LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-839146

Energy Resilience for Mission Assurance: Agile Co-simulation for Cyber Energy System Security (ACCESS), Model Advancements for Resilience Analysis

B. M. Kelley, H. Scott, C. Sun, N. Venethongkham

August 24, 2022

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Energy Resilience for Mission Assurance

Agile Co-simulation for Cyber Energy System Security (ACCESS) Model Advancements for Resilience Analysis

August 2022

Brian M. Kelley
Heather Scott
Chih-Che Sun
Noah Venethongkham

LLNL-TR-839146

Acknowledgements

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

We thank the ACCESS software development team members for their valuable contributions:

Nan Duan

Kendall Harter

Shayna Kapadia

Brian M. Kelley

Christopher Lawson

Aaron Otis

Steve Smith

Chih-Che Ryan Sun

Noah Venethongkham

Nathan Yee

Acronyms and Abbreviations

ACCESS - Agile Co-simulation for Cyber Energy System Security

CSV - Comma Separated Value

DCEI - Defense Critical Electric Infrastructure

ERMA - Energy Resilience for Mission Assurance

HELICS - Hierarchical Engine for Large-scale Infrastructure Co-Simulation

ICS - Industrial Control System

JSON - Java Script Object Notation

LAN - Local Area Network

LBNL - Lawrence Berkeley National Laboratory

LLNL - Lawrence Livermore National Laboratory

MDT - Microgrid Design Toolkit

NND - Ns-3 Network Definition

NREL - National Renewable Energy Laboratory

ONG - Oil and Natural Gas

SCADA - Supervisory Control and Data Acquisition

SNL - Sandia National Laboratories

QoS - Quality of Service

WAN - Wide Area Network

WNTR - Water Network Tool for Resilience

Contents

1 Introduction

Agile Co-simulation for Cyber Energy System Security (ACCESS) is a co-simulation platform developed by Lawrence Livermore National Laboratory (LLNL). The primary high-level use-case for ACCESS is to study existing or new cyber-physical critical infrastructure systems, with a heavy emphasis on 1) systems that utilize communication networks, and 2) studies that seek to understand cyber-related system impacts. ACCESS is currently used for several energy system resilience projects at LLNL.

In the Energy Resilience for Mission Assurance (ERMA) project, ACCESS is used in the *Modeling for Metric Calculation* task (specifically, subtask 4.3, *Communications and Cyber Modeling*) to model and simulate the cyber and communication system aspects of Defense Critical Electric Infrastructure (DCEI) systems, with a focus on computing specific communication system metrics that can impact system resilience and mission performance. Simulated communication system performance will be fed back to other ERMA system components so that mission performance can be evaluated holistically.

This report describes several enhancements to the ACCESS platform that were implemented during the execution of the ERMA project in support of reslience analysis. This includes the addition of new models and subsystems, enhancements to existing models, and integration with external systems.

The remainder of this report is structured as follows. In Section 2, a brief background description of the ACCESS platform is provided, including an outline of ACCESS components, example use-cases, and a set of communication network resilience metrics that can be computed with ACCESS. Section 3 describes the ACCESS model enhancements for ERMA in detail. Finally, Section 4 briefly outlines future integration opportunities between ACCESS and project participant capabilities identified during the progression of the project.

2 Background

ACCESS development was instigated by a LLNL initiative in 2019 aimed at streamlining the co-simulation development workflow for LLNL projects. Co-simulation, and modeling and simulation more generally, involves many activities, including:

1. Coupling of simulators to facilitate data exchange and time synchronization, using frameworks like the Hierarchical Engine for Large-scale Integrated Co-Simulation (HELICS) [2]
2. Creation and parsing simulator input files
3. Development of models
4. Development of connectors for simulators and subsystems
5. Workflow management and orchestration for ensemble simulations

ACCESS provides these services and simulation infrastructure to co-simulation projects so that they don't have to re-implement existing functionality, thus ultimately accelerating project execution.

2.1 ACCESS Components

At its core, ACCESS uses the ns-3 discrete event network simulator [7] to simulate communication networks. ACCESS defines a JSON-based input file format called Ns-3 Network Definition (NND) that describes the topology and composition of a simulated communication network. Users can manually and programmatically generate NND files that represent the communication networks under study. The current version of the NND format as of this writing is v0.4, and minor additions, described in section 3.1, were made to the NND format in support of the ERMA project.

