CHEMICAL ENGINEERING TRANSACTIONS
VOL. 91, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers

ISBN 978-88-95608-89-1; **ISSN** 2283-9216
DOI: 10.3303/CET2291087

An Interdisciplinary Approach Towards the Integrated Safety-Security Assessment of Process Facilities Operating in the Maghreb Context

Giulia Marroni[a], Andrea Piemonte[a], Francesco Tamburini[b], Gabriella Caroti[a], Gabriele Pannocchia[a], Gabriele Landucci[a,*]

[a] Department of Civil and Industrial Engineering, University of Pisa, Largo Lucio Lazzarino, 2, 56126 Pisa, Italy
[b] Department of Political Sciences, University of Pisa, Via Filippo Serafini, 3, 56126, Pisa, Italy
gabriele.landucci@unipi.it

External acts of interference towards industrial facilities have become a matter of increasing concern in recent years, especially in areas such as North Africa, where severe attacks to process facilities demonstrated the critical interface among integrated safety & security (ISS) aspects. The present work addressed this ISS concern and aimed at developing an interdisciplinary approach to support technical studies dedicated to the process industry. The first step consisted of a qualitative content analysis supporting the identification of critical ISS scenarios associated with process installations, as well as the critical socio-economic factors contributing to the terrorist threat. Next, the results of the qualitative analysis were implemented in a semi-quantitative methodology for the assessment of site attractiveness, with the aim of estimating the attack likelihood. Finally, the quantitative security risk assessment was carried out adopting: i) the attack likelihood estimated in the previous phase, and ii) a rigorous approach for the simulation of the dynamic evolution of ISS scenarios and related impact. For this purpose, the process simulator Honeywell UniSim® Design was used. The so evaluated accident impact and likelihood were combined using a risk matrix. The application to an industrial case study located in the Maghreb context was carried out in order to show the potentialities of the method and possible impact on the ISS enhancement of process industry.

1. Introduction

When compared to urban areas like malls or public transport, process and chemical facilities were not previously considered likely targets for acts of interference and terroristic (Baybutt and Reddy, 2003). Following the events of “9/11” the government of the United States enacted security-related legislation and established dedicated institutions, such as the Department of Homeland Security. In Europe, despite the fact that directives have been enacted for critical infrastructures (2008/114/EC), no published guidelines are yet available for the security of chemical and process plants. Security issues are not contemplated in the Seveso Directive (2012/18/EU) as well. However, data analysis of past physical (Casson Moreno et al., 2018) and cyber-attacks (Iaiani et al., 2021) showed the relevancy of security threats to industrial facilities. This situation is exacerbated among critical contexts, such as the Maghreb. In this area, the intense chemical and petrochemical industrial activity coexists alongside a high sociopolitical instability and the presence of a high number of terroristic cells (Martinez and Boserup, 2017), leading to a strong impact on the risk profile of such industrial installations.
In order to address these issues to support the safety and security management of industrial facilities, analysists may find guidance in international standards, such as the API/ANSI Std 780 (API, 2013), the CCPS guidelines for the evaluation of security vulnerabilities (CCPS, 2003), and the Sandia model for vulnerability of physical protection systems (Garcia, 2008). In the context of security, risk can be seen as the likelihood of a threat (T) considering an asset attractive (A), successfully exploiting Vulnerability (V) and causing a degree of Consequences (C) on an asset (API,2013). T and A can be further combined to obtain attack likelihood L.

Paper Received: 15 January 2022; Revised: 22 March 2022; Accepted: 26 May 2022
Please cite this article as: Marroni G., Piemonte A., Tamburini F., Caroti G., Pannocchia G., Landucci G., 2022, An Interdisciplinary Approach Towards the Integrated Safety-security Assessment of Process Facilities Operating in the Maghreb Context, Chemical Engineering Transactions, 91, 517-522 DOI:10.3303/CET2291087

This interpretation of risk implies the adoption of an interdisciplinary approach. In fact, when assessing L, it is crucial to consider the threats' intent, motivation, and capabilities (API, 2013); these factors are highly dependent on the geopolitical context where the facility operates, especially when dealing with critical contexts. However, a systematic method to integrate the aforementioned aspects and implement them into a quantitative analysis is still lacking. More in general, the integration among safety and security aspects is a critical task, which is necessary to prevent the propagation of accidents. However, sound approaches for this crucial integration are not offered in current literature.
The present work was aimed at developing an interdisciplinary approach towards the Integrated Safety-Security (ISS) assessment of process facilities operating in the Maghreb context. Qualitative and quantitative techniques were both applied to estimate the risk induced by intentional acts of interference adopting a risk-matrix approach. A case study, located in an LNG (liquefied natural gas) treatment facility in the Maghreb area, was analyzed in order to test the potentiality of the methodology.

