INL/EXT-20-59466-Revision-0

Cyber-Physical System Test Bed Data Sources, Communications and Controls Formulation

September 2020

Bjorn C Vaagensmith, Pierce Louis Russell, Craig G Rieger, Justin J Welch, Tyler Bennett Phillips, Stephen Arthur Bukowski, gideon hallman, Chathurika Brahmana, daniel marino

Changing the World's Energy Future

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

INL/EXT-20-59466-Revision-0

Cyber-Physical System Test Bed Data Sources, Communications and Controls Formulation

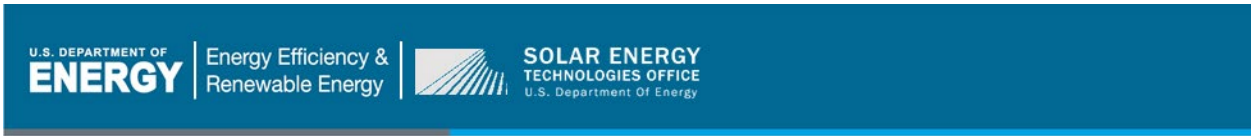
Bjorn C Vaagensmith, Pierce Louis Russell, Craig G Rieger, Justin J Welch, Tyler Bennett Phillips, Stephen Arthur Bukowski, gideon hallman, Chathurika Brahmana, daniel marino

September 2020

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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



Department of Energy Solar Energy Technologies: Advanced Systems Integration for Solar Technologies (ASSIST)

Solar-Assisted State-Aware and ResilienT Infrastructure System (SolarSTARTS) Project

Cyber-Physical System Test Bed

Data Sources, Communications and Controls Formulation

Developers
Bjorn Vaagensmith, Pierce L. Russell, Craig Rieger, Justin Welch, Tyler Philips, Gideon N. Hallman, and Stephen A. Bukowski (INL)
Chathurika Brahmana, Daniel Marino, Milos Manic (VCU)
Contributors
Mohamad El Hariri, Jairo Giraldo, Masood Parvania (UoU)
Amirkhosro Vosughi, Anurag Srivistava (WSU)

Revision: 09/30/20

ACKNOWLEDGEMENT

This material is based upon work supported by the U.S. Department of Energy´s Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-0008775.

DISCLAIMER

Page intentionally left blank

CONTENTS

FIGURES

ACRONYMS

AMI	Advanced metering infrastructure
ASR	Aggregated System Resources
CT	Current transformers
DER	Distributed energy resources
EERE	Energy Efficiency and Renewable Energy
GOOSE	Generic object-oriented substation events
GPS	Global positions system
HMI	Human-machine interfaces
ICCP	Inter-Control Center Communication Protocol
IED	Intelligent electronic devices
IP	Internet Protocol
LAN	Large area network
LDAP	Lightweight directory access protocol
LN	Logic nodes
NIST	National Institute of Standards and Technology
OPC	Open Platform Communications
OSGP	Open Smart Grid Protocol
OSI	Open systems interconnection
PLC	Programable logic controller
PMU	Phasor measurement units
PT	Potential transformers
RBAC	Role-based access control
RTAC	Real-time automation controller
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SEL	Schweitzer Engineering Laboratory
SER	Sequential events recorder
SolarSTARTS	Solar-Assisted State-Aware and ResilienT Infrastructure System
UA	Unified architecture
VLAN	Virtual large area networks
VPN	Virtual private network
WAN	Wide area networks

Page intentionally left blank

1. INTRODUCTION

Statement of Intent

The SolarSTARTS project has the objectives to explore the future landscape of advanced distribution management systems. One of the tasks for SolarSTARTS was to create a cyber-physical test bed with defined communication standards and data-sensing techniques representative of advanced distribution systems. In support of these specific SolarSTARTS tasks, this document outlines various data source and sensor types, control devices, and common communication standards used in industry, and provides justification for which of those were chosen to be represented in the hardware in the loop cyber-physical test bed. Both the SolarSTARTS partners [1]–[3] and other research entities [4]–[6] have developed cyber-physical test beds to evaluate consequence and resilience for cyber-physical, including industrial control systems, where a physical process can be negatively impacted by cyber attacks and damaging storms. Each of these designs considers some combination of hardware in the loop and emulated assets, and often focuses on the power grid. In our application, the evaluation is specific to achieving synergistic human and system resilience. Therefore, this document provides the basis for the design of the test bed, which will facilitate the testing and demonstrating advanced technologies aimed at enabling a future cutting-edge distribution management system.

Definitions

Aggregated System Resources (ASR) is a set of assets that have common objectives. Note that the ASR can be used for many scales. For example, the components of a microgrid, a set of customers in a neighborhood on the same distribution feeders, the whole distribution system, a transmission operator area, balancing authority, etc., could all be ASRs.

Background

The smart grid promises enhanced flexibility to facilitate greater distributed energy resources (DERs) capacity, coupled with improved situation awareness and automated response. The increased penetration of intelligent electronic devices (IEDs) and need for more communication networks between IEDs marks the early transition stages into a smart grid paradigm. The adoption of “smart” technologies arguably started in the 1980s [7], but mass integration into the bulk grid is typically a slow process due to a high focus on reliability. The barrier for smart grid technologies and control strategies adoption continues to escalate as they increasingly introduce new cyber dependencies. Advanced cyber-physical test beds that accurately represent the relationship between the physical power grid and cyber operations are needed to accelerate the development and adoption of smart grid technologies and management strategies. This document presents a hardware in the loop cyber-physical test bed design, which uses a real time power grid simulation via OPAL-RT coupled with network communication to various IEDs (e.g., Schweitzer Engineering Laboratory [SEL] real-time automation controller [RTAC] and relay) as representative of the cyber element. The flexibility of this test bed allows for a variety of power grid designs to be simulated within the OPAL-RT system as well as flexibility on how the model communicates over the network with the IEDs. For this work, the IEEE 33 bus system was chosen as an initial test case because its design is easily modified to test out advanced smart grid methodologies or represent a traditional power system configuration.

DATA SENSORS AND SOURCES

All distribution systems have sensor and source information that help inform power grid operations. Although most distribution system contain minimal measurement devices along feeders (if any). The advanced distribution system of the future will need to tolerate two-way power flow and, thus, require a greater resolution of situational awareness. This section outlines some of the major sensors that are used on power distribution systems today and which types will be included into the cyber-physical test bed.

Current Transformers

Current transformers (CTs) are predominately used for measuring and monitoring the operating current in a power system. CTs consist of a primary winding, a secondary wining, and a core. Utilizing a set ratio of primary and secondary copper windings, CTs step down the input current to a more-manageable, easy-to-measure current in the secondary winding. When an alternating current (AC) signal is passed through the primary, an alternating magnetic field is produced in the core, inducing a subsequent AC signal in the secondary. This secondary AC signal is proportional to the AC signal in the primary. The ration of primary to secondary current is determined by the number of turns in the primary and secondary and is given by the equation $I_S = I_P (N_P / N_S)$. CTs are employed in power systems as a convenient way to measure the large primary current, all while applying a negligible load to the system.

Potential Transformers

Potential transformers (PTs) are used in power systems to measure and monitor the operating voltage of a system. PTs also consist of primary and secondary windings to step down the primary voltage to a safer, more-convenient way to measure voltage. PTs are connected in parallel to the source with the primary windings directly connected to the measurement line and the secondary windings connected to the measurement device. Primary windings consist of many turns, inducing a voltage through the core to the secondary windings, which use less turns. The ratio of input to output voltage is determined by the number of turns in the primary and secondary windings, given by the equation $V_1 / V_2 = N_1 / N_2$. PTs are employed in power systems as a convenient and safe way to measure a large source voltage while applying a negligible load to the system.

