Electrical Power and Energy Systems 104 (2019) 817–826

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification

Eman Hammad[a], Mellitus Ezeme[b], Abdallah Farraj[a,*]

[a] University of Toronto, Toronto, ON M5S 3H7, Canada
[b] University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada

ARTICLE INFO

Keywords:
Smart grid
Offline co-simulation
Cyber security
Control
Testbed design and implementation
Cyber-physical systems

ABSTRACT

Smart power systems have recently shifted to accommodate distributed control systems, renewable sources of energy, consumer-centric energy management systems, and active distribution systems. The smart grid evolution is modeled by the integration of power systems and a communication network overlay to facilitate a bi-directional flow of information and energy in the grid. This article provides a detailed description of an offline co-simulation testbed for smart grids, that is developed by integrating well-established power and communication systems simulators. The testbed development approach, setup and implementation are described at a detailed level to enable similar test-bed developments. The developed testbed is envisioned as a tool to help smart grid researchers with the study of relevant research problems such as assessing power system resilience against cyber attacks and threats, and verifying the performance of cyber-enabled control schemes.

1. Introduction

Smart grid stakeholders continue to invest in employing communication systems and infrastructure that enable more flexible, efficient and reliable grid operations and control. By facilitating consumer-centricity and the integration of renewable resources within smart grid systems, the landscape of power systems operation is changing especially in terms of the flow of both information and power. Given the rapid evolution of smart power systems, it is critical that a rigirious investigation of the impacts of (cyber) information and communication technologies (ICT) on (physical) power systems and vice versa be considered by the research community [1–3]. Earlier research studies simplified the impact of communication network on a smart grid system as time delay to be accounted for within the control loop; however, this has proven to be insufficient in terms of investigating the cyber-physical coupling within the smart grid [4,5]. Interfacing existing ICT and power system simulators (termed *co-simulation*) is thought to be a practical and realistic approach to represent their smart grid interactions [6,7].

The introduction of recent interoperability guidelines and standards for smart grid development attests to the critical need for secure and sustainable operation of the cyber and physical subsystems. For example, the IEEE 2030–2011 standard provides principles for smart grid interoperability of power and ICT components [8,9]. This standard presents a *system of systems* view of the smart grid with three parts: power systems, communication, and information technology. As illustrated in Fig. 1, this high-level architecture inspires our proposed co-simulation testbed consisting of analogous abstractions.

Typically, the operation of smart grid power and control components can be described with well-defined mathematical formulations; however, the same cannot be said for the accompanying ICT system because of its often (unpredictable) stochastic behavior and event-driven layered protocol structure involved in data transmission. This motivates the need to combine existing communication and power simulators to enable formal and realistic studies including the verification of cyber-enabled control and analysis of cyber security threats and attacks. Hence, there has been a growing research interest in development of smart grid co-simulators. Approaches for co-simulation development can be categorized into two main approaches from an architecture perspective: 1) tool-based approach; where the test-bed is focused on integrating a specific set of simulators based on the understanding of tools architectures and interfacing capabilities. 2) A platform-based approach; where the focus is on developing a common coordinating framework that adopts a more standardized interfacing to support different simulation tools. The first approach is often adopted by researchers who have a known limited set of tools and require more understanding and control over subsystems interactions. The second approach is appealing for researchers with more complex simulation environments and studies that require the flexibility of a systematic

* Corresponding author.
E-mail addresses: ehammad@ece.utoronto.ca (E. Hammad), mellitus.ezeme@uoit.net (M. Ezeme), abdallah.farraj@utoronto.ca (A. Farraj).

https://doi.org/10.1016/j.ijepes.2018.07.058
Received 27 March 2018; Received in revised form 13 July 2018; Accepted 24 July 2018

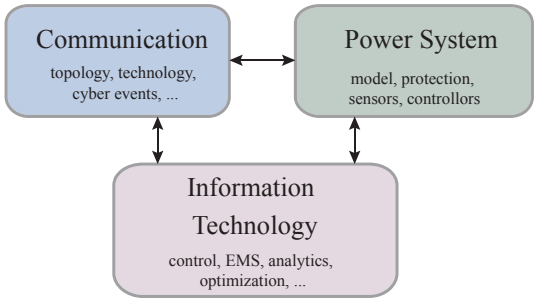

Fig. 1. System architecture in compliance with IEEE 2030.

interfacing approach without being involved in the details or architecture of either interfacing subsystem.

There has been a momentum of research into both approaches, a survey in [10] elaborates on some of the developed testbeds. Functional mock-up interface (FMI) is a popular framework that is used in platform-based co-simulation approaches [11]. The framework defines a standardized interface to integrate components of complex cyber-physical systems. High-level architecture (HLA) is another standardized co-simulation architecture developed to link different simulators into a distributed environment federation [12]. The ptolemyII platform-based framework is developed using hybrid-systems theory to enable the simulation of heterogeneous systems [13]. Further, other software tools are developed that utilize multi-agent architectures to integrate the simulation of different subsystems. Examples here include Multi-agent Environment for Complex SYstem CO-simulation (MECSYCO) [14], and Mosaik [15] which was developed with a focus on large scale smart grid systems.

