SAND2018-7595D

The Center for Cyber Defenders

Expanding computer security knowledge

Generic Hardware in the Loop Capability for SCEPTRE

Aaron W. Werth, University of Alabama in Huntsville, Ph.D. in Comp. Eng.

Project Mentors: Casey Glatter, Org. 5828; Chris Abate, Org. 5828; and Jerry Cruz, Org. 5824

Problem Statement:

- The project is to develop a generic hardware in the loop (HITL) capability for SCEPTRE, Sandia's premier simulation environment for Industrial Control Systems.
- This generic HITL capability will allow for a real hardware device, such as a Programmable Logic Controller (PLC), a remote terminal unit (RTU), or other Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) devices to interface with a computer simulation of a plant or physical system.
- HITL is already possible but it requires writing a custom module for each type of hardware device, which is time consuming, hence why a generic solution is necessary.

Objectives and Approach:

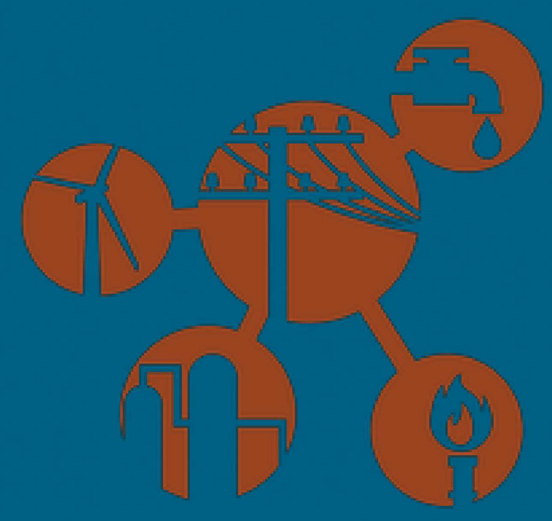
- The project involves creating a program (Sirin) that will interface with a LabJack Device and also with the data broker component of SCEPTRE.
- A LabJack device has a set of pins that are either inputs and outputs. Note that some pins may be configured in either direction. The hardware device is connected to the LabJack.
- Data from the device to the LabJack will be considered actuator commands that are to be transferred to SCEPTRE. Likewise data from SCEPTRE will be transferred by Sirin to the LabJack and in turn through the pins to the device and will be considered sensor data.
- Sirin will parse a configuration file that dictates how data is routed from various aspects of the simulation to specifc pins on the LabJack and vice versa.

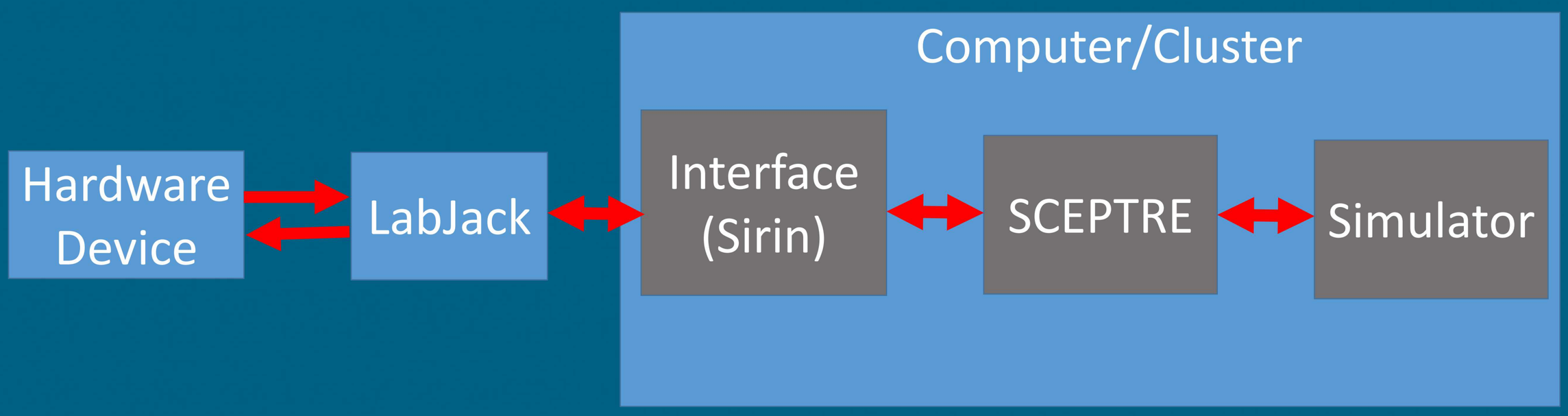
Results

- Ability to subscribe to SCEPTRE, a program that has a data broker for transferring data from one device to another in a simulation environment.
- Ability to interface with LabJack from Sirin and to transfer data from SCEPTRE to pins of LabJack.

Impact and Benefits:

- One main benefit is that this project would allow for simulations of complex SCADA systems with real PLC devices and other devices.
- Using real hardware devices allows for accurate assessments of cyber-vulnerabilities of these real devices.
- Furthermore, a less expensive testbed is developed since the physical system or process is simulated rather than implemented in the real world.
- An actual implementation would require purchasing expensive equipment for power systems, pipelines, etc.
- Another primary benefit is the ability to swap out one 'hardware device' with another, while still being able to interface with SCEPTRE because Sirin is written in a generic fashion. This is an improvement to current HITL implementations which require custom integration on a case-by-case basis.





Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.