12 and 20 of the Legislative Decree 334/99 concerning the internal and external emergency plan, and the domino effect in Seveso establishments. This is an important sentence, going beyond Directive 2008/114/EC (EC, 2008); it establishes, for seveso sites, a direct link between the safety and security issue and gives rise to the need of investigating if and to what extent their harmonization is possible.

3. Safety and Security issues for Seveso plants

Seveso sites have achieved, in the last decades, a high standard in safety. Various technical and managerial tools have been developed and implemented according to the traditional approach in which Seveso plants are considered as a risk source. From a security point of view, instead, seveso sites act as a potential target of deliberate interference actions. In Figure 1 are shown the main features of the approaches applied respectively on Seveso sites and critical infrastructures, while Table 1 illustrates a comparison between the Safety Report and OSP contents. Both approaches start with a screening criterion, based, respectively, on the quantity of hazardous substances which are stored, produced and handled in a plant, and the cross cut and sectoral criteria. Once obtained the status of Seveso site or CI, a risk analysis is required. This is the heart of any safety or security program. The Safety Report evaluates hazard scenarios from an initiating event, their likelihood, circumstances and consequences, and the safety measures required to limit the consequences of an accident. In the OSP the essential steps involved in a security risk analysis are threat analysis, vulnerability analysis, security countermeasures and emergency response (Bajpai and Gupta, 2005): threat analysis involves the study of identifying sources, type of threats and their likelihood, vulnerability analysis identifies the weakness in a system that adversaries can exploit. Depending on the threat likelihood and vulnerabilities, various security countermeasures are suggested to improve the plant protection. It must pointed out that, independently by the nature of the risk source, which can be accidental or intentional, the consequent events could be summarized in few alternatives; therefore safety and security risk analysis could be let to converge on a number of selected scenario for which develop a harmonized approach. As an example, the worst-case scenario, well known in safety analysis, need to be considered also in security vulnerability assessment. All conventional safety measures that have been applied for years in Seveso sites are certainly useful for security purposes. Moreover permanent or graduated security measures must be implemented in the OSP.

