Scenario Based Approach for Risks Analysis in Critical Infrastructures

Joaquín López-Silva
Pablo de OlavideUniversity
jlopsil@upo.es

Victor A. Bañuls
Pablo de OlavideUniversity
vabansil@upo.es

Murray Turoff
New Jersey Institute of Technology
murray.turoff@gmail.com

ABSTRACT

This paper proposes a Cross Impact Analysis for supporting critical infrastructures risk analysis. This methodology contributes to decision-makers and planners with analytical tools for modeling complex situations. These features are generally useful in emergency management and particularly within the critical infrastructures scope, where complex scenarios for risk analysis and emergency plans design have to be analyzed. This paper will show by an example how CIA methodology can be applied for risks and identification analysis with an application to a Data Centre of a Critical Infrastructure.

Keywords

Cross Impact Analysis (CIA); Scenarios, Crisis Preparedness; Resilience-Risk Analysis; Critical Infrastructures.

INTRODUCTION

Organizations obligation about security plans and emergency response is common in most states. This is a pressing need in organizations that manage Critical Infrastructures, due to the potential impact of any failure on our society. European standard 2008/114/CE defines as a Critical Infrastructure (CI) any element, system or part of system being essential for the maintenance of social vital functions, health, physical integrity, security, social and economic welfare of population, whose perturbation or destruction would affect seriously to a state member.

An operator [1] appointed as critical ought to make an Operator Security Plan (OSP). OSP will have to establish a risk analysis methodology assuring continuity of services provided by that operator. This methodology should gather the application criteria of the different security measures implemented against both physical and logical identified threatens over every assets typology.

There are national and international standards which regulate and advise practises and methodologies for assuring a suitable risk analysis of every CI. Those standards also aim to assure an increase and maintenance of their recuperation and absorption capacity against unexpected events (resilience) (2008/114/EC).

This work proposes Cross-Impact Analysis (CIA) for identifying and analyzing risks in CI. Cross Impact risk analysis is a dynamic process under uncertainty scenarios, where heterogeneous and objective risks are assessed. CIA has been successfully applied to emergencies management for crisis scenarios modelling in

[1] O*rganizations responsible of investments or operations of an installation, network, system, physical equipment or information technology appointed as critical infrastructures*.

a collaborative way to achieve "consensus" models (Bañuls et al, 2013) as well as for emergency plans generation (Lage et al, 2013).

Related to CI field it has been recently applied for modelling interrelations among a CIs network (Turoff et al, 2014). This research tries to contribute to its field making a pioneer application of CIA to a risk analysis of a specific CI.

This is done because of its suitability for detecting critical events, managing high level of uncertainty, analyzing cascade effects, and representing graphically complex scenarios with heterogeneous components.

CRITICAL INFRASTRUCTURES RISKS ANALYSIS

There exist some catalogues of CIs. United States of America, for instance, includes in those lists agriculture, (food), water, public health services, Defense Department industrial bases, telecommunications, energy, transport, banks finance, chemicals, hazardous material, and postal delivery (WH, 2013).

European commission (UE, 2005) enumerates different sectors. Therefore, what a CI exactly constitutes changes from a country, culture, time to others.

There are not too many references throughout literature –even less applications- of Scenario planning, in particular of Cross Impact Method for resilience improvement in Organizations.

Improving resilience requires a methodology that generates applicable results that support decision making in risk management (Petit et al, 2012). This has to be done considering today austerity age (Rogers et al, 2012).

A comparative table of methodologies capable of application is attached as an overview with the most relevant methodologies applied to CIs risk analysis (table 2).

Some authors (Giannopoulos et al, 2012) highlight as limitations of those methodologies that most of them lack in tools for to analyze cascade effects, make scenario simulations, integrate qualitative and quantitative skills and that they had been specifically designed for an organization .Therefore they may suffer bias because they consider only a part of the relevant threatens.

The here proposed methodology tries to address the lacks found in most of these methodologies at table 2. Besides, the algorithms which this methodology is based on are, in particular, computationally efficient, managing problems with high number of inter related risks, not affordable from a traditional approach (Turoff et al, 2014). CIA can be applied to any sector or type of risk, mixing qualitative and quantitative variables.

