CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331011

Interdependencies Between Industrial Infrastructures: Territorial Vulnerability Assessment

Benjamin Rey*[a], Jerome Tixier[a], Aurelia Bony-Dandrieux[a] , Gilles Dusserre[a] , Laurent Munier[b], Emmanuel Lapebie[b]

[a]Institute of Risk Science (ISR) , Ecole des Mines d'Alès, France
[b]CEA, Gramat, BP80200, 46500 Gramat, France
*benjamin.rey@mines-ales.fr

Industrial activities are increasingly dependent on each other. Several recent events (e.g. Tsunami and earthquake in Japan in 2011) illustrate the consequences (e.g. humans, economic…) of interactions between industrial infrastructures. The state-of-the-art review focused mainly on the risk assessment and interdependencies between critical infrastructures. The aim of this paper is to present an approach able to determine an infrastructure vulnerability level and risk scenarios development based on Seveso regulations and critical infrastructures. The vulnerability infrastructure level is assessed with a multi-criteria analysis. The goal is to identify several criteria according to physic, functional, economic, social and environment context of the infrastructure in the territory. The risk scenarios are developed in order to estimate the consequences in a territory of a threat on one or several infrastructures.

1. Introduction

The Japan earthquake and tsunami of 2011 that destroyed 30% of the electricity production plants illustrate the interdependencies between industrial infrastructures. This event simultaneously the shut-down of 4 other refineries and fires in two others refineries (Pitrat, 2011). The ice storm in Quebec in 1998, attacks on the World Trade Center in New York in 2001, the Indian Black out in 2012 are others examples of major failures. It enhances the need for research on the functional and spatial dependencies between industrial activities.
Based on the description of different events, this study aims at building a methodology able to describe an infrastructure vulnerability level and risk scenarios in a local context composed by critical and Seveso infrastructures. The study is particularly focused on domino effects because of the functional and geographic interdependencies between infrastructures at territorial scale.
In this article, the first part is a state-of-the-art review of the academic literature in the field of risk between infrastructures. The second part describes the different approach's steps to demonstrate the added-value of this study.

2. Main points of the literature

This part describes the elements of literature dealing with interdependencies between industrial infrastructures. At first, we made the choice to select for our research only critical infrastructures and infrastructures concerned by the SEVESO European Directive because of their relevance and their capacity to generate domino effects. These elements are introduced. Then, the notion of risk assessment for infrastructure protection is analyzed. Different modeling techniques of interdependencies between critical infrastructures and several studies on vulnerability infrastructures are outlined.

2.1 Elements of the system

Our survey is focused on critical infrastructures and infrastructures concerned by the SEVESO Directive. In the context of homeland security, the United States were pioneers to investigate in this field, with the publication in 1997 of the report of Critical Foundations Protecting America's infrastructure, after the

Please cite this article as: Rey B., Tixier J., Bony-Dandrieux A., Dusserre G., Munier L. and Lapebie E., 2013, Interdependencies between industrial infrastructures: territorial vulnerability assessment, Chemical Engineering Transactions, 31, 61-66 DOI: 10.3303/CET1331011

Oklahoma City bombing in 1995 (President's Commission on Critical Infrastructure Protection, 1997). After New York and Madrid terrorist attacks in 2001 and 2004, respectively, many programs appeared in several countries on critical infrastructure protection. The focus was clearly on terrorist attacks but also on natural disasters and industrial accidents. These infrastructures are defined critical because of their essential resource (e.g. electricity, gas).

In 2004, European Council and the European Commission concentrate their efforts on the analysis of critical infrastructure protection against terrorists threats (COM, 2004). The European Commission adopted in 2006 (COM, 2006) the basis and operations of the European Program of Critical Infrastructure Protection (EPCIP). The framework of the program is decomposed in several parts:

- Setting up a Directive which was adopted in 2008 (Directive 2008/114/CE) ;
- Measures in order to facilitate the EPCIP implementation : action plan, Critical Infrastructure Warning Information System (CIWIN) to improve the exchange of alert messages, experts, procedures to share information about critical infrastructure protection
- Help of member states of national critical infrastructures ;
- Intervention plans ;
- International scope (cooperation with external countries of Europe) ;
- Financials accompanying measures.

