
Jing Lin, Sahra Sedigh (Advisor), and Ann Miller (co-Advisor)
Department of Electrical and Computer Engineering
Missouri University of Science and Technology
Rolla, MO, USA
Email: {jlpg2,sedighs,milleran}@mst.edu

Abstract

The overarching objective of the proposed doctoral research is to build a qualitative and quantitative understanding of dependability in cyber physical systems (CPS). The existing body of knowledge includes frameworks and techniques for assessment, modeling, and simulation of the physical and cyber infrastructures, respectively, but such isolated analysis is incapable of fully capturing the interdependencies between these infrastructures. Understanding these interdependencies is a critical precursor to accurate representation and modeling of the CPS as a whole, especially with respect to dependability.

The physical water distribution infrastructure, coupled with the hardware and software that support intelligent water allocation, comprise the model CPS that will be used as a case study for the proposed research. A preliminary literature review has been carried out on dependability modeling for CPS, with very sparse results. Allocation algorithms for water distribution have also been investigated, with game theory appearing to hold the most promise.

An agent-based approach is suggested for linking the cyber and physical layers, where the agents retrieve information from sensors monitoring the physical components and provide this information to the cyber components. Fault injection will be used to investigate the propagation of failures between the cyber and physical layers. Markovian models will be used to capture the manifestation of cyber and/or physical faults as failures in water allocation, or containment of contaminants.

1. Introduction and Problem Description

Major physical infrastructures such as water distribution systems and the electric power grid are large-scale complex systems that are expected to be highly dependable. Modern versions of these infrastructures go beyond simple measures such as redundancy to incorporate intelligence into the system through extensive use of cyber components. The need for communication and control creates a cyber-physical system (CPS) with two parallel networks: a physical network of interconnected components of the infrastructure, and a cyber network comprised of intelligent controllers and the communication links among them. These networks interact; however, there is no one-to-one correspondence between their respective components.

Understanding and quantifying the effects of introducing intelligence into physical infrastructures can help us determine how cautious we need to be in deployment of such systems, enabling more efficient use of resources. This can also show, quantitatively, whether the resulting CPS is more or less dependable than the physical infrastructure system it hopes to improve. The existing body of knowledge includes frameworks and techniques for assessment, modeling, and simulation of the physical and cyber infrastructures, respectively, but such isolated analysis is incapable of fully capturing the interdependencies between these infrastructures. Understanding these interdependencies is a critical precursor to accurate representation and modeling of the CPS as a whole, especially with respect to dependability.

The overarching objective of this work is to develop a qualitative and quantitative understanding of dependability in CPS. We plan to achieve this objective through the four following tasks, which overlap in time.

1) Building a qualitative understanding of interdependencies in CPS
2) Quantitative representation of these interdependencies
3) Characterizing CPS dependability in terms of attributes of the physical and cyber components
4) Validation of the models using simulation and field data

Physical components, e.g., valves, pipes, and reservoirs, of water distribution networks (WDNs), coupled with the hardware and software that support intelligent water allocation, comprise the model CPS that will be used as a case study for this analysis. An example is depicted in Fig. 1. The primary goal of WDNs is to provide a dependable source of potable water to the public. Information such as demand patterns, water quantity (flow and pressure head), and water quality (contaminants and minerals) is critical in achieving this goal, and beneficial in guiding maintenance efforts and
We propose to take a first step, but their utility is limited. Qualitative models are of particular interest to the proposed research, as they are capable of capturing component interactions of a system-level reliability model for CPS that incorporates the effect of failures in both cyber and physical components. Sophisticated interdependencies among these components prevent the application of simple multiplicative models that assume independence of failures.

Other challenges arise from fundamental differences between attributes of the cyber and physical layers, especially where process “flow” is concerned. As described earlier, the cyber layer is comprised of elements such as sensors, computers, and telecommunication links, all of which contribute to collecting, processing, and communication of the information used for intelligent control of the physical system. The resulting cyber network can be visualized as a graph, with “information” serving as the flow along the edges. Attributes of importance in this flow are correctness, throughput, etc. In contrast, the devices that comprise the physical layer include reservoirs, valves, and pipes. The physical layer can also be visualized as a graph, but the flow transported along the edges is water, with the attributes of importance identified as chemical composition (quality) and pressure (quantity). The lack of one-to-one correspondence between the elements of the graphs representing the cyber and physical layers, respectively, is a fundamental research challenge with implications on all aspects of the work, in identifying vulnerable areas requiring fortification and/or monitoring. Sensors dispersed in the physical infrastructure collect this information, which is fed to algorithms (often distributed) running on the cyber infrastructure. These algorithms provide decision support to hardware controllers that are used to manage the allocation (quantity) and chemical composition (quality) of the water. As WDNs become larger and more complex, their dependability comes into question. The increasing use of Supervisory Control and Data Acquisition (SCADA) systems also raises concerns about the vulnerability of WDNs.