Ns-3 does not implement a native co-simulation capability, so ACCESS wraps ns-3 with an interface layer that allows ns-3 models to interact with other simulators using the HELICS co-simulation platform. ACCESS users can specify HELICS data subscriptions and publications in NND configuration files so that data is exchanged between components of different simulators; this is useful for modeling cyber-physical aspects of, for example, intelligent electronic devices in electric transmission and distribution systems that have a presence in both a communication network and a power system. New coupling and data exchange methods between ACCESS and external systems, both via HELICS and manually via input and output files, were developed during ERMA and are described in sections 3.3, 3.4 and, 3.5; thoughts on future integrations with external systems provided by ERMA project participants are outlined in section 4.

ACCESS expands the myriad communication system models provided by ns-3 with models for cyber-physical critical infrastructure systems. This includes a basic sensor, Industrial Control System (ICS) protocols, packet filtering, Supervisory Control and Data Acquisition (SCADA) data aggregators, and intelligent agents. A new generic controller model, described in section 3.2 was developed for ACCESS during the ERMA project.

Simulation workflow tools to support parameter studies, sensitivity analyses, and ensemble simulations in general, were integrated into ACCESS; this integration is described in section 3.6.

2.2 ACCESS Use Cases

Co-simulation can be used for situations where the interdependencies between domains must be studied. ACCESS is used to study the interdependencies between communication networks and other domains such as power distribution and transmission, and oil and natural gas systems. Focus areas of study include but are not limited to:

- Cyberattack Impact Studies

  It is often useful to understand how cyber adversary behavior on a communication network impacts power system operations. For example, consider a situation where a cyber adversary has obtained access to computers on a critical infrastructure (e.g., a power distribution system

for a residential area) communication network and is conducting a distributed denial of service attack on that network. The questions one might ask about this scenario include (but are not limited to): Is the operation of the power distribution system impacted by this attack? If so, what are the specific impacts?

- Communication System Architecture and Hardening

  Similar to cyberattack impact studies, it is also useful to understand if cyberattacks can be mitigated, and if so, what are "good" ways to accomplish the mitigation. Consider the case where sensors and mitigation mechanisms (such as intelligent firewalls, isolation, and traffic routing systems) can be placed in a communication network, but the precise required arrangement of these elements is not well-understood. The questions one could ask are: what are some viable combinations and locations of sensors and mitigation mechanisms that protect a communication network and its critical artifacts from attack? How well do these arrangements perform in terms of some specific performance criteria? What are the "best" arrangements of sensors and mitigations?

- Control System Studies

  Understanding how advanced distributed control algorithms for power systems behave in the presence of communication network disruptions, and how control system algorithm performance impacts the operation of a power system. For example, advanced distributed communication-based control may be required to integrate heterogeneous distributed energy resources (DERs) into a regional power distribution system so that they can perform ancillary services or power restoration functions. A question one might ask about this scenario is: how do different communication system characteristics impact the performance (in terms of known system constraints) of distributed optimization/control algorithms for large-scale heterogeneous DER deployments?

Some or all of these scenarios may be useful for evaluating and ensuring mission performance in the DCEI system context. ACCESS provides an environment and toolset to formulate these scenarios, build models, and execute simulations. The output from these simulations can then be visualized to understand the performance characteristics of the simulated model, and ultimately answer questions like those previously posed. Simulation output can also be fed back to other systems in a time-synchronized manner using HELICS (for studying systems with dynamic feedback loops), or in a more loosely-coupled manner without time synchronization (e.g., sharing Comma Separated Value (CSV) files or other data exchange formats). Section 3.4 describes a new loosely-coupled bi-directional data exchange process between the ERMA buildings modeling group and the communications modeling group that was developed for the ERMA project.

2.3 Communication Network Resilience Metrics

Ns-3 implements an event tracing feature that can produce arbitrary event-based output from any model. Packet capture data in the standard PCAP data format can also be produced by ns-3.

Between these two formats, several communication disruption metrics can be computed and used to study communication network resilience. Several of these communication disruption metrics are further described in [9]. Of note are the Quality of Service (QoS), Availability, and Reliability and Resilience metrics. For brevity, the definitions of these metrics are not reproduced here.

