INL/CON-09-15271
PREPRINT

Critical Infrastructure Modeling: An Approach to Characterizing Interdependencies of Complex Networks & Control Systems

HSI 2009

Stuart Walsh
Shane Cherry
Lyle Roybal

May 2009

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Critical Infrastructure Modeling: An Approach to Characterizing Interdependencies of Complex Networks & Control Systems

Stuart Walsh, Shane Cherry, and Lyle Roybal,
†Idaho National Laboratory, Idaho Falls, Idaho, USA

Abstract — **Critical infrastructure control systems face many challenges entering the 21st century, including natural disasters, cyber attacks, and terrorist attacks. Revolutionary change is underway to solve many existing issues, including gaining greater situational awareness and resiliency through embedding modeling and advanced control algorithms in smart sensors and control devices instead of in a central controller. To support design, testing, and component analysis, a flexible simulation and modeling capability is needed. Researchers at Idaho National Laboratory are developing and evaluating such a capability through their CIPRsim modeling and simulation framework.**

Keywords — **HLA, control system, modeling, simulation, CIPRSim, SCADA, emulation**

I. Introduction

Distributed real-time and embedded systems (DRE), such as SCADA and process control systems are growing in complexity and importance as they are becoming more decentralized and transferring more decision-making tasks previously done by human operators to smart sensors and field devices. Conceptually, this distributed approach provides many advantages over a centralized strategy. These include [8]:

- Physically Inherent: Many systems of interest are inherently distributed, and have autonomous control computing power.
- High Performance: There can be far greater processing power than in centralized systems. Communication between the various parts of the system allows the overall system performance to be optimized.
- Flexibility: If the system is physically changed, with a good design, only the interconnections need to be re-specified and re-programmed. Rewiring is simplified by using networked communications.
- Fault-tolerant: If some parts of the system fail, other may still be able to work in a degraded mode (i.e., with reduced communication and processing ability)
- Commercially economical: Stringing a single network cable is often less expensive than wiring point to point connections for each sensor and actuator. Also, components of a mechanical system provided by separate vendors may come with independently developed controllers which may need to be integrated.

However, there are challenges associated with distributed control systems which must be addressed to ensure an efficient, resilient and secure system. The proposed distributed control systems consist of hardware, software, and controllers connected through a network communications protocol in order to provide high-speed, reliable data flow among the various processing elements. These types of systems are required to provide quality of service support to process the right data in the right place at the right time over a networked grid of processors. Quality of service properties required by these systems include the low latency and jitter expected in conventional real-time systems, and the high throughput, scalability, reliability and security expected in conventional enterprise distributed systems. Achieving this combination of quality of service capabilities is difficult due to the systems often working in constrained environments with a limited amount of resources [13]. Therefore, optimal methods to distribute computational methods while allowing secure data exchange need to be considered. In addition to quality of service requirements, solutions where the interactions between control and implementation engineers, known as co-design, need to be improved. In both cases, modeling and simulation tools that allow for efficient testing and analysis of these systems is an important feature for evaluation of

†Work supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems Distinctive Signature (ICIS) of Idaho National Laboratory and to support the U.S. DoD Strategic Command.

distributed computation methods, evaluation of system performance, and for providing overall system design support. Modeling these systems is also a cost effective means for addressing the problem of security from an overall system view. In addition, evaluation of control system modeling and simulation tools, most of the theories and methods developed so far and implemented in the current tools are very specialized and aimed at performance analysis of systems rather than synthesis of various system processes and components [3].