METHODOLOGICAL FRAMEWORK

There exist several scenario generation methodologies as support for decisions making process within complex processes (Coates, 2000; Harries, 2003;Chermack, 2004; Bañuls et al, 2007; Van Notten et al, 2003). As already said, there also exist a lack of methodologies for complex scenarios simulation whose tools include those that: (1) analyze cascade effects, (2) make scenarios simulations, (3) comprehend qualitative and quantitative skills for emergency plans elaboration and risk detection in critical infrastructures. CIA methodology has been designed for covering this gap providing modeling and scenario analysis methodologies for planning. This approach gets more realistic emergency plans, since we increase data with subjective probabilities allowing more objective results in terms of risks and damages analysis (Yu et al, 1988). Bellow it is detailed the methodology background.

Cross Impact Analysis was developed by Gordon and Helmer (Gordon, 1994). The main objective of CIA is to estimate the occurrence of a set of events, given that those occurrences are not independent. Turoff's approach (Turoff, 1972a) was developed purposely for an interactive mode with computers at an efficient computational cost. Besides, his approach does not need a significant statistic history from which a specific occurrence probability of event could be inferred. This method also extends the original capabilities allowing the detection of scenario key events allowing us to work with large sets of events and make sensitivity analysis over results (Bañuls et al, 2007).

Analytically, cross impact or correlation coefficients (c_{ij}) are worked out using a variation of the distribution function of Fermi-Dirac fed by users answers (experts) about probabilities P_i following the below presented relation:

$$P_i = 1 / (1 + \exp(-G_i - \sum_{i=k}^{n} c_{ik}P_k)) \qquad (1)$$

Methodology	Sector/Hazards	Users	Objectives	Interdependencies	Crosssectoral risk	Resilience
BIRR Better Infrastructure Risk and Resilience	All sectors/All Hazards	Operators, asset managers, policy makers	Vulnerabilities assessment, risk reporting	YES	YES	YES
BMI	All sectors/All Hazards	Private companies, CI operators, Policy makers	Vulnerabilities and risk assessment, Foster collaboration between policy makers and private sector	YES	NO	NO
CARVER 2	All sectors/All Hazards	Policy makers	Risk evaluation, evaluation of alternatives, allocation of protective measures	YES	YES	YES (partially)
CIMS (Critical Infrastructure Modeling Simulation)	All sectors/All Hazards	Policy, decision makers	Rapid decision making, prioritization of emergency operations	YES	NO	YES (implicitly)
CIPDSS (Critical Infrastructure Protection Decision Support System)	All sectors/All Hazards	Policy makers	Risk informed design	YES	YES	NO
CIPMA (Critical Infrastructure Protection Modeling and Analysis)	Energy, Communications, banking and finance/All hazards	Policy makers, industry	Prevention, preparedness	YES	YES	YES (implicit)
COMM-ASPEN	telecommunications, electricity, finance	Policy makers	Impact assessment of ICT disruption	YES	NO	NO
COUNTERACT (Generic Guidelines for Conducting Risk Assessment in Public Transport Networks)	Transport, Energy/ Terrorist threats	Operators, asset managers	Risk reporting, Protection measures effectiveness evaluation	NO	NO	NO
DECRIS	All sectors/All Hazards	Policy makers, operators	Risk and Vulnerabilities assessment, prioritization of scenarios	YES	NO	YES (partially)
EURACOM	All sectors/All Hazards	Policy and Decision makers	Holistic, cross sectoral risk assessment	YES	YES	NO
FAIT (Fast Analysis Infrastructure Tool)	All sectors/All Hazards	Policy and Decision makers	Interdependencies Assessment and disruption impact	YES	Partial (economic impact)	NO
MIN (Multilayer Infrastructure Network)	Transport/ Technical hazards	CI operators and decision makers	Optimal allocation of resources for CIP	YES	Partial (consequences)	NO
Modular Dynamic Model	All sectors/technical hazards	CI operators and decision makers	Failure propagation effects by simulation	YES	Partial (consequences)	NO
N-ABLE (Next-generation agent-based economic laboratory)	All sectors/technical, economic hazard	CI analyst, researchers	Failure propagation effects in term of economy losses by simulation	YES	Partial (consequences)	NO
NEMO (Net-Centric Effects-based operations MOdel)	All sectors/technical hazards	CI operators and decision makers	What if analysis under Malicious attacks	YES	Partial (consequences)	YES
NSRAM (Network Security Risk Assessment Modeling)	All sectors/technical hazards	CI operators and decision makers	What if analysis under Malicious attacks	YES	Partial (consequences)	YES
RAMCAP Plus	All sectors/technical hazards	CI operators and decision makers	Risk assessment and mitigation, multi-level, cross-sector	YES	YES	YES
RVA (risk and vulnerability analysis)	All sectors/ Technical, sociotechnical hazards	CI Decision makers	Risk assessment, qualitative	Not explicitly addressed	YES	NO
Sandia Risk Assessment Methodology	All Sectors/Terrorism, man-made	CI operators and decision makers	Risk and protection system effectiveness assessment	Not explicitly addressed	NO	Implicitly
CIA-ISM	**All sectors/All Hazards / CI networks**	**All users**	**Comprehensive analysis**	**YES**	**YES**	**YES**

