27 June 2005

An Integrated Approach to Modeling, Simulation, and Analysis of Critical Infrastructure Systems

Steven Ball, Science Applications International Corporation
Mary D. Marshall, National Security Agency
Dr. Steve Schaffer, New Mexico Institute of Mining and Technology
Dr. Kevin J. Wedeward, New Mexico Institute of Mining and Technology

INTRODUCTION

Critical Infrastructure Systems (CIS) within the United States are crucial to national defense, economic stability, and public safety. Protection of these assets against attack is a major concern [1] and dictates that innovative approaches be developed for identification and mitigation of their vulnerabilities. Establishment of effective and viable vulnerability assessment techniques for CIS has proved challenging due to their inherent large-scale, interconnectivity, and dynamics. In response to these challenges, the science and engineering community has been recognized as a valuable national resource to initiate new critical infrastructure protection technologies [2].

This article summarizes an integrated approach to modeling, simulation, and analysis of CIS employed by the Institute for Complex Additive Systems Analysis (ICASA), a research division of the New Mexico Institute of Mining and Technology. Particular CIS of interest include technological systems such as energy, communications, and transportation, and socioeconomic systems such as financial markets and organizations. Key features of the approach include a strategy for systematic application to real CIS; a formal dynamical system modeling framework in which to work; computer simulations through which analysis can be performed and trajectories viewed; and mathematically well-posed objectives, analysis techniques, and results.

Other researchers (e.g., [3, 4]) have proposed frameworks for risk assessment of infrastructure systems and their interdependencies. As part of their assessment process Brown, Beyeler, and Barton [3] utilize dynamic models and simulation as a means of understanding the properties, interconnections, and interdependencies of these complex systems. The distinguishing feature of ICASA's approach is the formal dynamic model definition and subsequent application of system and control theory tools to specifically answer vulnerability questions within the context of relationships between system inputs, parameters, states, and outputs.

The iterative approach outlined in this article for modeling, simulating, and ultimately assessing vulnerabilities within CIS is shown in figure 1 along with resultant capabilities. Subsequent sections provide details of the various steps that comprise the process along with illustrative information on some of ICASA's applications.

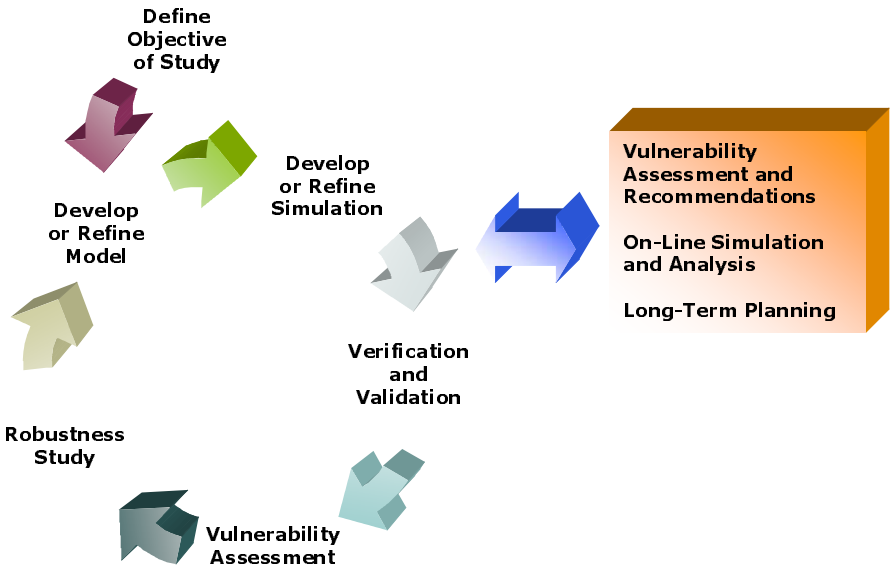

Figure 1: Process diagram for CIS studies and resulting capabilities

OBJECTIVE OF STUDIES

The study process begins with a vulnerability question posed by a person interested in or responsible for the safety of a specific critical infrastructure system. In general, the objective posed will be of the form "Determine if a potentially exploitable element can be used to degrade the performance of an asset within the critical infrastructure system." In particular, for an example electric power system such as the one shown in figure 2 the intent could be "Determine if a voltage control device (the exploitable element) at the bus indicated with an arrow can cause a degradation in voltage levels at the bus indicated with a star (the asset)." Depending on the nature of the control device and its ability to be varied continually or in finite discrete steps, the study objective can be recast in terms of inputs and outputs and/or parameters and outputs, respectively. It is this distinction that then guides the type of analysis appropriate for the study objective.

