Submitted for publication. Author copy -- do not redistribute.

Real Time Modeling and Simulation of Cyber-Power System

Ceeman B. Vellaithurai, Saugata S. Biswas, Ren Liu, and Anurag Srivastava

Abstract. Ongoing smart grid activities have resulted in proliferation of intelligent devices and associated Information and Communication Technologies (ICT) to enable enhanced system monitoring and control. Integration of ICT has led to an increase in the number of cyber assets and requires cyber-physical study for system analysis. In order to realize the vision of a smarter grid, it is necessary to understand the complex relationship between cyber and physical domains, and potential impacts on the power grid due to successful cyber-physical attacks. In order to understand this coupling, cyber physical test bed can help to model and simulate the smart grid with sufficient level of detail. In this chapter, an introduction to the smart electric grid and the challenges associated with the development of cyber-power test bed is presented. The integration of Real Time Digital Simulator (RTDS) and Network Simulator 3 (NS3) to realize a real time cyber-power test bed is discussed with the implementation of an example application.

Keywords: Application testing, Cyber-power system, Cyber security, Device testing, Network simulator 3, Real time, Smart grid.

1 Introduction

1.1 Electric Power Grid

The primary aim of the Electric Power Grid (EPG) is to reliably deliver power to load centers with high level of service continuity and minimal cost, while minimizing the

Ceeman B. Vellaithurai
Schweitzer Engineering Laboratories, Inc. (SEL), Pullman, WA, USA
e-mail: ceeman_vellaithurai@selinc.com

Saugata S. Biswas · Ren Liu · Anurag Srivastava
Washington State University, Pullman, WA, USA
e-mail: {saugatasbiswas,liuren248}@gmail.com,
asrivast@eecs.wsu.edu

© Springer International Publishing Switzerland 2015

S.K. Khaitan, J.D. McCalley, and C.C. Liu (eds.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Power Systems, DOI: 10.1007/978-3-662-45928-7_3

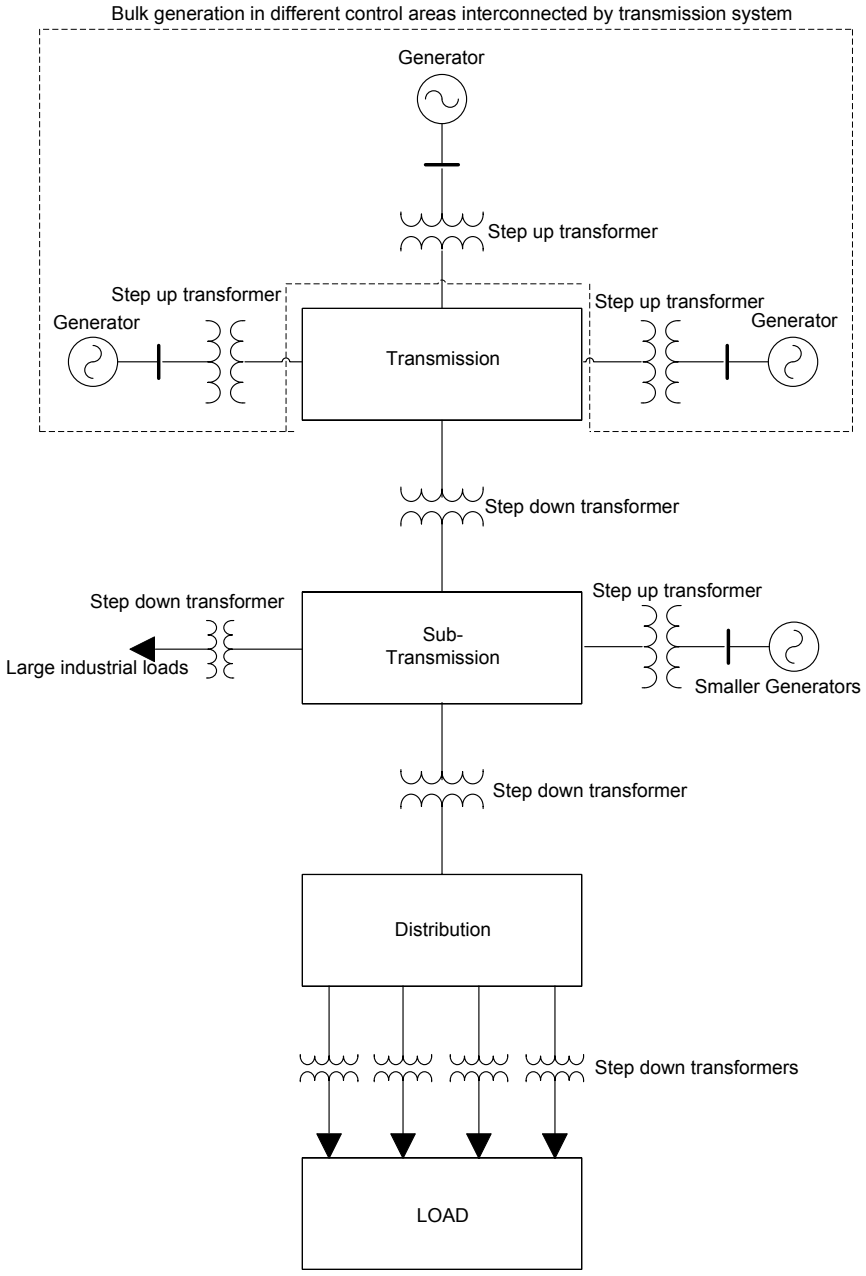

Fig. 1 Basic structure of electric power grid

impact of component failures. The physical EPG consists of four major domains: generation, transmission, distribution, and load.

Fig 1 describes the basic structure of EPG [1]. The generation system consists of several large generators generally located away from load centers. Distributed generation may feed into the grid at the subtransmission or distribution level. The power generated by these generators is delivered to the load centers through the transmission and distribution systems. To minimize power loss in transmission of electric power, the voltage level at generating substations is stepped up to high voltage levels. Transmission level systems have a meshed topology, while distribution systems are usually radial.

The power system has to maintain a constant balance between the electric power generated and consumed. This criterion needs to be satisfied in order for the power system to be stable and operate in synchronism within a specified band around rated frequency. In the past few decades, with the advent of power electronic devices, High Voltage Direct Current (HVDC) links [2] are also being used for bulk power transfer.

1.2 Power System Monitoring

The EPG is a complex network and dynamic system of systems. It is therefore necessary to monitor the system continuously and take appropriate control actions as required. Various monitoring and control methodologies have been used over time, usually driven by the needs and available technologies of that time. The earliest method of data acquisition for monitoring the EPG involved scanning of remote terminal units (RTU) in a sequential order to obtain measurements. This process usually took several minutes due to vast number of devices to scan in addition to communication network constraints. With the use of Supervisory Control and Data Acquisition (SCADA) systems, and upgrade to the advanced communication networks, the time taken to acquire data from RTUs was reduced from several minutes to a few seconds. The measurement devices are polled every few seconds to collect data in a routinely. SCADA systems are widely used throughout the EPG and industrial control systems for monitoring and control purposes. The data acquired from the devices need to be processed through a State Estimator to get more accurate system state estimate and to remove bad data. Power flow studies and other stability studies rely heavily on the collected data to determine control and mitigation strategies for contingencies in the system.

1.3 Power System Control

The control systems employed in the EPG can be broadly classified into local and wide area controls. Due to data availability constraints, most of the control systems that have been implemented so far make use of local information to take control decisions and actions. A brief survey of the control methodologies employed in the power grid are discussed here [3].

1.3.1 Local Controls

Local control systems typically make use of the data available within a single substation. These control systems do not take into account the state of the system in other locations to take control decisions and actions. The control action may be opening/closing of circuit breakers to reroute power, changing transformer taps in response to terminal voltage, switching in capacitors or reactors to alter power flow, or changing generator mechanical input to control output power.

Power System Protection: The EPG is prone to faults such as a tree branch falling on conductor leading to a short circuit. These faults are typically characterized by high current flows resulting in heating or burning of equipment. In order to protect the devices in the power system, several protection techniques are applied as needed. These systems usually have redundancy to protect against equipment failures.