In the Directive 2008/114/CE, European critical infrastructures are defined as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States" whereas Critical Infrastructure "means an asset, system or part thereof located in Member States 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 a significant impact in a Member State as a result of the failure to maintain those functions". Two sectors of European critical infrastructures are concerned by the directive: energy (electricity, oil, gas) and transports (road/air/rail transport, inland waterways transports, ocean and short-sea shipping and ports). For the moment, the others sectors (e.g. water, health) are decided by each member state for national critical infrastructure. In order to identify critical infrastructure, a survey highlights that geographic approach is very beneficial (Bouchon, 2011).

Furthermore, most of the literature deals with critical infrastructures and target on the assessment of the interdependencies. Hence, Rinaldi (2001) defines six main dimensions of interdependencies between critical infrastructures. Infrastructure environment (e.g. socio-economic context, public policy) is the only dimension that takes into account the concept of the context (Bouchon, 2011). The others are more technical: type of interdependencies (Figure 1), infrastructure features (e.g. operational and organizational factors), state of operation (e.g. disrupted, normal), coupling and response behavior (e.g. linear or complex interactions, coupling degree) and type of failure (e.g. common cause, escalating).

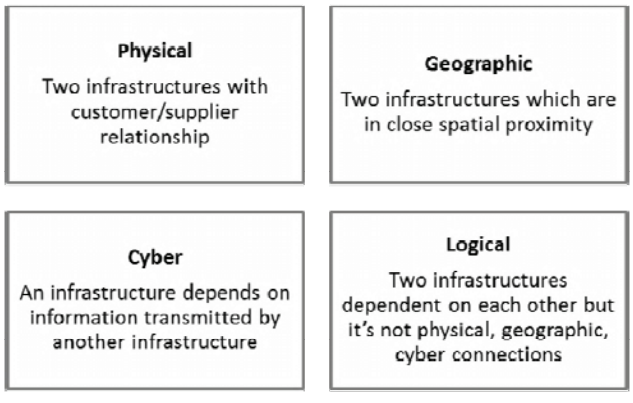

Figure 1: Type of interdependencies (based on Rinaldi et al., 2001)

These kinds of interdependencies between two entities are at the origin of domino effect (Robert and Morabito, 2011). In other cases, domino effects happen only because of the proximity between different elements (e.g. units, establishments). Within the European Union, domino effects are defined by Seveso II Directive as "establishments or groups of establishments where the likelihood and the possibility or consequences of a major accident can be increased because of the location and the proximity of such

establishments and their inventories of dangerous substances" (Council Directive 96/82/CE, 1996). Nowadays, domino effects are an important part of Seveso infrastructure issues.
SEVESO Directive requires member States and companies to identify the risks linked to industrial activities and to develop measures to minimize those risks (European Commission, 1996). In France, installations concerned by this Directive are called ICPE (Classified Installations for Environment Protection). A nomenclature of these infrastructures exists, classified according to activity sector, quantity and nature of substances used and produced on the site (Installations Classées, 2003).
Furthermore, an infrastructure concerned by the SEVESO Directive can also be a critical infrastructure. Protection of Critical Infrastructure and SEVESO Directive are established respectively to reduce potential consequences of a loss of resource and the destruction of the infrastructure.

2.2 Risk assessment methodologies for infrastructure protection

The aim of this part is to describe the features of risk assessment methodologies for infrastructure protection. Studies are mainly about the critical infrastructures. Several state-of-the-art reviews are produced (Giannopoulos et al., 2012) (Yusta et al., 2011) (Pederson et al., 2006). Authors emphasize the commons points and difference between these methodologies. Sector infrastructure, audience and maturity level, type of interdependencies, identification of threats, modeling technics are the most usual.
For instance, Yusta (2011) compiled a survey about methodologies and application for critical infrastructure with 55 references and discern this research with four features: types of critical infrastructures, modeling techniques, maturity and availability, risk management stages. This survey reveals two trends. The first one focused on the understanding of the structural and functional infrastructures. The second one concentrates on the representation of the dynamic behavior of the infrastructures. The article identifies five modeling techniques: multi-agent systems, system dynamics, rating matrices, relational data-bases and the network theory. Those modeling techniques are combined with computation methods and tools such as Monte Carlo simulation or geographic information system (GIS). Multi-agent and system dynamic are attractive because they can predict the behavior of critical infrastructure under emergencies situations. Network theory (e.g. Johansson and Hassel, 2010) and relational database enable to identify critical nodes. Rating matrices is also interesting because it uses semi-quantitative judgments.
Otherwise, we can find also methodologies that consider not exclusively critical. For instance, the Syner-G project "Systemic Seismic Vulnerability and Risk Analysis for Building, Lifelines Networks and Infrastructure Safety Gain" consists in the development of a methodology with three models: seismic hazard model, physical vulnerability model, functional and socio-economic system model (SYNER-G, 2012).
Regarding methodologies on the infrastructures concerned by the SEVESO European Directive, they deal with essentially of risk analysis on one industrial site and its environment (Tixier et al, 2002).
Finally, these methodologies are fundamentally oriented on the infrastructures (structural analysis, functional analysis and behavior analysis) and their interdependencies but without any spatial approach. Indeed, spatial approach allows studying infrastructures with the territory scale.

