Time-Based Risk Analysis of Cascading Failures

Georgia Lykou, George Stergiopoulos

{lykoug, geostergiop}@aueb.gr

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business, Greece

One of the most challenging problems in Critical Infrastructure (CI) protection is the assessment and mitigation of cascading failures across infrastructures. A Time Based Risk Analysis extension of previous C.I. methods is presented, which assesses the risk arising from cascading failures, triggered by common-cause events.

Impact is evaluated by using a time-related, functional analysis, taking into account the type of vulnerability and time performance of contingency plans. Fuzzy Logic control is used in order to quantify interdependence Risk on a time axis, into a form of many-valued logic.

Example Analysis

California Black Out scenario of cascading effects is used as a proof-of-concept example.

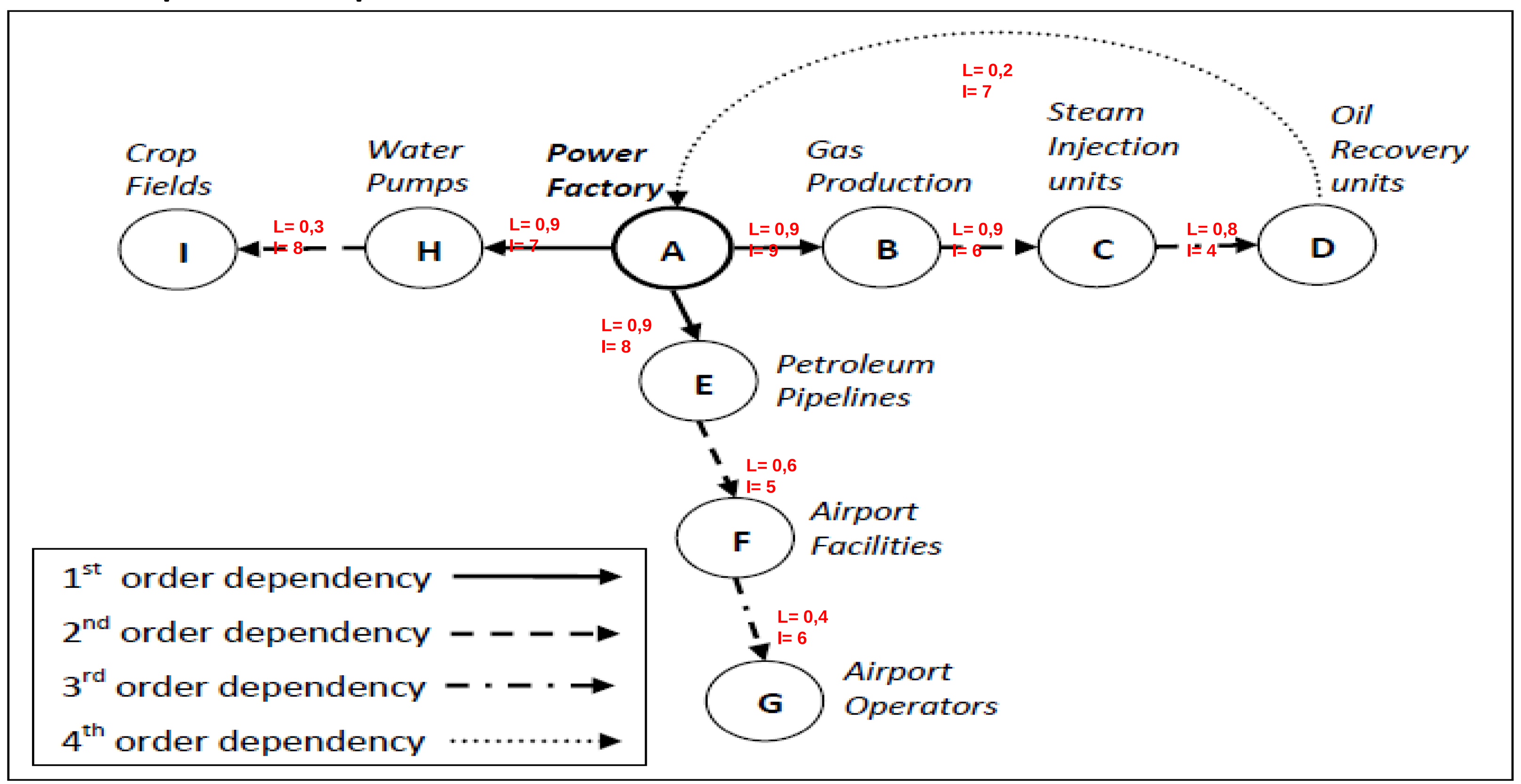


Figure 1: *California Black out Dependency Graph*

RISK PATH EVOLUTION THROUGH TIME

Time	Risk
15 min	4,49
1 hour	6,41
3 hours	8,32
12 hours	9,63
24 hours	11,38
48 hours	13,67
1 week	13,79
2 weeks	13,79
4 weeks	13,79
more	13,79

