CHEMICAL ENGINEERING TRANSACTIONS
VOL. 77, 2019
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216
DOI: 10.3303/CET1977148

Physical Security Barriers and Protection Distances for Seveso Sites

Alessandro Tugnoli[a], Matteo Iaiani[a], Gabriele Oliva[b], Ernesto Salzano[a], Roberto Setola[b], Valerio Cozzani[a,*]

[a]Department of Civil, Chemical, Environmental and Materials Engineering – University of Bologna, Via Terracini 28, 40131 Bologna (Italy)
[b]Complex System & Security Lab – University UCBM, Via A. del Portillo, 21, 00128 Roma (Italy)
valerio.cozzani@unibo.it

Seveso III Directive (2012/18/EU) requires operators to demonstrate that they have identified major accident hazards and scenarios, and that they have implemented adequate actions to prevent such accidents. Safety reports issued under the Seveso Directive specifically address accident scenarios caused by technical or human failures. Scenarios caused by intentional acts are usually not considered, even if they have a wide potential to harm the workers and the exposed population in the vicinity of Seveso sites. The present contribution focuses on the characterization of physical security-related scenarios in the framework of safety and security management of Seveso sites, identified taking advantages of the potential synergies between safety and security studies. The role of physical security barriers is explored. Finally, the use of protection distances from critical and vulnerable units is presented to support the selection of the barriers.

1. Introduction

Seveso sites inherently contain significant quantities of hazardous chemicals that may be a possible targets for malicious acts of interference. The Seveso III Directive (2012/18/EU) focuses on major accidents caused by unintentional causes (equipment failures, human errors, natural disasters, etc.), and safety reports do not require to include scenarios caused by intentional acts. The Seveso Directive requires operators to demonstrate that they have identified major accident hazards and scenarios, and that they have implemented adequate actions to prevent such accidents. The resulting safety reports specifically address accident scenarios caused by technical or human failures, but lack of insight on the possibility that those scenarios or similar ones can be caused by deliberate actions (Bajpai and Gupta, 2007). Nevertheless, the credibility and potential severity of such malicious scenarios was pointed out by several studies (Argenti et al., 2015). The concern raised dramatically in Europe in 2015, following the attacks perpetrated in France against a production site of a chemical company and an oil refinery (ARIA, 2015).
A fruitful synergy can rise from integration of safety and security analysis: while some competences and techniques are clearly specific to each field, some common elements would benefit from an integrated approach. A fundamental experience in this direction was developed in US, where following the tragic events of the attack of “9/11”, the security risks were included in formal risk assessment of sites where relevant quantities of hazardous chemicals are stored or processed (Argenti et al., 2017). A number of methods were therefore developed for this purpose (e.g. see American Petroleum Institute (American Petroleum Institute, 2013), American Institute of Chemical Engineering (Center for Chemical Process Safety, 2003) and Sandia National Laboratories (Jaeger, 2003)). Despite these developments, an organic and worldwide accepted procedure for integrated security assessment applicable to Seveso sites is still missing. The current paper frames an approach to the issue, and illustrates some methodologies applicable to meet this goal.

2. Characterization of security attacks of concern for Seveso sites

Seveso sites are potentially attractive from the security standpoint due to three many reasons:

Paper Received: 26 November 2018; Revised: 6 May 2019; Accepted: 26 June 2019

Please cite this article as: Tugnoli A., Iaiani M., Oliva G., Salzano E., Setola R., Cozzani V., 2019, Physical security barriers and protection distances for Seveso sites, Chemical Engineering Transactions, 77, 883-888 DOI:10.3303/CET1977148

- availability of large quantities of hazardous materials: this enables triggering high severity scenarios, with major adverse effects on local people and assets and, more broadly, large impacts on economy and public opinion; potential also exists for initiating domino chains and propagate the consequences beyond the pieces of equipment initially targeted (Pavlova & Reniers, 2011);
- access to chemical for manufacture of improvised explosive devices (IEDs): some chemicals normally unavailable on the market, can be a potential source for making IEDs and perpetrating further terrorist actions (Landucci et al., 2015);
- increased vulnerability to cyber intrusions: the increasing use of automated and integrated controls and safety instrumented systems may allow remote cyber attacks to the multiple facilities in the production system (Casson Moreno et al., 2018).