Global Positioning Systems

The global positions system (GPS) is a United States government-owned service that provides information on geolocation and time. Satellites that orbit the earth contain ultra-stable atomic clocks and are all synchronized to the same time. The satellites constantly emit radio frequency signals that may be intercepted by GPS devices on the ground or air. The GPS devices are then able to calculate their position based on the position and timing data received from a minimum of four satellites. GPS receivers must be able to determine signal propagation delays, any drift in its own internal clock compared to the GPS satellites, its distance from the GPS satellite, and ultimately is position based off of its distance away from multiple satellites. In power systems, GPS is a convenient way to synchronize the timing of multiple devices that are great distances apart geospatially. The synchronized time-stamped measurements across these devices enable a real-time snapshot of the system.

Fault Indicators

Fault indicators are a small device that clips onto the power line and senses the magnetic or electric field from the alternating current or voltage. When a fault occurs, a signature change in the electromagnetic field is detected, which triggers a flashing LED light (for easy visual discovery) and/or a radio signal to be sent with the location of the fault indicator unit. In the case of low fault current magnitudes (due to cases where the fault current would travel through a high resistance to the detection) the rate of change in the current values rather than magnitudes are used to for fault detection. More

advance fault indicators are able to reset themselves once normal electromagnetic fields are detected on the line for a specific duration of time.

Phasor Measurement Units

Phasor measurement units (PMUs) are used to estimate the attributes of a phasor quantity, such voltage or current. The attributes of the PMU estimates are the phase angle and the magnitude of the phasor. PMUs work by quickly capturing samples from a signal (typically from CTs) at different points in the system and reconstructing the phasor quantity using the angle and magnitude measurements along with a common time measurement from a GPS. The resulting measurement is known as a synchrophasor and provides important insight on frequency imbalances of a power system when compared together with synchophasor measurements throughout the grid. PMUs are employed to detect anomalous activity and abnormal or inconsistent operations. PMUs are primarily used in transmission rather than distribution systems.

Breakers, Reclosers, and Switches

Breakers and reclosers are types of protection devices used to interrupt over current in distribution system from damaging equipment, while switches are mainly used to redirect or interrupt power flow. Breakers are designed to detect and isolate faults quickly and remain isolated until commanded to again close. Reclosers are designed to recognize faults, isolate, and automatically reconnect a predetermined number of times to confirm whether the fault has cleared or is assumed permanent. Switches are designed for manual isolation only when such isolate is desired for maintenance or other reasons. These units typically have remote monitoring and control optional upgrades. The protocols available for remote monitoring or control may vary from vendor to vendor, but typically DNP3, Modbus, and International Electrical Commission (IEC) 16850 are all supported options. The remote status of the breakers, reclosers, and switches provide an understanding of the position, specifically open or closed, to an operator. The access to this status provides a richer, more-diverse data set that can be used for analyzing failures and distinction of cyber versus physical root cause. A direct understanding of this state also provides information that can be used in human or autonomous operations in smart distribution management.

Advanced Metering Infrastructure

Advanced metering infrastructure (AMI) includes communication networks, data management systems, and smart meters that are designed for residential and commercial use and include a number of functions, such as measuring customer electricity consumption on 5-, 15-, 30-, or 60-minute intervals and voltage levels [8]. While automatic meter reading includes only one-way data collection through wireless for nearby collection, such as a vehicle with a receiver, AMI is a two-way interchange. Specifically, voltage, power factor, current, and other electrical variables are transmitted directly to a collection server via wireless or hardwired connectivity for processing, analysis, that consist of feedback to customers and setting time-based rates. In addition, they also confirm outage information for the utility, but due to security considerations are the servers are normally not part of the supervisory control and data acquisition (SCADA) network connectivity. AMI can also be extended to include smart devices (i.e., loads) within a home capable of communicating with smart meters. During peak loading times when the distribution system is stressed, smart meters may reduce or curtail these smart devices to save the customers money and reduce energy demand.

AMI uses its own unique set of standards for transmitting and receiving data. The American National Standards Institute (ANSI) C12.22 was specifically created for transmitting and receiving AMI data and covers both wired or wireless options. The ANSI C12.22 standard has been adopted within North American markets, whereas other standards, such as IEC 61107 or the Open Smart Grid Protocol (OSGP), are more common in European markets. For the purposes of this testbed, no physical smart

meters will be connected to the OPAL-RT simulation and thus these standards are out of the scope for this work. Any AMI capability with the OPAL-RT model will be functionally simulated only.

Voltage Regulators and Tap Changers

Voltage regulators are designed to maintain voltage levels inside substations within acceptable ranges to ensure the proper operation of electrical equipment. Voltage regulators provide 32 steps, 5/8ths percent per step, for a total regulation of +/- 10% of system voltage [9]. Heavy electrical loads and long distribution lines drag down system voltages, providing basis for their use. A voltage regulator senses voltage and is able to add or subtract voltage through a tap changer to provide consistent system voltage levels. The status of the tap changer provides an information that can be used in cross-correlating setting with voltage readings within the substation.

Summary: Test Bed Representation of Data Sources

Modern distribution centers mainly utilize CTs, PTs, and status indications to inform the operations of IED's such as relays or reclosers. PTs are also placed along strategic buses along a feeder to measure the voltage drop and ensure buses further down the line do not experience an under voltage. PMUs are typically used on transmission systems as distribution systems typically experience much smaller changes in phase angles and therefor require a much higher precision measurement [9]. Micro-PMUs are a newly emerging technology that exhibits enhanced accuracy for phasor measurements within distribution systems but have not experienced widespread adoption.

Current implementations of the SolarSTART's cyber-physical test bed only contain real-time simulation of power systems operations within MATLAB/Simulink. Thus, all power system measurements and implementation strategies must also be simulated in the Simulink environment. Simulink provides an easy way to do this via current, voltage, and other measurement blocks such as AMI, which simulate CT and PT operations, and other status indications. The main drawback with the OPAL-RT MATLAB/Simulink solution is automatic synchronization of measurement through the way time steps are handed. In real systems, synchronization would require GPS and complex time management systems to handle variable-latencies of measurements throughout the network. While developing time management systems for power system networks is outside the scope for SolarSTARTS, it is worth noting as an underlying assumption that girding any results generated off OPAL-RT based test beds that simulate large systems, such as distribution networks. The smaller the system simulated with short line lengths, the less-relevant variable-latencies from measurement systems to IEDs becomes.

COMMUNICATION PROTOCOLS

Modern distribution power systems utilize many different types of communication protocols that vary based on regional popularity (e.g., Europe versus United States) or function of the communication. This section aims to highlight some of the more popular protocols that could serve as potential candidates for enabling advanced distribution communication and control systems and justifies the selection of protocols to be used within the proposed cyber-physical test bed.

Modbus

Modbus was first developed in 1979 as a communication protocol between programable logic controller (PLC) unit devices. The standard became very popular due to its easy implementation and open access to the standard. Modbus is supported by a variety of different transmission protocols for asynchronous serial transmission, TCP/Internet Protocol (IP), and Modbus plus, which allows the protocol to be used across many different device types across a large area network (LAN), such as human-machine interfaces (HMIs), PLCs, relays, network gateways, and other input/output (I/O) devices [11]. With the adoption of TCP/IP into the standard, communication to many power system devices and SCADA applications became possible. The data packets used over Modbus were variable in size depending on how large the data field was. This caused issues with data integrality as portions of very large-sized packets may have become corrupt or disrupted during transmission. The biggest drawback of the Modbus protocol was a lack of security with data or command authentication, which made systems using Modbus vulnerable to cyber attacks such as man-in-the-middle or spoofing.