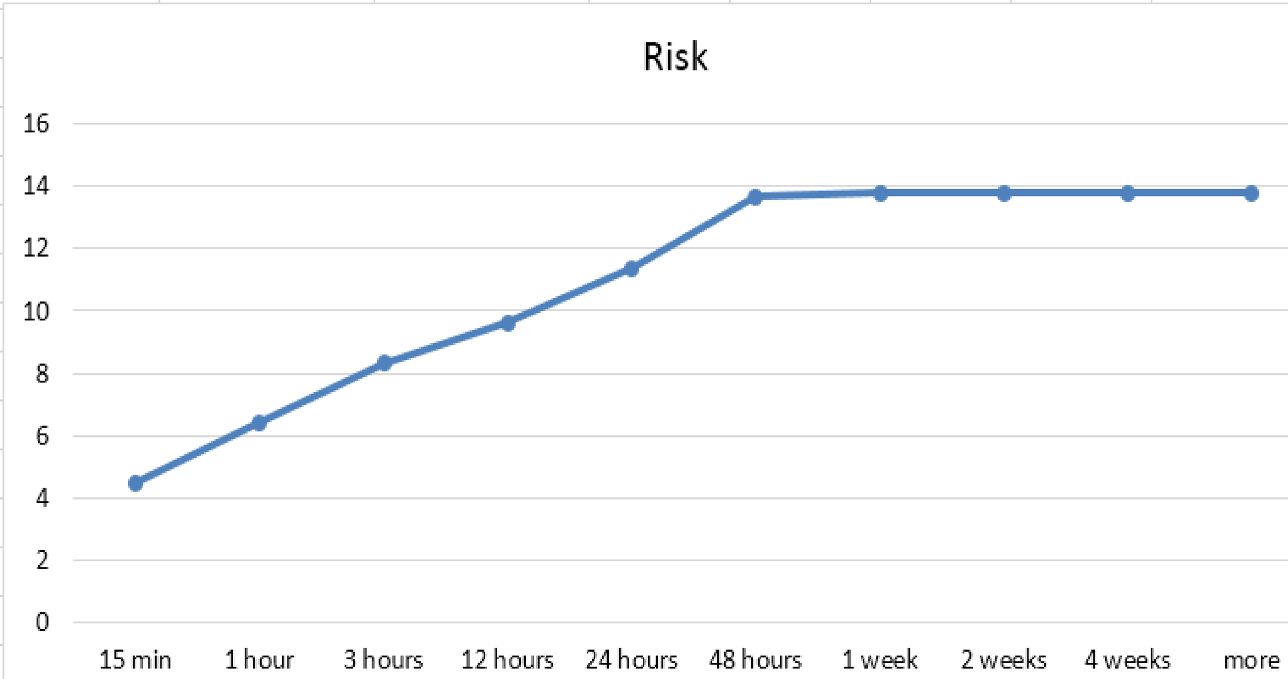


Figure 2: Example of *Sensitivity Analysis of Method*

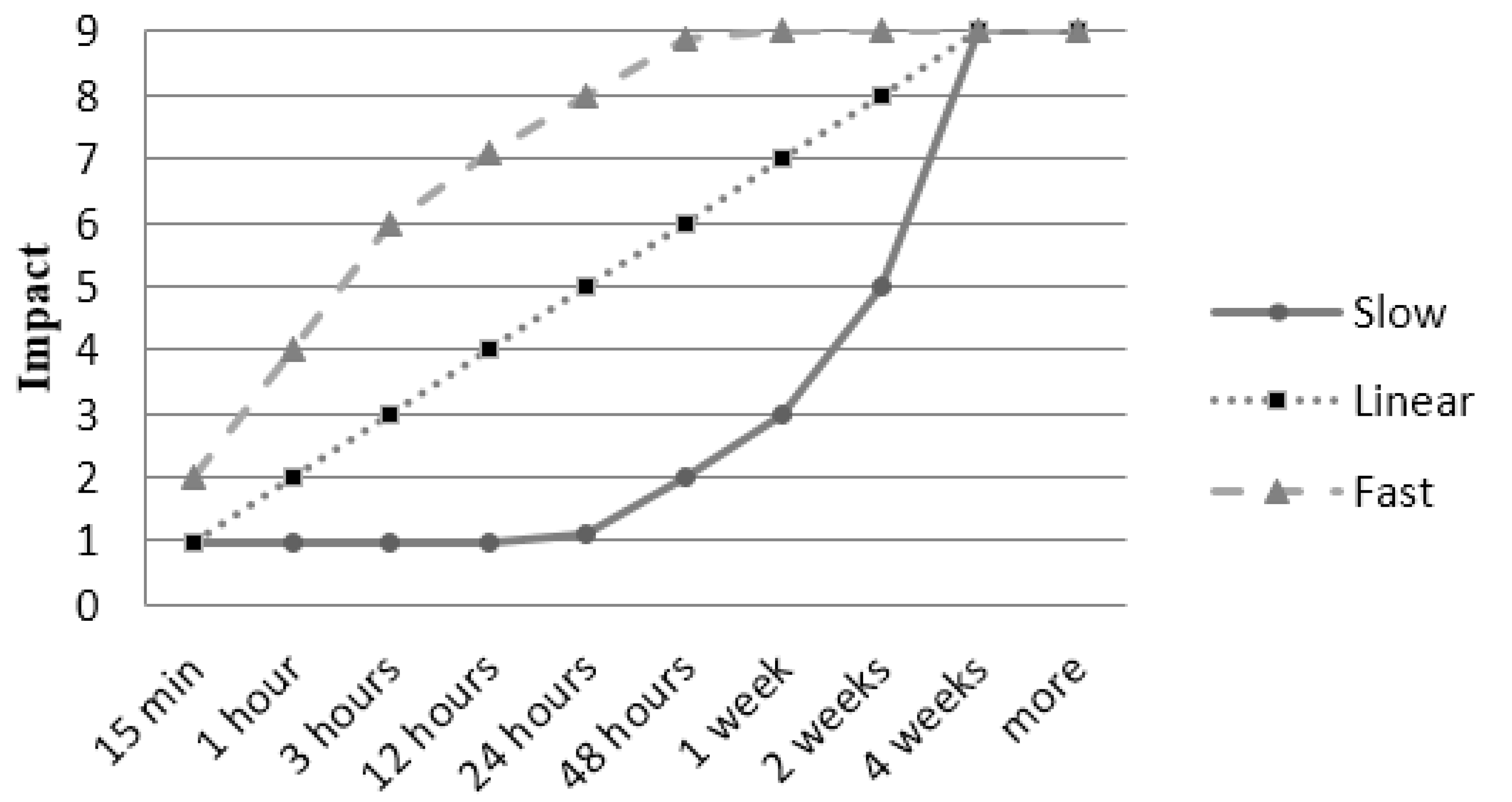
Dependency Risk chains (DRs) in Time points:

- Figure 2. depicts Risk of the most critical Cumulative critical path in each time point. Each graph point consists of a chain of Critical Infrastructure (CI) nodes.
- All CI nodes in each path have their own worst-case scenario: Impact rank, Time of occurrence and Impact evolution rate.
  - Slow Cascading Effects keep low Impact values at first but then show an exponential increase.
  - Medium cascading effects have a progressive evolution over time.
  - Fast Cascading develop slowly but radically increase after a specific time point.
- Overall DR evolution shows a close-to linear growth over time.

Time Related Impact

The impact is evaluated using a time-related functional analysis. Three different scenarios have been developed to approach variations of fast or slow cascading events. Evolution takes into account the type of vulnerability and time performance of contingency plans, using different evolution function.

Graph Representations:



Impact_T for ***Slow, Linear and Fast*** *cascading effects.*
Each one follows a different growth rate:
Slow (Exponential), Linear and Fast (Logarithmic)

Fuzzy Logic Control

We use a fuzzy Logic control system to quantify interdependence Risk on a time axis, into a form of many-valued logic. We experiment on real-world scenarios. Results show that the use of time related impact ranks is congruent with what is happening in common-cause failures.

Algorithmic steps of the method

- Step 1: Calculate 30 Impact Tables in 2D arrays: Impact/Time.
- Step 2: Input worst-case Impact and Time of occurrence from assessors.
- Step 3: Calculate Fuzzy membership sets = {Very Low ,Low , Medium, High ,Very High}.
- Step 4: Solve IF-THEN rules, calculate Fuzzy output and defuzzify to get a quantitative value.
- Step 5: Calculate Cumulative Dependency Risk with Impact_T for each time point in scale
- Step 6: Plot a graph with CDRs/time

Conclusions

- ✓ Results provided a sound and more accurate cascading risk analysis by taking into consideration a time-scale evolution scenarios and showed that the use of time related impact ranks is congruent with what is happening in common-cause failures.
- ✓ Capturing how interdependencies operate and lowering impact, when unavailability events are early confronted and restored, results in developing policies to improve recovery measures.

References

1. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D., "Assessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructures*, vol. 6, nos. 1/2, pp. 63–110, 2013.
2. 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 Information Infrastructure Security*, pp. 107-118, 2011.
3. 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, 2013.
4. 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, 2013.
5. Lekkas, D., Gritzalis, D., "e-Passports as a means towards a globally interoperable Public Key Infrastructure", *Journal of Computer Security*, Vol. 18, No. 3, pp. 379-396, 2010.
6. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D., "A multi-layer criticality assessment methodology based on interdependencies", *Computers and Security*, vol. 26(6), pp. 643-658, 2010.
7. 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.
8. Theoharidou, M., Gritzalis, D., "A Common Body of Knowledge for Information Security", IEEE Security & Privacy, vol. 4, no. 2, pp. 64-67, March/April 2007.
9. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D., "Risk-based criticality analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection* (CIP-2009), Springer, USA, 2009.
10. 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.
11. 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.