The remainder of this paper articulates our proposed approach to quantifying dependability for CPS. Section 2 presents a review of related literature. The main challenges associated with this research problem are discussed in Section 3. Section 4 details our proposed approach to addressing these challenges, including preliminary work carried out thus far, and plans for extending this work and completing the doctoral research. Section 5 concludes the paper.

2. Background and Related Work

The most significant problem in the study of dependability in CPS in general, and critical infrastructure systems in particular, is quantifying the interdependencies between cyber and physical components of the system. System complexity has been cited as the main challenge [1]. Other challenges articulated in the same study are the low probability of occurrence of critical events, differences in the time scales associated with these events, and the difficulty of gathering data needed for accurate modeling.

A number of modeling and simulation techniques for critical infrastructure are enumerated in [2]. Among these techniques, agent-based models and Leontief input-output models are of particular interest to the proposed research, as they are capable of capturing component interactions in an accurate, yet simple, fashion. The autonomy and adaptivity of agents enables them to capture the intricacies of critical infrastructure [3], and a sufficiently diverse set of agents provides valuable robustness to the model [4]. Furthermore, agent-based modeling facilitates representation of the behavior of individual components of a distributed systems, as well as representation of the interconnections among them [5]. The Leontief model originates from a probabilistic model for capturing the interconnectedness among different economical sectors, and as such, lends itself well to representing interdependencies in a CPS.

Existing modeling techniques for CPS rely upon semantics to represent the relationship between the cyber and physical layers of a CPS, which is necessary for accurate modeling of any system. The main shortcoming of current solutions is their qualitative nature. Qualitative models are a first step, but their utility is limited. We propose to develop quantitative models representing various facets of dependability for a CPS, similarly based on understanding of the semantics of specific systems, in particular WDNs.

Among critical infrastructure systems, research on dependability of the power grid has matured to the greatest extent. A number of recent studies implicitly or explicitly approach the problem from a cyber-physical point of view, including [6], which qualitatively analyzes interdependencies among the electric power infrastructure and the information infrastructures supporting its management, control and maintenance. Of particular note is a related project by our group [7], where a quantitative reliability model has been developed that spans both cyber and physical aspects of the power grid. Despite the difference in the model CPS chosen (power vs. water), the insights gained represent a first step towards linking failures in the operation of the cyber network to their physical manifestation.

The reliability of WDNs, from a purely physical point of view, has long been a topic of interest to the civil engineering community, and is critical to semantic understanding of the physical side of the CPS in focus. Salient studies include Haimes’s work on inoperability modeling [8], which will be used as a basis for analyzing the reliability of the physical layer. The proposed research encompasses both cyber and physical aspects of WDNs, and supplements the probabilistic models developed for the physical layer with quantitative data gathered by the cyber components.

3. Main Research Challenges

The main research challenge, in brief, is the development of a system-level reliability model for CPS that incorporates the effect of failures in both cyber and physical components. Sophisticated interdependencies among these components prevent the application of simple multiplicative models that assume independence of failures.

Other challenges arise from fundamental differences between attributes of the cyber and physical layers, especially where process “flow” is concerned. As described earlier, the cyber layer is comprised of elements such as sensors, computers, and telecommunication links, all of which contribute to collecting, processing, and communication of the information used for intelligent control of the physical system. The resulting cyber network can be visualized as a graph, with “information” serving as the flow along the edges. Attributes of importance in this flow are correctness, throughput, etc. In contrast, the devices that comprise the physical layer include reservoirs, valves, and pipes. The physical layer can also be visualized as a graph, but the flow transported along the edges is water, with the attributes of importance identified as chemical composition (quality) and pressure (quantity). The lack of one-to-one correspondence between the elements of the graphs representing the cyber and physical layers, respectively, is a fundamental research challenge with implications on all aspects of the work, in identifying vulnerabilities in WDNs.
Another research challenge arises from the heterogeneity in cyber control of WDNs. The deployment of large-scale physical infrastructure networks is typically incremental. The addition of cyber components, or “intelligence,” to such physical networks is also incremental, resulting in heterogeneity in information representation and access, communication, and computational capabilities. Independent ownership and governance, and autonomy of different segments of the CPS exacerbate this heterogeneity, which complicates the development of a broadly applicable model.