IEC 60870 Standard

The IEC 60870 standard was first introduced in 1990 for remote control of power system operations. The standard adheres to the open systems interconnection (OSI) model and focuses on the physical, data link, and application layer. The standard originally suffered from a broad execution interpretability, which led to a large variety of incompatible manifestations of the 60870 standards [12]. To solve this issue, the standard was updated in 2001 to better define how different devices should communicate. The updated standard also required devices on a network to have present instructions regarding packet structures to avoid sending this information within the packets themselves, which improves communication efficiency. Coupled with an update from 2000, the standard also supported TCP/IP communication between substations and control centers. Despite these updates, the standard still lacked clarity for specific use cases, again resulting in diverse implementations, and the TCP/IP implementation was operationally restrictive, limiting information types and configuration parameters.

Distributed Network Protocol 3 (DNP3)

The distributed network protocol 3 (DNP3) was originally designed for SCADA applications and made available to the public in 1993. DNP3 focused on sending multiple smaller sized packets in a deterministic sequence to enhance communication reliability and error detection. DNP3 has been widely adopted by North American power utilities as well as gaining popularity within the water, oil, and gas industries [11][12]. For use over LANs, DNP3 needs to be wrapped up inside an IP such as TCP/IP. DNP3 has adapted to support a wide range of communication modes, such as traditional client/server, peer-to-peer, multi-master, and hierarchical. The adaptivity and flexibility of DNP3 to industry demands coupled with its high degree of reliability has made it the dominate protocol of choice for modern-day power distribution networks in North America today [11][12].

Open Platform Communications Unified Architecture (OPC-UA)

The Open Platform Communications (OPC) was first introduced as on open standard in 1996 for automation control devices to interface with HMI. The standard was later updated in 2008 to the unified architecture (UA) version, which included many of the legacy feature of previous versions, such as

accessing process data, transmitting events or alarms, transferring historical data, and leveraging eXtensible Markup Language (XML) to encode data access. OPC-UA also aimed to be operating system agnostic and offered security features, such as encryption and user authentication. Although popular within industrial processes, OPC-UA was not widely adopted within the power system community [13]. Microgrids on the other hand, have made OPC-UA a popular choice for communicating their automation controls [13][14].

Telecontrol Application Service Element 2 (TASE.2)

The Telecontrol Application Service Element 2 (TASE.2), also referred to as Inter-Control Center Communication Protocol (ICCP), was first standardized by the IEC in 1997 for control center communication over wide area networks (WAN). To support better situational awareness, TASE.2 enables time stamping for an effective real-time snapshot of system data and is also helpful for historical data analysis. TASE.2 leverages message manufacturing service standard for the transfer of timestamped data, which was already an established protocol within industry [17]. The object-oriented approach used in TASE.2 enables compatibility across many applications and devices [18]. The preset list of defined objects in the protocol can also be updated with time to suit the needs of the power industry. In the U.S., TASE.2 is widely used to tie regional operators together [11], but is not found on distribution systems. Important features for smart grid operations contained within TASE.2, such as timestamping, have also been made available with protocols more commonly used in distribution systems (e.g., DNP3).

IEC 61850 Standard

First published in 2003, the IEC 61850 sought to introduce a standard focused on automation and flexibility for intelligent substations. The United States National Institute of Standards and Technology (NIST) has identified this as one of five “foundational” standards for smart grid interoperability and cybersecurity [19].

The standard introduces its own substation configuration language based of XML, a high-level programming language compatible with a wide variety of communication protocols, to facilitate system wide component configuration. Substation communication is binned into one of three different categories: process level (e.g., I/O devices and sensors), unit level (e.g., protection and substation devices), and substation level (the control computer or operators control HMI). Within each of these communication levels, a series of protection and control function are defined for various objects (also referred to as logic nodes [LN]). Each object (LN) corresponds to various substation device functions and can be grouped to from logical devices, which represent IEDs. The protocol also includes provisions for transmitting generic object-oriented substation events (GOOSE). Although previous protocols allowed for custom applications to configure and automate substation settings and operations, the IEC 61850 includes specific instructions for how to do this with definitions for over 100 LN and more than 2000 data objects or data attributes. Additionally, users can access information hierarchies based on all LN and objects to gain a sense for how substations are logically organized.

The main drawback of the IEC 61850 is the higher degree of complexity compared to legacy protocols. The IEC 61850 is cited to have a steep learning curve and require a significant effort to implement [11]. Because of these difficulties and the lack of manpower to support a significant upgrade, the IEC 61850 has not been widely adopted within North America [15][16].

Summary: Test Bed Representation of Communication Protocols

Due to its wide adoption in North America, DNP3 was chosen for the cyber-physical test bed. Those actions that would normally require a high-frequency-communications protocol are already integrated within the model; therefore, a hardware implementation is not necessary. Additional expansion of the DNP3 protocol coupled with Modbus and OPC-UA may be considered for external control and communication with local microgrids within the distribution network within the cyber-physical testbed.

CONTROLS

System controls and monitoring are the core of a future distribution management system. In a modern grid, data is collected by IED's in the field and transmitted back to control center for remote control and monitoring of the system. While monitoring some of these operations has been discussed previously, this section discusses the control features that are pertinent for consideration in a cyber-physical test bed.

Voltage Regulators and Tap Changers

As mentioned in Section 2.8, voltage regulators are designed to provide distributed voltage controls through the variation of tap changers. The tap changer operation changes the configuration of the auto transformer coil resulting in a change in the voltage. These changes can be preprogramed for time of day or other automated switching and settings updates where no communication is needed. There are also smart tap changers that can be controlled, monitored, and updated remotely, these units typically communicate with DNP3 and Modbus.

Reclosers

Remote control of reclosers would allow for reconfiguring the distribution system for repairs or special cases, as these are designed for automated response to failures and clearing by design. Most large manufacturers (SEL, ABB, Siemens) incorporate multiple communication hardware into their IEDs. This not only allows for a larger customer market, but it enables a customer to have multiple communication methods. For example, SEL devices have serial and IP communication standard, with options to add a secondary isolated IP, fiber, or serial communication cards for redundancy. The test bed is model for North American utility systems and will use their predominant communication choice, previously mentioned in section 3.3, DNP3 over TCP/IP for control, monitoring, and remotely updates.

Capacitor Banks

The remote control of capacitor banks is provided for the reactive power controls, that can include monitoring and feedback to maintain the prescribed power factor within the bus monitored. These devices can have drastically different controls based on the desired use. Some units require their own CT/PT connections to power the controls and are preprogramed to operate the capacitor bank when needed. Other devices are designed for remote control and monitoring and require DNP3 over TCP/IP or IEC 61850 connections. For the test bed modeled after the North American utilities, DNP3 over TCP/IP will be used for communication.

Summary: Test Bed Representation

The test bed representation of the controls will be through the ability to modify switch and variable settings within the IEEE 33 bus model to initiate the operations required. The inclusion of recloser, breaker, and relay devices, as well as and reactive power controls and voltage regulation can be incorporated, as needed, to allow for testing of the individual cyber-physical scenarios. The functionality of these smart devices will largely be simulated without the need for communication protocols to reduce the computational expense of the model. Where it is relevant to represent cyber traffic in the model, these devices will be monitored and controlled with the DNP3 over TCP/IP standard, as that is the best representation of the North American utility systems.