Clearly enough, the first of the reasons above is the most important in the synergy between security and safety studies: the accident scenarios caused by the hazardous materials are in most cases of similar nature, no matter the initiating cause. Therefore, they can be studied with similar tools in an integrated way. On the other hand, security-related accidents may have specific accident scenarios which are not considered in a conventional safety study. A recent accident review by Casson Moreno et al. (2018), who collected a database of about 300 security-related accidents in industrial facilities where relevant quantities of hazardous materials were stored or processed, evidenced that loss of containment and explosion were the more frequent outcomes of the attack (Figure 1). A more detailed analysis of the 26 events that affected the chemical and petrochemical industry revealed that the occurrence of the event required the attackers to penetrate the layered structure typical of security barriers (see section 4). The use of explosives (both military and improvised explosive devices) was by far the more frequent attack mode, although armed attacks and arson are also possible.

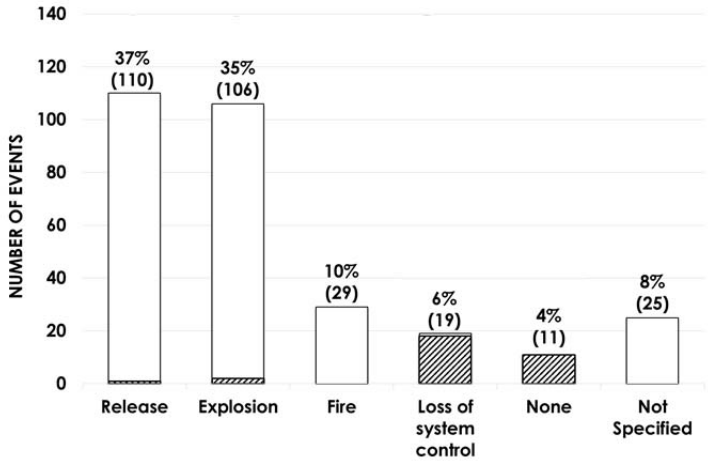

Figure 1: Final events form the analysis of the database by Casson Moreno et al. (2018). The contribution of cyber-attacks is shown in striped colours.

In recent years, cyber attacks to Seveso sites emerged as another possible initiator of malicious accident chains. Cyber security threats are becoming a growing concern for all those industrial sectors in which automation is high, which include the chemical and petrochemical industry. The study by Casson Moreno et al. (2018) concluded that, currently, cyber threats hold the fourth position among those related to security, following terrorism, vandalism and physical theft. According to some estimates, the percentage of cyber attacks is bound to increase in the coming decades.

An example of the potential for this type of attack in causing scenarios similar to the ones considered in safety reports is the accident occurred in 2008 at the BTC Pipeline in Turkey. Hackers shut down alarms, cut off communications and over-pressurized a crude oil pipeline. This resulted in the failure of the pipeline, that caused the spill of more than 30,000 barrels of oil in an area above a water aquifer and cost BP and its partners $5 million a day while the line was shut down. The explosion was followed by a fire which lasted for two days until the damaged section was emptied of its contents. No casualties were reported. The BTC Pipeline remained closed for two weeks. The worst damage was felt by the State Oil Fund of the Republic of Azerbaijan, which lost $1 billion in export revenue (RISI, 2018).