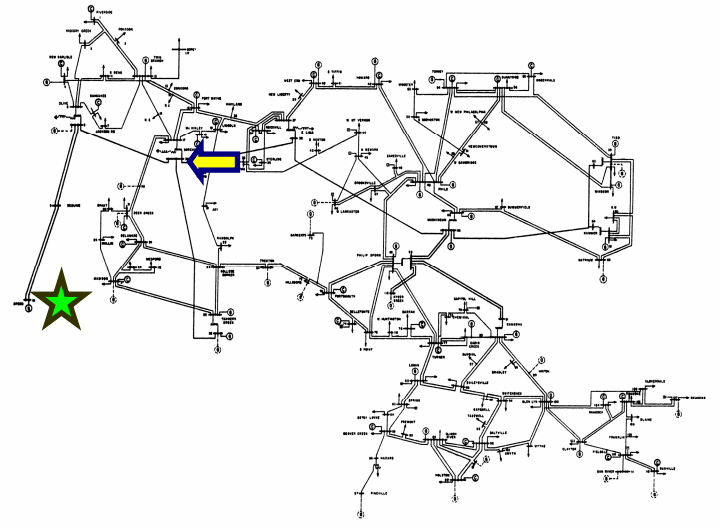

Figure 2: IEEE 118-bus electric power system test case [5] with an example exploitable element (arrow) and asset (star) indicated

MODELING

Critical infrastructure systems of interest are composed of two fundamentally different, yet joined systems: the network of interconnected dynamic components and the logical switching designed to maintain a desired level of performance. This structure permits CIS to be modeled within a well-defined Hybrid Dynamical Systems (HDS) framework [6]. The significance of the HDS model is not only in the definitions, but also in the implications for organization of associated computer simulations and applicability of analysis tools.

In general, HDS are those systems with interacting continuous and discrete system dynamics [6]. A common HDS example is one composed of a finite-state machine (the discrete system) that selects from a set of right-hand sides for ordinary differential equations (the continuous system). This structure is shown conceptually in figure 3 with {A, B, C} the states of the discrete system, y the (measured) output of the continuous system compared with critical thresholds y_{cr1} and y_{cr2}, u the system input, and x the state of the continuous system with behavior governed by the multi-valued right-hand side $f_i(x,u)$ where $i \in \{A, B, C\}$.