APPROACH/DESIGN/IMPLEMENTATION

High-level System Configuration

Automation can enhance system response times to changes or disturbances and optimize power delivery efficiency with system performance. For example, current systems may rely on a single-voltage regulator at the substation and a voltage measurement at a midway point in the feeder to tune voltage levels and manage the voltage droop at the end of the feeder. The integration of IEDs and multiple DERs may solve the voltage droop issue and enable a flatter voltage profile along the feeder, thus freeing up thermal capacity within the system.

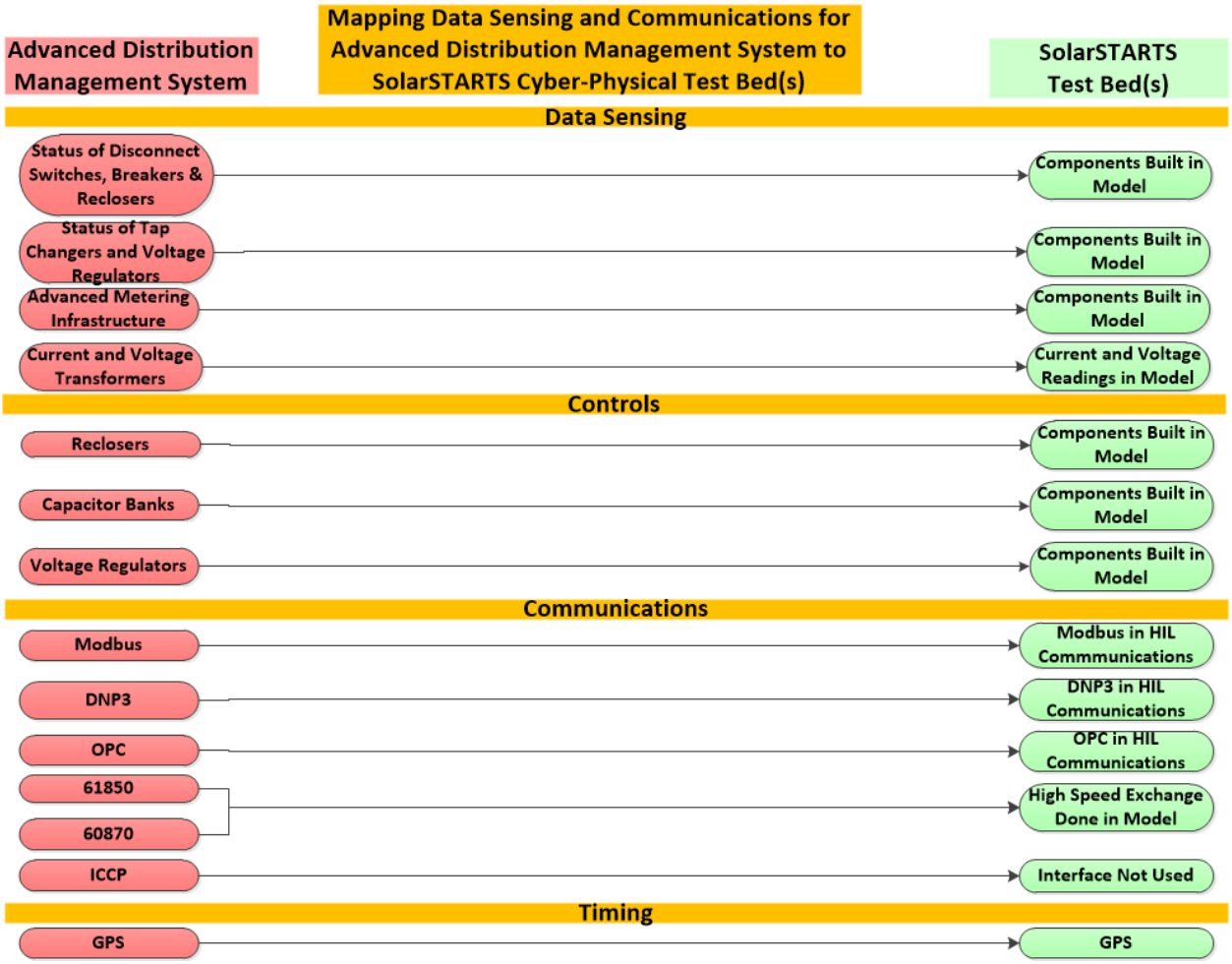


Figure 1. Mapping of advanced distribution management to SolarSTARTS test bed application.

In addition to voltage regulation, IEDs may also facilitate two-way power flow control. This enables systems to have much greater flexibility to support the bulk power grid compared to the old hierarchical-based paradigm and allow more parties to compete in power grid energy markets. Despite complex distributed real-time controls providing a larger cyber-attack surface, the enhanced system flexibility lends itself to a higher degree of resilience against physical scenarios like natural disasters—the number one threat to modern power grid systems.

To address the cyber and system reliability concerns for implementing complex distributed control systems, a hardware in the loop cyber-physical test bed designed to test power grid cybersecurity and modern control schemes will be designed, leveraging SolarSTARTS partner contributions. For the data

sensing and sources, communications, controls and timing, the mapping in Figure 1 provides a crosswalk on how each will be implemented. As the power distribution system model integrates direct access to many of the data sensing and sources previously described, many of the specific communications protocols, such as IEC-61850, are not necessarily needed to demonstrate the advanced research and development products of this effort. Therefore, normal data highway communications, such as between a substation automation controller and the HMI would be the only necessary to implement in hardware, in particular DNP3 but also potentially Modbus and OPC for external communications. To provide certain data source and controllable aspects, such as reclosers, logic would be added to the power model as needed to represent disturbance conditions defined in the separate cyber-physical scenarios report.

A modified IEEE 33 bus distribution system was developed in MATLAB/Simulink to serve as the power model and run on an OPAL-RT for real-time communication on a control network, from which cyber data was generated. The use of OPAL-RT systems allows for flexible implementation of various DER and control schemes within the IEEE 33 bus model. Malicious payloads and attacks may also be carried out over the control network to test and fine tune innovative cybersecurity practices. Background detail on the IEEE-33 bus model will next be described.

IEEE-33 Bus Mode

Figure 2 shows a one-line diagram of the proposed modified IEEE 33 bus model. For enhanced flexibility, tie lines according to [20][21] have been added. Each bus is equipped with various types of faults (line-ground, line-line, etc.) that may be implemented to test physical system response and reconfiguration control schemes. The system is divided up into logical control units, ASRs, which were selected based on logical bus groupings (e.g., Buses 23–25, 26–33, and 19–22) or by breaking up a large string of buses into even parts (e.g., breaking up Buses 1–18 to groupings of 1–6, 7–12, and 13–18). Each ASR contains an intelligent control agent that govern and coordinate with neighboring ASRs.

