INL/EXT-19-55969

Modeling and Simulation

Introducing hardware-in-the-loop capabilities to the Human Systems Simulation Laboratory

Brandon Rice, Jacob Lehmer, Robert England

September 2019

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

INL/EXT-19-55969

Modeling and Simulation

Brandon Rice, Jacob Lehmer, Robert England

September 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

ACRONYMS

API	Application Programming Interface
DOE	Department of Energy
DOE-NE	Department of Energy, Nuclear Energy
gPWR	generic Pressurized Water Reactor
HIA	Hardware Interconnection Application
HITL	Hardware-in-the-loop
HMI	Human-Machine Interface
HSSL	Human Systems Simulation Laboratory
INL	Idaho National Laboratory
LWRS	Light Water Reactor Sustainability
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol/Internet Protocol
TCS	Turbine Control System
US	United States

Intro

The Human Systems Simulation Laboratory (HSSL) shown in Figure 1 is a full scope, full-scale nuclear power plant simulator that can virtually represent a nuclear power plant control room. It is a research facility originally conceptualized by the Department of Energy's (DOE) Light Water Reactor Sustainability Program (LWRS). The core mission of the HSSL is to support control room modernization efforts across nuclear energy utilities within the United States. As plants begin to age, finding replacement parts or reverse-engineering old components is challenging. Instead, many utilities have opted to do "piecemeal" upgrades to individual control room systems during their normal, scheduled outages. As a nuclear power plant control room simulator, the HSSL can mimic any utility control room, as well as house these new upgrades (e.g., digital turbine control systems, auxiliary feed water systems), as well as other digital components.

Figure 1. Human Systems Simulation Laboratory.

The DOE Office of Nuclear Energy (DOE-NE) cybersecurity program would like to expand the use of the HSSL to include capabilities for cybersecurity research and development. Specifically, the introduction of hardware-in-the-loop (HITL) simulation of nuclear power plant architecture into the HSSL will enable researchers and nuclear utilities the ability to identify impacts generated by sophisticated hostile cyber adversaries, including the consequences of simulated potential attack vectors, and to develop solutions for detecting or preventing these cyber attacks.

It is not uncommon for a nuclear reactor or enrichment facility to become a target of a cyberattack campaign, as seen in Ukraine and Iran. With nearly 20% of the United States' base load power coming from nuclear, investigation into this critical infrastructure sector is necessary to better understand how these events could impact utilities. Creating defense mechanisms to guard against such attacks is critical to the long term sustainability and reliability of nuclear power.

Hardware-in-the-loop

Typically, the HSSL is primarily used as a human-in-the-loop research facility. Studies conducted in the HSSL by human factors scientists focus on nuclear power plant operator responses to new human-machine interface (HMI) plant modifications as well as cyberattack scenarios.

Expanding the HSSL capability by introducing hardware would greatly improve the participants that could be brought in for research. For example, if INL could bring in both field operators, as well as control room operators, the scenarios would garner more information and realism.

Other research scopes would benefit from the ability to 'drop in' multiple hardware components for research, testing, and validation. These could include cyber security (e.g., secure architecture), human factors research (LWRS), and university partnerships who are looking to utilize a facility like the HSSL.

GSE Hardware Rack

One of the nuclear control room simulators that the HSSL hosts is called the generic Pressurized Water Reactor (gPWR). The gPWR simulator was developed by GSE Systems. It is based off of a nuclear utility in the United States and has all identifying features removed. Further, the gPWR is an ideal platform for conducting research because any findings can be made available for public release.

To compliment the gPWR, a hardware rack (Figure 2) was purchased from GSE Systems. Unfortunately, support was not available for this rack and it was not a straight-forward process to successfully connect it to the gPWR.