3 ACCESS Model Advancements

This section describes the ACCESS model advancements for resilience analysis performed during the ERMA project to date. These advancements include additions to the NND file format, the implementation of a new cyber-physical "controller" model, integration of an oil and natural gas simulator, loosely-coupled integration with a building simulator, a new feature for generating network models programmatically, and integration of a HPC-based workflow management tool for running ensemble simulations.

3.1 Ns-3 Network Definition Enhancements

The NND file format was enhanced to support increased model fidelity and the inclusion of new and existing models as follows:

- Controller Application: A significant advancement was the implementation of a custom ns-3 application model, the controller application; this application is described in section 3.2. Additions were made to the NND specification to support inclusion of this model in ACCESS simulations.
- Routing Protocol: The NND specification now allows a user to specify the packet routing protocol.
- Agent Configuration: ACCESS implements an "agent" feature that allows arbitrary behavior to be executed on a ns-3 node. The NND specification was enhanced to allow finer-grained control over this behavior.
- WiFi Channel: Ns-3 supports the modeling and simulation of wireless networks, but this functionality was previously not exposed in the NND specification. The NND specification was enhanced to allow modelers to specify wireless network channels between network nodes.
- Position Information: The NND specification was enhanced to allow positional information to be associated with ns-3 nodes. This allows nodes to be located in a 3-d space, which, for example, yields higher fidelity for network simulations involving mobile nodes, or wireless nodes within a building.

3.2 Controller Model

An important concept in a cyber-physical critical infrastructure system simulation is a device that both monitors and controls a physical process and is communicable on a network. Such a device model must capture the essence of real-world devices like programmable logic controllers, protection relays, smart switches and meters, and microgrid controllers. Ns-3 does not natively implement an abstract model of such a device. Instead, one must build upon the native node and application models in ns-3. Several projects that use ACCESS have required an application model with the previously described features. During the ERMA project, the ACCESS team developed a new ns-3 application model, the controller, to satisfy this need.

The ACCESS controller model is conceptually fairly simple. It consists of the following elements:

- An internal memory to store measured values and configuration parameters.
- A state machine to model arbitrary device behavior.
- Execution of arbitrary user-defined logic that operates on (reads and writes) the internal memory, and invokes external communications and state transitions.
- Optional coupling to other simulators via HELICS, to both receive data from a simulated physical process and control aspects of that process.
- Communication with other hosts on a network to publish process data and receive data and commands.

While the initial use-case for the controller application was to model a simple microgrid controller and several intelligent field devices, much more advanced systems may be modeled. One or more controller models may be instantiated on a ns-3 node, and controllers can be designed to communicate with each other across a network to achieve a common control system goal.

In addition to the basic controller model framework, a Python capability for specifying controller logic was implemented. Models in ACCESS are typically written in the C++ programming language, and the Python capability allows users to develop controller functionality without needing to be proficient with C++.

3.3 Oil and Natural Gas Integration

ACCESS simulations have been focused on critical infrastructure systems with communications and *electricity* aspects. To address the recent adversarial focus on Oil and Natural Gas (ONG) systems, the ACCESS team integrated the Synergi Gas [3] simulator with ns-3 to support cyber-physical studies of ONG systems.

A complicating factor for this integration is the fact that the Synergi Gas simulator is purely Windows-based, while ACCESS is purely Linux-based. Since the Synergi Gas simulator is a commercial product, the source code is unavailable, and the product cannot be ported to Linux. Porting

ACCESS to the Windows platform would have been too time-intensive, so a bridging layer was built to support the interoperability of these two platforms which allows them to communicate effectively using HELICS.

The Synergi Gas product provides a .NET interface to its core simulation facilities. This interface was wrapped with a Thrift-based [1] RPC server that allows clients to connect to and control the execution of the simulator remotely over a network. A HELICS federate was implemented to interoperate with the RPC server so that time control and data exchange could be achieved with ns-3 in ACCESS. Finally, a simple test case was built to demonstrate the co-simulation of Synergi Gas with ACCESS.

The integration of the Synergi Gas simulator with ACCESS adds a new capability for studying the resilience of cyber-physical ONG systems that rely on communication networks.