In this work, a tool-based approach is adopted because there is a defined set of accessible simulators to use, and a more control on the interfacing between the chosen simulators is preferred. Further, the developed testbed aimed to simplify its approach to enable other research teams to quickly reproduce similar testbeds.

An example subset of previously-developed smart grid co-simulation testbed is captured in Table 1. The table summarizes available tools from both domains (cyber and power) and the research problems studied using these testbeds. The EPOCHS testbed [16] is developed using a multi-agent approach based on the HLA architecture and run-time infrastructure (RTI) middleware [16]. The testbed is among the first to adopt a platform-based approach and is provided as an open-source to interested researchers. GECO [17] presents a tool-based co-simulation testbed that embeds a discrete events scheduler into the power simulator for events coordination and data exchange. A GridLAB-D based integrated simulation engine is described in [18] where a middle interfacing and coordinating layer is developed to be shared between GridLAB-D and NS3. The ORNL power system simulator presented in [19] follows a similar tool-based approach where the ADEVS is developed as a discrete events wrapper around the power simulator THYME. ADEVS defines and coordinates the interfacing between THYME and the OMNeT++ communication simulator. In GridSim testbed [20] the authors develop their own data delivery module denoted GridStat, and integrates the power simulator TSAT within the testbed. A SCADA Cyber Security Testbed integrating PowerWorld and RINSE is illustrated [21]. The testbed implements a protocol converter that is envisioned to enable interfacing with hardware systems/components.

A realtime co-simulation testbed developed in [22] integrated RTDS realtime digital power simulator with hardware controllers, relays and real Ethernet network. The approach is made possible by the interfacing capabilities of the RTDS which do not require additional customization by the testbed developer. Another realtime co-simulation testbed is described in [23] integrating Opal-RT power simulator and OPNET communication simulator. The testbed capitalizes on the features provided by both simulators allowing an easy integration. It is important here to note that realtime co-simulation testbeds often have plenty of features provided by the expensive simulators allowing for seamless integration in many cases. A disadvantage of these testbeds is recognized when considering communication protocols that are not supported by either simulator, where more elaborate development is needed to add that capability [24].

It can be noted that a detailed implementation and setup of co-simulation testbeds are not appropriately detailed in the existing co-simulations literature especially to enable reproducing and comparing research results. The lack of such details forces interested research teams to create, from scratch, their own co-simulators. This paper is motivated by the need for a comprehensive exposition on offline co-simulator development for smart grid applications that can be reproduced or easily modified to support smart grids studies. Offline co-simulation is a cost-effective approach to analysis that is not only more accessible (less expensive), but typically easier to implement while being useful for a variety of "what-if" analysis and analytics for system planning. However, offline co-simulation has few limitations such as it's extended time of simulation because of the added interactions between subsystems. Moreover, offlines testbeds do not have the capability to integrate hardware systems (e.g. PMU, relays, controllers).

A main challenge of interfacing two simulators, each of distinct characteristics, is to integrate both simulated systems while effectively maintaining the core independence of each. Enabling different simulation platforms to work hand in hand to represent a realistic smart power system behavior requires dealing with synchronization and data exchange challenges [25]. Synchronization issues typically occur between interfaced simulators because of the differences in the size of simulation time-step and the execution sequence [26]. On the other hand, data exchange issues at the interface between the two simulators should be scalable to have a minimal impact on the overall performance of the co-simulation testbed.

Table 1
Sample co-simulation testbeds.

ID	Power simulator	Cyber simulator	Offline/realtime	Investigated problem
EPOCHS [16,29]	PSCAD/EMTDC & PSLF	NS2	Offline	Protection, special protection schemes
GECO [17,30–32]	PSLF	NS2	Offline	PMU based wide area monitoring systems
Integrated simulation engine [18]	GridLAB-D	NS3	Offline	Distribution & demand response (DR)
ORNL power system simulator [19]	THYME model	ADEVS (NS2 & OMNeT++)	Offline	Control & communication
GridSim [20]	TSAT (DSATools)	GridStat	Offline	Wide area control & protection schemes
SCADA Cyber Security Testbed [21]	PowerWorld	RINSE	Offline	SCADA Cyber Security
[33,34]	OpenDSS	OMNeT++	Offline	Electric vehicles (PEV) coordinated scheduling
[35]	OpenVZ(emulator)	S3F(simulator)	Offline	advanced metering infrastructure (AMI) attacks
[22,36]	RTDS	NS3	Realtime	cyber vulnerability & mitigation
[23]	Opal-RT	OPNET[a]	Realtime	communication latency impact on microgrid control
[37]	Opal-RT	hardware network	Realtime	adaptive mitigation of cyber incidents
[38]	Opal-RT	communication adapter	Realtime	energy battery management

[a] The communication network simulator OPNET was later acquired by Riverbed and became known as Riverbed Modeler.