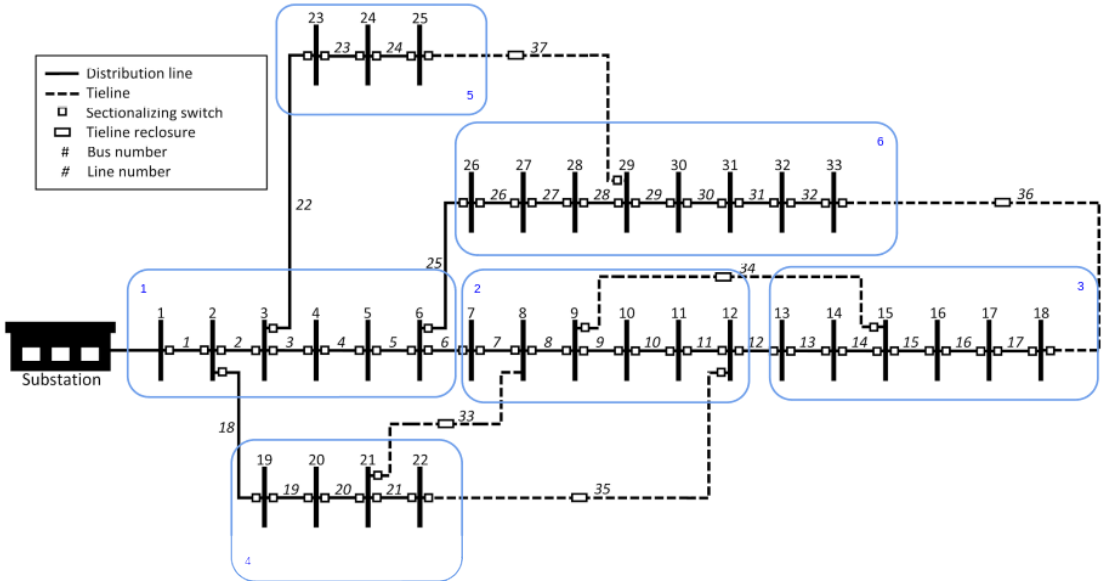


Figure 2. One-line diagram of the modified IEEE 33 bus system with ASR designations.

The Simulink model simulates breaker commands, reclosure commands, disconnect commands, and voltage/current/breaker status measurements. Information from these model components can be fed into the control system network via DNP3 protocols through the digital output connections from the OPAL-RT I/O ports. The control system network is composed of an SEL RTAC and relays from which commands over DNP3 can be sent back into the IEEE 33 bus model running on the OPAL-RT system.

Pi-lines were used to model power lines in the distribution system as they provide lower computational burden and tolerate larger time steps of 50 microseconds, as opposed to Simscape's distributed parameter line block. Although PI-lines are less accurate compared to distributed parameter blocks, they are an appropriate approximation for power lines less than 3,105 miles in length, which is less than the length of distribution power lines. These power lines modes also include three phase breaker control as well as a fault block, which can generate any type of fault desired (e.g., line-to-line or line-to-ground of various phase combinations).

OPC/DNP3 Connections

Figure 3 shows one high-level network diagram of one of the SolarSTARTS partners responsible for generating the cyber traffic within the test bed. The power model within the OPAL-RT system (see Figure 2) will communicate via OPC-UA protocol or DNP3 with RTAC and relay devices through a Cisco switch connected to the Internet. Although power control system networks will likely be air gapped, this can be defeated by planting a rogue device within the control network. Access to this air-gapped network may become more available as the bulk distribution network experiences increased deployment of control devices and communication lines. A connection through Idaho National Laboratory's demilitarized zone network will allow project collaborators to also access this test bed. Various virtual large area networks (VLANs) have also been set up to simulate various roles in the test bed: grid operator HMIs, CySTAR, a malicious attacker, and a database to log and store data from the test bed.

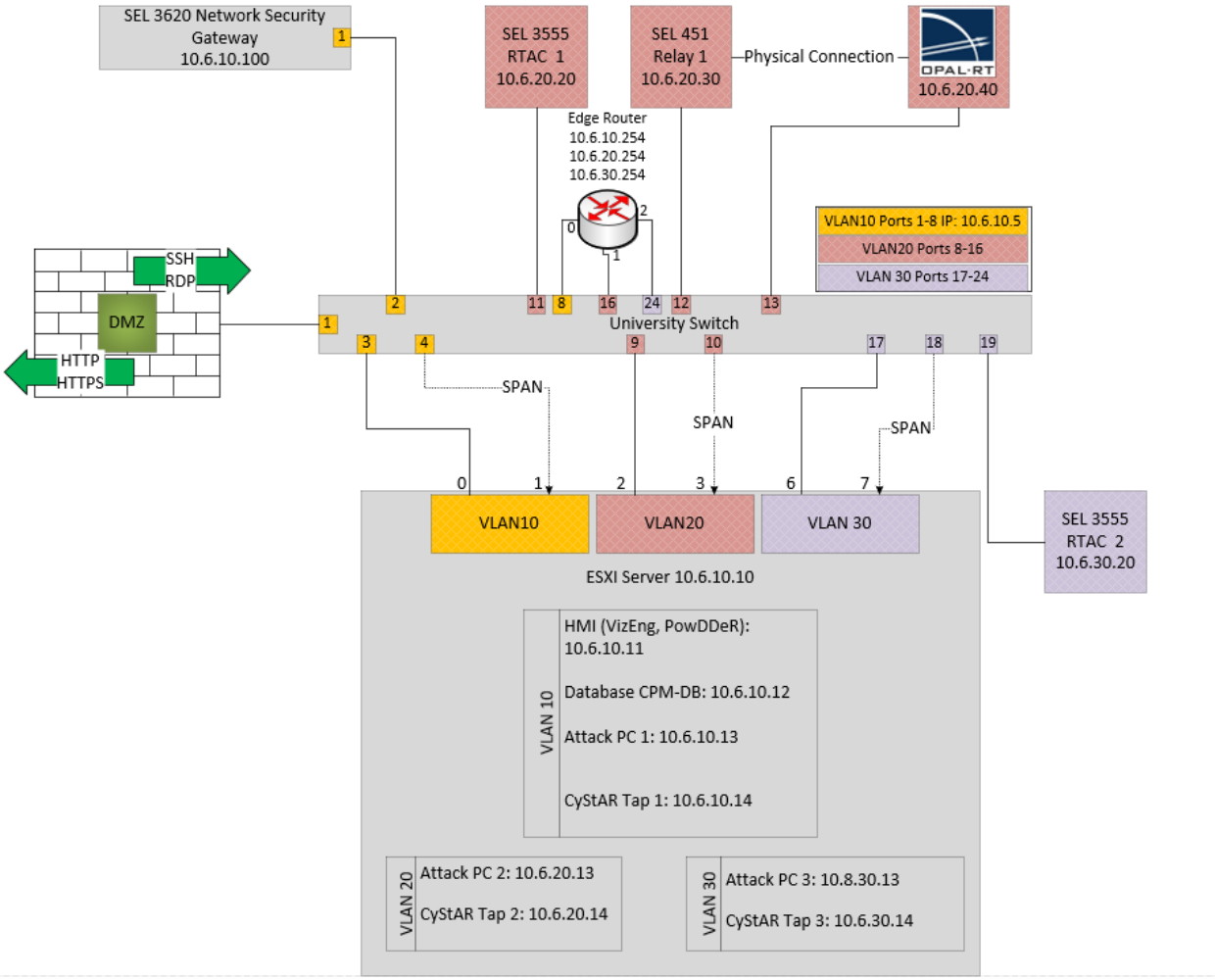


Figure 3. High-level network diagram of one SolarSTARTS partner.

Other External Hardware

The IEEE 33 bus system currently utilizes three different SEL equipment: a RTAC 3555, Relay 451, and a SEL-3620 security gateway. The model can be configured to communicate with both the RTAC and relay from any ASR within the model.

