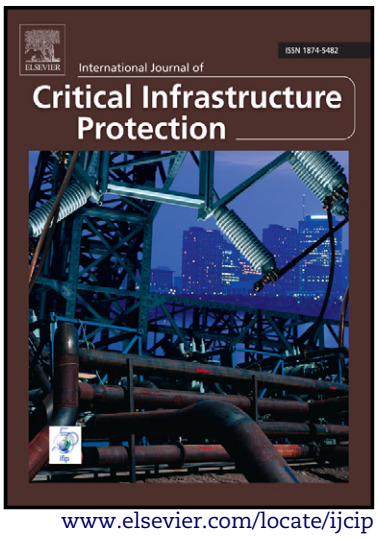

www.elsevier.com/locate/ijcip

A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures

Béla Genge, István Kiss, Piroska Haller

PII: S1874-5482(15)00024-4
DOI: http://dx.doi.org/10.1016/j.ijcip.2015.04.001
Reference: IJCIP160

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 12 January 2015
Revised date: 3 April 2015
Accepted date:
17 April 2015

Cite this article as: Béla Genge, István Kiss, Piroska Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, *International Journal of Critical Infrastructure Protection,* http://dx.doi.org/10.1016/j.ijcip.2015.04.001

A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures

Béla Genge,[1] István Kiss, Piroska Haller

Department of Informatics, Petru Maior University of Tirgu Mures, N. Iorga Street, No. 1, Tirgu Mures, Mures, 540088 Romania

Abstract

The massive proliferation of information and communications technologies (hardware and software) into the heart of modern critical infrastructures has given birth to a unique technological ecosystem. Despite the many advantages brought about by modern information and communications technologies, the shift from isolated environments to "systems-of-systems" integrated with massive information and communications infrastructures (e.g., the Internet) exposes critical infrastructures to significant cyber threats. Therefore, it is imperative to develop approaches for identifying and ranking assets in complex, large-scale and heterogeneous critical infrastructures. To address these challenges, this paper proposes a novel methodology for assessing the impacts of cyber attacks on critical infrastructures. The methodology is inspired by research in system dynamics and sensitivity analysis. The proposed behavioral analysis methodology computes the covariances of the observed variables before and after the execution of a specific intervention involving the control variables. Metrics are proposed for quantifying the significance of control variables and measuring the impact propagation of cyber attacks.

Experiments conducted on the IEEE 14-bus and IEEE 300-bus electric grid models, and on the well-known Tennessee Eastman chemical process demonstrate the efficiency, scalability and cross-sector applicability of the proposed methodology in several attack scenarios. The advantages of the methodology over graph-theoretic and electrical centrality metric approaches are demonstrated using several test cases. Finally, a novel, stealthy cyber-physical attack is demonstrated against a simulated power grid; this attack

[1]Corresponding author: Béla Genge (bela.genge@ing.upm.ro)