4. Proposed Approach and Research Plan

We propose to use agent-based modeling for quantitative analysis of reliability in CPS. The agents will bridge the gap between the cyber and physical layers of a CPS, by serving as stewards for information representing attributes of both layers. An agent-based model can represent diverse characteristics and behaviors at high resolution, a feature essential to capturing the intricacies of CPS. More specifically, we plan to use a multi-agent model, as a centralized observation architecture would be a poor match for the highly distributed structure of the physical and cyber layers of a CPS [9]. Our choice is supported by related studies, including [3], which discusses in detail the suitability of the agent-based paradigm for modeling systems whose complexity renders traditional methods ineffective. Further support for the choice is lent by [10], which specifically investigates the application of agent-based modeling and simulation to the study of interdependencies in critical infrastructure, and reports that the method is capable of modeling such systems at different levels of abstraction.

Our first case study for model development will be an urban WDN, instrumented by sensors that quantify the volume, pressure, and aspects of the chemical composition of water at various locations in the city. The data from these sensors is communicated to a number of multiplexors for aggregation, then forwarded to a control center. Actuators, in the simplest form, valves, typically controlled by SCADA systems, utilize this data in conjunction with software algorithms to manage the quantity and quality of water allocated to various areas within the city. The availability of data that captures information such as usage, temperature, and precipitation patterns facilitates dynamic control of the WDN, which can increases system utilization and improve the reliability of water distribution.

4.1. Preliminary Work

The work completed thus far includes a comprehensive literature review on reliability modeling for CPS, in particular critical infrastructure; physical aspects of WDNs; and intelligent control of WDNs. A very concise summary is presented in Section 2.

We have also investigated appropriate modeling techniques, and have selected agent-based modeling, for the reasons outlined above. Furthermore, we have studied various simulators for the cyber and physical layers of WDNs, and mechanisms for linking the simulators to enable bi-directional data flow. For simulating the physical layer, EPANET 2.0 [11], which is an open-source software developed by Environment Protection Agency (EPA), was found to be an appropriate candidate, as it captures a wide range of attributes of the WDN, including water pressure, and presence and amounts of chemical elements such as fluoride or chlorine. We were unable to identify a single simulator capable of encompassing both communication and computation in the cyber layer. ns-2 [12] is capable of accurately representing the communication network. An overlay will be developed to represent the game-theoretic algorithm used
for control of the WDN. Both Perl scripts and Matlab are being investigated as tools for linking the overlay, ns-2, and EPANET.

4.2. Research Plan and Future Work

Our intermediate goal is to capture the physical manifestation of failures in cyber control. This will enable use of the Markov Imbedded System (MIS) model [13] to define “safe” states for the CPS as a whole, i.e., identify states where the physical and cyber components are sufficiently operational to allow the system to be classified as “functional.” The corresponding numeric thresholds can vary, based on reliability specifications of the WDN.

Fault injection will be used to investigate failure propagation from the cyber layer to the physical layer. Specifically, faults will be injected in the distributed software algorithm used for control of water quality and quantity, as well as in the supporting hardware and communication links. Game-theoretic algorithms appear to hold the greatest promise [14], and as such, will be the first category investigated.

The doctoral research described in this paper will be carried out in the course of the four following tasks, which overlap in time.

1) Building a qualitative understanding of interdependencies in CPS
2) Quantitative representation of these interdependencies
3) Characterizing CPS dependability in terms of attributes of the physical and cyber components
4) Validation of the models using simulation and field data

Task 1 will be accomplished through simulation of an intelligent (cyber-controlled) WDN, and encapsulation of the information gained into a qualitative agent-based model. The MIS model will be used to quantify these results in Task 2. The model will be refined in Task 3. The simulation developed in Task 1 will be refined in Task 4, and supplemented with field data to validate the models developed.

5. Conclusion

The overarching objective of the proposed doctoral research work is to develop a qualitative and quantitative understanding of dependability in CPS. WDNs have been selected as the case study, as they represent a vital category of critical infrastructure. Significant research challenges result from the need to encompass both cyber and physical aspects of CPS in a single dependability model. A multi-agent model is proposed to bridge the cyber and physical networks and facilitate accurate study of their interdependencies. Fault injection will be used to populate an MIS model quantifying these interdependencies. Research results will be validated through simulation, supported by actual field data from deployed WDNs. Our hope is that quantitative modeling of dependability for CPS will alleviate concerns associated with the introduction of intelligent control to critical infrastructure systems, paving the way for more widespread application of CPS.

References