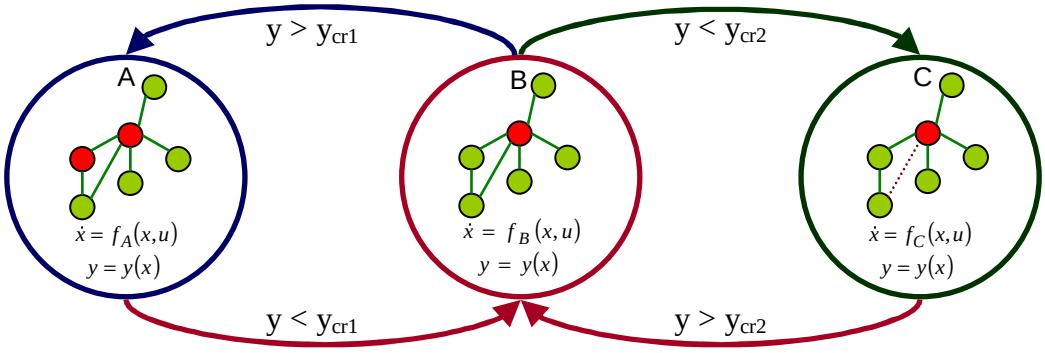

Figure 3: Conceptual diagram of HDS structure

The purpose of mathematically modeling CIS is to provide a means through which system dynamics and interactions can be studied. Descriptions of system behaviors or processes often give rise to several different mathematical descriptions that only approximate the behavior of the actual system, and in many cases the complexity of the physical system defies exact mathematical formulation. Moreover, a mathematical model of a system can often be further simplified prior to analysis through reduction techniques. Properly developed mathematical models should be as simple and tractable as possible while reliably capturing phenomena consistent with the study objective. Development of critical infrastructure system models involves a continual interaction between analysts, researchers, subject matter experts, and programmers. It is important to realize that although a computer is a useful tool it is in no way an adequate substitute for proper scientific interaction while developing mathematical models and computer simulations.

SIMULATION

Due to the large size and complexity of typical CIS, solving or analyzing the set of ordinary differential or difference equations that make up the continuous component of the model becomes difficult. In addition, as the system solution trajectory crosses critical values intrinsic switching occurs selecting a new continuous model that would in turn need to be solved or analyzed. These analytical difficulties motivate the use of computer simulations to numerically solve critical infrastructure system models and service event switching. Thus, following model construction a simulation code is typically developed, expanded, and/or refined based upon the chosen model equations and analysis goals. A well designed simulation code plays an integral part in the study of these systems; therefore, it is vital that the code design, in its initial and longer term development, draw from the expertise of the researchers, subject matter experts, programmers, and analysts. Example simulation results are presented in figure 4 for HDS-based models/simulations that were utilized in financial market and electric power system studies. The goals of these particular studies were to construct a one-stock financial market that matched empirical power law statistics in size of returns and view the effect of a line trip on voltages within an electric power system, respectively.

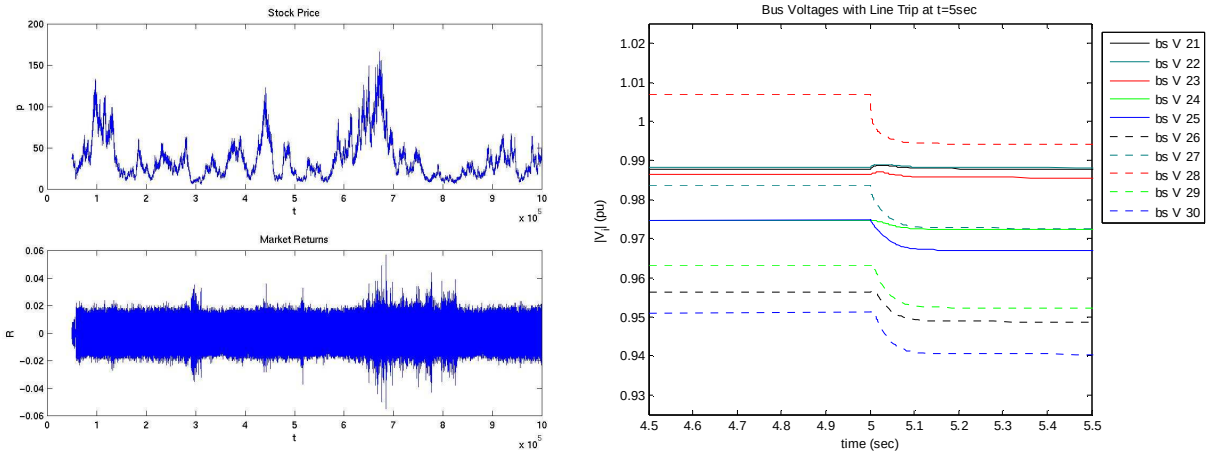

Figure 4: Example simulation results for a one-offering financial market (left) and an electric power system with a disturbance (right)

VERIFICATION AND VALIDATION

Given that the computer simulation encompasses the HDS model and serves as the basis for the analysis process, the next step is to verify that the models are correctly implemented into the simulation code, and validate that the models as accurately as possible represent the critical infrastructure system of interest. There is great variation in the availability of data through which a model can be constructed and recorded responses to which simulated responses can be compared; especially in CIS where experiments on the real system are generally discouraged. Due to its importance and associated difficulties, considerable effort has been placed in verification and validation of computational engineering and physics [7]. Here an overview of an approach based upon that of Colbaugh and Glass [8] is presented with four stages of validation that depend upon study objectives and data availability. The four stages are shown in figure 5 and outlined below.