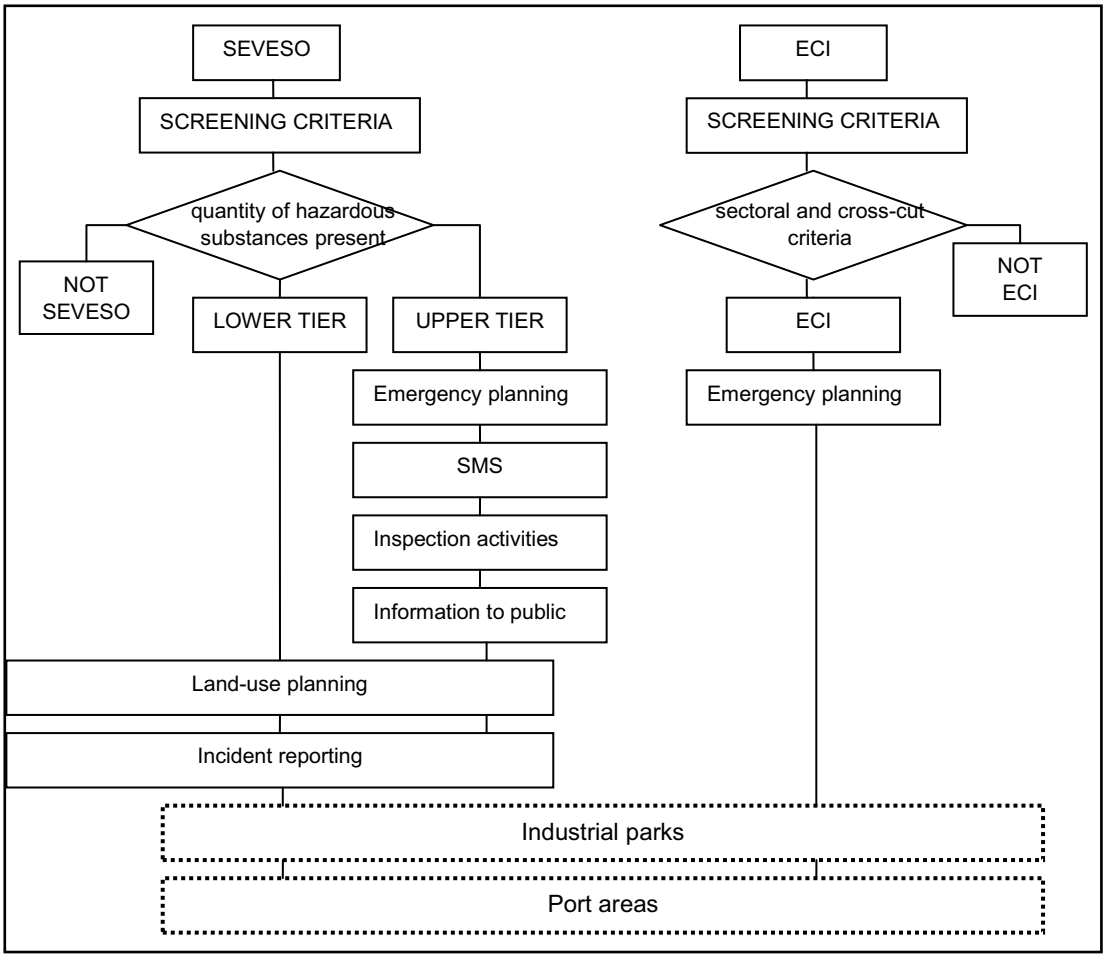

Figure 1: Main features of Seveso and CI approaches

Table 1: Comparison between Safety Report and OSP contents

Data	Safety Report	OSP
Organization	Information on the SMS and the organization of the establishment with a view to major accident prevention	
Infrastructure's environment	presentation of the environment of the establishment	
Infrastructure's description	description of the installation	Identification of important assets
Risk analysis	identification and accidental risk analysis and prevention methods	risk analysis based on major threat scenarios, vulnerability of each asset and potential impact
Counter measures	measures of protection and intervention to limit the consequences of an accident	identification, selection and prioritization of permanent and graduated security measures

The former identifies indispensable security investments and means which are relevant to be employed at all times; this heading will include information concerning general measures such as technical and

organisational measures: control and verification measures; communication; awareness raising and training; and security of information systems. The latter can be activated to varying risk and threat levels. According to the experiences obtained so far, the safety management system has revealed as the one of the most effective tool of the Seveso philosophy. Proposals to broaden it in order to include security aspects have already been advanced at research level (Bubbico and Luccone, 2007). As before mentioned, OSP must apply the art. 11, 12 and 20 of the Legislative Decree 334/99 (Legislative Decree, 1999) concerning the internal and external emergency plan, and the domino effect in Seveso establishments. Emergency plans are designed to meet the abnormal events like technological malfunctioning, human error and expected natural disasters and afford the consequences of these events with the primary objectives of safety of people and environment, protection of property and restoration of normal operation with a minimum delay. More difficult results anticipate the events which follow a terroristic attack and planning the consequent emergency; therefore, a deeper reflection is required to evaluate if the existing emergency responses are exhaustive or need to be modified in view of process security. Harmonization of these two sectors could benefit from the fact that both sectors, at local level, refer to the same competent authority: this is the prefect with territorial jurisdiction which is responsible for the external emergency plan of seveso sites as well as for the protection of a CI. In the Seveso legislation special attention is dedicated to the interaction between different plant sections or different neighbouring establishments (i.e. domino effect); this is due to the fact that some of worse major accident happened in the past were caused by the domino effect, as shown by the analysis of accident databases. From a security point of view, an external attack on a seveso sites should be considered as a potential trigger for severe accidental scenarios as well as for domino effect: this means that in spite of the difference among the external hazard factors, the escalation effects and the consequences assessment may be very similar and therefore can be analyzed trough the same approach. Therefore security sector could benefit from the research efforts which are carried out to develop and standardize methodologies or technical tools to analyze the domino effect (Cozzani et. al., 2007), (Reniers et al., 2008). An important measure in preventing or impeding terrorist attacks can be keeping sensitive data about a potentially hazardous plant confidential; this procedure is explicitly foreseen in the new decree, as mentioned in the previous paragraph. For Seveso sites, this implies a conflict of objectives with the right of the public, and especially of neighbours, to get information about potentially hazardous plants, a right which has been increasingly in recent decades. The Directive “Seveso II” has, in fact, established strict standard in this area. Conflicts have to be solved between a possible need not to disclose information for security reasons and the public’s right to know: efforts must be made in order to achieve a balance between information to the public and protection of sensitive information. Duties related to inspection activities, land-use planning or incident reporting, still remain prerogatives of the Seveso sites; however, since experience acquired in the last decades of application of Seveso tools demonstrated their effectiveness in preventing and limiting accidental consequences, further efforts should be made to take advantage of these tools in a security context. Finally, a reference is due to lower tier establishments. Analysis case–by-case is required if vulnerable objects are in their vicinity: for instance, a major tank of liquefied natural gas in a crowded area can cause a severe risk even if its inventory is below the upper threshold established by the “Seveso II” Directive.