Voltage Control: Voltage is generally maintained at the required level either through changing the taps of a tap changing transformer or by use of switched capacitor or reactor banks to provide/absorb reactive power. Power electronic devices have augmented these capabilities in recent years.

Generator Control: Generators may use a combination of local controls such as governor control, excitation control and power system stabilizers for controlling power input, voltage output and damping oscillations respectively.

Power Flow Control: Similar to voltage control, this type of control typically involves the use of switched capacitors or reactors in the transmission lines to either reduce or increase the effective line impedance or angle. Traditional methods involved the use of slow response controls such as AC phase shifting transformers. Power electronic devices provide faster control.

Note that, several of these above local control can also be coordinated and need not to be always based on only local measurements.

1.3.2 Wide Area Controls

Controls that require information from not just the local devices but also remote devices through use of communication channels are classified as wide area controls. The scope of wide area controls may vary involving just two substations to multiple substations. A few typical wide area control methods are described in this section.

Coordinated Frequency Control: The balance between power generation and load has to be maintained at all times. If there is any imbalance, the generators begin to speed up or slow down depending on whether generation is higher or lower. Governors provide a local and fast control to regulate speed by changing the mechanical power input. A second level of control called Automatic Generation Control (AGC)

utilizes the generator output data from the generators and sends raise or lower commands to the governor control to maintain inter-tie schedules and frequency. This control is generally slow as it involves collection of data from the different generators and running algorithms to determine appropriate set points for the generators to minimize control area error. In the North American power grid, this control may take place every few seconds as the frequency requirements are strict.

Coordinated Voltage Control: In addition to local voltage control, wide area voltage control applications have been employed on a limited scale to achieve coordinated voltage regulation across the system through actuation of local devices.

Remedial Action Scheme(RAS): These schemes involve elaborate systems that may trip generators, loads, or transmission lines in response to a contingency. A RAS typically require extensive data for offline simulations and studies to determine control actions for particular contingencies.

1.4 Evolving Smart Electric Grid

The EPG has remained largely unchanged over the last few decades. According to the U.S. Department of Energy report, the average demand for electricity in the past two decades has been increasing at the rate of 2.5 percent annually [4]. At the same time electric grid is going through several changes including generation mix, load types, electricity markets, difficulty in building new transmission lines, and environmental constraints. A long list of blackouts in the past has pointed to the need for continued improvements. Energy storage needs, need for better visibility and situation awareness, automated control, ,and sustainable energy are some of the key factors which have generated the push towards to the development of a smarter grid. Analysis of past blackouts in the North American grid have shown that the lack of visibility of the grid and unavailability of high resolution information to make critical decisions were the main cause of the blackouts. Operators in control centers are trained to make informed decisions based on their knowledge of the system. However, the response times during critical periods are too short for operator intervention highlighting the need for automated systems. Once the system enters the cascading stage of a blackout, an operator can hardly take any corrective control actions. The state of the grid needs to be monitored continuously and appropriate action need to be taken to prevent a blackout condition. This may involve islanding the grid into several sub systems, shedding loads, or a combination of both.

The smart grid is a major upgrade to the electric grid infrastructure for improved efficiency, reliability and safety, with smooth integration of renewable and alternate energy sources, through use of automated control and modern communication technologies. The technology needed to realize a smarter grid such as processing power to handle large amount of data, remote access for monitoring and control, and automation to enable self healing capabilities need to be integrated with the EPG.

The U.S. Energy Independence and Security Act of 2007 directed the National Institute of Standards and Technology (NIST) to lead the related research work of smart grid. According to the NIST report [5], the smart grid has the following key characteristics:
1. Enables informed participation by customers
2. Accommodates all generation and storage options
3. Enables new products, markets and services
4. Provides the required power quality for a range of needs
5. Optimizes asset utilization and operates efficiently
6. Operates resiliently to disturbances, attacks and natural disasters.

Fig 2 shows the framework for a smart grid as defined by the NIST report [5]. In addition to the power delivery domains, the smart grid also includes the following domains: electricity markets, system operation and service providers. Each domain and their respective sub-domains have a group of actors and applications. Information flows within each domain as well as between domains. Actors may not be restricted to just one domain. For instance, distribution service providers may have actors not only in the distribution domain, but in the operations and markets domain as well.

1.4.1 Advanced Power Grid Communication Networks

In the existing power system, the various communication requirements of the grid are supported by independent and often dedicated networks. For example, data delivery between substations and control centers is a dedicated independent network in most cases. In a typical communication network used in the grid at present, fiber optic cables are generally used between critical substations and control center. Fiber optic cables can be laid along the transmission lines in the power system for data transmission. All Dielectric Self Supporting (ADSS) fiber optic cables are installed along the transmission lines using the same tower support infrastructure. Redundancy is provided to cover for failure of one or two links in the system. If it is not feasible to lay a fiber optic line, private WiMAX networks are used. For distribution network communications such as Advanced Metering Infrastructure (AMI) and Distributed Automation (DA), low speed networks with bandwidth in the range of 200 kbps are used. In some cases, public communication lines may be leased. Multiprotocol Label Switching (MPLS) is used for managing the Internet Protocol (IP) network traffic. Some of the different service segregation used to differentiate traffic is telemetry protection, AMI, SCADA and enterprise access. With the replacement of old bandwidth restricted networks with high capacity fiber optic links, the first step towards realization of fast inter domain information flow has been taken. However, in order to fully realize the goals of a smart grid, it is necessary to expand the information network inter-connectivity so that information may flow securely between the different domains in the smart grid.

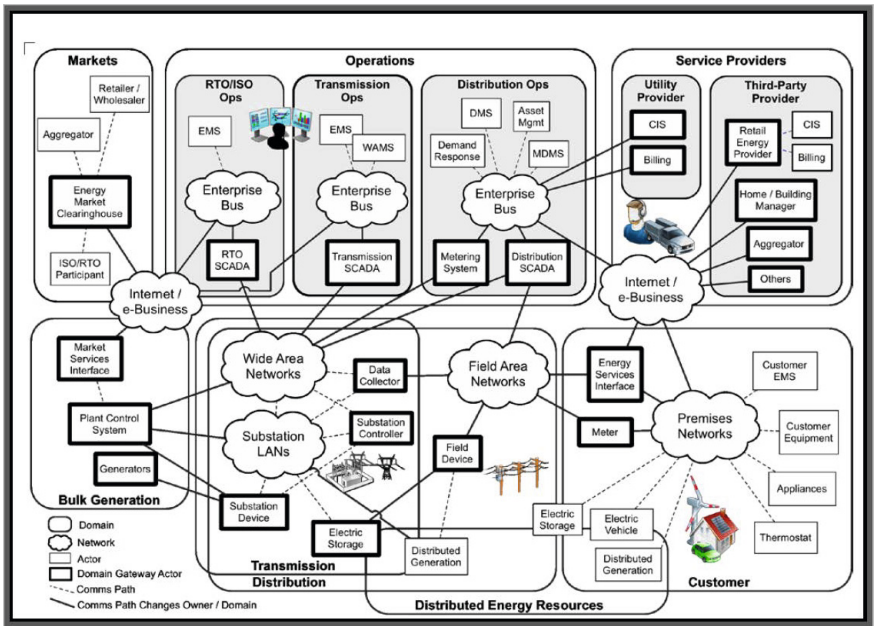

Fig. 2 Structure of a smart grid

1.4.2 Advancements in Monitoring and Control Systems

Recent developments in the field of measurements have led to the development of Phasor Measurement Units (PMU), which can provide data at a rate greater than thirty samples per second. The major advantage of this device is the availability of phasors values taken with reference to a single time source provided usually by a Global Positioning System (GPS) clock. This essentially means that all the measurements are taken on a common reference and a linear state estimator can be used to filter bad data in presence of PMU at all buses. The filtered data is used for real time monitoring and control purposes. The wide area controls described in Sect 1.1.3.2 can be greatly improved with the use of PMU data. Frequency control is inherently restricted by the speed, at which governor controls respond to changes. However, the availability of data at such high resolutions is of great value to RAS and voltage control algorithms to implement real time control. Operators in control centers have a better situational awareness of the grid. Adaptive control algorithms, contingency mitigation strategies, and self healing capability are some of the goals that can be attained through the use of real time data. A real time voltage stability monitoring algorithm using PMU data is described in Sect 1.4.

