Risk Mitigation for Critical Infrastructures: Research Initiatives

George Stergiopoulos, Panagiotis Kotzanikolaou, Marianthi Theocharidou, Dimitris Gritzalis

July 2015

Risk Mitigation for Critical Infrastructures: Research Initiatives

George Stergiopoulos [1], **Panagiotis Kotzanikolaou** [2],

Marianthi Theocharidou [3], **Dimitris Gritzalis** [1]

[1]. INFOSEC Laboratory, Dept. of Informatics,
Athens University of Economics & Business, Greece

[2]. Dept. of Informatics, University of Piraeus, Greece

[3]. European Commission, Joint Research Centre,
Institute for the Protection and Security of the Citizen, Italy

Outline

Critical Infrastructures: *The heart of a Nation*

- Need for high-level multi-sectoral risk assessment

Basis: *A Multi-risk dependency analysis methodology*

- Modeling cascading and common-cause failures

Current research: *Extending dependency analysis*

I. Time-based analysis of cascading and common cause failures

II. Risk mitigation strategies based on graph centrality analysis

Conclusions and future work: *The road so far*

Critical Infrastructures: The heart of a nation

- **Critical Infrastructure:** *"An asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens." (Directorate-General of Migration and Home Affairs, the European Commission)*

- Backbone of a nation's economy, security and health.
  - Provide Energy and Transport
  - Support transportation and communication systems
  - Must be protected against all types of hazards along with their services and systems
  - Failures can be cross-border. Particular valid in Europe since many Member States are affected (e.g. blackouts)

Critical Infrastructures: The heart of a nation

- Critical Infrastructures (CIs) can be modeled as cyber-physical systems
  - Inherently complex systems
- Interconnected and interdependent with other CIs
  - Different sectors (such as energy, ICT or transportation)
  - Failure in one infrastructure may affect operation of others
- Protection from dependency failures an active and recent area of research
  - Goal make key nodes more resilient (avoid propagation of failures)

Critical Infrastructures: Multi-sectoral risk assessment

Disruptions in CIs usually categorized as:

- ***Cascading failure***: Disruption in infrastructure A affects >1 components in infrastructure B. Partial or total unavailability of B
- ***Escalating failure***: Disruption in one infrastructure exacerbates independent disruption of another infrastructure
  - Usually by increasing severity or time needed for recovering
- ***Common-cause failure***: Two or more infrastructure networks are disrupted at the same time
  - Components within each network fail because of some common cause
  - Infrastructures usually co-located (geographic interdependency) or if root cause of failure is widespread (e.g. a natural or a man-made disaster)

Basis: A multi-risk dependency analysis methodology

- ***Infrastructure Dependency***: "One-directional reliance of an asset, system, network, or collection thereof – within or across sectors – on an input, interaction, or other requirement from other sources in order to function properly"
- Modeled as directional graphs:
  - *Nodes* depict infrastructures or components
  - *Edges* depict infrastructure dependencies
- Estimations quantify the ***impact*** and ***likelihood*** of a disruption realized
  - Impact ($I_{i,j}$) and Likelihood ($L_{i,j}$) of edge connecting *i* to *j*

Research Initiatives: Extending dependency analysis

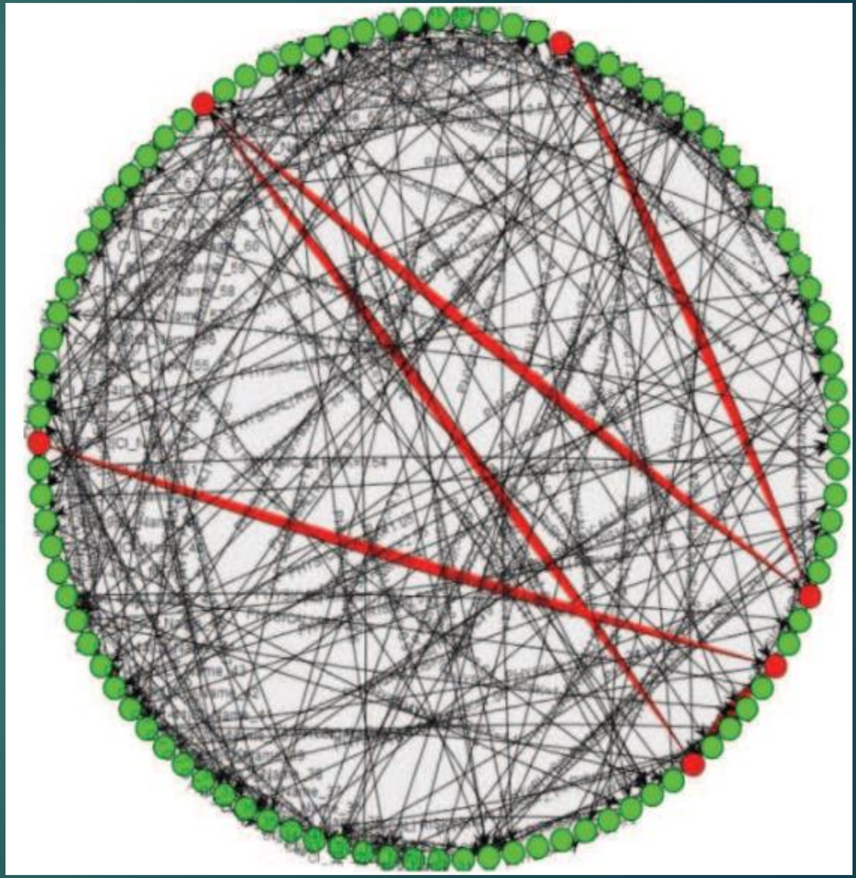
A. Time-based analysis of cascading and common cause failures (CIDA tool)