2. Methodology

Figure 1 shows the methodology used in this study to address ISS scenarios. Step 1 (see Figure 1) consists of the identification of critical scenarios in the Maghreb area; firstly, a qualitative depiction of the socio-political context of the area is given; the criticality of the context is corroborated by the application of a semi-quantitative methodology for attractiveness assessment developed by (Argenti and Landucci, 2016).
The second step in the methodology (Step 2 in Figure 1) aims at the estimation of the attack success frequency F. This term depends on the likelihood of attack L and vulnerability V. L can be derived from the API/ANSI Std 780 (API, 2013) using the qualitative context analysis to identify possible threats, their intent, and capabilities; V is related to the performance of security barriers (Physical Protection System - PPS). The failure of PPS is based on its effectiveness in detecting an intrusion, communicating the detection to the response force, and in the capability of the response force to act on time (Garcia, 2008). Therefore, PPS performance strictly depends on the time needed by the adversary to cover the intrusion path T_p and on the time RFT that the response force takes to intervene. Table 1 summarizes the approach and equations adopted in Step 2 to define the attack success frequency F.
Step 3 (see Figure 1) consists of the evaluation of physical effects associated with the escalation of successful attack scenarios. Given the dynamic nature of the scenarios and the impacts induced by intentional attacks vs. the "conventional" safety scenarios, physical effects models based on integral approaches (Van Den Bosh and Weterings, 2005) were implemented in a Dynamic Process Simulation (DPS). The rigorous process simulator adopted in the present study was Honeywell UniSim® Design R460 (UniSim in the following).
Finally, Step 4 (see Figure 1) consists of the eventual estimation of of risk. The approach proposed in this work was to use a risk matrix that features a qualitative ranking for F and C. Figure 2 shows the selected matrix and the description of each qualitative class. The matrix is representative of the typical approach adopted in the Oil and Gas sector (Petrone et al., 2011). The green part of the matrix is associated with a tolerable risk level and measures of continuous improvement; the red part is where the risk level is not tolerable and further preventive or mitigative actions need to be taken to lower risk a tolerable level. Finally, the yellow part is the "as Low as Reasonably Practicable" (ALARP) risk zone.

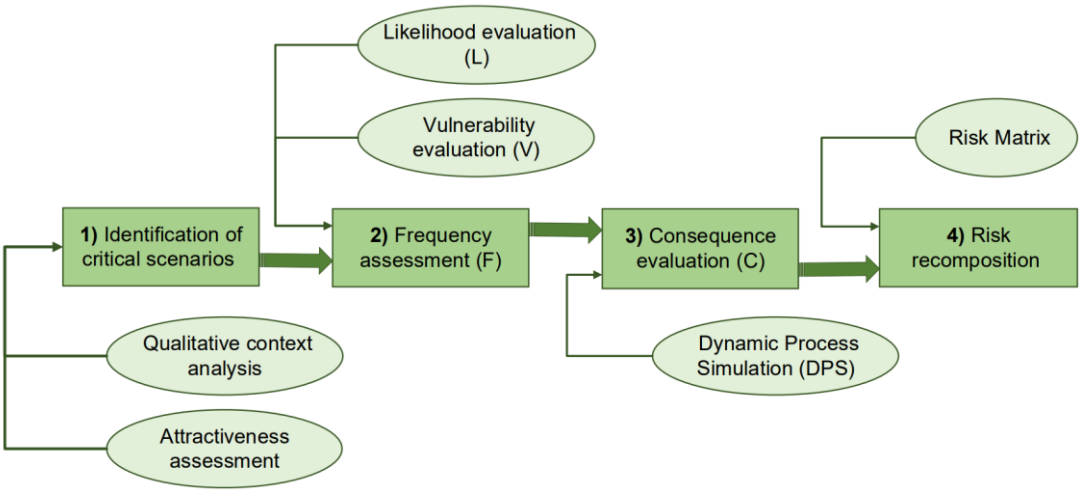

Figure 1- Flowchart of the methodological approach developed in this work to support ISS studies