2.3 Synthesis

The part shows that the protection of the interdependencies between infrastructures is a recent subject. Seveso and critical infrastructures can generate domino effects because of the different types of interdependencies. Risk assessment methodologies for infrastructures protection are based mainly of the structure, the operation and the behavior of the interdependencies between infrastructures. Geographic approach has a little attention whereas it can deepen the risk analysis of these infrastructures.
Consequently, we created an innovative approach called Interdependencies between Industrial Infrastructures Approach (I3A) in a local context.

3. I3A Methodological approach

3.1 Research approach

In the state-of-art, we indicated that SEVESO regulations and critical infrastructures are distinct. Most of recent studies deals with interdependencies between infrastructures are about critical infrastructures. Although SEVESO infrastructures may be critical infrastructures; the state-of–the-art shows a need of improvement on that concern. Moreover, these infrastructures can generate several domino effects because of their interdependencies (e.g. functional, geographic) and cause many losses in a territory.
Our new approach is meant to provide a level of vulnerability for infrastructures and risk scenarios in a local context.

3.2 Organization of the approach

I3A (Interdependencies between Industrial Infrastructures Approach) is based on four steps (Figure 2).

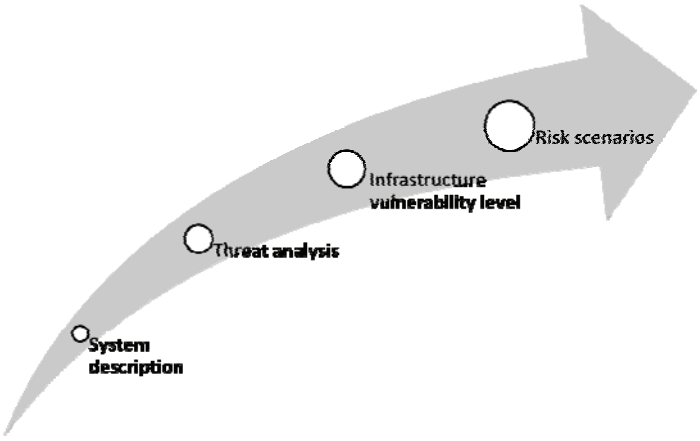

Figure 2: Methodological steps

- Step 1: System description

To develop the model, it remains essential to identify the system and their components. In our approach, the system is the territory composed by critical and SEVESO infrastructures. The methodology can have two scale levels: local and regional. Moreover, our tool can integrate several activities sector regarding the choice of critical infrastructures. Users of methodologies have to choice into the following list: energy, water, transport, industries. SEVESO infrastructures are considered in the list.

- Step 2: Threats Analysis

Several threats can impact infrastructures in a territory. The origin of the threat can be caused by man-made acts (e.g.: terrorism), industrial accident (e.g. fire), natural disaster (e.g. flood, earthquake). The aim of this step is to identify the different threats that we can find on a territory composed by several infrastructures interdependencies.

- Step 3: Infrastructure vulnerability level

In this step, we want to assess the infrastructure vulnerability level (Figure 3). The goal is to identify several criteria family according to physic, functional, economic, social and environment context of the infrastructure in the territory. It's also necessary to identify a threat (e.g. flood) to examine these criteria family which depend on:

- Importance of the infrastructure to the territory (e.g. economic potential);
- Intrinsic parameters of the infrastructure (e.g. accessibility);
- Interdependencies of the infrastructure (e.g. functional)
- Resiliency, prevention, protection measures (e.g. repetition)

Then, it is possible to specify the criteria family in several criteria (e.g. number of functional connections).
A multi-criteria analysis by expert judgment is going to classify the different dimensions (e.g. physic, functional) of the context, criteria family and criteria in order to have the infrastructure vulnerability level. It's possible to compare the levels to class the infrastructures.