3.4 Buildings Integration

LLNL and Lawrence Berkeley National Laboratory (LBNL) collaborated early in the ERMA project to explore the coupling of buildings and communcation network models. The teams hypothesized that a building's structure can have an impact on communcation network structure, and that computing and communication infrastructure can have an impact on the thermal dynamics and characteristics of buildings. Accounting for these details may have an impact on system resilience studies, e.g., 1) building thermal loads may be significant if housing a data center or other equipment that both requires power and produces heat, and 2) Local Area Network (LAN) structure for buildings may impact both inter and intra -building communication, and accounting for this structure may affect communication system resilience metrics.

The labs exchanged data in the context of a standard building model [8] to add fidelity to both communication system model and building thermal model. The outcome of this data exchange resulted in the development of a Python-based communication network model generator script that produces a model for a building LAN in NND format; this generator script is further described in section 3.5.

The communication system modeling team produced a power density profile of a prototypical LAN model (including network infrastructure and communication nodes such as workstations) for the standard building model, in Energy+ format, and provided this data to LBNL for integration into the building thermal model. It is expected that these enhancements in model fidelity will improve resilience assessments for both buildings and communication networks.

3.5 Network Model Generator Scripts

As mentioned in section 2.1, the NND file format allows ACCESS users to model communication networks by specifying the network topology and composition. Manual construction of NND files for non-trivial networks is a time-consuming and error-prone task. To address this issue, a new NND serialization library, nnd-tools, was implemented to enable programmatic manipulation of NND files. This library allows users to read, write and modify NND files in Python scripts using a

standardized object model, which eliminates errors introduced by manually typing out JSON code, and speeds up the network modeling process.

During the collaboration with LBNL on buildings modeling, described in section 3.4, the ACCESS team utilized the nnd-tools library in a new network generator Python script that produces a communication network for the DOE medium office building prototype model. This script is used to quickly generate building LANs that can be assembled into larger Wide Area Networks (WANs), which adds fidelity to communication network models and improves resilience analyses that involve buildings.

3.6 Advanced Workflows for Ensemble Simulations

Communication network simulations are stochastic in nature in that they exhibit randomness by design. For example, algorithms for non-deterministic collision avoidance often use a random variable as part of the computation of data retransmission times. Running a single network simulation that has elements of non-determinism is akin to rolling a die once, and conclusions drawn from a single run may not be reliable [10]. Multiple simulation runs are also necessary to perform sensitivity analyses to understand which parameters have a more pronounced effect on the behavior of a simulated system than others.

Prior to ERMA, ACCESS did not have a native mechanism for easily running large scale ensemble simulations for experiments and hypothesis testing. To address this shortcoming, the Merlin tool [4] for building, running and processing large-scale HPC workflows was integrated into ACCESS. Python scripts were implemented for 1) generating sample spaces for numeric variables such as packet size, and 2) manipulating variables in NND model files based on the generated sample spaces. A simple microgrid co-simulation example was implemented that demonstrates the use of these scripts with Merlin on HPC systems; the example adjusts data packet sizes for messages between network-enabled control system devices. A similar type of parameter study could be performed in ERMA to evaluate communication network resilience metrics for a set of parameters of interest.

4 Future integration opportunities

In addition to the many model enhancements implemented in ACCESS, discussions among project participants highlighted potential points of interconnection between national lab capabilities. This section outlines some high-level thoughts on integration of these capabilities with ACCESS in pursuit of resilience analysis for the ERMA project.

4.1 Sandia National Laboratories Microgrid Design Toolkit

The Microgrid Design Toolkit (MDT) [5] developed by Sandia National Laboratories (SNL) is a decision support software tool for microgrid designers that identifies and characterizes the trade

space of alternative microgrid designs. MDT is emerging as the locus of control for the execution of resilience analyses in the ERMA project. Thus, establishing a path towards data exchange between MDT and ACCESS is important for incorporating communication system and cyber resilience into the overall system analysis effort. SNL and LLNL have held early and informal discussions to generate ideas for data exchanges between MDT and ACCESS.