The availability of data and automated control in the distribution system has been very limited. This is fast changing with the implementation of advanced metering infrastructure as part of the smart grid initiative. With the installation of these smart meters, the degree of resolution of distribution systems will be improved greatly.

Additionally, through customer participation, it will be possible to raise or lower load levels at varying times of the day benefiting both the utility and the customer. The customer may receive monetary benefit, while the utility is able to vary load and achieve better security and reliability from a power system operation perspective. Distribution automation systems are gaining traction among utilities and are being installed at many locations.

1.4.3 Smart Grid: A Cyber-Physical System

Traditionally, communication networks have been considered to be support infrastructure that aid in the operation of power systems with little attention paid to cyber-security. The vulnerability of smart grid cannot be assessed as two separate metrics: cyber vulnerability and physical vulnerability. In a smart grid, the compromise of a cyber-asset such as a control, protection, or monitoring device by an attacker maybe used to cause damage to the physical power system components such as generators and transformers. Depending on the severity of the attack, it may take a long time to replace/bring these devices back to the service. In February 2014, the Wall Street Journal reported that a planned attack on a California substation involving sniping of transformers resulted in repairs that required twenty seven days to complete [6]. This illustrates the difficulty in servicing and replacing these devices. Successful cyber-attacks typically make use of vulnerability in the communication protocol, routing, or authentication of a cyber-asset to install malware, deny legitimate services, or directly intrude into an information system [7]. The level of physical consequences due to a cyber-attack is dependent on the nature and depth of the attack. Thus, the smart grid should be treated to its true nature of being a cyber-physical system (CPS) and security of the grid should be assessed with this view. CPS security systems must be able to differentiate between physical and cyber-attacks and respond accordingly. It is important to guard against coordinated cyber-physical attacks as the potential consequences may be severe.

1.4.4 Need for Cyber-Physical Security Analysis

Over the past few years, there have been several reports on industrial control systems vulnerability and victims of cyber-attacks. In March 2007, Idaho National Laboratory conducted an experiment in which physical damage was caused to a diesel generator through the exploitation of a security flaw in its control system by disabling the sync check element in the protective relay [8]. In April 2009, the Wall Street Journal reported that cyber spies had penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. The most significant of cyber-attacks on industrial control systems was Stuxnet, which happened in 2010. Stuxnet, a large complex piece of malware with many different components and functionalities, targeted Siemens industrial control systems and exploited four zero day vulnerabilities running Windows operating systems [9]. Increasing connectivity within the smart grid, interfacing with legacy devices, proliferation of access points, use of internet for remote access, common operating systems and platforms

contribute to the increase in risk factor. From Fig 2, it is clear that there is a proliferation of access points and routers scattered across the domains. This makes it possible for intruders to gain access to other domains. For example, attackers can start intruding into the system from a home network and work their way gradually into the enterprise networks and gain privileged information. This may then be used in arbitrage for illegal economic benefits or for causing unwanted operations in the power system. This necessitates the development and maintaining of authentication procedures and relevant best practices for cyber-physical security.

In general, the cyber security requirements of a system deployed in response to cyber threats include three main properties: confidentiality, integrity and availability [10]. These three properties are designed around the cyber paradigm and are not directly applicable for cyber-physical system security. However, these properties help in establishing basic security requirements. Confidentiality prevents an unauthorized user from obtaining secret or private information. Integrity prevents an unauthorized user/attacker from modifying the information. Availability ensures that a resource is available to the legitimate user when needed.

2 Modeling and Simulation of Cyber-Power System

A survey of the design methodologies adopted for cyber-physical system design, modeling and simulation; and the underlying issues involved are discussed in [11] [12]. In order to conduct cyber-physical analysis of the smart grid, it is necessary to develop modeling and simulation methodologies with sufficient detail. Fig 2 shows the different domains that exist in the smart grid. Of particular interest from a power system operation perspective are the generation, transmission, distribution ,and system operation domains. There are a number of tools available for modeling and simulation of these domains; traditionally the focus of power system modeling. Integration of the following simulators/devices is required to realize a tightly coupled cyber-power simulator: power system simulator, communication network simulator/emulator, data measurement and collection simulator, and end user application simulator. Digital power system simulators are usually discrete time based and communication system simulators are usually discrete event based. Data measurement and collection devices need to be simulated to measure and export power system data to end user applications through the communication simulator/emulator.

A modular approach to the development and integration of these simulators is preferable as it may not be necessary to have all the domains integrated together at all times. For example, in order to test an application running in a control center, it is enough to model the power system with data measurement and collection devices, communication network and control center. If any specific inter-dependency needs to be modeled, modules for that particular domain can be added. The simulation environments used for studying the coupling of the systems maybe broadly classified as centralized simulation environments and co-simulation environments.

2.1 Centralized Simulation Environments

These environments involve the development of a single simulator for the purpose of modeling and simulating both the power and communication networks. Such an implementation would help in alleviating the problem of time synchronization and coupling between the different components in the simulation. However, significant effort needs to be directed towards the development and validation of detailed models incorporating both static and dynamic behaviors of the system components. The major challenge associated with this methodology is the need for implementation of comprehensive validated models for both the power and communication system. Additionally, since these are generally implemented using software packages, it may be possible to test applications but not the physical devices. Power System Computer Aided Design (PSCAD) is a power system simulation tool. Implementation of a synchrophasor device in the simulator is discussed in [13]. Through the implementation of communication network components as discussed in [14], the simulator can be used for cyber-physical simulation. However, these models need to be tested and validated extensively.

2.2 Co-simulation Environments

A more practical and feasible approach is to keep the simulation of power and communication systems in different simulators and integrate them through a common framework to work together. The common framework is used to realize the required time synchronization and data flow interface between the two simulators. The main advantage is that industry grade commercial tools can be used for creating a cyber-physical simulation environment.

The Electric Power and Communication Synchronizing Simulator (EPOCHS) was the first one of this kind of simulation environments. Two different commercial power system simulators PSCAD/Electromagnetic Transients including DC (EMTDC) and Power System Load Flow (PSLF) were integrated with Network Simulator 2 (NS2). The connection between the simulators is realized through the implementation of a Run Time Infrastructure responsible for maintaining the same time scale on all the simulators. This is required due to the different time scales of the two simulators. The Global Event driven Co-simulation framework (GECO) combines the PSLF and NS2 to provide a co-simulation framework. The main goal here is the modeling and simulation of wide area monitoring, protection and control schemes [17]. The test bed developed at University of Arizona called Test Bed for Analyzing Security of SCADA Control System (TASSCS) is used for SCADA analysis [18]. It uses OPNET system-in-the-loop (SITL) emulation along with PowerWorld simulator. It is primarily used for research activities related to intrusion detection. SCADA Cyber Security Testbed [19] is another platform that is similar to TASSCS except that Real-Time Immersive Network Simulation Environment (RINSE) is used to simulate the cyber system. The Virtual Control Systems Environment (VCSE) developed by Sandia National Laboratory uses OPNET and PowerWorld simulator [20]. The Virtual Power System Test bed (VPST) developed at

the University of Illinois at Urbana-Champaign utilizes RINSE and PowerWorld simulator [21]. The major advantage of co-simulation is the ability to integrate simulators, emulators and physical hardware devices for integrated simulation.

2.3 Guidelines for Modeling and Simulation of Cyber-Power System

This chapter focuses on the modeling of power system, data measurement services, data collection services, and communication networks used to deliver data to the control center. The models used in different power system simulators might vary slightly in the level of detail but the underlying core generally remains the same. The basic models used in power system simulators are already available. For data measurement and collection models, it is preferable to have these models implemented inside the power simulator. In some simulators, the data measurement and collection devices are not modeled explicitly. For simulation of communication system networks in the power system, generalizations and acceptable assumptions need to be made to design a feasible system. The layout of communication networks is affected by the structure of power system as the communication links are usually laid along transmission lines with substations representing nodes in the network. Guidelines that can be used for modeling of communication systems for the power grid are presented in the next section.