Table 1 – Equations used to support the simplified evaluation of the attack frequency F

Factor	Description/Notes	Value/Equation	Source
Threat T [y^{-1}]	A credible threat exists against the asset or similar assets based on knowledge of the threat's capability and intent to attack the asset or similar assets. Some indication exists of the threat specific to the company, facility, or asset	0.20	(API, 2013)
Attractiveness A	Given the Maghreb area context, the assets have the maximum attractiveness value.	1.00	(API, 2013)
Likelihood L [y^{-1}]	Likelihood of attack to the facility	L = T·A = 0.20	(API, 2013)
Vulnerability V	Vulnerability is associated to the failure of PPS. It is sufficient for one function to fail to obtain attack success (gate OR)	$V = P_D+P_A+P_I$	(Garcia, 2008)
P_D	Probability of failed intrusion detection	0.10	(Garcia, 2008)
P_A	Probability of failure of alarm communication	0.05	(Garcia, 2008)
P_I	Probability of failure of timing of response force	$1-\frac{1}{\sqrt{\pi\cdot\beta}}\cdot\int_0^T e^{-\frac{t^2}{\beta}}\cdot dt$ $\beta = 2\cdot\left(\sigma_{RTF}^2+\sigma_P^2\right)$ $T = T_P - RFT > 0$ T_P: penetration time; RFT: response force time; σ: variance of T_P or RFT	(Garcia, 2008)
Frequency (F)	Frequency of attack success	F=L·V	

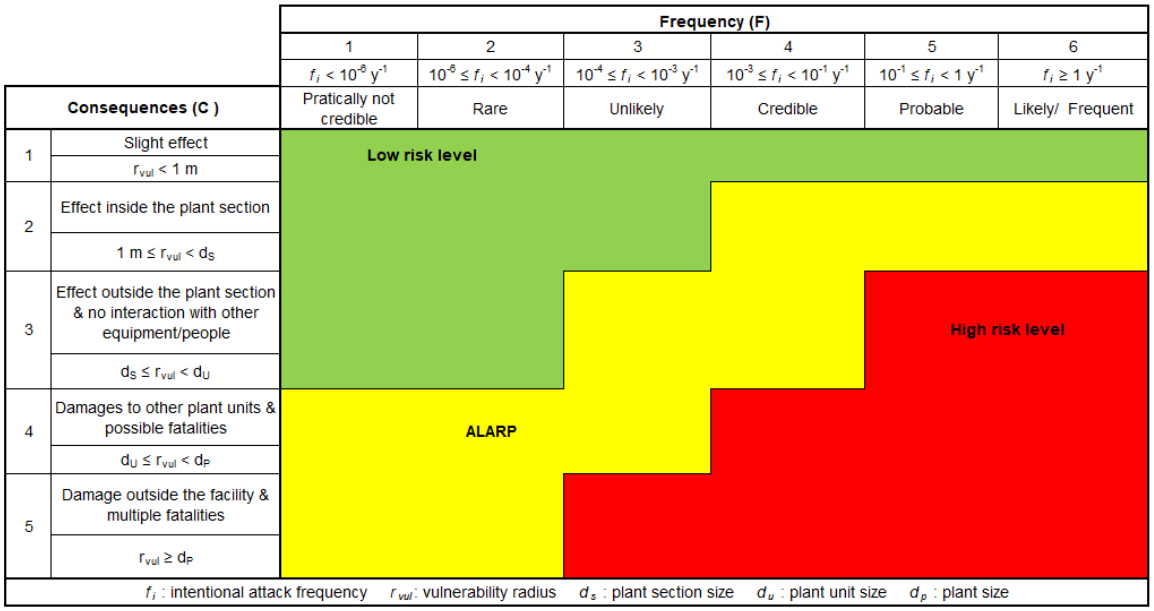

Figure 2 – Risk matrix proposed for the present work; qualitative categories and their range are shown.