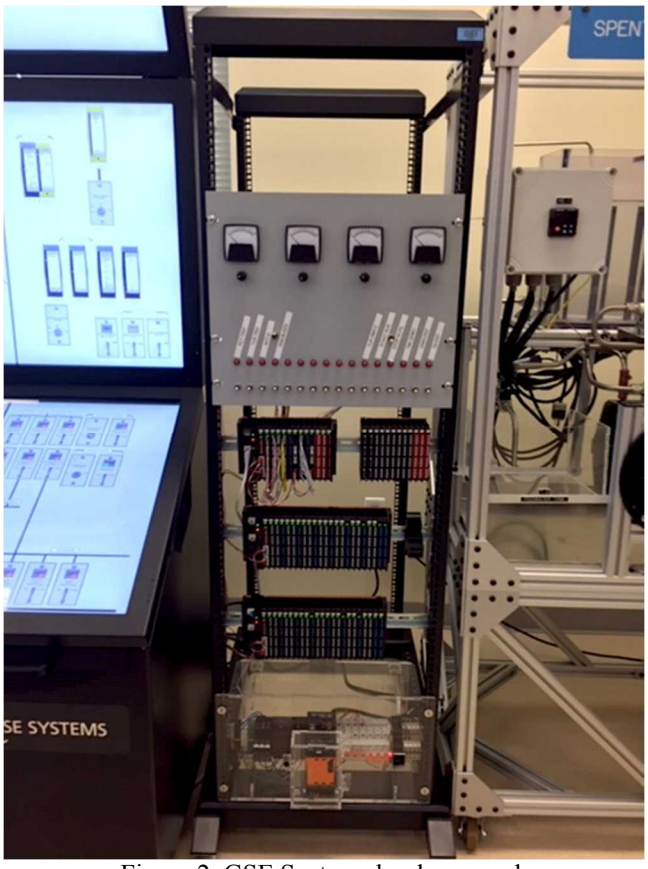

Figure 2. GSE Systems hardware rack

The supplied rack consisted of Weidmüller components comprised mostly of controllers, power supplies, and switches, and had no logic-based systems that could be programmed to work directly with the gPWR. Further, because the components were read-only and could not send commands directly to the simulator, a solution had to be developed in-house to achieve the desired results.

To overcome this challenge, a 'middleware' software was created to act as the messenger between the simulator and the hardware components. Each switch on the rack was given a purpose, with a binary result of on or off. For example, if one switch was assigned the purpose of reactor trip, once activated, the

software would read the switch state as ‘on’ and pass that information to the simulator. The simulator would then trip as intended, albeit in an indirect manner, due to an inability to send a direct signals to the simulator itself.

In recognizing that communication method could be a burden in future development, a new solution was determined to simplify the current manual process of assigning roles to different hardware types. This software solution is called the HSSL Hardware Interconnection Application.

The Hardware Interconnection Application (HIA) is a move towards more generalizable interfaces for any possible configuration of the HSSL. However, integration generalization always poses one multifaceted problem: how to account for the future, specifically, how to allow HSSL configurations that have not been imagined yet. Other solutions to this problem have compromises that require focusing on either hardware or the simulator, or to have a custom solution for every configuration. The HSSL HIA takes the approach of breaking the problem into constituent parts and optimally solve each. The parts of the problem are as follows:

- Hardware Interfacing
- Simulation Interfacing
- Controlling the mutual interfacing

Communicating with a software-based simulator running on a general-purpose computer is radically different to communicating with a hardware rack talking over the Modbus network protocol. Application Programing Interfaces (APIs) abound that are focused on one of these problems. The HSSL HIA uses these APIs as plugins that are then able to be automatically multithreaded with deadlock and race condition prevention. The communication between them is handled by a custom language that is executed on the HSSL HIA. This custom language is entirely event-based, which allows control structures to be developed that respond to system changes, rather than having to incorporate hardware polling or simulator communication into the control algorithm.

The end result of the HIA is a virtual machine that allows for plugins that interface with an arbitrarily large number of hardware or software products, irrespective of the make, model or vendor. The interfaces would only need to be made when new hardware is introduced, whereas control algorithms can be changed arbitrarily often by anyone, without knowledge of software development.

The HIA is currently in its developmental infancy, but has already provided connection capability to the hardware rack as well as to the HMI. With further development the HIA will be able to connect any number of systems to any number of other systems. The driving force behind development is to be able to provide the simplest way to connect systems without needing to reengineer the systems themselves in any way.

Human Machine Interface Demonstration

A goal for this fiscal year was to integrate and demonstrate an operational HMI (Figure 3) with the gPWR simulator. With an initial goal of one button performing one action, a reactor trip (or scram) was implemented. The completed integration was demonstrated to INL DOE-NE Cybersecurity program management in early September. Though simple the successful integration establishes a path forward for more hardware integration. Since this test validated that HITL was possible with the HSSL, future expansion of HITL capabilities is planned with integration of a fully functional turbine control system (TCS).