3. Interaction of security-related scenarios and conventional scenarios

In case of an attack aimed to cause an accident scenario either via the use of explosives/firearms or by altering the process variables (cyber-attack or attack after physical access to the control room) an “intentional” primary scenarios is triggered (e.g. an explosion). This scenario, which has per-se adverse consequences, is even more worrying for its potential to initiate to a domino scenario or “cascading event” (Darbra et al., 2010). This potential constitutes an essential link between unintentional Seveso scenarios and the ones form malicious actions.Table 1 shows some attack patterns identified by Argenti et al. (2018), which can be deemed as representative of the typical situations in a Seveso site. It can be observed as in most cases the vector associated to the attack is qualitatively similar to the ones typically involved in domino escalations (Cozzani et al., 2009), and therefore potentially able to cause the loss of containment of hazardous materials form process and storage equipment. Moreover, in many cases the primary scenario also provides an ignition source (flames, hot spots, damage to electric equipment, etc.).
It is important to notice that while some attack patterns require access to the domain of industrial site (i.e. the entering the fence), it is also possible to conceive attacks that are initiated outside the plant boundaries (Reniers and Audenaert, 2013). Moreover, intentional attacks to non-industrial targets (e.g. strategic buildings, urban areas, infrastructures) in proximity of Seveso sites may in turn trigger domino effects in the industrial facility.

Table 1: Examples of attack modes (adapted form Argenti et al. (2018)) n.a. = not applicable

State	Description	Associated attack vector
Deliberate misoperation	Deliberate acts involving simple operations without the use of instruments	n.a.
Interference using simple aids	Deliberate interference using tools and aids that are present on site	n.a.
Interference using major aids	Prepared destruction of installation parts by force using heavy tools	n.a.
Arson using incendiary devices	Incendiary attacks	Heat load
Use of explosives	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	Overpressure
Use of vehicle bomb	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	Overpressure
Shooting 1	Interference at close distance, using different types of weapons	Projectile impact
Shooting 2	Interference at distance, using different types of heavy weapons	Projectile impact
Vehicle accident	Vehicle accident in the establishment aimed to release hazardous substances or damage/destroy important parts of the installation	Vehicle impact
Aircraft accident	Aircraft accident aimed to release hazardous substances or damage/destroy important parts of the installation	Aircraft impact

The assessment of the potential for security-triggered domino accidents and of the expected consequences can be carried out with tools similar to the conventional consequence evaluation in quantitative risk assessment studies (Lees, 1996). This type of study allows to identify the possible interactions between security and safety related events and to profit on the systematic information available from the safety study. An example, reported by Landucci et al. (2015) is provided in Figure 2. This considers a plant where flammable chemicals are stored in a tank farm. The site was first analyzed in the Seveso safety report form the point of view of safety accidents. If an improvised explosive device is triggered in different positions around the fence of the plant, the resulting blast is able to damage multiple equipment in the plant. The analysis of the damage criteria from blasts and the simulation of the consequences of loss of containment from the tanks was already available from the safety study and can be used to characterize the consequences of the malicious attack. In this case it is evidenced as different outcomes are expected and, therefore, as different security measures can be effectively implemented at the different areas of the facility.
Vulnerability is often considered in security studies as a measure of the extent of adverse effects caused by the occurrence of a specific hazardous event. This interpretation of vulnerability is thus closely related to the

definition of risk as typically intended for Seveso Plants. However, the difference is that in the case of vulnerability the identification and characterization of scenarios are conditioned upon the occurrence of a specific hazardous event or strain.
A quantitative estimation of the likelihood of success of external attack scenarios is derived conducting a performance-based assessment of vulnerability, as recommended for facilities with high-consequence loss physical assets (Garcia, 2006). According to Vellani (2006), the vulnerability assessment is commonly based either on an asset-based or on a scenario based approach. In the case of asset-based vulnerability assessment, a broad evaluation of assets and threats that impact on those assets is carried out without considering and analyzing the attack scenario(s). On the contrary, the scenario-based approach focuses on the attack in order to foresee by which means, methods, and tools targets may be affected, thus also identifying possible countermeasures.