3. Definition of the reference case-study

In order to exemplify the methodology a case study was defined. In particular, the reference facility is an LNG treatment plant located in Algeria. Figure 3 shows a simplified plant layout and the equipment position. The critical equipment chosen for this work is a three-phase separator, which was assumed to process essentially natural gas entering the liquefaction plant. For the sake of exemplification and in absence of more specific

data, process scheme, operative conditions, and gas composition were derived from a previous work (Landucci et al., 2018).

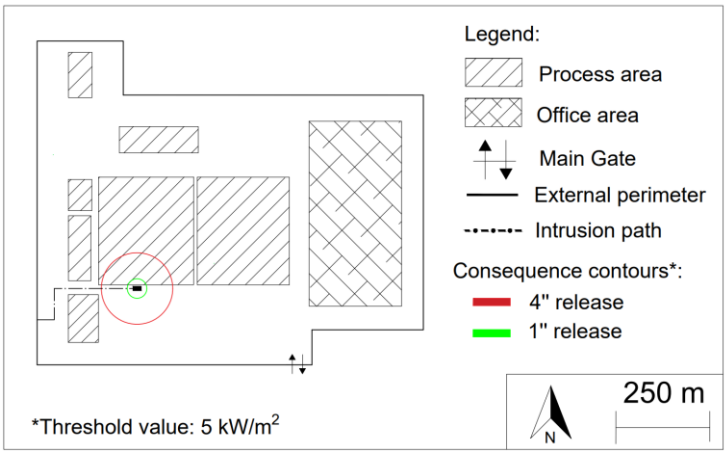

Figure 3 –Plant layout considered for the case study and consequence contour maps obtained by DPS (see Section 5).

4. Qualitative context analysis and attractiveness assessment

As the considered case is located in Algeria, a specific qualitative content analysis for this area was preliminarily carried out to support the reference scenarios identification and the simplified likelihood assessment.

Throughout the last decade, the broader area of North Africa has undergone significant geopolitical changes (Martinez and Boserup, 2017). The developments taking place in the region have become increasingly interconnected and their impact has extended far beyond their borders, especially to Europe. According to (Tichy and Eichler, 2018), there are at least four interconnected dynamics which define the security landscape in North Africa: 1) energy sources (gas and crude oil), 2) geopolitical antagonisms and new (im)balances of power, 3) new (human) security imperatives, and 4) increased interest in the area from external powers. Although Islamist terrorism was already a destabilizing factor in the region, 2011 marked a turning point in the escalation of the attacks because of the development of a new energy strategy by the two main Islamic militant organizations, namely Al-Qaeda and IS (Tichy and Eichler, 2018). The energy industry and its incomes are of fundamental importance for these two groups; in fact, gaining control or damaging plants eases their criminal activities, such as contraband or drug trafficking; the attacks to the facilities of In Amenas (Algeria) in 2013 carried out by Al-Qaeda is emblematic in this sense. Therefore, understanding Islamic militant organizations and their strategies is of utmost importance to improve the security over the energy systems of the Maghreb area. Based on these considerations, the security aspects of process facilities operating in the Maghreb area represent a critical concern and the peculiar socio-political elements of this critical context were considered in the development of the present work.

The qualitative context outlined in this Section was corroborated by the application of a semi-quantitative methodology for attractiveness assessment developed by Argenti and Landucci (2016), to which the Reader is referred for more details. For a given industrial facility, attractiveness is associated with site-specific induction elements that account for “non-technical” aspects. The aspects contemplate geopolitical, social and political elements that characterize the context of the area where the industrial facility under analysis is located. The results of the methodology showed that the socio-political context of the Maghreb area causes a raise of up to 70% in overall attractiveness with respect to the baseline value obtained for the European context (Argenti et al., 2016). This enabled for the evaluation of threat and attractiveness summarized in Table 1, which, on turn, supported the estimation of the attack likelihood for the present study.