B. Risk mitigation strategies based on graph centrality analysis

Current research: Time-based analysis of failures

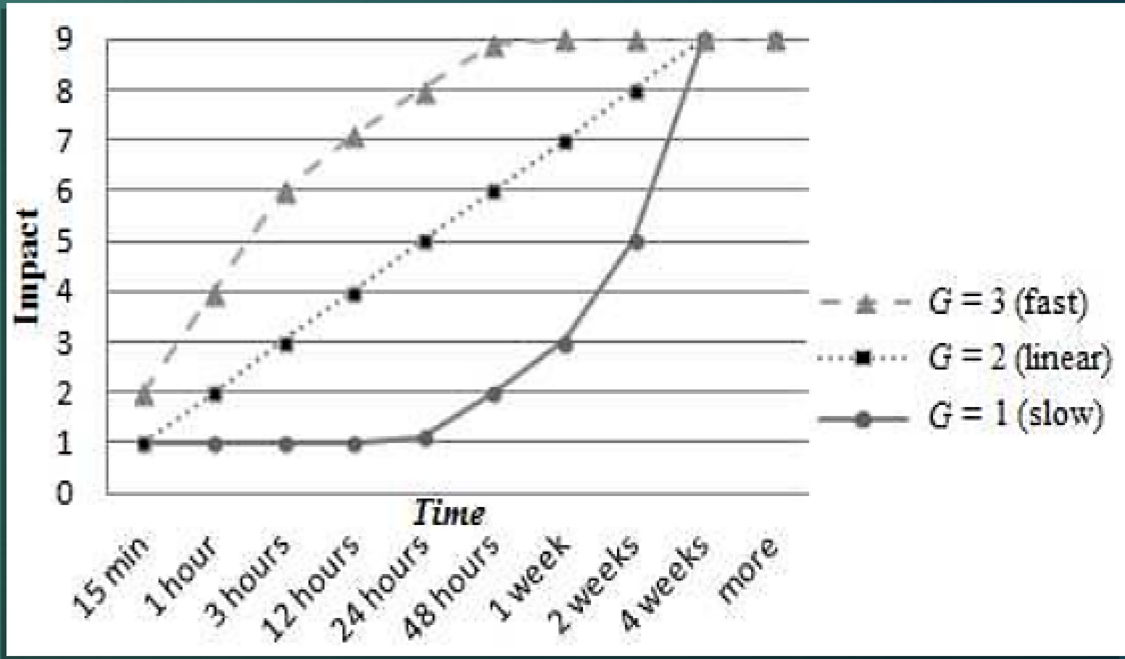
Critical Infrastructure Dependency Analysis (CIDA) tool

- Neo4J graph database
- Developed using Java
- Accepts risk assessment input
- Supports 17 different CI sectors, including communications, energy, transportation
- Computes risk for each individual dependency path



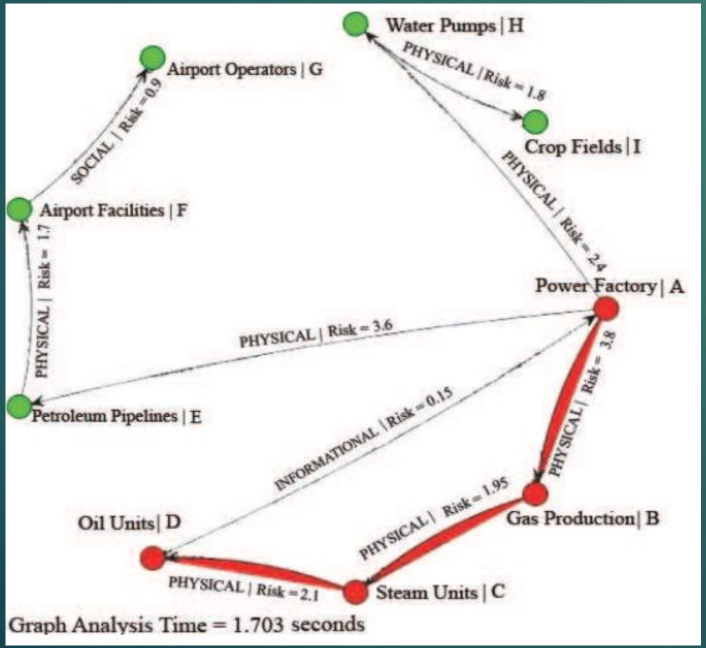
Current research: Time-based analysis of failures

