An Overview of Critical Infrastructure Analysis Software

Christos Koukoumialos, George Stergiopoulos

christoskuku@hotmail.com, geostergiop@aueb.gr

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece

Critical infrastructures are the backbone of our nation's economy, security, and health. Consequently, maintaining the operation of critical infrastructures as stable as possible should be our main concern. This can only be achieved through critical infrastructure analysis software tools. Their main use is to analyze the interconnections (interdependencies) between multiple critical infrastructures and presents us with accurate results. In this way we are able to prevent accidents that could be catastrophic or even fatal. In this thesis, we are going to present the background knowledge of critical infrastructure protection (CIP) as some of these tools and explain the main steps of CIP.

Definitions

In order to comprehend the main section of our results it is vital to explain the next definitions:

• **Critical Infrastructure Sectors**: Every critical infrastructure (CI) can belong to one or more CI sectors depending on the area that directly or indirectly affects. Usually it's easy to define the main sector that belongs to, but the tricky part is to define the secondary, less obvious, sectors.

• **Critical Infrastructure Approaches**: CI approaches are techniques of making CI tools and their are chosen by the intended functionality of every tool. Of course, all approaches serve risk assessment purposes but there are some unique characteristics to every approach and in this research the tools are categorized by the main five types of existing modelling and simulation approaches that are presented at Ouyang's paper [1].

•**Critical Infrastructure Interdependencies** : The notion that a nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, is pretty obvious. Having this in mind what "interdependencies" stand for are the interconnections that exist between multiple CIs.

Table 1 shows the five (5) main approaches as referred at Ouyang's paper [1] and the sixteen (16) sectors as referred at the official site of the Department of Homeland Security [2].

Approach	Sectors	
Agent based	Chemical	Food and Agriculture
Network based	Commercial Facilities	Government Facilities
Empirical	Critical Manufacturing	Healthcare and Public Health
System dynamic based	Dams	Information Technology
Economic theory based	Defense Industrial Base	Nuclear Reactors, Materials, and Waste
Other	Emergency Services	Transportation Systems
Undefined	Energy	Water and Wastewater Systems
	Financial Services	Communications

***Table 1**: Approach and Sector list*

Categorization Tables of CIP Tools

Our results are mainly presented on a table. ***Table 2*** shows an example of this presentation. Each tool's approach is mentioned next to the tool. Every approach that is marked with the * symbol indicates that it's approach is defined by the manufacturer of the tool and couldn't be categorized by the aforementioned approaches. The next column shows the tool's main purpose of use and in the last column are presented the sectors that this tools affiliates with.

CIP Tools	Approach	Purpose	Sector
HURT [7]	Empirical	Hurricane relocation	HPH

***Table 2**: example of CIP tool presentation*

Also, ***Table 3*** shows a further presentation example of frameworks. Frameworks are set of tools that co-operate and serve a new and more complete purpose.

Frameworks	CIP Tools	Approach	Purpose	Sector
CIPR/Sim [6]	RTDS	Electromagnetic transients program simulation*	Testing the dynamic behavior of the power systems in real time	E
	QualNet	Network based	Telecommunication analysis	C
	PC Tides	Mathematical equation*	Wind speed and flood surge analysis	HPH, ES

***Table 3**: example of framework presentation*

Conclusions and Results

Our research showed some interesting results upon CIP tools approach distribution. Through a collection of seventy (70) CIP tools the most common approach proved to be the agent based approach with twenty four (24) tools followed by the network based with sixteen (16), empirical with nine (9), system dynamic based with two (2) and last by the economic theory based with only one (1) tool. ***Figure 1*** shows a pie chart of the results in a more compact way.

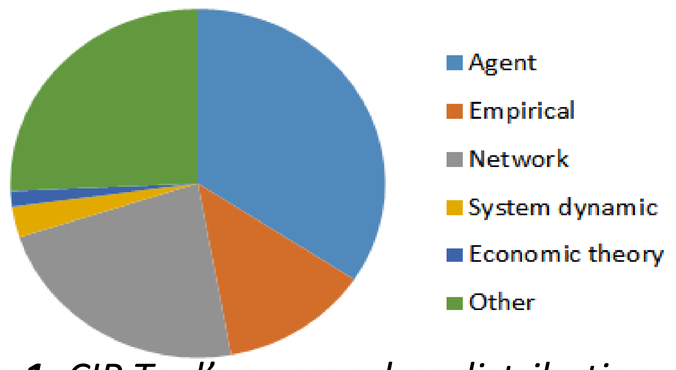

***Figure 1**: CIP Tool's approaches distribution*

References

1. Min Ouyang. "Review on modeling and simulation of interdependent critical infrastructure systems", Reliability Engineering and System Safety, www.journals.elsevier.com/reliability-engineering-and-system-safety, June 2013.
2. Critical Infrastructure Sectors, Dept. of Homeland Security, http://www.dhs.gov/critical-infrastructure-sectors, accessed 25 April 2015.
3. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", International Journal of Critical Infrastructures, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection (CIP-2013), pp. 171-182, Springer (AICT 417), USA, March 2013.
5. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in Proc. of the 6th International Conference on Critical Infrastructure Security (CRITIS-2011), pp. 104-115, Springer (LNCS 6983), 2013.
6. NISAC Tools, Los Alamos National Laboratory, http://www.lanl.gov/programs/nisac/tools2.shtml, accessed 26 May 2015.
7. Rainey L., Tolk A., "Modeling and simulation support for System of Systems Engineering Applications", March 2015.
8. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", International Journal of Critical Infrastructure Protection, September 2015.
9. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Using centrality metrics in CI dependency risk graphs for efficient risk mitigation", in Proc. of the 9th IFIP International Conference on Critical Infrastructure Protection (CIP-2015), Springer, USA, March 2015.
10. Stergiopoulos G., Theoharidou M., Gritzalis D., "Using logical error detection in Remote-Terminal Units to predict initiating events of Critical Infrastructures failures", in Proc. of the 3rd International Conference on Human Aspects of Information Security, Privacy and Trust (HCI-2015), Springer, USA, August 2015.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent critical infrastructures", International Journal of Risk Assessment and Management, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
12. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer Criticality Assessment methodology based on interdependencies", Computers & Security, Vol. 29, No. 6, pp. 643-658, 2010.
13. Theoharidou M., Xidara D., Gritzalis D., "A Common Body of Knowledge for Information Security and Critical Information and Communication Infrastructure Protection", International Journal of Critical Infrastructure Protection, Vol. 1, No. 1, pp. 81-96, 2008.
14. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection", in Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009), C. Palmer, S. Shenoi (Eds.), Springer, USA, March 2009.
15. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer Criticality Assessment methodology based on interdependencies", Computers & Security, Vol. 29, No. 6, pp. 643-658, 2010.
16. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability (ICGS3-2011), pp. 171-178, Springer (LNICST 0099), Greece, 2012.