4. Seveso chemical clusters

As above illustrated, there is room for improvements in the field of harmonization between safety and security for seveso sites (Reniers and Amyotte, 2012). All issues mentioned in the previous paragraph result amplified in complex areas such as industrial parks or port areas, in which the coexistence of a multiplicity of risk source and vulnerable targets could aggravate the effects of terrorist attacks (Reniers et al., 2008). It is well known that cross-company accidents or accidents involving several chemical plants at once may cause significant losses of human lives, devastating damage to these plants and huge financial losses. Any plants composing a chemical cluster should be interested in joining forces to optimize safety and security management at any level: operational, by exchanging data and information or implementing preventive measures, tactical, by implementing risk assessment, and strategic, by planning investment for preventive and mitigation measures. However, generally

speaking, cooperation among companies is a not easy task to achieve, due to trust and confidentiality concerns. Italian Seveso legislation however, provides for a specific technical instrument to cope with complex areas which, i.e. the integrated safety study, specifically designed for the industrial parks; it foresees the environment characterization, risk analysis and emergency plan. Efforts are required in order to opportunely include security aspects in this study. Specific concern is related to industrial port areas. Not only the Italian implementation of the “Seveso II” Directive provides for a specific decree dealing with the safety issues and establishing the need of an Integrated Safety Report for port areas (Ministerial Decree 293/2001), but they are also specifically mentioned in the security legislation among transport subsectors, and therefore object of a security vulnerability analysis. A special mention is due to the transport systems of hazardous chemicals (by road, rail cars, ships, pipelines, etc..) which are explicitly cited in the security legislation; they represent a serious concern from terroristic perspective due to the fact that the hazard may be greater than chemical plants because of territorial vulnerability. Protecting such assets, in fact, is really difficult due to the difficulty in limiting the degree of access: energy or chemical pipelines, rail or road lines, are less secure and much easier to attack without notice. However, since transport sector of dangerous goods is not included in the field of application of the seveso directive, the need to implement safety requirements can represents a good opportunity to reflect in a coordinate way on safety and security of this important sector.

5. Conclusions

Security legislation, recently issued, introduces a link between safety and security issues and practices in the seveso sites management. In the paper, main features of safety and security approaches for Seveso sites have been analyzed in order to yield an overview of aspects which can be harmonized. The leading purpose of this analysis is to contribute, as far as it is possible, to avoid duplication of efforts, to simplify administrative procedures, to prevent overlap of role and responsibilities, and, over all, to strengthen the protection of citizens, environment and the process industry. To this end, the expertise achieved in several decades of application of the Seveso legislation has proved crucial and further benefits could be produced for the development of guidelines dealing with the security of Seveso-sites critical infrastructure.

References

Bajpai S., Gupta J.P., 2005, Site Security for chemical process industries, Journal of Loss Prevention in the Process Industries 18, 301-309.

Bubbico R., Luccone L.G., 2007, Proposal for an integrated safety and security management system for Seveso plants, 12-th Loss Prevention and Safety Promotion in the Process Industries, 22-24 May 2007 IChemE SIMPOSIUM SERIES N° 153, Edinburgh, UK,.

Cozzani V., Salzano E., Campedel M., Sabatini M., Spadoni G., 2007, The Assessment of major accident hazards caused by external events, 12-th Loss Prevention and Safety Promotion in the Process Industries, 22-24 May 2007, IChemE SIMPOSIUM SERIES N° 153, Edinburgh, UK.

EC, 2008. Council Directive 2008/114/EC, Official Journal of the European Union, L 345, 75-82.

EC, 1996. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. of the European Union, L 010 , 13–33.

EUROPA, 2011. <europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm>, Accessed 10.12.2011.

Legislative Decree, 2011. Legislative Decree n.61 from 11 April 2011. Italian Official Journal, 4 May 2011, n. 102.

Legislative Decree, 1999. Legislative Decree n. 334 from17 august 1999. Italian Official Journal, 29.09.1999, n. 228.

Ministerial Decree n. 293 from 16 may 2001. Italian Official Journal, 18 July 2001, n. 165.

Reniers G., Dullaert W., Audenaert A., Ale B.J.M., Soudan K., 2008, Managing domino effect-related of industrial areas, Journal of Loss Prevention in the Process Industries, 21, 336-343.

Reniers G., Amyotte P., 2012, Prevention in the chemical and process industries: Future directions, Journal of Loss Prevention in the Process Industries, 25, 227-231.