A notional workflow for loosely coupling ACCESS and MDT for resilience analysis is as follows:

1. The communication system modeling team associates communication network equipment with power system equipment in the MDT model.
2. MDT provides a time series of power state (e.g., on/off) for communication system components to ACCESS in an agreed-upon data exchange format.
3. ACCESS runs simulations with these power states, generates communication system metrics, and feeds the metrics back to MDT.
4. MDT includes communication system metrics in its computation of mission performance.

This type of workflow is achievable with the implementation of a mechanism for incorporating the dynamic power state of communication system device from MDTs. One approach might involve the implementation of a simple HELICS federate that consumes the power system state produced by MDT and controls the availability of communication system nodes during the simulation. Communication system metrics produced by ACCESS simulations could be provided in a MDT-native format.

4.2 National Renewable Energy Laboratory Cyber Range

The National Renewable Energy Laboratory (NREL) Cyber Range [6] allows researchers and partners to study energy systems' interation with and dependence on digital communication devices and networks. This capability can virtualize, emulate and visualize multi-scale energy systems and communication networks. Integrating the Cyber Range with ACCESS simulations for communication and cyber resilience analysis has two benefits for the ERMA project: 1) it may extend the set of devices, protocols and other systems to interact with, for which there may be no existing models in ACCESS, and 2) it may help to validate pure network simulations performed by ACCESS alone, giving confidence in simulations if results are well-correlated. Possible tasking for realizing these two benefits is discussed below.

Ns-3 implements a real-time scheduler feature that is designed to integrate with virtual testbeds and virtual machine environments. The real-time scheduler ties the ns-3 simulation time to an external time base like a system clock. To integrate ACCESS with NREL's Cyber Range, ACCESS must use the real-time scheduler. Future discussions between LLNL and NREL can resolve the specifics of the Cyber Range execution environment for ACCESS, and determine the points of interconnection between the simulated and the emulated systems.

To validate ACCESS simulations in the Cyber Range, it will be useful to provide a description of the simulations to the Cyber Range operators. A natural mechanism for this is to share the ACCESS NND format and the nnd-tools library, and translate NND files to a form that is directly consumable by the Cyber Range capability. A script that utilizes the nnd-tools Python library could facilitate the translation of ACCESS communication system models into a form usable by Cyber Range.

4.3 Sandia National Laboratories Water Network Tool for Resilience

The Water Network Tool for Resilience (WNTR) [11] developed by SNL is an open source package designed to simulate and analyze water distribution network resilience. It has been applied to resilience scenarios involving earthquakes, power outages, water quality, supply and demand uncertainty, and cyberattacks. WNTR implements a device model that may be compatible with the ACCESS controller model. While the specific integration pathway for WNTR and ACCESS is unclear at this point, it will be useful to pursue additional technical details of WNTR so that water and communications system integration can be achieved in the ERMA project for improved resilience analysis.

5 References

[1] Apache Thrift. `https://thrift.apache.org`.

[2] HELICS: Hierarchical Engine for Large-scale Infrastructure Co-Simulation. `https://docs.helics.org/en/latest/index.html`.

[3] Hydraulic modelling and simulation software - Synergi Gas. `https://www.dnv.com/services/hydraulic-modelling-and-simulation-software-synergi-gas-3894`.

[4] Merlin: Machine Learning for HPC Workflows. `https://merlin.readthedocs.io/en/latest/`.

[5] Microgrid Design Toolkit. `https://www.sandia.gov/csr/center-for-systems-reliability/tools/mdt/`.

[6] NREL Cyber Range. `https://www.nrel.gov/security-resilience/cyber-range.html`.

[7] ns-3: A Discrete-event Network Simulator for Internet Systems. `https://www.nsnam.org`.

[8] Prototype Building Models. `https://www.energycodes.gov/prototype-building-models`.

[9] Salman M. Al-Shehri, Pavel Loskot, Tolga Numanoglu, and Mehmet Mert. Common metrics for analyzing, developing and managing telecommunication networks, 2017.

[10] Thomas J. Gogg and Jack R. A. Mott. Introduction to simulation. In *Proceedings of the 1993 Winter Simulation Conference*, pages 9–17, New York, NY, USA, 1993. Association for Computing Machinery.

[11] K.A. Klise, R. Murray, and T. Haxton. An overview of the Water Network Tool for Resilience (WNTR), July 2018.