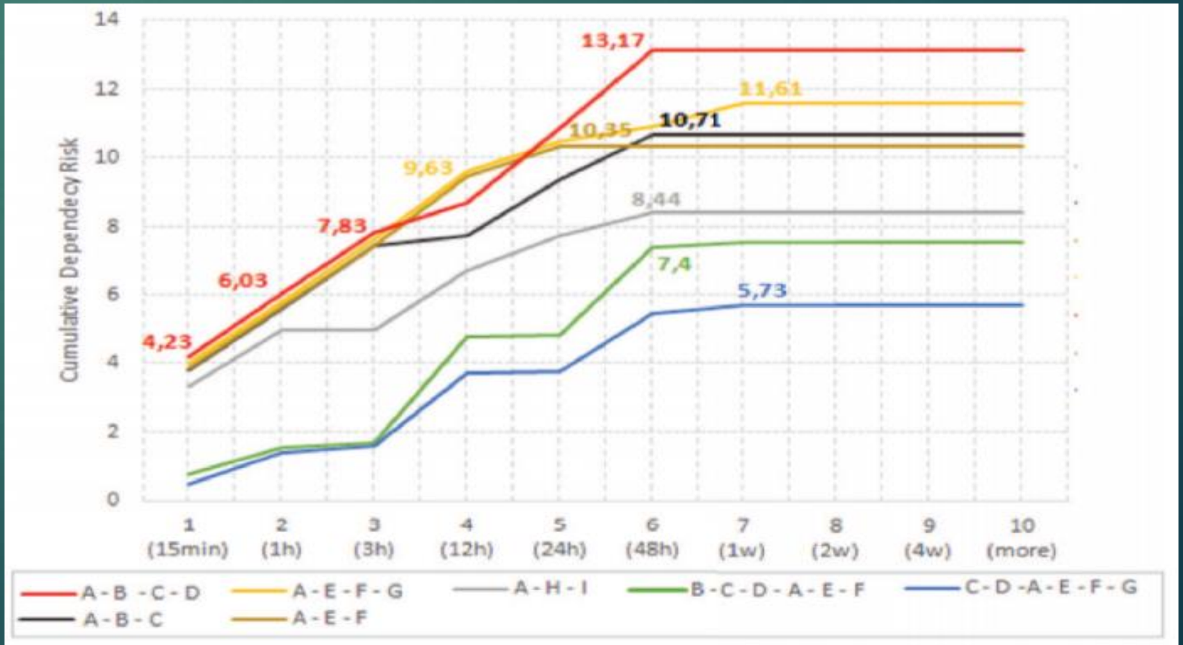
- Calculates edge (dependency) impact for each time slot
  - Gives estimate of impact progression from failures
- Values T and G provided by risk assessors
- Supports ***Slow***, ***Linear*** or ***Fast*** evolution of consequences after failure



Current research: Time-based analysis of failures

- Preemptive analysis detects dangerous risk paths
  - Pinpoints most critical paths for each time-frame of events
  - Detects the most critical path in each time slot after a cascading failure since our methodology can model different impact growth rates and time periods (path A-E-F-G).
  - Although path (A-B-C-D) is highest risk path, its sub-path (A-B-C) already exhibits impact higher than the threshold within 1 hour. Necessary to implement mitigation controls at the first or second order.