Stage 1: Computer simulation employs component-level models that are justified through physics or empirical data.

Stage 2: Computer simulation yields high-level results consistent with CIS of the type under study.

Stage 3: Computer simulation yields high-level results consistent with particular critical infrastructure system under study.

Stage 4: Computer simulation yields component-level responses consistent with those of particular critical infrastructure system under study.

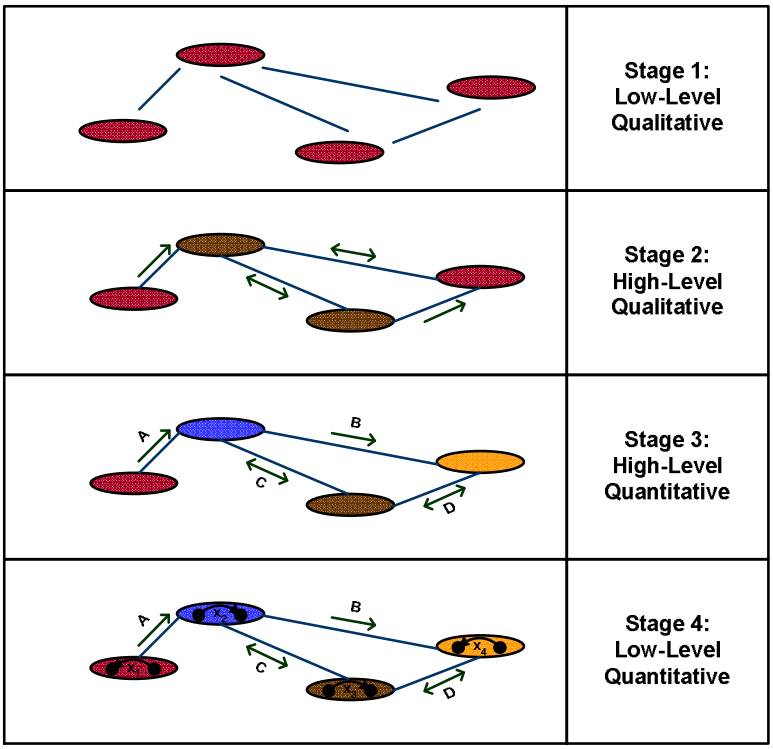

Figure 5: Stages of validation for modeling and computer simulation

VULNERABILITY ASSESSMENT

Convinced of an adequate representation for a specific critical infrastructure system, a well-defined and rigorous vulnerability analysis is then performed to quantitatively answer the study objective. Approaches utilized thus far to study the input-output and parameter-output characteristics of CIS have tended to be based upon nonlinear systems and control theory, properties of complex networks, and trajectory sensitivities [8-11]. Following the presentation of references [8-10] an exploitable element that can be varied with time is considered a system input, system outputs or states of interest are considered assets, and the notions of accessibility and feedback linearization can be applied in the context of vulnerability analysis. Accessibility involves constructing and checking the span of the accessibility algebra from which reachable sets, i.e., states reachable from a given initial condition, can be determined. The first five Lie Brackets of the accessibility algebra are shown graphically in the left hand portion of figure 6 for the example power system in figure 2. A generator voltage set point at bus 30 was selected as the input and all bus voltages as the states of interest. Note the propagation of the control action through the network and system dynamics indicated by the dark gray areas.

An alternative approach to vulnerability analysis that has been employed is the concept of trajectory sensitivity when the exploitable element considered can be changed once. Here the exploitable element is thought of as a parameter and the assets are once again system outputs and states. Trajectory sensitivities capture the influence of parameter changes on the dynamic behavior of the system. An example cross-section of a set of

trajectory sensitivities is shown in the right portion of figure 6. It shows at a certain time how much the trajectory would vary from its nominal trajectory had the parameter been changed at a specified time in the past. Here the generator voltage set point at bus 30 was again chosen as the study parameter and all bus voltages as the states of interest. The size of the bar gives an indication of how much the trajectory would vary for a small change in the parameter value.