Table 2. Comparison of risks analysis methodologies for Critical Infrastructures. Adapted from Giannopoulos et al., 2012

Where

P_i	Represents the occurrence probability of i event.
G_i	(Gamma factor) effect of all external events not specified within the model.
c_{ik}	Represents the impact of k event over i event. Positive c_{ik} means that it contributes to the occurrence of the event and negative that inhibits it.

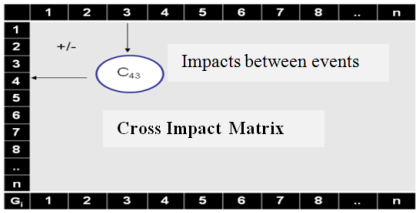

Figure 1. Cross Impact factors. Source: own elaboration.

CRITICAL INSFRASTRUCTURE CIA APPLICATION

Once CIA methodological basis have been revised let's show one application to a CI real context. The interaction to be shown has been made with one of the interviewed experts: the responsible of Data Processing Centre of a CI (public Research Centre) with juridical independence and financial funding plans through the Council for Innovation and Science from a local Government.

Determining events to be analyzed

The interviewed expert has to design a set of events close to the ones initially proposed. In our case, the scenario is set within the field of Information Systems Security as a partial scenario of crisis or emergency in a CI. It is also going to be carried out for validating the built working model. After this step, the following list of events is obtained (Table 3):

	Uncontrollable Events
1.	Very unfavorable economical context affecting to public financial funding
2.	Emergence of massive attacks to security
3.	Staff reduction for different causes (contracts failing, politics) shortage of qualified personnel to assist, not covering minimum places.
	Controllable Events
4.	Technological obsolescence in term of technological infrastructure.
5.	Lack of strategic/master plans for the research centre and DPC (Data Processing Centre), specific for the department.
6.	Compulsory implementation of 100% freeware policy
7.	Discontinuity in policies about compulsory electronic administration tools.
	Result Event
8.	Bring the entire institution into disrepute

Table 3. Expert Final Events

Results

Field work

The method is applied as it has been referred at preceding sections from the expert inputs about estimation of the events occurrence in the fixed time horizon (five years). Results from the expert inputs are listed below at table 4.

Event	P_i
1. Very unfavourable economical Situation.	0.7
2. Emergence of massive attacks to security.	0.7
3. Staff reduction, not covering minimum places.	0.6
4. Technological obsolescence.	0.2
5. Lack of strategic/master plans.	0.6
6. Compulsory implementation of 100% freeware policy.	0.8
7. Discontinuity in policies about compulsory tools of electronic administration.	0.6
8. Bring the entire institution into disrepute.	0.3

Table 4. Overall Probabilities estimated.

Namely, it is obtained a structural model which can be used as input for the following phase.

Cross Impacts Matrix

Based on the estimated overall and conditional probabilities is obtained cross impacts factors matrix (table 5) using the software developed with this purpose (see http://cim.criticaleventlab.org/). Both arrows and columns of the matrix are the events, and the cells are cross impacts factors or influence factors C_{ik}. Associated to this matrix is Gamma vector, who represents the influence of external events to the model over every of *i* events. G_i arrow is zero, because considered events (internal) do not influence to external (not considered) but in reverse they do (See Figure 1 and Table 5).

	1	2	3	4	5	6	7	8	G_j
1	OVP	0	0	0	0	0	0	0	0.85
2	0.33	OVP	0	0.67	1.08	0.29	0	0	-0.39
3	3.72	0	OVP	-0.76	0.34	0.26	-0.36	0	-2.24
4	2.23	0	0	OVP	1.35	0	-0.9	0	-3.22
5	0.29	0	0	0.27	OVP	0	0	0	0.15
6	0	-1.16	0	-1.23	-1.35	OVP	-0.58	0	3.6
7	0	0	0	-0.76	0	-0.27	OVP	0	0.77
8	1.93	0.77	0.9	1.57	1.48	-0.29	0	OVP	-4.25

Table 5. Cross Impacts Matrix and G vector

Scenario Simulation

It is analytically possible to change initial probabilities of every individual event at the computer once all phases have been completed the first time and check the degree of influence of such change over the remainder events. In this sense we can list the most influencing events over the rest and even to detect by means of process internal indicators the incoherencies and inconsistencies in estimations. Similarly, gamma variation indicates us how much are we changing and explaining the reality with this model and its events (although examples and most of the charts are omitted because of space).

