Two-layered Cyber-Physical System Simulation

Tobias Koch[1], Dietmar P. F. Möller[2], and Andreas Deutschmann[1]

[1] German Aerospace Center, Lilienthalplatz 7, 38108 Braunschweig
[2] TU Clausthal, Institute of Applied Stochastics and Operations Research,
Erzstraße 1, 38678 Clausthal-Zellerfeld, Germany

Abstract. With the increasing exposure of critical infrastructures to external factors, critical infrastructure protection gained attention within security research. To develop protection methods the effect of external factors on critical infrastructures has to be known. In this paper we present an event-based, dynamic modeling approach using power flow analysis and network flow analysis to simulate the effect on the critical infrastructure with object-based programming. The highly interconnected cyber-physical system is defined as a two-layered system with separated cyber and physical properties. Network stability and cyber infection status is checked with two control feedback loops to maintain grid stability and to observe infection status. Therefore with given object load powers and network interconnections the working capability of infrastructure parts can be predicted for various scenarios.

1 Introduction

Due to an increasing number of cyber-attacks and damage related to them [1], cyber-security gained a lot of attention not only in the media, but also from governmental side. The main interest from governmental side is critical infrastructure protection (CIP) [2,3]. Nowadays critical infrastructures (CIs) have to be considered as cyber-physical-systems (CPS) i. e. their operability depends on information and communication technology (ICT) and physical properties such as power supplies. Control systems build the interface between the physical and cyber level and are therefore an excellent point to attack a CPS. Cyber attacks on these control systems occurred in many different types of CIs e.g. water services [4], nuclear power plants [5], or electricity distribution stations [6]. Incidents are not always caused by human attacks. Especially the CI power supply is vulnerable to environmental hazard (falling trees, geomagnetic storms etc.) or even human failures [7]. To improve the resilience and preparedness of CIs we have to understand the impact of external factors on the system. Modeling and simulation approaches are powerful tools to gain knowledge about complex systems and help to identify vulnerable points within the system. This is one of the most important parts within risk management and a necessary step to develop emergency plans in case of successful cyber attacks. Therefore, a time dependent operability check for network components is needed from the physical as well as the ICT side.

2 Cyber-Physical System Simulation

We use a two-level network system for our description of the cyber-physical system. The first one describes physical and the second one ICT properties. In addition lists with all directly connected objects are assigned to each single object for both levels. Due to power line communication physically connected objects are also considered to be connected on ICT level. To check operability at each timesteps we use two control feedback loops. The first one checks wether voltage and frequency are within a tolerance interval that enables operability and the second one is the status of software infection of the object. The input for this feedback loops is calculated via a dynamical load flow analysis and network infection flow.

2.1 Load Flow Dynamics

The principle of static load flow analysis is a commonly used method to determine the voltages and phases within power distribution systems at given load powers [8] via solving a system of non-linear equations with iterative methods. As load power conditions at object i vary over time we introduce time dependent apparent power $S_i(t_j)$ as a dynamic boundary condition. Repeating the load flow analysis at several time steps leads to a time-series for voltage magnitude $U_i(t_j)$ and phase $\phi_i(t_i)$. The frequency can be obtained by the change of phase with time (1). The timestep Δt to resolve f_{max} is limited by the Nyquist-Shannon sampling theorem via $\Delta t_{max} = \frac{1}{2f\,\mathrm{max}}$.

$$f(t) = \frac{1}{2\pi}\frac{d\phi}{dt} \approx \frac{1}{2\pi}\frac{\Delta\phi}{\Delta t} = \frac{1}{2\pi}\frac{\phi_{n+1} - \phi_n}{t_{n+1} - t_n} \tag{1}$$

Under the constraints that the voltage magnitudes $U_i(t_j)$ and frequency $f_i(t_j)$ determined for object i at time t_j is within an a priori defined tolerance interval and that the source is able to deliver the demanded power, the operability of object i on physical side is guaranteed. If the grid is not stable, load shedding schemes are used to balance demanded and supplied power.. In addition blackouts can be simulated by directly setting object working status to false.

2.2 Network Infection Flow

We represent the ICT network level as an undirected, weighted graph. This weights are introduced to combine all factors affecting propagation time like the operating system, computer architecture, data transfer rate, type of connection, used protocols and encryptions or security precautions into one macroscopic measure (in seconds) being a weighting parameter w_{ij} for the edge between objects i and j. If objects i and j are not connected w_{ij} is set to infinity. From there on Dijkstra algorithm is applied to determine the shortest path from the intrusion point of the network, which is defined within the cyber attack event. This pathlength sets the time $t_{i,inf}$ for an infection of object i. The second control loop checks whether the for the object indispensable applications are affected or not. This is done via a simple comparison of listed properties of the object and the defined event. If the software is afflicted, the objects functionability is set to false.

3 Conclusions

A new simulation approach for CPS was presented that is based on a two-layered network approach, dividing physical from software properties. The static load flow analysis, know from electrical engineering, was enhanced to a time-dependent network stability control method driven by dynamic boundary conditions. Occuring events may trigger (partial-)blackouts or the intrusion of malicious software. The propagation time of the infection within the network is calculated via solving the shortest graph problem in an undirected graph with weighted edges.

Though, this approach needs a lot of information about the network structure, the consideration of expert knowledge is possible. Moreover, even in more modern CIs the data needed for data-driven machine learning approaches [9] is not available. As the simulation approach can be adapted to other CIs, the application within the field of CIP might be very diverse. However, a lot of work has to be done, while connecting the operability of single objects or object groups with CI specific processes.

References

1. "Managing cyber risks in an interconnected world - Key findings from The Global State of Information Security Survey 2015," PricewaterhouseCoopers International, Tech. Rep., 2014.
2. "Critical Infrastructure Protection - Challenges and Efforts to Secure Control Systems," U.S. Government Accountability Office, Tech. Rep., 2004.
3. "On a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure," 2013.
4. M. Abrams and J. Weiss, "Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia," The MITRE Corporation Applied Control Solutions, Tech. Rep., 2008.
5. B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights, Tech. Rep., 2011.
6. "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center, Tech. Rep., 2016.
7. "Report by the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways on the disturbance in the German and European power system on the 4th of November 2006," Bundesnetzagentur, Tech. Rep., 2007.
8. J. J. Grainger and W. D. Stevenson Jr., *Power System Analysis*, 1st ed., ser. Electrical and Computer Engineering. McGraw-Hill Education, 1994.
9. O. Niggemann, G. Biswas, K. J. S., H. Khorasgani, S. Volgmann, and A. Bunte, "Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control," in *International Workshop on Principles of Diagnosis*, 2016.