II. INL Modeling Approach

The Idaho National Laboratory (INL) is addressing these challenges and tool gaps by leveraging the Critical Infrastructure Protection and Resilience simulation (CIPRSim) framework developed at the INL and described in section III. Specifically, the High Level Architecture (HLA) used in CIPRSim is being used to provide a mechanism to support messaging between distributed control system models and components, and as an efficient means to aid in the design, testing and evaluation of distributed control systems and their components with regard to performance, resilience and security. CIPRSim was initially developed as a modeling and simulation framework to allow users to link multiple hazard and specific critical infrastructure sector analysis modules, including physical components, through a distributed environment. This dynamic linkage provides the capability to simulate and visualize cascading effects and cross sector interdependencies associated with an initiating hazard or threat event. Our hypothesis is that this framework may also provide a mechanism to assist in assessing control system component interactions and performance. The CIPRSim framework is based upon the IEEE 1516 HLA standard. The HLA provides a common architecture for distributed modeling and simulation, linking simulations and interfaces to live systems. This is shown in Fig. 1. There, the CIPRSim HLA bus provides the infrastructure needed to support dynamic communication between any hazard or initiating event model, such as a cyber attack, and a physical model of the infrastructure such as a power grid model. In addition to model connectivity, the CIPRSim bus provides functionality to distribute communication to other locations in a timely manner. It is a communication bus that allows disparate models and physical devices to dynamically interact within a common temporal and spatial context. Other benefits include:

- The ability to provide infrastructure to support plug-n-play models/components – scalability and hardware-in-the-loop,
- A distributed architecture that eliminates connectivity limitations,
- An analysis platform to test connections between control system models and components with other models, such as a power or cyber threat model,
- Support for standard control system communication protocols to simplify integration of new bus components.,
- Time synchronization of models and messages on the bus.

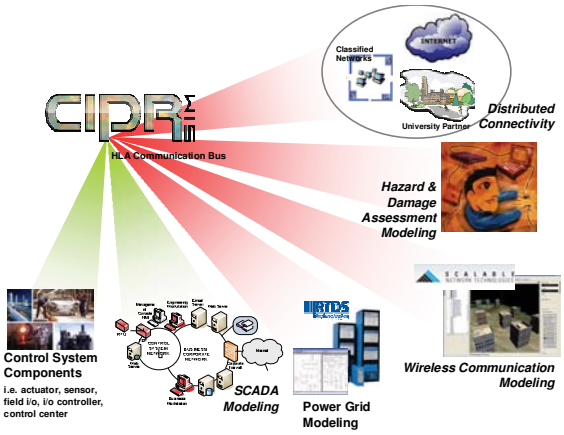

Fig. 1. CIPRSim Conceptual View

III. The CIPRSim Architecture

The CIPRSim modeling environment used the concept of Federates to describe areas of activity in the modeling architecture. There are hazard federates used to model the intensity of an initiating event such as a flood or a hurricane. There are damage federates used to model the response and damage inflicted onto the physical infrastructure federates by the hazard. There are infrastructure federates such as the power grid that model how that particular federate responds as pieces and parts of that federate fail. Lastly, there is an interdependency federate that communicates and models the effects and responses of physical federates among each other. For example, if parts of the power federate fail, they may be an effect on other federates such as a wireless communication federate due to the loss of power within the wireless federate. All of these federates communicate via an HLA bus architecture.

HLA is deeply embedded within the U.S. DoD and war-gaming activities and is widely recognized as representing the state of the art technology for the integration of distributed simulation models [9] for a diverse range of focus areas such as emergency response [10], [11] and urban chemical disasters.[12] In addition to these applications, INL recognized HLA as a viable means to base dynamic and distributed simulations and analyses related to critical infrastructure systems as it provides a common architecture for component-based simulations where multiple simulations are combined to provide a more comprehensive simulation. Components, or in the case of CIPRsim, models or physical devices, within the HLA framework are known as federates, which collectively, operate within a federation that can run across multiple computers. HLA and CIPRSim provide

the connection to link users and infrastructure models via distributed connections to hazards and other models.

The models participating in CIPRSim use the IEEE 1516 HLA standard for simulation communication and time/event management. The format, content, encoding and decoding of all objects and interactions on the simulation bus is specified using the HLA Object Model Template (OMT) definition. In order to promote interoperability with third party display and analysis tools, the Federation Object Model (FOM) used is based on the Real-time Platform-level Reference (RPR) FOM version 2.0. The RPR 2.0 standard is nearing approval at the Simulation Interoperability Standards Organization (SISO), with draft 17 being the latest release. This version is used as the basis for the CIPRSim FOM and existing classes defined in RPR 2.0 Draft 17 was utilized whenever appropriate. A recognized and approved FOM simplifies integration with arbitrary third party models and provides consistency with the rest of the simulation world.