2.3.1 Communication Network

Two types of communication network topologies are possible: point to point star topology and mesh topology. The star and mesh topologies are shown in Fig 3. Star topologies are essentially single hop networks where a packet originating at the source makes just one hop to reach the destination. Such networks are very costly to build for large systems, since it involves building dedicated lines for each substation and may not be economically feasible. In the distribution system where few localized control points maybe connected to devices in the network through dedicated communication networks over short distances, star topology may be used. Mesh topologies on the other hand involve the use of a single communication link by multiple nodes thereby increasing link utilization. This leads to a more efficient use of the available infrastructure. These networks are multi-hop networks where a packet might need to be routed through multiple nodes before reaching its destination.

The communication network for a given power system is generally derived using a top down approach.
1) The first step is to reduce the power system network topology into substations/nodes to obtain the nodal representation of the network. Usually a bus represents a substation in a power system layout. However, in the event that a transformer is present between two buses, it is reasonable to assume that the transformer and the associated buses are located in the same substation. For distribution systems, control

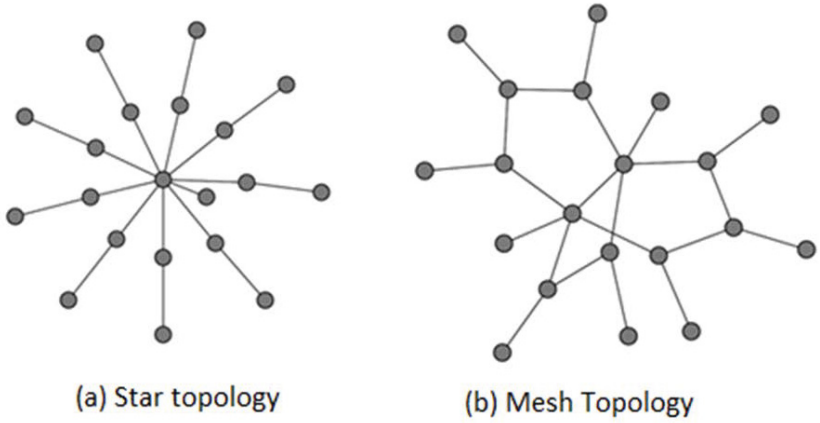

Fig. 3 Communication network topologies

or monitoring points which collect and/ transmit data can be represented as nodes. Fig 4 shows the IEEE 14 bus power system one line diagram and the reduced communication network nodal diagram.

2) Fiber optic cables can be laid along the transmission lines in the power system. It is reasonable to deduce the length of these data transfer lines from the transmission line length. The length of the transmission lines are derived using [15] for appro-

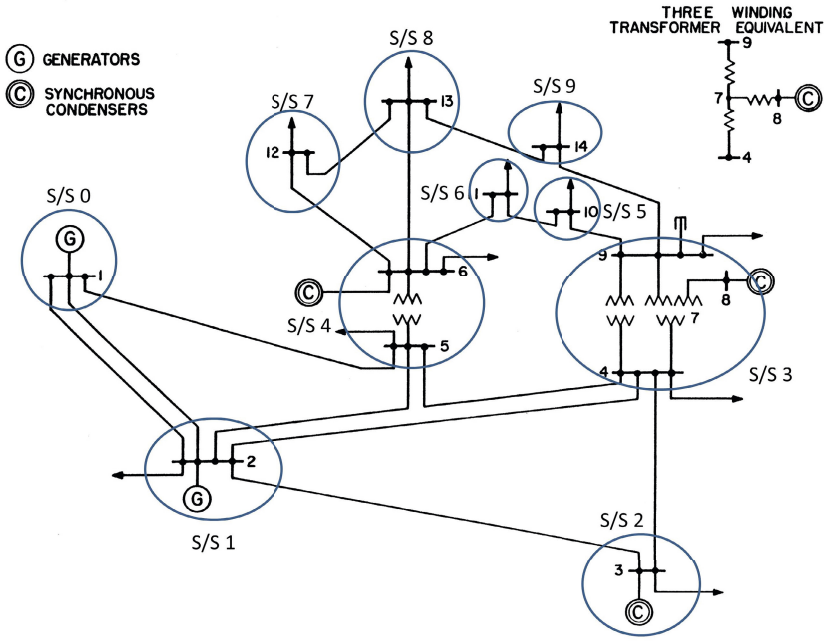

Fig. 4 Communication network node assignments

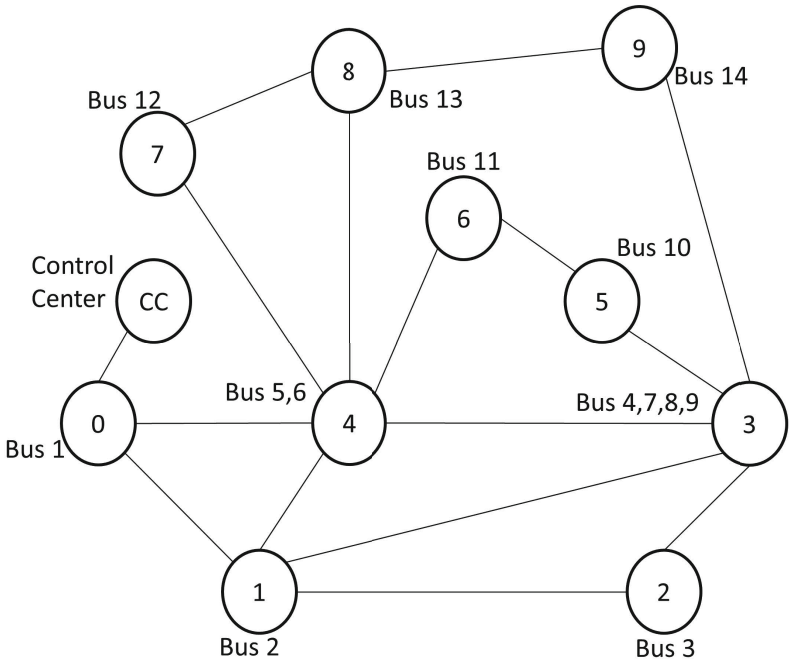

Fig. 5 Communication model for the IEEE 14 bus system

priate voltage levels. For distribution level voltages, it is reasonable to assume a per mile reactance of 0.5 ohm. Fig 5 shows the communication network topology derived from the one line diagram of power system. In this figure, the location of control centers, special protection scheme centers and other regional control points are also added as nodes. This forms the top level view of the communication network.

3) For transmission level systems, multiple control centers maybe assumed to be present depending on the size of the system. Control centers are usually located near the reference bus or near strategic locations. For distribution systems, certain nodes may have control devices associated with them.

4) The next level of the communication network view is the intra node view. Intra-node communications are local area network interactions and can be modeled accordingly. In a power system substation, it can be assumed that a single or multiple server(s) provide access to the IEDs and relays at that substation through a dedicated gateway. Wired or wireless network or a combination of these can be used. At the transmission level, it is reasonable to assume that each node will have a gateway associated with it. Distribution network nodes may not always be equipped with gateways as the information may pass through a radial network with very few devices. A generalized intra node view is depicted in Fig 6. The intra-node view depicts the different devices that could be part of a node.

One of the objectives of a smart grid is to achieve interoperability between multiple vendors, and compatibility with legacy systems. Legacy systems refer to the devices, which do not possess advanced technology and are in use in the power system. It is worth noting that a lot of electromechanical relays are still in use and have not been replaced by digital relays completely. For a transmission level system node, it is possible to have all the devices shown in Fig 6. For a distribution system level node, it is likely that an automation controller and few metering devices will be present. Substation computers may act as a means for providing authentication to engineering access used to modify the settings in the relays remotely. It can be used as an asset management device. Additionally, it may be used to execute local monitoring and control tools.