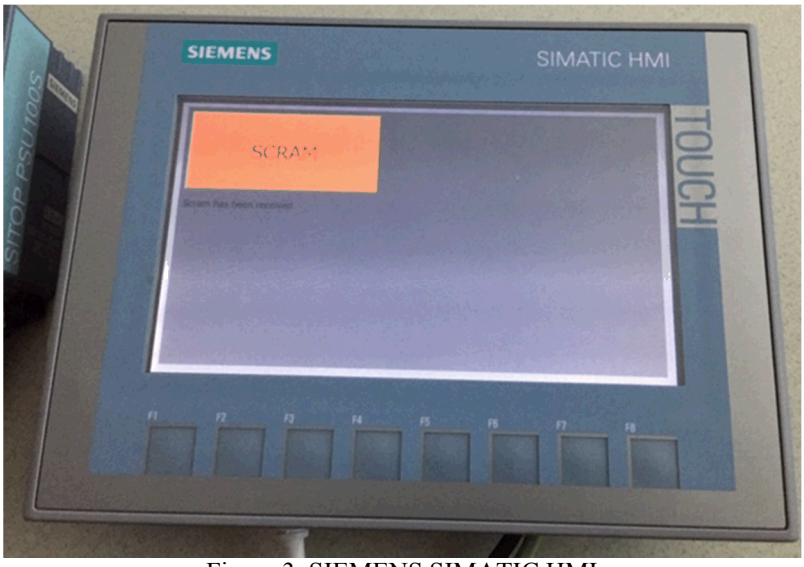

Figure 3. SIEMENS SIMATIC HMI

Continued development of the hardware will allow full integration of the functional control and human interface components within the simulator environment. This will require programming elements within three areas:

- Simatic Step 7 programming within the context of the PLC will be logical programming, allowing the PLC to control basic plant operations through a series of ladder logic implemented functions.
- Siemens HMI programming to create the graphical interface components that will allow human interaction with the code implemented within the PLC.
- HIA programming to allow the executed ladder logic outputs to be read into the simulator to provide operational elements to control designated plant functions.

The first area will require the creation of a code framework that can control and execute commands based on user input from the HMI. Future development may allow the HMI/PLC to take actions based on input from the simulator software. In this way, the HSSL will be able to effectively simulate the environment of a field implemented control system that has active inputs and outputs from field devices and instrumentation, as well as accept a user's command inputs through use of the HMI. The initial implementation of this logic will be somewhat basic, allowing the HMI to actuate functions within the PLC, which will then be read by the simulator interface software and cause changes to simulator parameters.

The second area will include graphical development of an interface that can display plant data/conditions and allow for user input to flip switches, turn knobs, or allow input of discrete values to given plant systems. This can be modified to be more complex over time, including control features and functions that are then implemented on control hardware.

The third area will take the form of a Modbus TCP/IP link that connects to the interface software to achieve two-way communications between the PLC and the simulated environment. Once this link has been established and tested, it can be used to actively display current plant operating conditions, as well as provide control input to the simulator for the selected functions. The Modbus TCP/IP link takes the control and data parameters used within the PLC and encapsulates them within a standard network data

packet. This can then be examined by the HIA software and the specific bits of data relevant to any one control or data function can be read and replicated to feed into the simulator through the HIA.

Conclusions and Future Directions

As the HITL capabilities of HSSL are developed, there are added benefits in the form of a multi-application usable interface that can be utilized not only for human factors testing, but also for the testing of future control system hardware. The interface will allow for other hardware types to be easily adapted and connected to the simulation environment. This could be leveraged to test hardware and conceptual hardware implementations without the need to connect them to a plant and incur all of the costs and engineering overhead involved in such a venture. In this way, the simulator removes costs and simplifies the process of understanding how new hardware and software systems can be leveraged to improve operational aspects of the plants. Additionally, as this capability grows, industry partnerships can be created and leveraged in order to create solutions to control and instrumentation issues which have not yet been investigated creating additional efficiencies in areas not now understood. This hardware capability can streamline the process of implementing changes into plant systems and provide the necessary testing and proof of concept efforts required for control room modernization.

This successful demonstration of hardware-in-the-loop functionality into the HSSL provides for many promising expansions and capabilities that will greatly enhance future research. Other pathways in the DOE-NE cybersecurity program, such as secure architecture, supply chain, and risk management, can benefit from this new capability. For example, Field Programmable Gate Arrays (FPGAs) could be introduced and analyzed for cyber security risk. Network traffic analysis on controlled and specific cyber events could be performed with no risk to an actual Supervisory Control and Data Acquisition (SCADA) network. Data-driven and network-based intrusion detection methods can be modeled and studied to evaluate their effectiveness for detecting or mitigating attack scenarios. And finally, installation of critical digital assets procured for the U.S. nuclear fleet into the HSSL could potentially provide new methods for verifying their authenticity and trustworthiness as well as evaluating their response during cyber events.