Reliability Engineering and System Safety 165 (2017) 89–101

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Hybrid systems modeling for critical infrastructures interdependency analysis☆

Constantinos Heracleous, Panayiotis Kolios, Christos G. Panayiotou*, Georgios Ellinas, Marios M. Polycarpou

KIOS Research and Innovation Center of Excellence, Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus

ARTICLE INFO

Keywords:
Critical infrastructure systems (CISs)
Interdependencies analysis
Hybrid systems
Open hybrid automata
Cascading failures

ABSTRACT

Critical infrastructure systems (CISs) are large scale and complex systems, across which many interdependencies exist. As a result, several modeling and simulation approaches are being employed to study the concurrent operation of multiple CISs and their interdependencies. Complementary to existing literature, this work develops and implements a modeling and simulation framework based on open hybrid automata to analyze CISs interdependencies. With the proposed approach, it is possible to develop accurate models of infrastructure components, and interlink them together based on their dependencies; in effect creating larger and more complex models that incorporate interdependencies. By implementing specific setups using varying operating conditions, one can study the cascading effects of interdependencies, perform a detailed vulnerability assessment and conduct an extensive planning exercise. To demonstrate the applicability of the proposed framework, a setup with three different types of CISs (i.e., power, telecom and water) components is investigated. Extensive simulation results are used to provide insights on the cascading effects, vulnerabilities and maintenance planning strategies.

1. Introduction

Critical infrastructure systems (CISs), such as power distribution systems, telecommunications networks, and water distribution networks, provide the necessary services that are vital to the security and well-being of the society. Disruption, damage or complete destruction to these infrastructures, due to natural disasters, accidents or malicious attacks, can have significant negative consequences and thus actions, to improve their protection and reliability, are of paramount importance [1].

Although each CIS is usually treated as an individual system, all CISs are highly interconnected with various interdependencies among them. For example, communication systems need a steady supply of electricity to maintain a good quality of service (QoS), while electric systems need reliable communications to maintain an accurate system state estimation. These bidirectional relationships between infrastructures enhance their overall performance, but at the same time increase their complexity and vulnerability [2,3].

Interdependencies are often unnoticeable when CISs maintain their normal operations, however, they can become critical during failures (e.g., due to operation errors, aging, poor maintenance etc.), deliberate attacks and natural disasters [4]. Moreover, cascading interdependencies can increase the scale of destruction in multiple CISs. This was observed in a number of events worldwide, such as the 2001 World Trade Center Attack [5], the 2005 Hurricane Katrina [6], the 2011 Fukushima Daiichi nuclear disaster [7], and several others [8,3]. Interdependencies, based on their characteristics and effects on infrastructures, are classified into the following four principal types [2]: (a) *physical*, if the operations of one infrastructure depends on the physical output(s) of the other and vice versa, (b) *cyber*, if there is information/signal transmission between different infrastructures, (c) *geographic*, if components of different infrastructures are in close spatial proximity, and lastly (d) *logical*, due to any other mechanism (e.g., policy, legal, or regulatory regimes) that can link logically two or more infrastructures.

Currently, the best way to study the characteristics and operations of multiple interconnected CISs is through accurate modeling and extensive simulation, where interdependencies should be carefully considered [9]. For this reason, several solutions have been proposed in the literature (as discussed extensively in Section 2). However, there is still a need to develop new and more accurate frameworks that will more closely represent component dependencies and handle the

☆ This work is supported by the European Research Council Advanced Grant FAULT-ADAPTIVE (ERC-AdG-291508).

* Corresponding author.
E-mail address: christosp@ucy.ac.cy (C.G. Panayiotou).

http://dx.doi.org/10.1016/j.ress.2017.03.028
Received 5 August 2016; Received in revised form 8 February 2017; Accepted 22 March 2017
Available online 23 March 2017
0951-8320/

increasing complexity of larger system (as widely recognized in [3,10]). In accordance, this work introduces a framework based on open hybrid automata for modeling CISs interdependencies by adopting and extending our previous work in [11]. More specifically, the proposed framework uses open hybrid automata for modeling components of different CISs taking into account their dependencies. These models can be composed together to create even larger and more complex models which can then be used in detailed simulations to: i) study the cascading effects of (inter)dependencies, ii) perform vulnerability assessment, and iii) develop maintenance planning strategies. The main advantage of using open hybrid automata is the common modeling framework they provide, where generic CISs components can be modeled. Moreover, open hybrid automata allows the development of models at various levels of abstraction, i.e., very detailed models with many variables or quite simple ones, depending on the modeling objectives and the available data (more details on the modeling abstraction are provided in Section 3).

The important benefit of the proposed approach is that it provides a unified and convenient framework for modeling the various components that make up a critical infrastructure. The modeling framework allows to model both continuous-time and discrete-event dynamics and can easily incorporate decisions made by operators as well as component faults that may occur during operation. The various component models can be reused using composition to build bigger infrastructures and can be connected in various ways to capture different network topologies. Furthermore, the interconnections of the various components seamlessly capture the intradependencies in a critical infrastructure and the interdependencies between infrastructures. The modeling framework can be used to build large scale infrastructures through the model composition and reuse them to build larger models. At the same time, it is flexible to use more or less detailed models depending on the required level of abstraction such that it becomes more scalable during run time.