If we now use CIASS software (http://www.ciass.org/) for the simulations it can be encompassed a sensitive analysis. Here are displayed simulation results from the chosen following scenarios:

A. Good context
B. Staff shortage
C. Security attacks
D. Security attacks & Staff shortage
E. Economic crisis
F. Economic crisis & Staff shortage
G. Economic crisis & Security attacks
H. Economic crisis & Security attacks & Staff shortage

		A.	B.	C.	D.	E.	F.	G.	H.
Event	**Pi**	Pi	Pi	Pi	Pi	Pi	Pi	Pi	Pi
1. Very unfavorable economical Situation.	**0.7**	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
2. Emergence of massive attacks to security.	**0.7**	0.00	0.00	1.00	1.00	0.00	0.00	1.00	1.00
3. Staff reduction, not covering minimum places.	**0.6**	0.00	1.00	0.00	1.00	0.00	1.00	0.00	1.00
4. Technological obsolescence.	**0.2**	0.05	0.05	0.05	0.05	0.33	0.33	0.33	0.33
5. Lack of strategic/master plans.	**0.6**	0.55	0.55	0.55	0.55	0.62	0.62	0.62	0.62
6. Compulsory implementation of 100% freeware policy.	**0.8**	0.90	0.90	0.74	0.74	0.90	0.90	0.74	0.74
7. Discontinuity in policies about compulsory tools of electronic administration.	**0.6**	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70
8. Bring the entire institution into disrepute.	**0.3**	0.04	0.08	0.08	0.17	0.21	0.39	0.36	0.58

Table 6. Simulation changing overall probabilities. Source: http://www.ciass.org/

Among cases D, F and G it can be checked case F (see above) as the most influencing one over the event result ("Institution into disrepute"), apart from the most negative context (case H).

If we assume now as certain (p=1) events "Very unfavorable economic Situation" and "Staff reduction, not covering minimum places" –as we already know they have happened in reality - the model predicts (case F, table 6) "Bring the entire institution into disrepute" probably not to occurs (p=0.39), as it has happened in reality (case F, table 6).

This result hints at the idea of this working model is coherent. Once the expert is consulted after 5 years he fixes case F as the closest to reality not only at the three first controllable events but at the rest. Expert´s hypothesis about probabilities of the real scenario five years later is coherent with the feasible results given by the working model. There are coincidences in senses of mutual events influences and if we work out the percentage of deviation between the expert´s estimations on events 3, 4, 5, 6, 7, and the result of the simulation once we fix events 1 to 3 with the reality, it is found a 15% of non-explained variability among the rest of event.

We can conclude this allow us to validate both the tool and the working model.

CONCLUSION

European Council on June of 2004 urged to construct a global strategy for Critical infrastructures protection. There may be some pending issues for being improved within Risk Analysis field despite it has been researched in detail. In particular, related to risk identification, where we can detect and identify risks in terms of its probability of occurrence (despite the wide range of definitions of "risks").

This paper has made clear that the CIA approach makes a global contribution to the field of Critical Infrastructures Risk Management where traditional tools are not enough. This is mainly due to (1)the ability of this methodology for modeling complex systems and their uncertainty, since it could be implemented to any sector or type of hazard, mixing qualitative and quantitative variables, (2)its great functionality for feasible forecasting adding value to the organization, thus improving its decision making and its resilience to crisis, (3)the graphic-analytical

analysis of events interactions allowing to work with large group of them being a computer efficient tool, (4) The robust theory behind its basement that allows simulation and sensitivity analysis coming up to estimate probabilities of likely scenarios, (5)to allow critical events detection at likely risks scenarios within a critical infrastructure, to asses theirs interdependencies and their cascade effect.

Apart from its widespread use, the use of the above proposed methodologies would be fully justified where: (a) to work out the occurrence probabilities by means of subjective estimations makes sense, (b) experts collaboration is available, (c) events from the same risk scenario are heterogeneous, (d) abstract, hard to be quantified or their combined actions are difficult to be simulated (Yu et al, 1988), (e) a combination with Delphi simulation method is needed.

ACKNOWLEDGES

This research has been funded by the Spanish Ministry of Science and Innovation by means of research grant TIN2010-19859-C02.