2.3.2 Energy Management System Modeling

In the Energy Management System (EMS) domain, of particular interest, is the control center and regional transmission operator centers where end use power system applications are implemented and state of the system is constantly monitored on a Human Machine Interface (HMI). The application software packages used are typically from multiple vendors. A common model as defined by the IntelliGrid Architecture (IGA) [16] depicted in Fig 7 can be used to model these control centers to achieve inter-operability. The major advantage of following this model is that the interfacing between the data collection devices and the application will be universal. The applications can be developed to support integration with this common

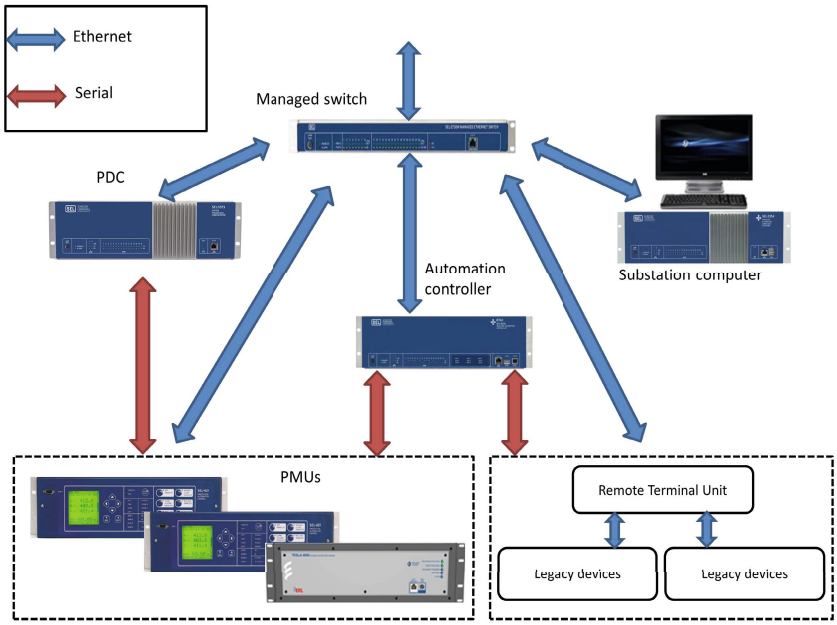

Fig. 6 Generalized intra node view

interface. Object Linking and Embedding (OLE) for Process Control Standard (OPC) is used for implementing this data transfer interface in this work. The OPC specification defines a set of objects, interfaces and methods for use in process control and manufacturing automation applications to facilitate interoperability. The OPC Data Access (OPC DA) specification is used to read and write data in real time. OPC Historical Data Access (OPC HDA) is used for access and retrieval of archived data. A OPC DA server needs to be implemented for the data aggregation device, and a OPC DA client needs to be implemented for interface with the application to be used. For example, if Citect SCADA software implements OPC DA server and MATLAB supports OPC DA client. This allows for Citect SCADA to be used for aggregation of Distributed Network Protocol (DNP) 3.0 data and MATLAB for data processing. Through implementation of OPC DA server for other data aggregation devices and software it will be possible to facilitate interoperability seamlessly.

In the event that OPC DA implementations are not possible, there are alternate options to transfer data from data aggregation device to the application. If SEL 5073 software Phasor Data Concentrator (PDC) is to be used, then a python script can be written to directly access the storage database and retrieve data. In case OpenPDC is used, then additional options exist. Data can be exported from OpenPDC into a SQL database or to a Comma Separated Value (CSV) file and data may be fed into the applications as necessary.

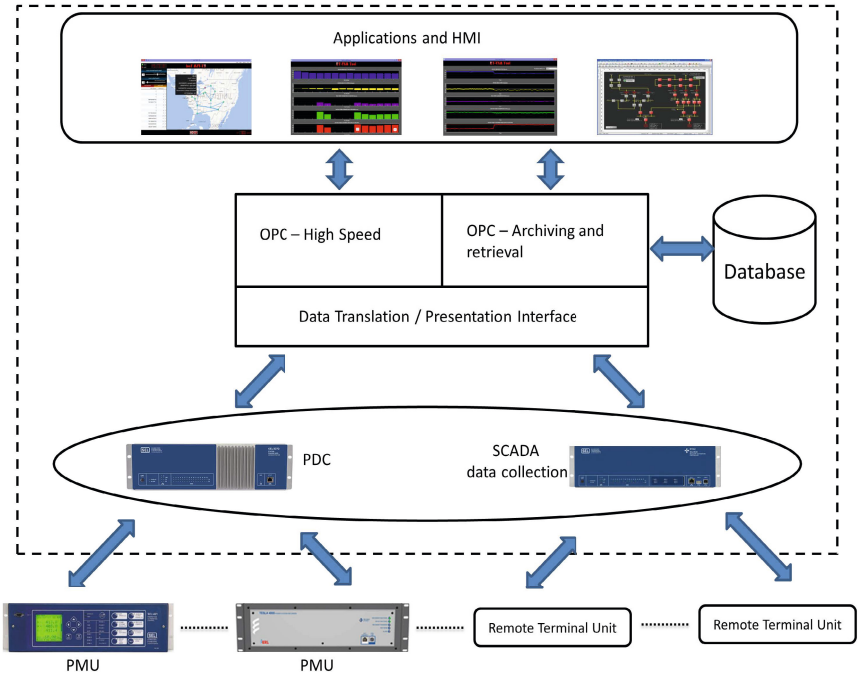

Fig. 7 EMS layer architecture

3 A Real Time Cyber-Power Test Bed

The development and implementation of a comprehensive cyber-power test bed consisting of simulation, emulation and real devices is discussed in this section. Real Time Digital Simulator (RTDS) is used to simulate the power system while network simulator -3 (NS3) is used to simulate the communication system. The data measurement and collection system comprises of commercial hardware, software and simulated devices. The major advantage of the test bed lies in the modular approach. The test bed can be segregated into four separate layers; physical power system layer, monitoring systems layer, communication layer, and energy management layer. The developed test bed is explained through the implementation and simulation of a electric power transmission level system.

3.1 Test Bed Components

Fig 8 is a self explanatory picture showing the different devices and the typical interconnections between them. This figure shows the base test bed without the communication simulator integrated into it. RTDS is used for power system and

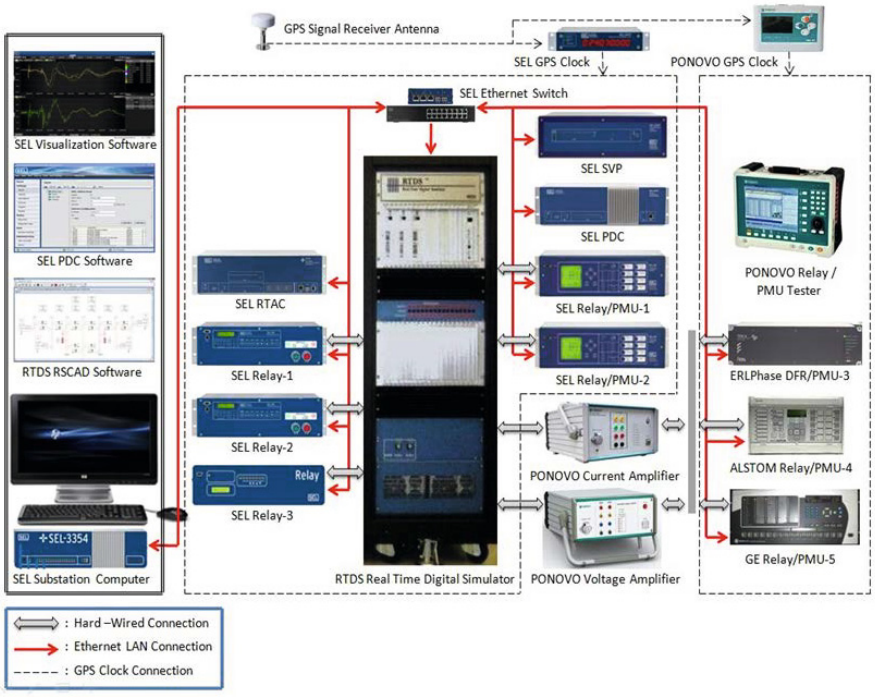

Fig. 8 Smart grid research test bed at WSU

sensors simulation. Intelligent Electronic Devices (IED) from multiple vendors such as SEL, GE, ERLPhase, Alstom are used in the test bed. These IEDs may combine functionality of a relay and phasor measurement unit (PMU) can interface with the RTDS to receive measurement signals. For IEDs that have a low level input interface for measurement signals, hardwired interface is provided with the RTDS. For devices without this option, amplifiers are used as shown in the figure. Automation controllers such as the Synchrophasor Vector Processor (SVP), and Real Time Automation Controller (RTAC) serve to implement and test local or centralized algorithms. These devices receive measurement information from the IEDs through the Ethernet Local Area Network (LAN) connection as shown in the figure. Software and hardware PDC from SEL are used for data aggregation at substations. OpenPDC is an open source PDC software maintained by the Grid Protection Alliance (GPA) is also used at the EMS layer. All the devices in the test bed are time synchronized by a single GPS clock which provides IRIG-B signals for this purpose. The test bed is designed for implementation and testing of smart grid devices and algorithms.