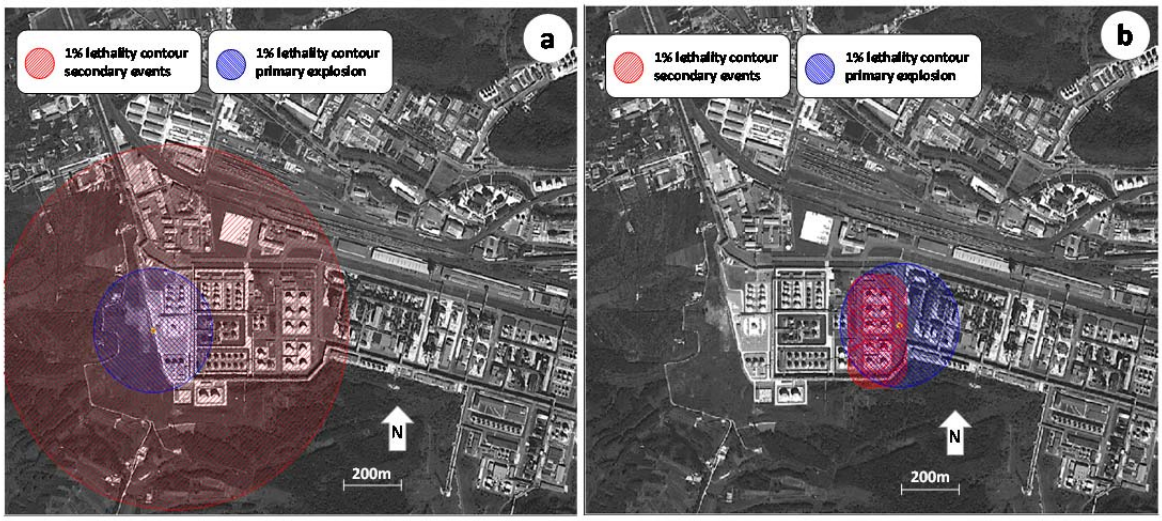

Figure 2: Calculated area of effects (1% lethality) for an industrial site exposed to an attack by 50'000 kg of home-made explosive (50% Ammonium Nitrate / 50% Dolomite mixture with fuel) from two different locations near the fence of the facility (adapted from Landucci et al. (2015)).

4. Security barriers and protection distances

The study by Nunes-Vaz on Physical Security (Nunes-Vaz et al., 2011) identified the concept of security barriers and its role in the model of layered security (security-in-depth). Nunes-Vaz describes four independent security layers to manage the risk of a terrorist attack against a given facility: deter, prevent, protect and contain. Deter and prevent focus on likelihood reduction and on stopping the event sequence. If deterrence fails, then prevention is intended to stop the progress of the attack. Protect and contain concern the consequence management. Protection manages, and potentially eliminates, the consequences of the attack by putting controls in place prior to the occurrence of damage; the contain layer is a combination of incident response and consequence management capabilities and actions. Layers require the coordination of one or more security functions, which allow for the accomplishment of the protection objectives. The layers and functions are implemented by security barriers: a security barrier is a physical, procedural, technical, or other device that performs or contributes to one or more security functions. (Garcia, 2008).
Argenti et al. (2017) explored the application of quantitative assessment of the effectiveness of Physical Security Systems (PPSs) currently adopted to protect process and storage facilities, with particular reference to the prevention layer, identifying security functions of PPSs from an elicitation of experts in the chemical and process industry. The main barrier considered in their study are summarized in Table 2.
For the scenarios described in section 3, the concept of protection distance can be used in the assessment of the effectiveness of the barriers. The protection distance (or stand-off distance) is the minimum distance between the asset of interest and the location where a terrorist can carry out his attack without causing damages (Salzano et al., 2014). For example, a terrorist placing a given home-made explosive device at distances greater or equal than the protection distance, will not be able to damage the target equipment. This clearly depend on the characteristics of the attack vector (explosive type and quantity, bullet/missile type and kinetic energy, etc.) and on the characteristics of the target. Landucci et al. (2015) developed reference diagrams to estimate protection distances for some common home-made explosives with reference to the

typical equipment more commonly present in the process industry (Figure 3). The diagram is based on the Hopkinson-Cranz methodology to calculate the mass-scaled distance from a point-source explosive (Baker et al., 1991) and on typical energy of explosion and efficiency data for improvised explosives.