Additional analysis tools under development include robust parameter and state estimation techniques. The list of analysis tools is constantly growing and includes both experimental as well as more established methods. Redundant testing is often used in the analysis of CIS wherein information about a particular aspect of the system is analyzed using a number of different techniques. Agreement of the conclusions from the various methods strengthens confidence in the results.

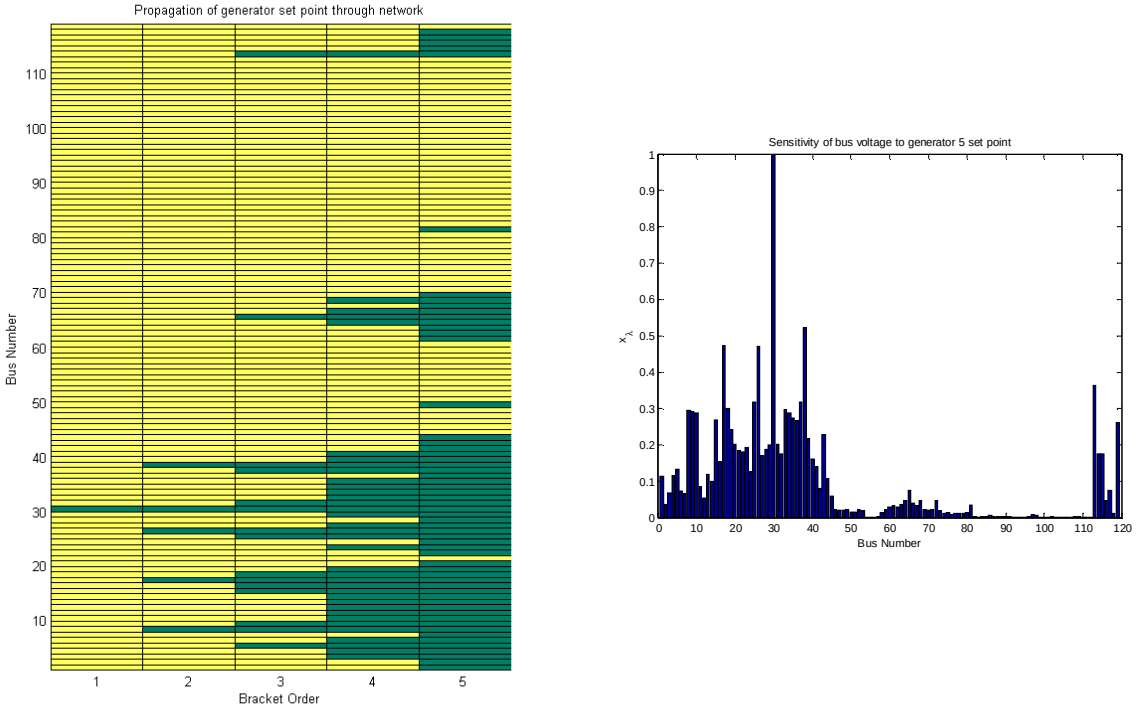

Figure 6: Vulnerability assessment results as graphical depictions of part of accessibility algebra (left) and trajectory sensitivity at a particular time (right)

ROBUSTNESS STUDY

Since the model is only an approximation of the real critical infrastructure system, it is important that the robustness and sensitivity of the vulnerability analysis conclusions to parameter and model uncertainty be investigated. These robustness results provide a degree of confidence in the vulnerability assessment results, and in the event more accurate descriptions are required for a higher confidence level, the process would be repeated as shown in figure 1. Two mechanisms are currently implemented to

characterize the effect of model uncertainty. The first is a standard Monte Carlo analysis where random parameter sets are generated for typical ranges of parameter values. The resulting range of trajectories then provides a means to quantify uncertainty in the system's behavior. For example, figure 7 shows the range of voltage trajectories for a selected uniform set of generator parameters. The second method utilizes trajectory sensitivities in a manner similar to their vulnerability assessment application (see right hand side of figure 6 for example application). Trajectory sensitivities express the impact of parameter variation on system responses, and thus provide guidance as to which parameters are most influential.