- Step 4: Introduction of risk scenarios

Last step of this approach is to create risk scenarios and compare these scenarios with a consequences approach in a territory (Figure 4). In first time, it's necessary to describe a scenario with a choice of threat and elements of the system which are related to this step. With this description, several input data (e.g. element locating) are selected for application of different tools. Five tools are provided to assess the consequences in a territory:

- Tool 1, simulation of phenomena accidental can visualize a dangerous product if an element is impacted. For example, Garbolino (2010) uses PHAST software to simulate the consequences of failure in an industrial site (e.g. dispersion of a toxic cloud).
- Tool 2, real distance matrix and effect distances matrix enable to know if one or several elements are destroyed. Effect distances matrix are built for each type of event (e.g. Bleve). Reniers (2006) uses these tools in a methodology to reduce domino effects in a chemical installation.
- Tool 3, map of population density is created in order to be coupled into the tool 1 and 2. The goal is to assess the consequences of the social dimension (e.g. number of person who is intoxicated).

- Tool 4, inoperability input-output matrix is used to quantify the impact of the scenario on the operational capabilities of the activities sectors. Setola (2009) apply this tool to analyze the cascade effects between the critical infrastructure sectors with interviewing experts and fuzzy number.
- Tool 5, economic multipliers have to give a translation between the different consequences of the others dimensions to obtain their financial costs.