The essential components in an HLA simulation are 'objects'. Objects are shareable elements that are published by each model interacting in the simulation. They expose elements of a model to other models. For instance, a model in a simulation may publish a valve as an object. The valve object may have parameters which change the behavior of the valve or provide a status, such as whether the valve is open or closed. The definition of possible object types is contained in a standard OMT. Since the HLA is directed towards interoperability, object templates are intended to focus on descriptions of the critical aspects of models which are shared. They are intended to be the means for open information sharing across the community to facilitate reuse of simulations.

Several federates have been developed for the CIPRSim framework and many tests have been completed investigating how wide area disasters effect critical infrastructures. For these studies high fidelity models were developed of power and wired, wireless and emergency communications infrastructures. Simulations were completed evaluating the resiliency of infrastructures against earthquakes and hurricanes at various locations in the United States. The federates for these tests included the following:

1.1. Power Federate

The electrical asset module, or Power Federate, is responsible for modeling power assets and their interconnections. The objective is to model accurately the effects of damages to the power components in the power grid by creating power models that accurately replicate the power grid in the areas selected for analysis. The power assets are modeled in RTDS (Real Time Digital Simulator), which is a hardware/software system that models power systems. The RTDS Simulator is a fully digital electromagnetic transient power system simulator that provides technology for a fast, reliable, accurate and cost-effective for the study of power systems with complex High Voltage Alternating Current (HVAC) and High Voltage Direct Current (HVDC) networks. It is a combination of advanced computer hardware and comprehensive software.

1.2. Communications Federate

The communications module, or Wireless Federate, is responsible for modeling wired, wireless, and emergency communications assets and their interconnections. The objective is to depict the effects of damages to the wireless communications components in the wireless network accurately. This is achieved by creating wireless communication models that replicate the wireless networks in the geographic areas selected for analysis. The wireless communications assets are modeled in QualNet, which is network modeling software that predicts real-time performance of wireless and wired networks through simulation and emulation.

1.3. Hazard Federate

The hazard module, or Hazard Federate, is responsible for modeling the hazardous events in a scenario that act as initiators of infrastructure damage in the simulation. This includes hazards from hurricanes, such as storm surge, flooding, and high winds and earthquakes, such as ground. In addition, the hazard federate can also model point failures or a sequence of point failures, such as a failure of a sensor within control system. The failures can be intermittent or purposeful with associated timing. This is helpful when modeling cyber threats.

1.4. Damage Assessment

The damage assessment module uses the concept of fragility functions to describe the failure of infrastructure components. Fragility functions are cumulative probability density functions that provide the probability of failure as a function of hazard level. The damage assessment module currently uses three types of fragility functions. Most damage assessments will be described by using a threshold-level Weibull distribution function [14], [15]. However, the damage assessment module may use a straight-line distribution function, or a simple threshold-based failure model. The form of the Weibull distribution function is shown below in equation III-1.

$$P_f = 1 - e^{\left(\frac{x-a}{b}\right)^c} \quad \text{, where } x > a$$

Equation III-1, Weibull Distribution

Here, x represents the hazard level. The coefficients a, b, and c are constants that are used to adjust the threshold and shape of the distribution function. The constant ***a*** is the lower threshold of the function. The constant ***b*** is used to set the 63% failure level of the distribution with respect to the threshold value. The constant ***c*** modifies how steep or fast the function approaches 100% failures.

A larger exponent corresponds to a steeper function. An exponent of 3.5 approximates a normal distribution. Weibull functions are desirable because of they can be made to resemble a normal distribution function, are flexible, and are easy to configure.

1.5. Interdependency Federate

The interdependency federate provides the functionality to evaluate interdependencies and resulting cascading effects between the power and wireless federates. These asset state changes are then published to the HLA bus where the Interdependency federate reads the new asset state changes due to hazard effects and evaluates them for interdependencies for local or physical interdependencies. Local interdependencies compare locations of participating model assets to evaluate possible areas of influence, depending on the type of assets that are being compared.