The rest of the paper is organized as follows. Section 2 summarizes the existing interdependency modeling approaches. Section 3 provides a short introduction to hybrid systems and explains why they are suitable for modeling CISs interdependencies. Section 4 describes the open hybrid automata framework for modeling components of different CISs, and also their composition with respect to their dependencies. Section 5 derives six open hybrid automata component models of three interdependent CISs (i.e., power, telecom and water), and then links them together to create an overall composition model. Section 6 identifies and analyzes the problems that can be tackled by the proposed framework, and Section 7 provides detailed analysis on the insights gained by applying the proposed framework in a simulation setup. Finally, Section 9 provides concluding remarks and future directions for research.

2. Related interdependency modeling approaches

Interdependency modeling is an emerging research field, that includes several innovative modeling approaches. Existing models are summarized and compared in several review works [12,3,13,10,14], making it quite easy to study the state-of-the-art. Among the most popular ones are the input-output methods, agent-based modeling and network based approaches.

Input-output methods are based on the economic equilibrium theory of W. Leontief, and they can estimate at a holistic level the inoperability (i.e., the percentage of malfunction) of infrastructures using the dependency coefficients (also known as Leontief coefficients). However, these coefficients are difficult to calculate correctly, thus they are generally high level approximations following the assumption that interdependencies are related to high economic interaction [15,16].

Agent-based modeling (ABM) approaches take advantage of the fact that CISs can be characterized as complex adaptive systems (CAS) (i.e., complex collection of interacting components that can be altered from learning processes). ABM uses a bottom-up design strategy, and the different CISs components are represented as autonomous agents with attributes, behaviors, and decision-making rules, while interdependencies usually emerge from the agent interactions [17,18].

Network based approaches generally assume that each CIS consists of a set of components (usually represented as nodes) forming a network, and any existing dependencies are represented as relationships between nodes belonging to different networks [19]. Using network-based models for interdependent CISs, it becomes quite easy to perform topological analysis (i.e., describe qualitative connectedness for a set of components). For functional analysis however, network-based models are quite poor. Usually they assume simplifying hypotheses, with functional models able to capture only the basic features of the networks and not the complex effects related to the exact technological implementations [4,20].

There are also several other approaches for modeling CISs interdependencies. For example, there are methodologies based on petri nets, stochastic activity networks and bayesian networks [21–23]. The System Dynamic (SD) approach was also used for interdependency modeling to determine the best allocation strategies from the available infrastructure services when CISs suffer disruptions [24]. Multi-layer modeling approach was also proposed, where infrastructures are seen at different layers (i.e., holistic, service, reductionistic, etc.), with interactions and functional relationships between components and infrastructures modeled at different levels of granularity [25]. Federated simulations using the High Level Architecture (HLA) standard were also used in interdependency modeling studies, with HLA generally acting as communication middleware between different infrastructure simulators, allowing the capture of interdependencies within a “system-of-systems” approach [26,27]. Lastly, empirical approaches have been used to analyze CISs interdependencies according to historical accident or disaster data, and expert experience [8].

So far, the approaches that have appeared in the literature may serve different purposes and have their strengths and weaknesses, but no single approach has become the state-of-the-art of the field. Furthermore, the difficulty in accessing data due to confidentiality and privacy issues, coupled with the fact that CISs are becoming increasingly larger and more complex, makes the validation of interdependencies quite challenging [3,10]. Thus, there is a need to further develop existing interdependency modeling approaches or to propose new ones that are both efficient and effective.

When dealing with critical infrastructures, scalability is an issue faced by all methods that can be used to model interdependencies simply due to the large scale involved in such infrastructures. The proposed approach is both modular and scalable in the sense that it allows for the flexibility of incorporating both highly accurate and simple models in an all-encompassing framework. Modularity is achieved through composition while scalability exists in two forms; scalability in building a model (topology and functionality) of the critical infrastructure as well as scalability in terms of the computational power required to run the model. In terms of modeling, the methodology allows for the composition of multiple models which can be made into higher level components that can be reused to build bigger models. Thus, one does not need to always start from a single component. For example a power plant is a collection of several generators. Thus, one can build the model of one generator and then reuse and connect several generators together to make the power plant. In terms of the needed computational power to run the model, again the methodology allows one to use the appropriate level of modeling abstraction. For example, a switch can be modeled by a simple 0/1 function or, if one requires to also capture the transient effects when a switch opens and closes, these can also be incorporated in the model at the expense of more computational power. The framework provided by hybrid automata allows accurate investigations to be conducted on component dependencies and system interdependencies for studying cascading effects, for vulnerability assessment and for proper planning, as shown in the sequel.