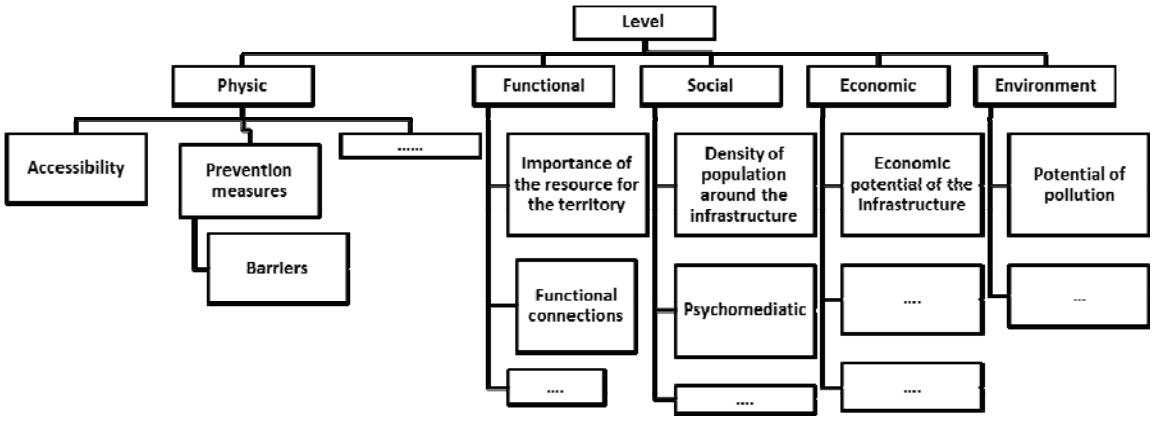

Figure 3: Infrastructure vulnerability level

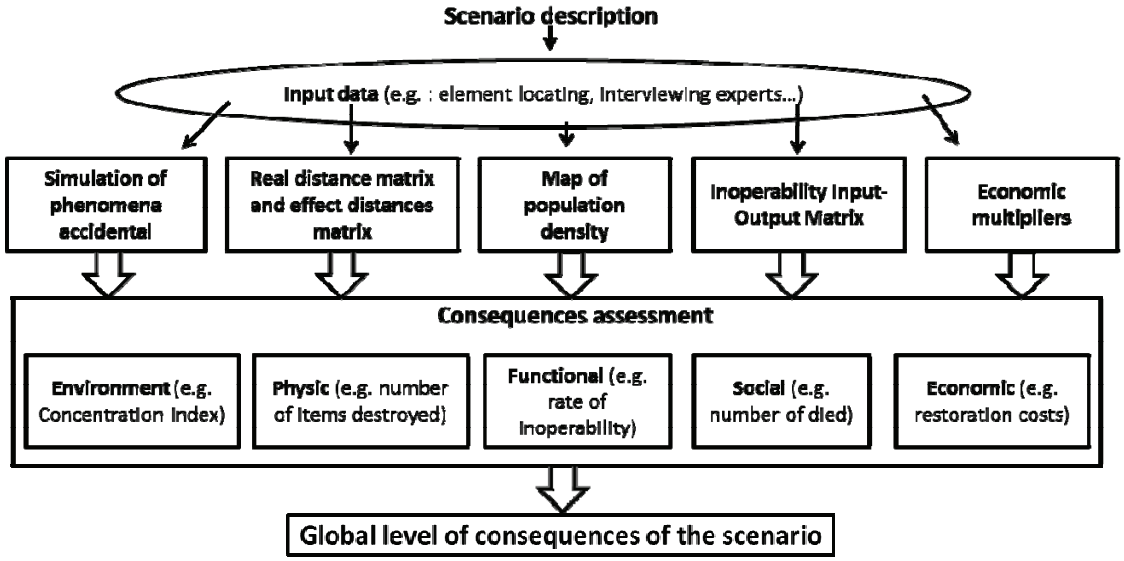

Figure 4: Framework of risk scenario assessment

4. Conclusion

The article produces a state-of-the-art based on mainly on the risk assessment for critical infrastructure protection. In a second time, the different steps of the new approach are given in order to develop an infrastructure vulnerability level and risk scenario in a local context. The different scenarios observe the consequences of a threat in a territory.

The I3A (Interdependencies between Industrial Infrastructures Approach) developed in this article provides a framework of the project. The different steps must be developed and applied to add an innovative contribution in a local context of this current problematic.

References

Bouchon S., 2011, Critical infrastructure identification: reflection with the European example, Geography thesis, University of Paris Ouest Nanterre La Défense, Gecko Laboratory, France (in French).

COM (2004) 702 final, 2004, Communication from the commission to the council and the European parliament “Critical Infrastructure Protection in the fight against terrorism”, Brussels, Belgium.

COM (2006) 786 final, 2006, Communication from the commission on a European Programme for Critical Infrastructure Protection, Brussels, Belgium.

Council Directive 2008/114/CE, 2008, The identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union.

Council Directive 96/82/CE, 1996, The control of major accident hazards involving dangerous substances, Official Journal of the European Union.

European Commission (EC), 1996, <www.ec.europa.eu/environment/seveso/index.htm> accessed 23.08.2012

Garbolino E., Chéry J.P, Guarnieri F., 2010, Dynamic model of risk industrial systems, Lavoisier Edition, France (in French)

Giannopoulos G., Filippini R., Schimmer M., 2012, Risk assessment methodologies for Critical Infrastructure Protection. Part I: State of the art, Publications Office of the European Union, Luxembourg, doi: 10.2788/22260

Installations classées (IC), 2003, <www.installationsclassees.developpement-durable.gouv.fr/> accessed 23.08.2012

Johansson J., Hassel H., 2010, An approach for modelling interdependent infrastructures in the context of vulnerability analysis, Reliability Engineering and System Safety, 95, 1335-1344, doi:10.1016/j.ress.2010.06.010

Pederson P., Dudenhoeffer D., Hartley S., Permann M., 2006, Critical Infrastructure Interdependency Modeling: A Survey of Critical Infrastructure Interdependency Modeling, Idaho National Laboratory, United-States of America.

Pitrat D., 2011, Impacts of Tohoku earthquake on Japanese industry, Face au risque n°474 juin-juillet 2011, 28-31, France (in French).

President’s Commission on Critical Infrastructure Protection, 1997, The Report of Critical Foudation Protecting America's Foundation, USA.

Reniers G.L.L, Dullaert W., DomPrePlanning: User-friendly software for planning domino effects prevention, Safety science, doi:10.1016/j.ssci.2006.10.004

Rinaldi S. M., Peerenboom J. P., Kelly T. K., 2001, Identifying Understanding and Analyzing, IEEE Control Systems Magazine, 11-25.

Robert B., Morabito L., 2011, Reducing vulnerability of critical infrastructure-Methodological Manual, Presses Internationales Polytechniques, Montreal, Canada.

Setola R., De Porcellinis S., Sforna M., 2009, Critical infrastructure dependency assessment using the input-output inoperability model, International journal of critical infrastructure protection, doi:10.1016/j.ijcip.2009.09.002

SYNER-G, 2012, Systemic Seismic Vulnerability and Risk Analysis for Buildings, Lifeline Networks and Infrastructures Safety Gain, <www.vce.at/SYNER-G/> accessed 27.08.2012

Tixier J., Dusserre G., Salvi O., Gaston D., 2002, Review of 62 risk analysis methdologies of industrial plants, Journal of loss prevention in the process industries.

Yusta J. M., Correa G.J., Lacal-Arántegui R., 2011, Methodologies and applications for critical infrastructure protection: State-of-the-art, Energy Policy, 39, 6100-6119 doi:10.1016/j.enpol.2011.07.010