3.2 Physical Power System Layer

Advancements in the field of power system simulators have facilitated the near real time simulation of the power system. The RTDS is a virtual power system simulator designed for real time simulation with a typical time step of fifty microseconds, if no power electronic devices are modeled. This means that the state of the power grid is updated every fifty microseconds. Even though the simulation is discrete time based, due to the number of points computed within a given power system cycle, the simulation approximates the continuous time power system appropriately. The RTDS draft software module includes accurate power system component models required to represent the complex elements of the physical power system. The network solution technique employed in the RTDS is based on nodal analysis. The underlying solution algorithms are those introduced in [27] known as Dommel's algorithm. Dommels solution algorithm is used in most digital simulation tools designed for the study of electromagnetic transients.

The RTDS can be interfaced with external devices through dedicated analog and digital signal interface cards. Support for use of DNP3 protocol, software PMUs compliant with the IEEE C37.118.1 standard, GOOSE messaging and IEC 61850-9-2 sampled value messaging for power system voltages and current are also available [28]. RTDS is a commercial tool and is used extensively by academia, research organizations, service providers, and utilities for real time simulation. The basic model library provided by RTDS can be extended through implementation of user defined models. The use of RTDS enables hardware in the loop simulation through signal interface devices. Analog and digital signals can be exported and imported into the RTDS simulation environment through these dedicated devices. Hence, both monitoring and control environments are supported inherently.

For simplicity, a relatively small IEEE 14 bus test case is presented in the following sections The steady state values obtained during normal system conditions has been verified to validate the test case model.

3.3 Communication Layer

NS3 is used for the purpose of emulating the communication system for the simulated power system. NS3 has a modular implementation and contain a core library which takes care of the generic aspects of the simulator and a library dealing with specifying simulation time objects, schedulers and events. Protocol entities are written to be closer to the real world implementation. Packet implementations are based on the real data packets in order to enable communication between simulated agents and external world. This makes it suitable for emulation purposes. NS3 is running in a dedicated server to emulate the communication network in real time. It is to be noted here that the real time implementation of NS3 uses the system time to schedule events. This time is synchronized to a high precision GPS clock input which is used to time synchronize the devices in the test bed. NS3 is an open source simulator offering great flexibility in developing modules. This is of particular interest as a separate module such as security module can be implemented easily as long as the user has an understanding of NS3 development. The emulated communication network is protocol independent and can be used to transfer any data packet from source to destination.

The derivation of the communication network using the top down approach has already been presented in Sect 1.2.3.1. The reduced network for the IEEE 14 bus system has been shown in Fig 9. In NS3, each node represents a gateway to which the devices belonging to a particular private LAN can communicate. For communication with devices belonging to another private network, the gateway routes data to the receiving private network gateway.

Fig 9 depicts the communication between two private networks. In order to understand information flow, it is important to distinguish the layers involved. The power system simulation layer and EMS layer are not shown here for sake of simplicity. The communication network is represented by the nodes in the layer, interconnected by lines which represents the transmission media between the LANs. Assume that each node represents the gateway of that particular LAN number. The monitoring network is represented by the PMU at LAN 9, and PDC at LAN 0. Consider that the PMU at LAN 9 is going to send data to a PDC at LAN 0. The device in LAN 9 will view the gateway inside NS3 as being on its local physical link. It forwards the data packet to be sent to the PDC at LAN 0 to the gateway. In this way, the packet to be sent from node 9 to node 0 enters the NS3 simulation where the communication network is being simulated. The gateway node inside NS3 decides the shortest path to send the packet to the destination and forwards the packet to the next hop based on the routing table. In this example, it is node 3. In this way, the packet follows the red line and reaches node 0 gateway. The gateway then forwards the packet to the intended device. The delays that are experienced by the data packets are described as follows:

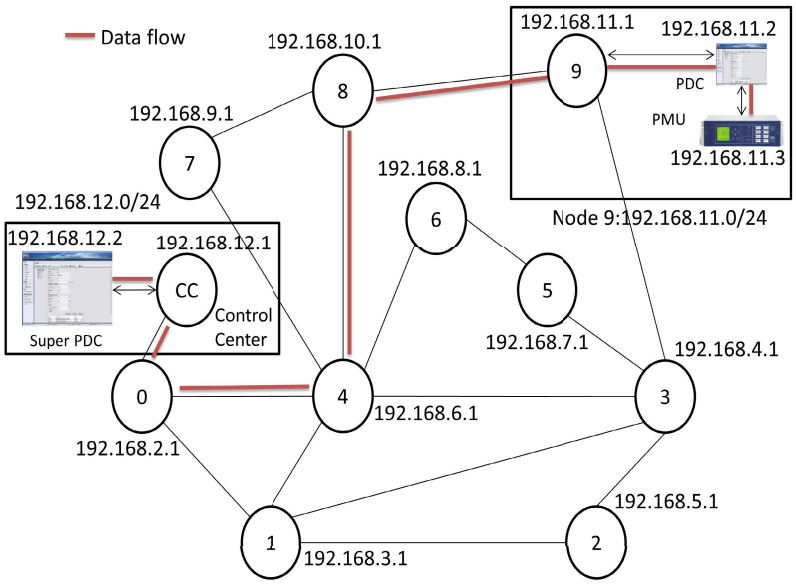

Fig. 9 Communication between two private networks

1) Network Processing Delay: These delays are incurred when the network gateways, firewalls and servers decide what needs to be done with an incoming packet. The delay depends on the network equipment technology and the specific processing function.

2) Signal Propagation Delay: It is the time taken for a signal to travel in the physical propagation medium, and depends on the medium itself and the distance. The propagation speed of the signal through fiber optic medium is about seventy percent of the speed of light in vacuum.

3) Transmission Delay: There is a definitive time delay for a packet to be completely pushed on to the physical link layer. This delay is called the transmission delay and is dependent on the bandwidth of the link and packet size.

4)Queuing Delay: This kind of delay occurs when multiple packets from an ingress port need to be routed to the same egress port. One packet is transmitted at a time, and a queue is maintained to hold the remaining packets. The queuing delay experienced by a packet is the time that a packets waits in a queue before being processed by a node. The total end network latency is the sum of all these delays.

Hence, a packet that is transmitted from a device at LAN 9 to a device at LAN 0, experiences all these delays as a result of communication network emulation by NS3.

3.4 Power Systems Monitoring Layer

The monitoring systems layer of the test bed is represented by the intra node substation view. It comprises of the sensor devices such as potential transformers (PT) and current transformers (CT), and the IEDs that use the signals from the sensor devices. A substation might have several devices interconnected and interacting with each other through IEC 61850 compliant protocols or other standard protocols. The interaction between the devices is flexible and configurable according to user requirements. In this example, it is assumed that the transmission level system is fully PMU enabled and that each bus has at least one PMU.

The substation view for such a system is shown in Fig 10. Only one PMU is shown here as an example. Depending on the node of interest, the number of PMUs might be higher with possible interaction between the PMUs. The PMU output data stream is concentrated in a PDC for transmission to super PDCs. Each substation is considered to be on its own private network with access to other private networks through its gateway. Engineering access is used to gain access to the private network to change settings and configuration files in the relays from the control center. A substation computer may or may not be present locally to make use of the data archived to run any algorithms and serve as an asset management device.