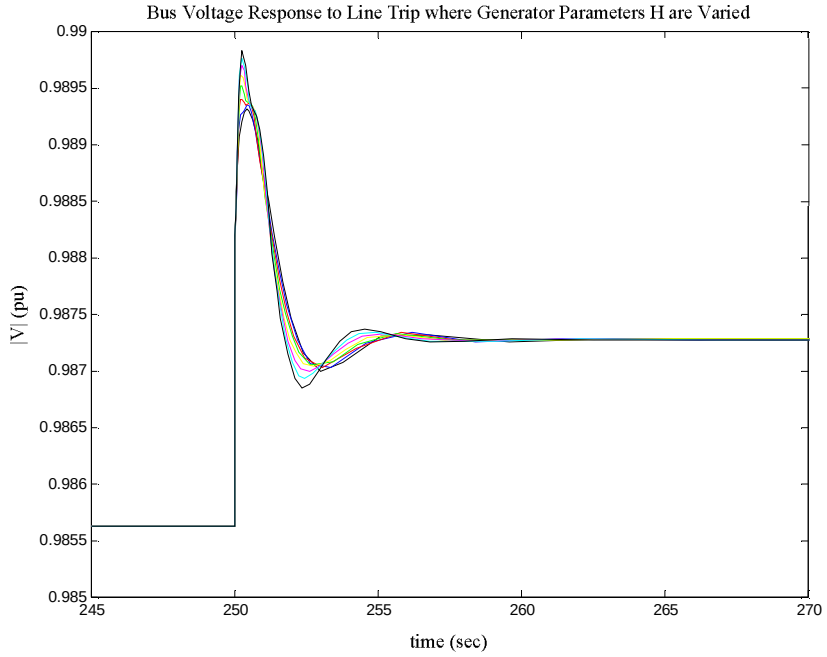

Figure 7: Bus voltage responses to a transmission line trip where generator parameters H are taken from typical range of values

CONCLUSIONS

A summary of the approach taken by ICASA for modeling, simulation, and analysis of CIS was presented. Notable features of the approach include involvement of individuals with varied backgrounds, emphasis on systematic techniques applicable to CIS in general, and an eye towards analysis and flexibility at all times. The basic outline of the process will continue to be followed as new CIS are studied, and research will drive the continual evolution and expansion of the process.

REFERENCES

1. U.S. General Accounting Office, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321, Washington, DC, May, 2004.

2. National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington, DC, The National Academy Press, 2002.

3. Brown, T., W. Beyeler, and D. Barton, "Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems," *International Journal of Critical Infrastructures*, Vol. 1, No. 1, pp. 86-99, 2004.

4. Robert, B., "A Method for the Study of Cascading Effects within Lifeline Networks," *International Journal of Critical Infrastructures*, Vol. 1, No. 1, pp. 108-117, 2004.

5. Power Systems Test Case Archive: 118 Bus Power Flow Test Case. Retrieved March 9, 2005, from <www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm>.

6. Matveev, A. S. and A.V. Savkin, *Qualitative Theory of Hybrid Dynamical Systems*, Birkhäuser Boston, 2000.

7. Oberkampf, W.L., T.G. Trucano, and C. Hirsch, "Verification, Validation, and Predictive Capability in Computational Engineering and Physics," *Applied Mechanics Review*, Vol. 57, No. 5, pp. 345-384, 2004.

8. Colbaugh, R. and K. Glass, "CASA: Introduction and Examples," *ICASA Internal Report*, April 2001.

9. Nijmeijer , H. and A. Van Der Schaft , *Nonlinear Dynamical Control Systems*, Springer-Verlag, 1990.

10. Vidyasagar, M., *Nonlinear Systems Analysis*, Society for Industrial and Applied Mathematics, 2002.

11. Hiskens, I.A. and M.A. Pai, "Trajectory Sensitivity Analysis of Hybrid Systems," *IEEE Transactions on Circuits and Systems Part I Fundamental Theory and Applications*, Vol. 47, No. 2, pp. 204-220, 2000.