The SEL RTAC 3555 (Figure 4) has many applications in secure power systems and offers a wide range of features. The SEL-3555 can be used as a network security device, providing a secure access point with access control protocols, such as lightweight directory access protocol (LDAP) and role-based access control (RBAC). The SEL-3555 features a substation HMI that allows the user to directly connect to the RTAC for local or remote monitoring and control. The SEL-3555 can also be used as a SCADA remote terminal unit (RTU) for integration and automation for small or large projects that need customizable data collection, logic functions, and output logic. The SEL RTAC 3555 is typically leveraged to enable precise control and automation of critical infrastructure.

Figure 4. Photograph of SEL RTAC 3555.

The SEL Relay 451 (Figure 5) is a standalone bay control protection and automation system from Schweitzer Engineering Laboratories. The SEL Relay 451 provides critical bay control and breaker protection functionality to power systems infrastructure. This bay control system contains a variety of protection applications with high-speed breaker failure detection, breaker wear monitoring, and high-impedance fault detection to decrease downtime and costs, and help determine the need for proactive maintenance. The SEL 451 also provides users with local and remote control of motor-operated switches, capacitor banks, and field I/O with easy access to relay status, information from meters, sequential events recorder (SER) data, and settings. The bay control system also provides a web server to access password-protected read-only information. The SEL Relay 451 is currently implemented in the protection, automation, and control of bay systems, providing access and control to critical system information.

Figure 5. Photograph of SEL Relay 451.

The SEL-3620 (Figure 6) is a robust ethernet security gateway from Schweitzer Engineering Laboratories. The SEL-3620 provides applications in network security, acting as a virtual private network (VPN) endpoint, router, and firewall device. The SEL-2620 provides a centralized point of entry for the protection of ethernet-based IEDs, as well as access controls and activity logs. In addition, the SEL-3620 provides security features with embedded antivirus algorithms, user access time stamp logs, and a powerful firewall with a menu-driven interface. The SEL-2620 is being implemented in power systems as a robust security gateway for IEDs, providing protection to critical cyber assets in power systems engineering.

Figure 6. Photograph of SEL 3620 ethernet security gateway.

SUMMARY AND CONCLUSIONS

This document has provided the planned groundwork for establishing a cyber-physical test bed representative of a future advanced distribution management systems in support of the SolarSTARTS project tasking. A mapping of the data sources or sensing, communications in addition to controls and timing are illustrated in Figure 1. Various voltage, current, and other sensors and sources will be included in the real-time OPAL-RT simulation. DNP3 were chosen as the communication states that would be more representative of North American utilities. Some hardware implementation to validate real-world results include the at least one relay and RTAC, and an HMI will be used in addition to security appliances to communicate with the real-time simulation to generate cyber traffic. Lastly, the IEEE 33 bus system broken up into six controllable areas was chosen for its flexibility to transition between operating as a modern-day distribution system or as a future advanced distribution management system.

REFERENCES

[1] B. Vaagensmith, J. Ulrich, J. Welch, T. McJunkin, and C. Rieger, "IEEE 13 Bus Benchmark Model for Real-Time Cyber-Physical Control and Power Systems Studies," in *2019 Resilience Week (RWS)*, 2019, Vol. 1, pp. 112-120.

[2] M. M. S. Khan, A. Palomino, J. Brugman, J. Giraldo, S. K. Kasera and M. Parvania, "The Cyberphysical Power System Resilience Testbed: Architecture and Applications," in *Computer*, Vol. 53, No. 5, pp. 44-54, May 2020.

[3] V. Venkataramanan, P. S. Sarker, K. S. Sajan, A. Srivastava and A. Hahn, "A Real-Time Transmission-Distribution Testbed for Resiliency Analysis," *2019 IEEE Industry Applications Society Annual Meeting*, Baltimore, MD, USA, 2019, pp. 1-7.

[4] U. Adhikari, T. Morris and S. Pan, "WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining," in *IEEE Transactions on Smart Grid*, Vol. 8, No. 6, pp. 2744-2753, Nov. 2017

[5] A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," in *IEEE Transactions on Smart Grid*, Vol. 4, No. 2, pp. 847-855, June 2013

[6] S. Poudel, Z. Ni and N. Malla, "Real-time cyber physical system testbed for power system security and control," International Journal of Electrical Power & Energy Systems, Vol. 90, September 2017, pp. 124-133.

[7] I. S. Bayram and T. S. Ustun, "A survey on behind the meter energy management systems in smart grid," *Renewable and Sustainable Energy Reviews,* Vol. 72, pp. 1208-1232, 2017/05/01/ 2017.

[8] Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investment Grant Program, Department of Energy Report, September 2016.

[9] Voltage regulators: fundamentals of voltage regulators, http://eaton.com.

[10] A. v. Meier, D. Culler, A. McEachern, and R. Arghandeh, "Micro-synchrophasors for distribution systems," in *ISGT 2014*, 2014, pp. 1-5.

[11] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in *2009 IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1-9.

[12] A. Volkova, M. Niedermeier, R. Basmadjian, and H. d. Meer, "Security Challenges in Control Network Protocols: A Survey," *IEEE Communications Surveys & Tutorials,* Vol. 21, No. 1, pp. 619-639, 2019.

[13] I. González, A. J. Calderón, J. Figueiredo, and J. Sousa, "A Literature Survey on Open Platform Communications (OPC) Applied to Advanced Industrial Environments," *Electronics,* Vol. 8, No. 5, p. 510, 2019.

[14] P. Jafary, S. Repo, M. Salmenpera, and H. Koivisto, "OPC UA security for protecting substation and control center data communication in the distribution domain of the smart grid," in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, 2015, pp. 645-651.

[15] R. Borscia. (June 8). *IEC61850 companion specification for electrical substation automation systems*. Available: https://opcfoundation.org/markets-collaboration/iec61850/

[16] B. Milschiltz. (2018, September) IEC 61850 What Are You Waiting For? *EET&D Magazine*. Available: https://electricenergyonline.com/energy/magazine/1164/article/IEC-61850-What-Are-You-Waiting-For-.htm#:~:text=Since%20its%20release%20in%202003,do%20so%20in%20North%20America.

[17] S. G. Shanmugham, T. G. Beaumariage, C. A. Roberts, and D. A. Rollier, "Manufacturing communication: A review of the MMS approach," *Computers & Industrial Engineering,* Vol. 28, No. 1, pp. 1-21, 1995/01/01/ 1995.

[18] C. Guo, Y. Cao, Y. Tang, and Z. Han, "An open architecture for information communication systems for multi-level electric power control centers," *Kybernetes,* Vol. 39, No. 8, pp. 1270-1281, 2010.
[19] D. C. Mazur, J. Sottile, and T. Novak, "An electrical mine monitoring system utilizing the IEC 61850 standard," in *2013 IEEE Industry Applications Society Annual Meeting*, 2013, pp. 1-10.
[20] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Transactions on Power Delivery,* Vol. 4, No. 2, pp. 1401-1407, 1989.
[21] H. Hong, Z. Hu, R. Guo, J. Ma, and J. Tian, "Directed graph-based distribution network reconfiguration for operation mode adjustment and service restoration considering distributed generation," *Journal of Modern Power Systems and Clean Energy,* Vol. 5, No. 1, pp. 142-149, 2017/01/01 2017.