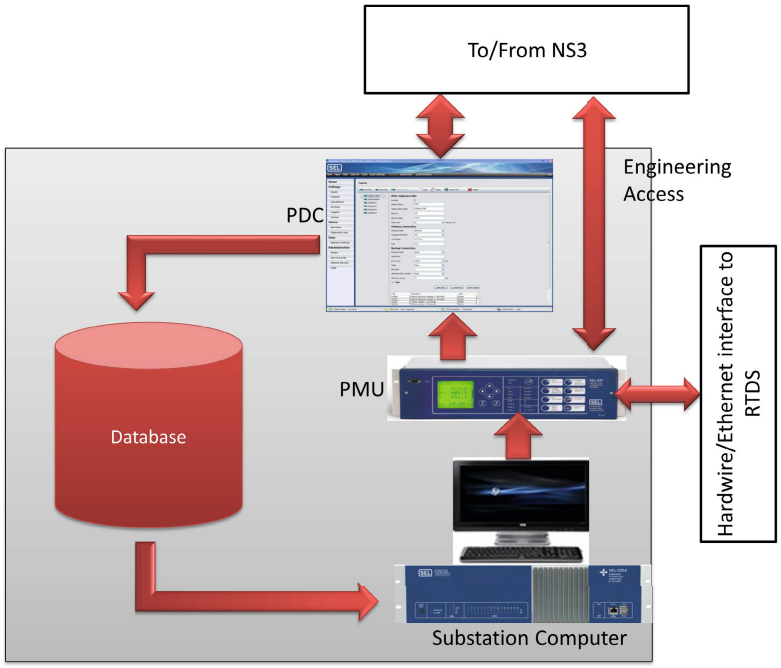

Fig. 10 Substation view for transmission system

3.5 *Energy Management System Layer*

The EMS layer of the test bed is represented by the control center. It mainly consists of a super PDC for collection of data from all the other nodes for data archiving. This data stored in the database maybe used by the real time and non real time applications.

Fig 11 shows the control center view for the PMU enabled transmission system. Here the control center has a super PDC, which aggregates data from all the PDCs in the system. Human Machine Interface (HMI) and visualization tools may be used depending on the application or algorithm to be implemented in the test bed. In this configuration, it is assumed that no other super PDCs are available except at the control center.

For the IEEE 14 bus system, with a PMU at each bus, fourteen PMUs are required to monitor the entire system. The communication topology is made up of ten nodes, eleven if the control center is included. Each node is considered to be a substation and houses one software or hardware PDC. This brings the total number of PDCs used to eleven including the super PDC at the control center. The test bed can support up to six hardware PMUs due to the limited availability of signal interface devices in the RTDS. The remaining eight PMUs are software PMUs simulated in a

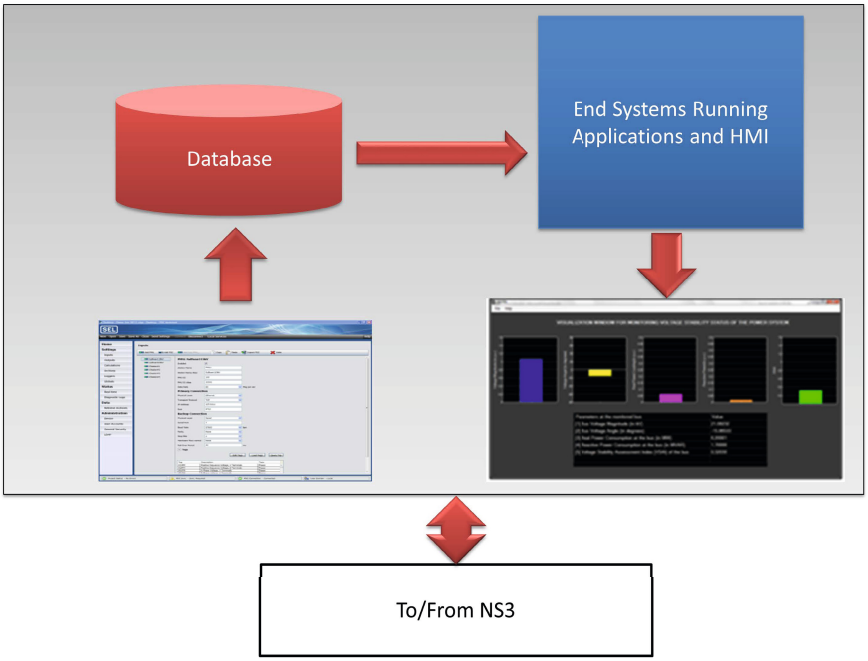

Fig. 11 Energy management system view for transmission system

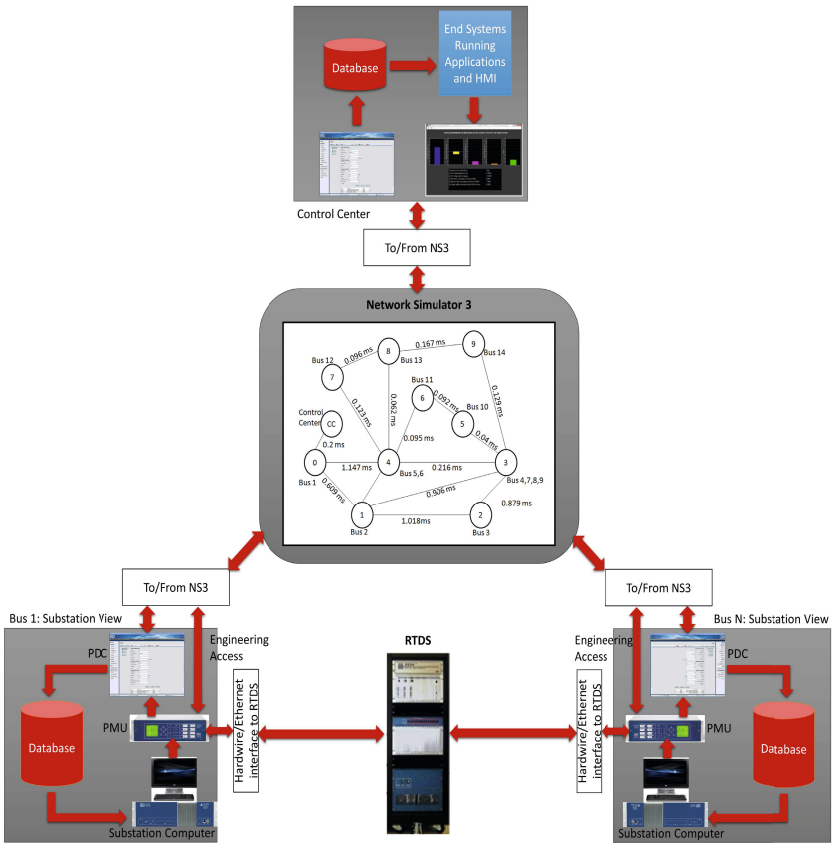

Fig. 12 Cyber-power system test bed

dedicated expansion card in RTDS. The PDC requirement is met through the use of SEL 3373 hardware PDC, SEL 5073 software PDC and openPDC. A simple scripting interface is provided to deliver data from the PDC to the application. The overall integrated cyber-physical test bed is shown in Fig 12. Validation of this test bed is presented in [22] A four layered view showing the separation and interconnection of the different layers is shown in Fig 13.

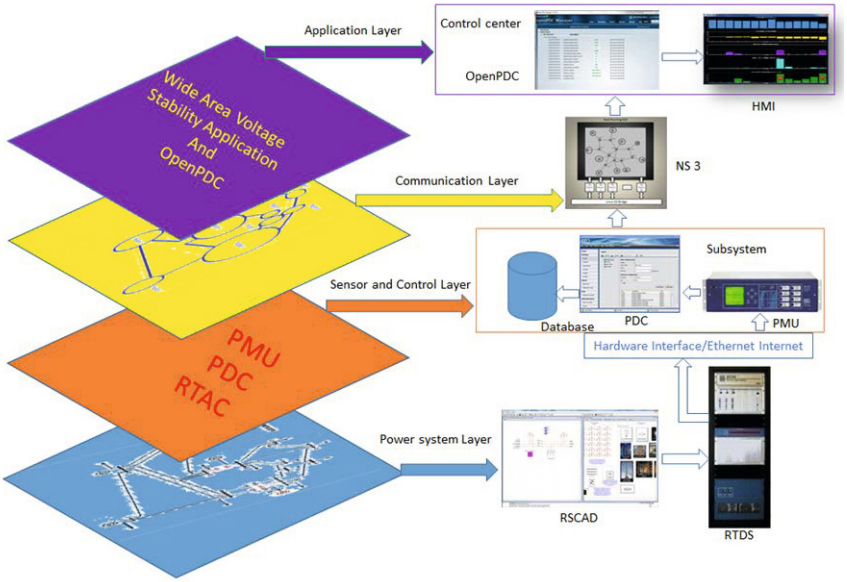

Fig. 13 Four layer view of the cyber-power test bed

4 Applications of Cyber-Power Test Bed

This section provides examples of applications for cyber-physical analysis using different configurations of cyber-power test bed. In addition to the application testing, the test bed can also be used for device testing such as PMUs and PDCs [23].