IV. Test Conducted

The first step in determining if a HLA-based framework provides an acceptable distributed control system simulation and testing environment is to quantify the messaging capabilities of the simulation bus. This means understanding the number and time required to create, manage, and update objects on the simulation bus.

Several tests were conducted to evaluate the throughput capabilities of an HLA communication bus. The tests looked at the maximum messaging rate for small and large packet data in both a continuous and burst transmit mode. Data was collected to evaluate transmit and receive latency and the time required to initialize and modify objects as the number of simulated objects increases. All tests were conducted using a standard Windows XP based workstation and the models and simulation bus were tested on the same machine to eliminate possible network latency issues. Figure 2 & 3 summarize the results from several runs of 50 time steps each. From both graphs a noticeable slow down of message processing capabilities occurs when the number of shared objects between models is greater than 50,000. In addition, from the results, the optimal number of objects on the bus is less than 5,000. This is still a significant number for most simulations.

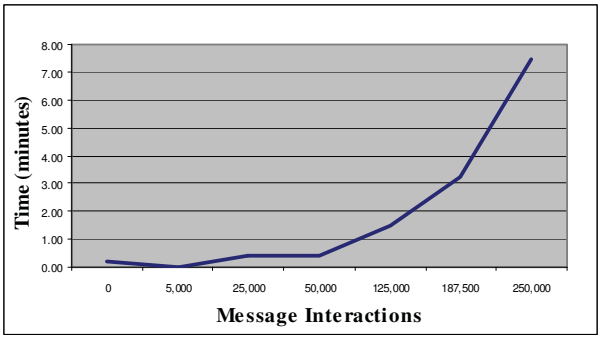

Fig 2. Continuous Messaging on the Simulation Bus

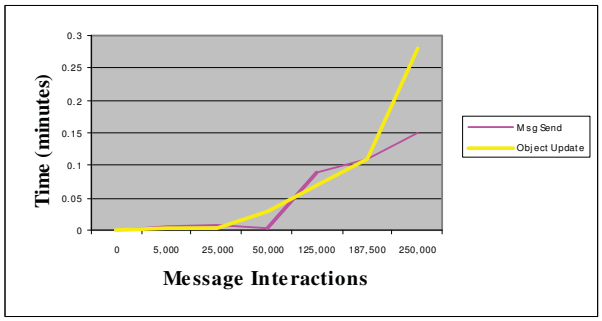

Fig 3. Burst Messaging on the Simulation Bus

Object creation is done at the start of the simulation and, from the results, slows significantly between 25,000 and 37,500 objects. For most simulations, the time to create objects is not much of an issue because it is done only at startup. The more important value is the object update time. From the table, object update time slows significantly between 5,000 and 10,000 objects. The time required to update 5,000 objects in one time step is 0.15 seconds. This may prove to be too slow for some simulations.

For all tests during the simulation a 0% error rate was recorded. All messages send were received and acknowledged. Also no attempt was made to optimize the communication settings of the HLA communication bus. Several configuration parameters exist that may improve the results. For all tests the default configuration parameters were used.

V. Path Forward

The path forward is to apply the CIPRSim HLA framework and existing federates to smaller geographic areas with the focus on a distributed modeling capability for testing of advanced control systems. Doing so would capitalize on existing federate capabilities. For instance, the effects to the control system can propagate to other dependant infrastructures, such as facility power, communications, or a facility process. HLA is the mechanism that provides the ties between models. The models are decoupled, but dynamically execute within the same time base and spatial context. Another future use of the CIPRSim HLA framework is to run Monte Carlo simulations to investigate how a hazard, such as a denial-of-service cyber attack can effect communication of a supervisory computer system in a much larger control system model. Once a test environment is set up, it can be reused, not only for other systems/products, but also incrementally during the development of new protocols, data aggregation techniques, or security algorithms.