5. Consequences based on DPS

Given the historical threat record for the area (see Section 4), two attack scenarios were considered in order to estimate their impact and relative risk contribution for the present case: 1) the adversary shoots from the outside of the plant with a firearm against the separator, causing a 1’’ (25.4 mm) leak; 2) the adversary penetrates through a hole in the fence on the west-side of the perimeter and detonates 15 kg of an improvised explosive device in proximity of the separator, causing a major release scenario. A 4’’ (101.6 mm) hole is

assumed in this case. For the sake of simplicity, a single final outcome is associated with this attack scenario, i.e., a jet-fire resulting from the immediate ignition of the natural gas. Figure 3 shows the intrusion point and intrusion paths.
The consequences of the jet fire have been studied using a DPS, implemented in UniSim (Landucci et al., 2018). This piece of equipment has been implemented on the simulator in dynamic mode. The actual dimensions of each piece of equipment have been considered to account rigorously for any thermal effect, as well as the relation between flowrate and pressure. Then, a specific template was developed to simulate the physical effects associated with the jet fire scenario. The template is embedded in the DPS and consists of a calculation spreadsheet which features an adapted version of the Chamberlain model (Van Den Bosh and Weterings, 2005). Given the source term, the template calculates the features of the flame and finally provides an estimation of damage distances, following a threshold-based approach. For this study, a threshold value of 5 kW/m^2 has been chosen, which corresponds to irreversible damages according to (Italian Ministry of Public Works, 2001). The consequence contours resulting from the DPS application are shown in Figure 3.

6. Simplified risk evaluation

The attack likelihood L was evaluated for the case study using the data summarized in Table 1 supported by the qualitative analysis discussed in Section 4. For scenario 1, V has been imposed as unitary since the attack starts from the outside of the perimeter; therefore, no PPS can intervene. On the other hand, for scenario 2, probabilistic data on PPS performance and intrusion path information are needed to quantify V. The intrusion time T_p was evaluated from Figure 3 considering a walking velocity of the intruder of 1.5 m/s, a time to pass through the fence of 90s and a time to place the explosive of 20s (Garcia, 2008); the RFT was 240 s (see Table 1). For both times, a variance σ of 30% has been considered.
For the evaluation of consequences, the DPS was conducted using the defined source term for each scenario to obtain the maximum consequence contours. As shown in Figure 3, the consequence contour for scenario 1 covers a radius of about 25 m, while for scenario 2 the damage distance is almost quadrupled. Using these values, the consequence category C in the risk matrix of Figure 2 was determined. Table 2 summarizes the results of this simplified risk evaluation.

Table 2 – Risk assessment for critical scenarios using the risk matrix approach

Scenario ID	Scenario description	V	F	C	R
1	Jet fire from 1'' (25.4 mm) hole	1.00	5	2	ALARP
2	Jet fire from 4'' (101.6 mm) hole	0.86	5	3	High risk level

For both scenarios, the frequency falls into the category 5, which means that a successful external attack is probable following the present qualitative classification. This may be explained considering two factors: firstly, the plant operates in a critical geographical area, which causes a very high threat and attractiveness level (see Table 1). Moreover, the low effectiveness of PPS in detecting and consequently stopping an intruder reduces the vulnerability V only by 14%; thus, both the external attack scenario (1) and the internal attack scenario (2) fall in the same frequency category.
The consequences of scenario 1 only affect a small portion of the plant section where it is located. On the other hand, the consequence contour of scenario 2 is extended towards a different plant section. However, it also involves an empty area and for this reason consequence category 3 has been chosen. This raise in consequences is reasonable given the higher release diameter of scenario 2 compared to scenario 1.
For what concern the risk screening (see Table 2), scenario 1 falls into the ALARP zone, while an intolerable risk level is associated with Scenario 2. Moreover, the jet fire may affect neighboring process units, with the potential of higher-level domino effects, with amplification of consequences (Landucci et al., 2013). Hence, the contribution of integrated safety and security barriers is critical in the view of reducing the risk induced by intentional scenarios (Chen et al., 2019).
Finally, it is worth mentioning that the probabilistic assessment was extremely simplified but able to derive straightforward indications on the relevant security-related scenarios and a more systematic assessment compared to the available standard techniques (API, 2013). However, likelihood assessment may be improved my means of more advanced probabilistic techniques, such as Bayesian Networks or other graph theoretical approaches (Chen et al., 2019), and PPS performance data may be as well improved to better estimate the site vulnerability. In fact, baseline literature PPS data were adopted in this study, whilst a tailored PPS assessment for the specific context may lead to a better performance analysis of the protections.