Appendix A

OpOutput Block

OpOutput block allow measurements to be read off the model into OPAL-RT user console or various I/O ports. Figure A-1 shows an example of how these blocks by tie into the model, and where the data lines from Out1, Out2, and Out3 correspond the real and reactive power consumption from the loads modeled inside the magenta block. These OpOutput blocks could also be tied into the V_{abc} or I_{abc} measurements from the 634 V-I block. OpOutput and OpInput tags are commonly used by OPAL-RT to communicate between master, slave, and user console sections of the model.

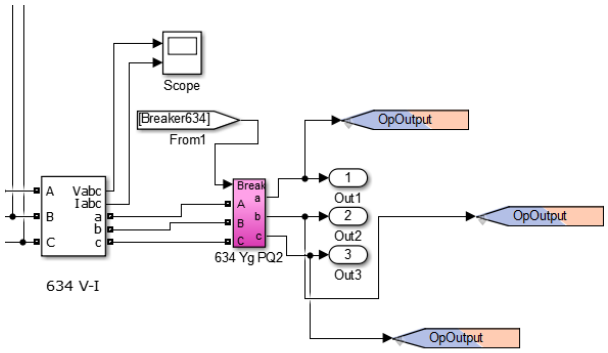


Figure A-1. Simulink example of how to tie OpOutput blocks into the model.

To communicate with OPAL-RT OPC-UA server, the user is required to create two ASCII text files: connections.opal and OPC_UA_Server_sfg.opal. An example of the connections.opal file and how its parameters inform the server where to tie into the model is shown in Figure A-1. The file has two main sections containing outputs and inputs, which are used to send data from the OPAL-RT OPC server to the client and from the client to the OPAL-RT OPC server, respectively. Within each of these sections contains information about the varrable names (as displayed in the OPC server), filepath, simulink OpOutput/OpInput identifier, and if the varaible is a scalar or array of a specified size. A useful feature of arrays is that they are able to contain multple vairables. For example, from Figure A-2 the OpOutput blocks contain real and reactive power data (i.e., P and Q data); therefore, the block must be stored in an array with two elements.

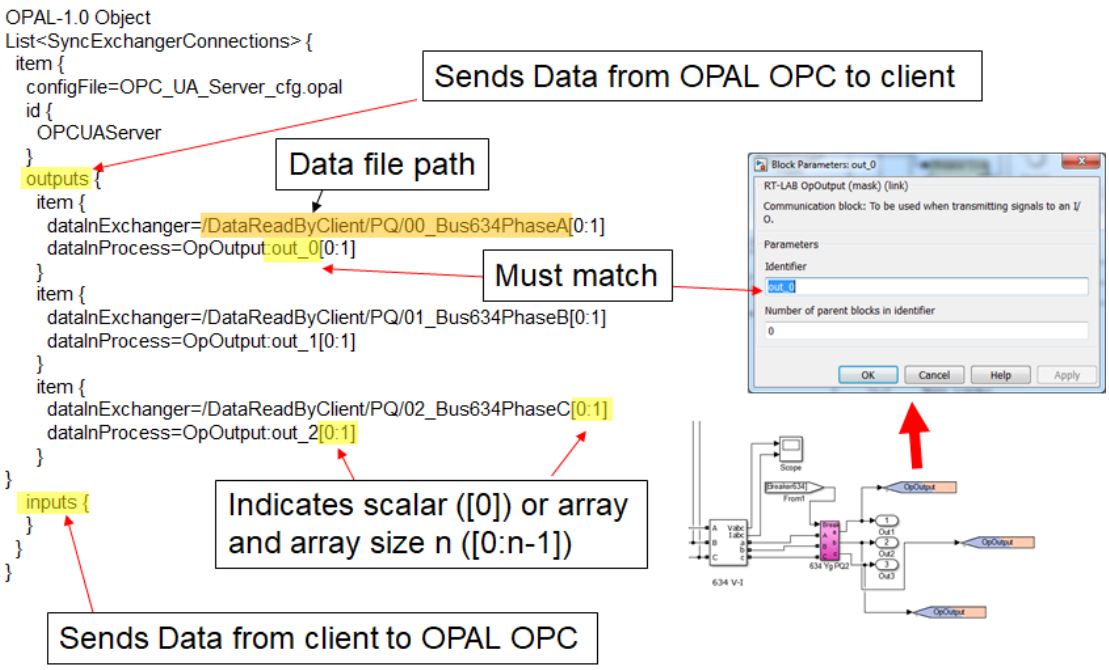


Figure A-2. Example of how the connections.opal file ties into the model to allow for OPC communications.

The second file, OPC_UA_Server_sfg.opal, configures the OPC-UA server to process the data it recieves from the model. Figure A-3 illustrates the configuration file format and how it ties together with the connections.opal file. The configuration file has a series of items that list information about each variable that will be exchanged between the model and the server. It lists information about the variable name (as desplayed on the OPC server), variable type, intial values of the variables, direction (as to whether its being sent to or form the server), variable file path (to diplay on the OPC-UA server), DNP3-type connections can be implemented via the RT-LAB GUI interface. In the project Explorer panel, expand the project folder and right click on ***I/O Interfaces*** then select ***New →New I/O Interface***. The following dialog box is opened in Figure A-4, which allows you to select the type of DNP3 interface to add into the model. Once added, a new DNP3 tab (Figure A-4) will be available to configure the DNP3 settings as well as view different data types available from the OpOutput and OpInput blocks (see Figures A1-A3) within the model.