If proven capable of providing an effective communications and modeling/simulation means for distributed control systems, CIPRSim's HLA-based framework will provide a needed testing, analysis and developmental aid capability, the most important of which may be the testing capability [3]. The strength of testing

through simulation is (at least) four-fold:

- There are few limitations in the types of systems that can be tested, e.g., works for non-linear systems and for hybrid systems
- The test conditions can be well defined and the tests are repeatable
- The tests can be automated
- The tests can support a wide variety of purposes including verification in early development stages as well as analysis of failures during maintenance

VI. Conclusion

The tests revealed the limitations of using an HLA bus for messaging between models. For our simulation of 5,000-10,000 active objects or less, HLA will respond in a timely manner at each time step in a simulation. In the context of a control system test network this may be sufficient. Objects are the elements that are shared between models. This may translate into needing a single HLA object to represent a valve, a subset of a valve, or an entire node in a control system. The next step and path forward is to apply the framework within the context of a modeled and physical control system environment. This will help identify the shared objects needed for a control system test bed network, tie those objects to other dependant infrastructures, and demonstrate a proof of concept.

References

[1] DOE Office of Electricity Delivery and Energy Reliability, National SCADA Test Bed: Enhancing Control Systems Security in the Energy Sector. Fact Sheet. Available: http://www.oe.energy.gov/DocumentsandMedia/NSTB_Fact_Sheet_11-5-07.pdf

[2] IEEE (ed.): Standard for Modeling and Simulation (M and S) High Level Architecture (HLA). 1516 (2000)

[3] Torngren, M., D. Henriksson, O. Redell, C. Kirsch, J. El-Khoury, D. Simon, Y. Sorel, H. Zdenek, and K. Arzen, 2006, Co-Design of Control Systems and their Real-Time Implementation – A Tool Survey, Mechatronics Lab, Department of Machine Design, Royal Institute of Technology, Stockholm, Sweden.

[4] U.S. Computer Emergency Readiness Team, Available: http://www.us-cert.gov/control_systems/.

[5] U.S. Department of Energy and U.S. Department of Homeland Security, 2006, *Roadmap to Secure Control Systems in the Energy Sector,* Energetics Corporation, January

[6] U.S. Department of Energy, 2004, *"Grid 2030", A National Vision for Electricity's second 100 Years*, July

[7] U.S. Department of Energy, 2004, National Electric Delivery Technologies Roadmap, July

[8] Yook, J.K., D.M. Tilbury, and N.R. Soparkar, 2001, A Design Methodology for Distributed Control Systems to Optimize Performance in the Presence of Time Delays. International Journal of Control, Volume 74, Number 1, pgs. 58-76.

[9] Tolk, A., 2002, "Avoiding Another Green Elephant – A Proposal for the Next Generation HLA Based on the Model Driven Architecture," *2002 Fall Simulation Interoperability Workshop (SIW)*, Orlando, FL, September 2002.

[10] Jain, S. and C. McLean, 2003, "A Framework for Modeling and Simulation for Emergency Response," *Proceedings of the 2003 Winter Simulation Conference*.

[11] Coolahan, J.E., 2006, "Planning for an Integrated M&S Framework for Catastrophic Event Response," http://www.pacercenter.org/pdf/coolahanPublication.pdf

[12] Coolahan, J.E., M.T. Kane, J.F. Schloman, R.P. Koomullil, A.M. Shih, I. Yasushi, K.I. Evangelos, K.K. Walsh, and M.M. Abdullah, 2007, "Design of an Urban Chemical Disaster Simulation Federation for Preparedness and Response," *2007 Fall Simulation Interoperability Workshop (SIW)*, Orlando, Florida, September 2007.

[13] Hill, J.H., Schmidt, D.C., Slaby, J.M., "Evaluating Quality of Service for Enterprise Distributed Real-time and Embedded Systems"

[14] Weibull, W., 1951, "A Statistical Distribution Function of Wide Applicability," *J. Appl. Mech.-Trans. ASME* 18(3), 293-297.

[15] National Institute of Standards and Technology, *Engineering Statistics Handbook*, http://www.itl.nist.gov/div898/handbook/apr/section1/apr162.htm