Table 2: Examples of security barriers typically implemented in chemical and process industry

Function	Security barriers
Detection	External IDS based on VMD
	Intrusion detection by roving guards
	Intrusion detection by employees
	Entry control, supervised automatic credentials check (people)
	Entry control, unsupervised automatic credentials check (people)
	Entry control, manual credentials check (people)
	Entry control, unsupervised automatic biometrics check (people)
	Entry control, supervised automatic credentials check (vehicles)
	Entry control, manual credentials check (vehicles)
Alarm Assessment	Alarm assessment through CCTV system
	Alarm assessment by roving guards
	Alarm assessment by employees
Alarm communication	Communication to/among response force

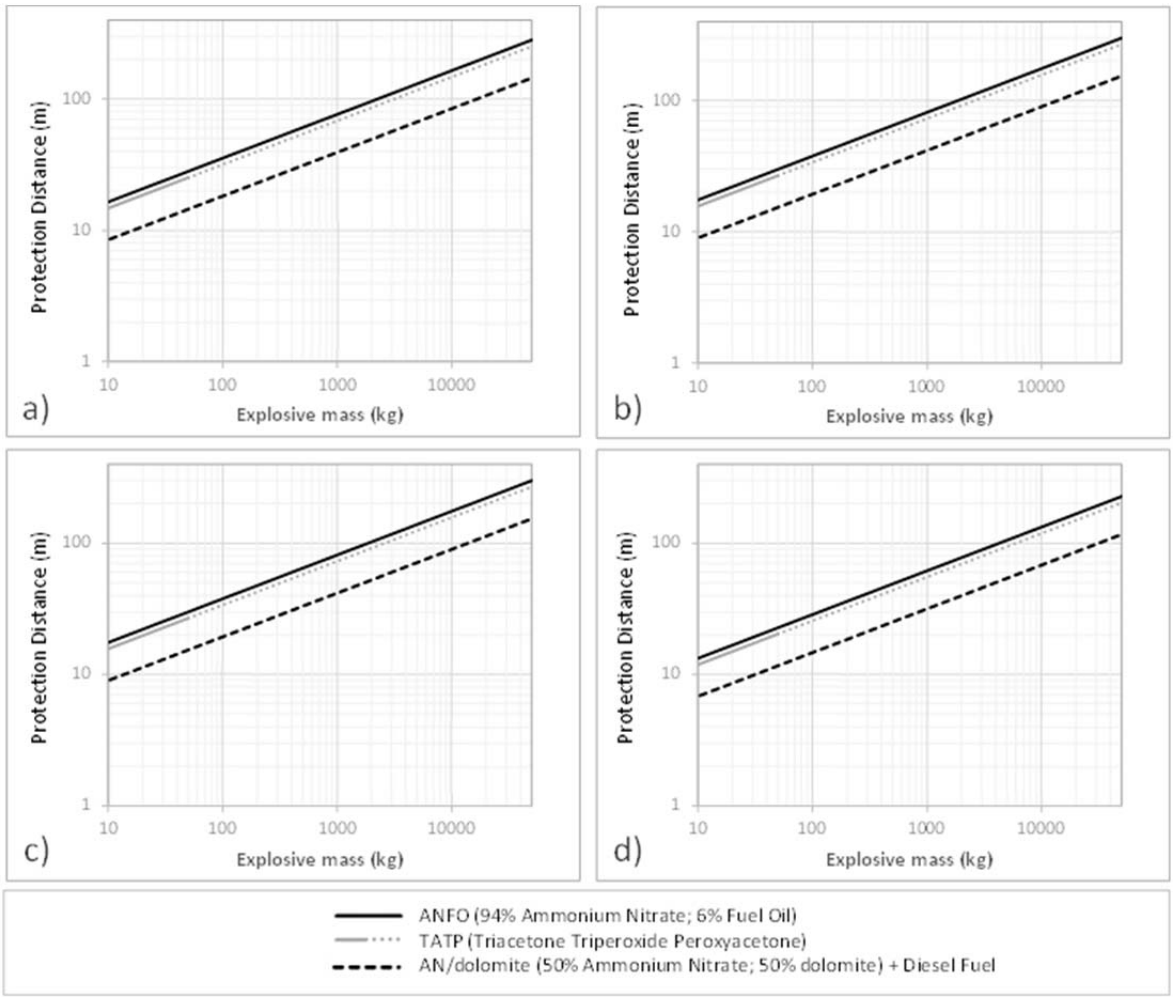

Figure 3: Estimated protection distance form selected home-made explosive devices required for different equipment categories for target process equipment: a) Atmospheric vessels; b) Pressurized vessels; c) Pressurized horizontal vessels (toxic content); d) Pressurized horizontal vessels (flammable content).