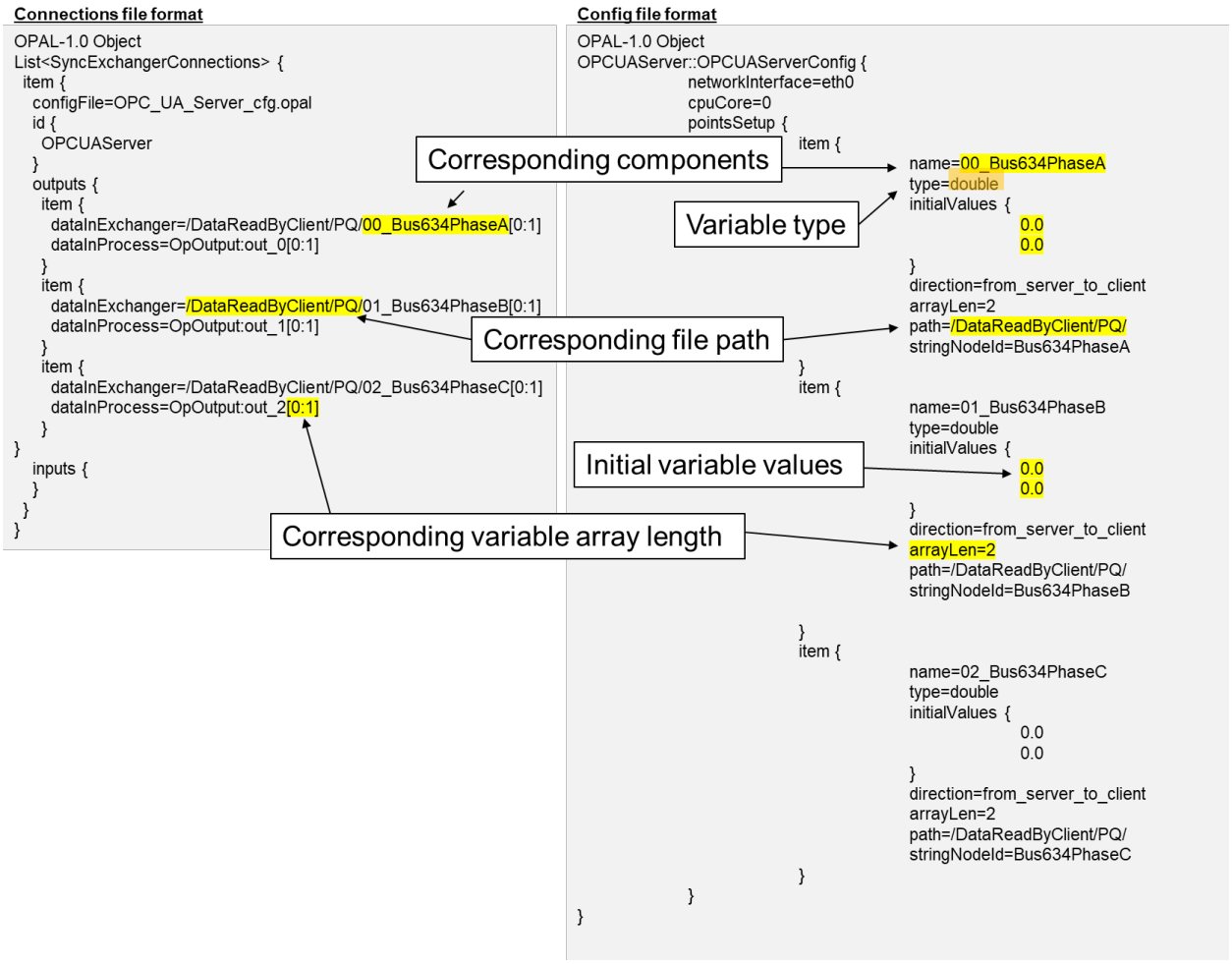
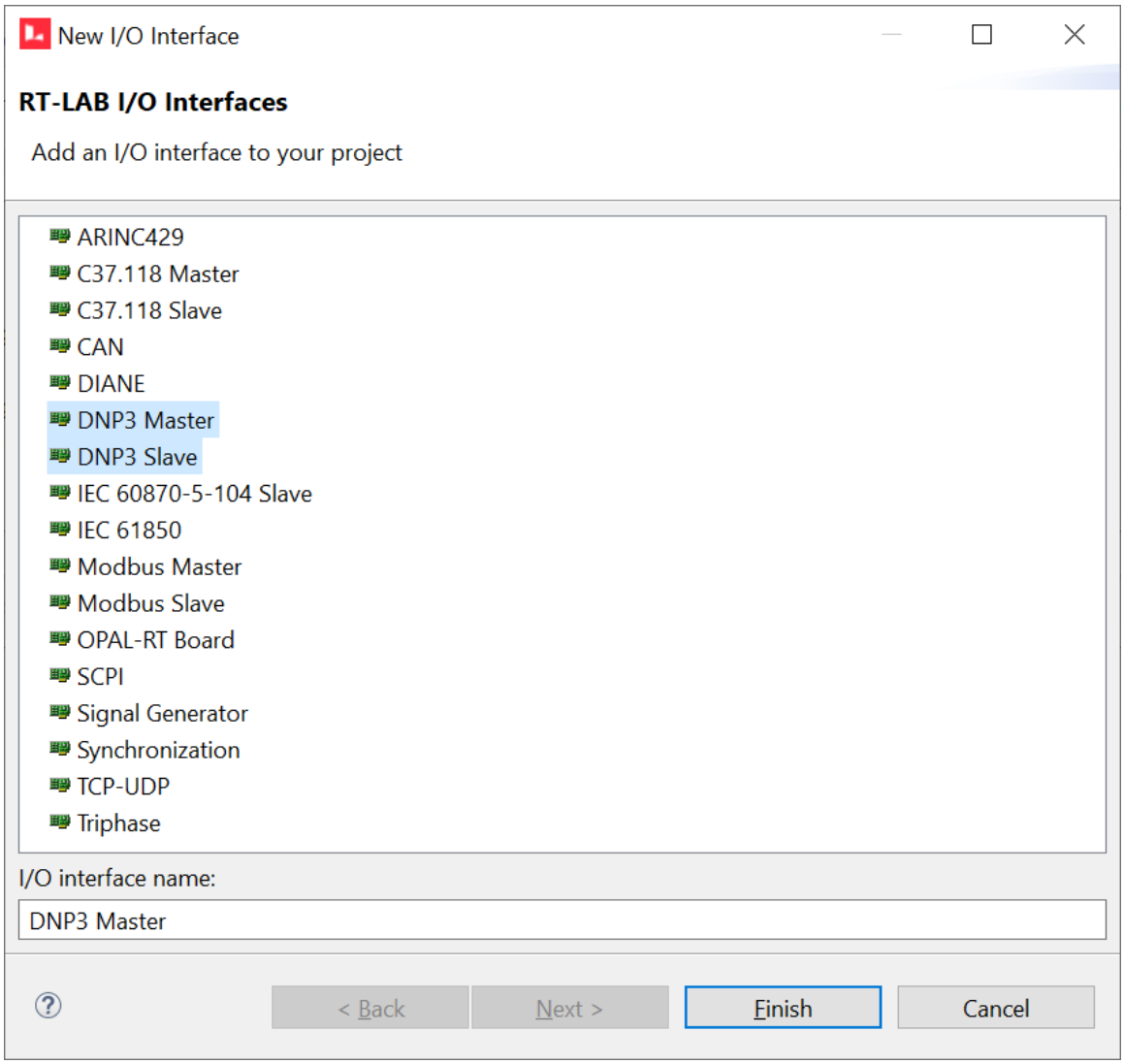


Figure A-3. Illustration of how the OPC_UA_Server_cfg.opal file connects to the connections.opal file.

(a)



(b)

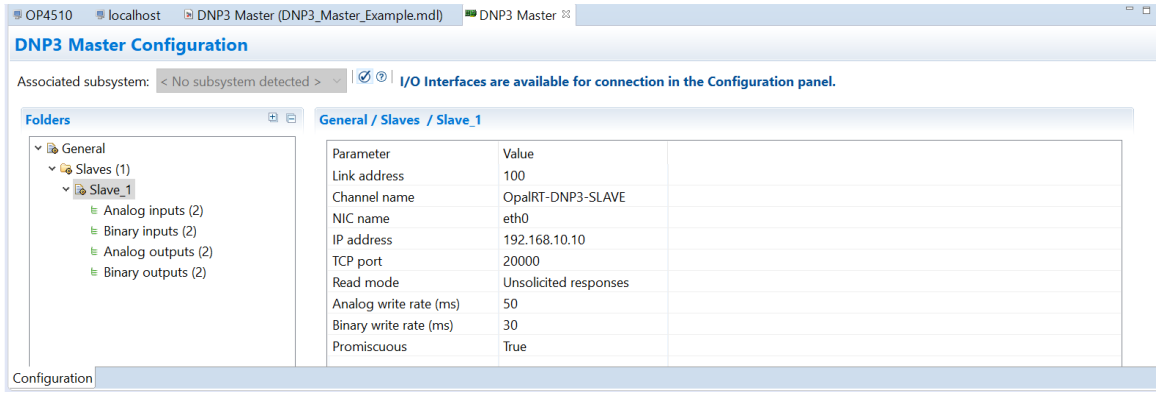


Figure A-4. (a) RT-Lab I/O interface option panel for addition additional communications protocols to the model and (b) the additional DNP3 tab that becomes available after selecting the DNP3 from (a).