7. Conclusions and future works

In this work, an interdisciplinary approach to security scenarios was used for an integrated safety-security risk assessment with particular focus on the Maghreb region. Qualitative and quantitative techniques were combined in order to apply a simplified risk matrix approach.
The results show the high criticality of security scenarios affecting chemical and process facilities operating in the Maghreb area. The improvement of PPS performance and, at the same time, gathering specific performance data for the PPS is of utmost importance, given that both an external and internal attack scenario fall under the same attack frequency category.
Future works are devoted to the improvement of the current approach by means of a systematic likelihood and vulnerability assessment. Moreover, other risk assessment metrics may be adopted. For instance, a specific GIS (Geographic Information System) tool is under development to allow for the visualization and georeferencing of the results, obtaining security vulnerability and risk maps in the areas considered in the analysis. In conclusion, the present contribution shows the effectiveness of using an interdisciplinary approach towards the complex integration of safety and security aspects.

Acknowledgments

Support by the University of Pisa through the “Progetti di Ricerca di Ateneo PRA 2020-2021” funding program is gratefully acknowledged.

References

American Petroleum Institute (API), 2013, ANSI/API Standard 780 – Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry, American Petroleum Institute, Washington, District of Columbia, USA.

Argenti F., Landucci G., 2016, Advanced attractiveness assessment of process facilities with respect to malevolent external attacks, Chemical Engineering Transactions, 53, 133–138.

Baybutt P., Reddy V., 2003, Strategies for protecting process plants against terrorism, sabotage and other criminal acts, Homeland Defence Journal, 2, 1.

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 for Chemical Process Safety (CCPS), 2003, Guidelines for Analysing and Managing the Security Vulnerabilities of Fixed Chemical Sites, American Institute of Chemical Engineers, CCPS, New York, USA.

Chen C., Reniers G., Khakzad N., 2019, Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach, Reliability Engineering and System Safety, 191, 106470.

Garcia M. L., 2008, The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Newtown, Massachusetts, USA.

Iaiani M., Casson Moreno V., Reniers G., Tugnoli A., Cozzani V., 2021, Analysis of events involving the intentional release of hazardous substances from industrial facilities, Reliability Engineering and System Safety, 212, 107593.

Italian Ministry of Public Works, 2001, Requisiti minimi di sicurezza in materia di pianificazione urbanistica e territoriale per le zone interessate da stabilimenti a rischio di incidente rilevante, DM 9 May 2001

Landucci G., Cozzani V., Birk A.M., 2013, Heat radiation effects, Chapter in: G Reniers, V Cozzani (Ed.), Domino effect in the process industries: modelling, prevention and managing, Elsevier, Amsterdam, the Netherlands, 70–115.

Landucci G., Pupillo A., Mencaroni A., Pannocchia G., 2018, Quantitative consequence assessment of industrial accidents supported by dynamic process simulators, Chemical Engineering Transactions, 67, 139-144.

Martinez L., Boserup R.A., 2017, Beyond Western Sahara, the Sahel-Maghreb Axis Looms Large, Chapter in: R Ojeda-García, I Fernández-Molina, V Veguilla (Ed.), Global, Regional and Local Dimensions of Western Sahara’s Protracted Decolonization, Palgrave Macmillan, New York, USA, 143-163.

Petrone A., Scataglini L., Cherubin P., 2011, B.A.R.T (Baseline Risk Assessment Tool): A Step Change in Traditional Risk Assessment Techniques for Process Safety and Asset Integrity Management, SPE Annual Technical Conference and Exhibition, Denver, Colorado, USA

Tichy L., Eichler J., 2018, Terrorist attacks on the energy sector: The case of Al Qaeda and the Islamic state. Studies in Conflict & Terrorism, 41(6), 450–473.

Van Den Bosh C.J.H., Weterings R.A.P.M., 2005, Methods for the calculation of physical effects (Yellow Book), Committee for the Prevention of Disasters, The Hague, The Netherlands.