5. Conclusions

The current contribution reviewed the main points of contact between security and safety studies for a Seveso plant. The possibility of domino scenarios triggered by malicious actions was identified as the core link between the two disciplines. The definition of security cases and the assessment of protection barriers can benefit from the tools and information developed for the safety assessment. In particular, consequence modeling of the loss of containment scenarios and the concept of layer of protections were pointed out as key elements in this integration. The analysis of some previous studies evidenced the potentially achievable results. In this context, the use of protection distances as physical security barriers emerged as a promising application.

References

American Petroleum Institute (API), 2013, ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry, American Petroleum Institute, New York, USA.

ARIA - Analyse, Recherche et Information sur les Accidents, 2015, French ministry of ecology and sustainable development <www.aria.developpement-durable.gouv.fr/> accessed 03.09.2018.

Argenti F., Landucci G., Cozzani V., Reniers G., 2017, A study on the performance assessment of anti-terrorism physical protection systems in chemical plants, Safety Science, 94, 181-196.

Argenti F., Landucci G., Reniers G., Cozzani V., 2018, Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network, Reliability Engineering and System Safety, 169, 515-530.

Argenti F., Landucci G., Spadoni G., Cozzani V., 2015, The assessment of the attractiveness of process facilities to terrorist attacks, Safety Science, 77, 169–181.

Bajpai S., Gupta J.P., 2007, Terror-proofing chemical process industries, Process Safety Environmental Protection, 85, 559–65.

Baker W.E., Westine P.S., Dodge F.T., 1991, Similarity Methods in Engineering Dynamics: Theory and Practice of Scale Modeling, 1st ed., Elsevier Science B.V., Amsterdam, The Netherlands.

Casson Moreno V., Reniers G., Salzano E., Cozzani V., 2018, Analysis of physical and cyber security-related events in the chemical and process industry, Process Safety and Environmental Protection, 116, 621-631.

Center of Chemical Process Safety (AIChE-CCPS), 2003, Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites, American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, USA.

Cozzani V., Tugnoli A., Salzano E., 2009, The development of an inherent safety approach to the prevention of domino accidents, Accident Analysis and Prevention, 41(6), 1216-1227.

Darbra R.M., Palacios A., Casal J., 2010, Domino effect in chemical accidents: Main features and accident sequences, Journal of Hazardous Materials, 183, 565–73.

Garcia M.L., 2006, Vulnerability Assessment of Physical Protection Systems, Elsevier Butterworth-Heinemann, Burlington, UK.

Garcia M.L., 2008, The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Oxford, UK.

Jaeger C.D., 2013, Chemical facility vulnerability assessment project, Journal of Hazardous Materials, 104, 207–213.

Landucci G., Reniers G., Cozzani V., Salzano E., 2015, Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios, Reliability Engineering and System Safety, 143, 53-62.

Lees F.P., 1996, Loss prevention in the process industries (2nd ed.), Butterworth-Heinemann, Oxford, UK.

Nunes-Vaz R., Lord S., Ciuk J., 2011, A more rigorous framework for security-in-depth, Journal Applied Security Research, 6(3), 372–393.

Pavlova Y., Reniers G., 2011, A sequential-move game for enhancing safety and security cooperation within chemical clusters, Journal of Hazardous Materials, 186, 401–6.

Reniers G.L.L., Audenaert A., 2013, Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects, Process Safety and Environmental Protection, 92(6), 583-589.

RISI - Repository of Industrial Security database, 2018, Security Incidents Organization <www.risidata.com/> accessed 03.09.2018.

Salzano E., Landucci G., Reniers G., Cozzani V., 2014, Domino effects related to home-made explosives, Chemical Engineering Transactions, 36, 349–54.

Vellani K., 2006, Strategic Security Management: A Risk Assessment Guide for Decision Makers, Butterwoth-Heinemann, Oxford, UK.