REFERENCES

1. Bañuls, V.A, Turoff, M. and Hiltz, S.R. (2013). Collaborative Scenario Modeling In Emergency Management through Cross-Impact. *Technological Forecasting and Social Change*, 80(9), 1756–1774.
2. Bañuls, V.A. Turoff, M. y Lopez-Silva, J. (2010). Clustering Scenarios using Cross-Impact Analysis, *ISCRAM 2010*, Seattle, May 2010.
3. Bañuls, V.A. and Turoff, M. (2011). Scenario Construction via Delphi and Cross-Impact Analysis. *Technological Forecasting and Social Change* 78 (9), 1579–1602.
4. Bañuls, V.A. andSalmeron, J.L. (2007). A Scenario-based Assessment Model – SBAM. *Technological Forecasting and Social Change*, 74 (6), 750–762.
5. Bañuls, V.A. and Turoff, M. (2007). Scenario Construction via Cross-Impact, *The Network Nation and Beyond*. Newark.
6. Chermack, T.J. (2004). Improving Decision-making with Scenario Planning. *Futures*, 36 (3), 295–309.
7. Coates, J. F. (2000). Scenario planning.*Technological Forecasting & Social Change* 65, 115–123.
8. Duval, A. Fontela, E. y Gabus, A. (1974). Cross Impact: A Handbook of Concepts and Applications, in Portraits of Complexity, *Application of Systems Methodologies to Societal Problems*. Battelle-Geneva, Geneva.
9. European Union. COM (2005) 576 Green book about European program for critical infrastructures protection. *European Communities Comission*.
10. European Union. Directive 2008/114/EC, December 8th 2011 On the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection.
11. Giannopoulos, G., Filippini, R., Schimmer, M., (2012) Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. EUR 25286 EN - Joint Research Centre – *Institute for the Protection and Security of the Citizen*. Luxembourg: *Publications Office of the European Union.*
12. Godet, M. (1994). From Anticipation to Action. París: *UNESCO Publishing*.
13. Gordon, T. (1994). Cross-Impact Method. UNU´s Millennium Project Feasibility Study.
14. Harries, C. (2003) Correspondence to What, Coherence to What? What is Good Scenario-based Decision Making? *Technological Forecasting and Social Change*, 70(8), 797–817.
15. Lage, B.B., Bañuls, V. and Borges, M., L. (2013). Supporting Course of Actions Development in Emergency Preparedness through Cross-Impact Analysis, *ISCRAM 2013*, Baden-baden (Germany).
16. Lendaris, G. (1980). Structural Modeling, IEEE Transactions on Systems. *Man and Cybernetics*, SMC, 10–12.
17. Petit, F. D., Eaton, L. K., Fisher, R. E., McAraw, S. F., &Collins,Michael J.,

(2012). Developing an index to assess the resilience of critical infrastructure. International *Journal of Risk Assessment and Management*, 16(1-2), 28.

18. RD 704/2011. Spain. Royal Decree 704/2011, of 20th May, approving the regulations on critical infrastructures protection. *BoletínOficialdel Estado* of May 21st 2011, 121, 50808 –50826.
19. Rogers, C. D. F., Bouch, C. J., Williams, S., Barber, A. R. G., Baker, C. J., Bryson, J. R., Quinn, A. D. (2012). Resistance and resilience - paradigms for critical local infrastructure. *Proceedings of the Institution of Civil Engineers*. Municipal Engineer,165(2), 73.
20. Turoff, M. (1972). An Alternative Approach to Cross Impact Analysis, *Technological Forecasting and Social Change*, 3(3), 309–339.
21. Turoff, M., Bañuls, V. A., Plotnick, L., &Hiltz, S. R. (2014) Development of a Dynamic Scenario Model for the Interaction of Critical Infrastructures. *ISCRAM2014*, State College, U.S.
22. Van Notten, P.W.F, Rotmans, J., Van Asselt, M.B.A and Rothman, D.S. (2003). An updated scenario typology. *Futures* 35, 423–443.
23. White House, (2003). Report to Congress on Combating Terrorism. Office of Management and Budget.
24. Yu, X. M.; Pen, W. B., (1988). Carlo method for risk analyses of climatic damage affecting the yields of crops Agricultural and Forest Meteorology, 43(3-4), 183–191.

Short Paper – Analytical Modeling and Simulation
Proceedings of the ISCRAM 2015 Conference - Kristiansand, May 24-27
Palen, Büscher, Comes & Hughes, eds.