Current research: Risk mitigation using graph centrality

- Dependency chain analysis is not by itself sufficient for developing an efficient risk mitigation strategy
- We explore graph centrality metrics to design and evaluate effective risk mitigation strategies
  - ***Degree***, ***Closeness***, ***Betweenness***, ***Eccentricity*** and ***Eigenvector*** graph centrality metrics used
- Experiments based on random graphs that simulate CI dependency characteristics

Current research: *Risk mitigation using graph centrality*

- Feature selection used to ***detect correlations*** between high centrality metrics and CI nodes
- Metrics help ***detect dangerous CI nodes*** in dependency graphs
- Tests on 32,950 nodes extracted from 700 graphs with 774,015,270 paths

INFORMATION GAIN	Inbound Test	Outbound Test
Betweeness	0.259	0.277
Eccentricity	0.238	0.285
Closeness	0.387	0.345
Eigenvector	0.151	0.260
Intersection of all Centralities	0.176	0.248
Inbound degree (sinkholes)	-	0.302
Outbound degree	0.281	-

Table 1: Weka's output ranking using the Information Gain algorithm

GAIN RATIO	Inbound Test	Outbound Test
Betweeness	0.08	0.101
Eccentricity	0.08	0.101
Closeness	0.14	0.120
Eigenvector	0.06	0.09
Intersection of all Centralities	0.458	0.550
Inbound degree (sinkholes)	-	0.103
Outbound degree	0.101	-

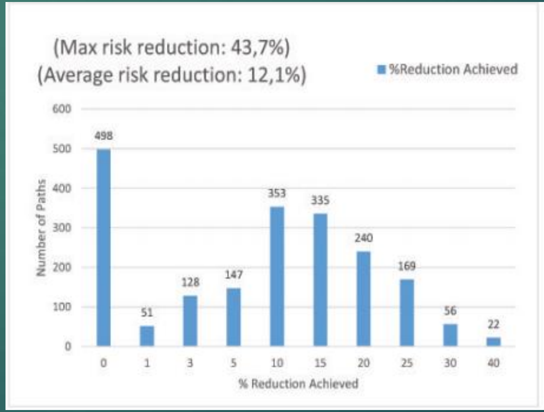
Table 2: Weka's output ranking using the Gain Ratio algorithm

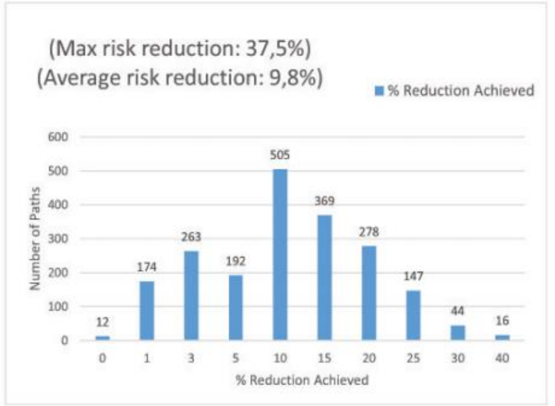
Current research: *Risk mitigation using graph centrality*

- Proposed ***algorithm*** for efficient risk mitigation strategy
- Algorithm ***selects best subset of CI nodes*** for risk mitigation
- Evaluated on 2000 random experiments
- Compared with two other mitigation strategies

Strategies / *Risk Metrics*	Information Gain	Top Initiators	Top Sinkholes
Most critical path	43.7% (max) 12.1% (avg)	38.4% (max) 11.8% (avg)	34.5% (max) 10.3% (avg)
Top 20 critical paths	37.5% (max) 9.8% (avg)	28.7% (max) 10.0% (avg)	29.8% (max) 7.3% (avg)
Entire graph	12.2% (max) 7.5% (avg)	10.1% (max) 5.3% (avg)	10.8% (max) 6.7% (avg)

Table 3: Comparison of results from all mitigation strategies





Conclusions and future work: The road so far

- Both initiatives complement each other
- Each one helps solve a different problem:
  1. Need for time-based analysis of impact evolution in failures
  2. Need to detect dangerous CI nodes that greatly affect the dependencies of interconnected infrastructures
- Test results from both initiatives look promising when evaluated on real-world scenarios

References

1. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, March 2009.
2. 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.
3. 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.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in *Proc. of the 6th International Workshop on Critical Infrastructure Security*, pp. 107-118, Springer (LNCS 6983), Switzerland, September 2011.
5. 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*, pp. 171-178, Springer (LNICST 99), Greece, 2012.
6. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk assessment of multi-order interdependencies between critical information and communication infrastructures", *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 151-170, IGI Global, 2013.
7. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, Nos, 1-2, pp. 93-110, 2013.
8. 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*, pp. 171-182, Springer (AICT 417), USA, March 2013.
9. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., *CIDA: Critical Infrastructure Dependency Analysis Tool*, https://github.com/geostergiop/CIDA, September 2014.
10. Stergiopoulos G., Theocharidou M., Kotzanikolaou P., Gritzalis D., "Using centrality measures in dependency risk graphs for efficient risk mitigation", in *Critical Infrastructure Protection IX*, pp. 25-40, Springer, 2015 (to appear).
11. 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 (to appear).
12. 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*, Springer (LNCS 9190), USA, August 2015 (to appear).