4.1 Local Voltage Stability Monitoring Algorithm

The test bed setup for the local voltage stability monitoring algorithm (LVSMA) is shown in Fig 14. Only the implementation of LVSMA is discussed here and further details about the implementation can be found in [24].

The requirements of the algorithm are stated as follows:

1) The Local Voltage Stability Monitoring Algorithm (LVSMA) will be running in the substations only. A substation computer is required to carry out the analysis locally at the substation. For this purpose, the SEL 3354 substation computer is used.

2) In addition to the local phasor data, the algorithm requires the use of voltage angle of the slack bus to obtain the angles with reference to the slack bus. So, the slack bus voltage angle is sent to each substation in the network.

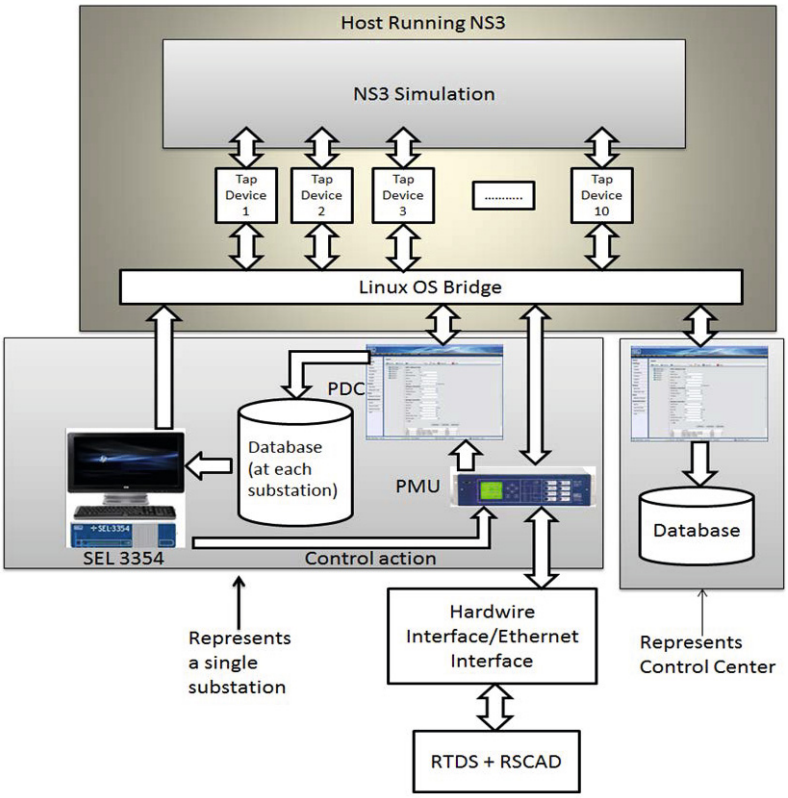

Fig. 14 Test bed setup for testing LVSMA

3) The calculated voltage stability index is then transferred to the control center through the communication network. A control algorithm may be present at the local or the control center. This algorithm is responsible for taking any control actions necessary to avoid voltage collapse.

4) The application running time is in the range of microseconds. Therefore, the application running frequency is restricted only by the availability of data and requirement.

The substation PDC receives the voltage angle from the slack bus through the control center PDC. The scripts for obtaining data from the database at the substation are executed locally in the substation computer. The local VSMA is successfully implemented to compute the index for voltage stability monitoring.

4.2 Wide Area Voltage Stability Monitoring Algorithm

The wide area voltage stability monitoring algorithm (WAVSMA) in EMS layer uses a non iterative methodology for computing voltage stability indices and is based on system centric reduced network equivalent method [25]. The algorithm makes use of system wide voltage, voltage angle measurements, and system topological information to compute the distance to the point of voltage collapse (PoC) for the load buses in the power system. An index termed Voltage Stability Assessment Index (VSAI) that ranges between '0' and '1' is used to specify this value. A value near '0' indicates a highly voltage stable load bus and a value near '1' indicates that the load bus is near the point of voltage collapse.

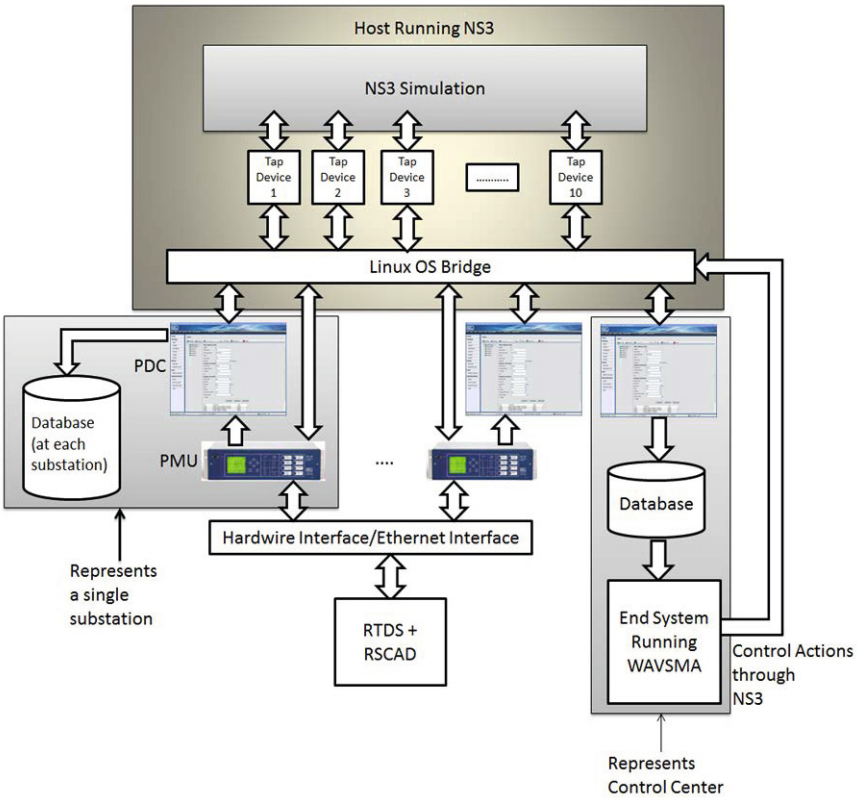

Fig. 15 Test bed setup for testing WAVSMA

As the developed algorithm is non iterative, it is computationally less burdensome than the existing multiple power flow based approaches. Hence it is suitable for the real time monitoring of the system voltage stability. The typical run time of the application is in the range of a few milliseconds, allowing it to process PMU data

Fig. 16 RT-VSM Tool showing VSAI of all load buses for IEEE 14 bus system

Fig. 17 RT-VSM Tool showing VSAI of all load buses for IEEE 14 bus system following load increase

as available. Additionally, the algorithm can integrate and operate with traditional monitoring systems as well as PMU based systems governing the time step required to run this application.

The requirements of this application are summarized as follows:

1) The WAVSMA tool is assumed to be running at the control center. However, it could be used at different locations as needed. One of the Dell precision workstations available in the test bed is used as the platform for running the tool. 2) The application needs the voltage phasor and voltage angle values only. Breaker statuses are not required if a topology processor is providing the topological information.

3) The WAVSMA calculates the voltage stability assessment index, and based on this any necessary control action may be taken. The control action is relayed to the appropriate substation.

All substation PDCs send the phasor data aggregated at the substation to the control center PDC. At the control center, a script is used to retrieve the data in the format as needed by the application. It is to be noted here that the algorithm running time is small, and the frequency of application execution is restricted generally by the rate of data input. Any control action specified by the application is relayed to the appropriate substation through NS3.

A tool that can enable power system operators to visualize the real time voltage stability condition has been developed using the proposed algorithm and has been named Real Time Voltage Stability Monitoring (RT-VSM) Tool. C# Language and

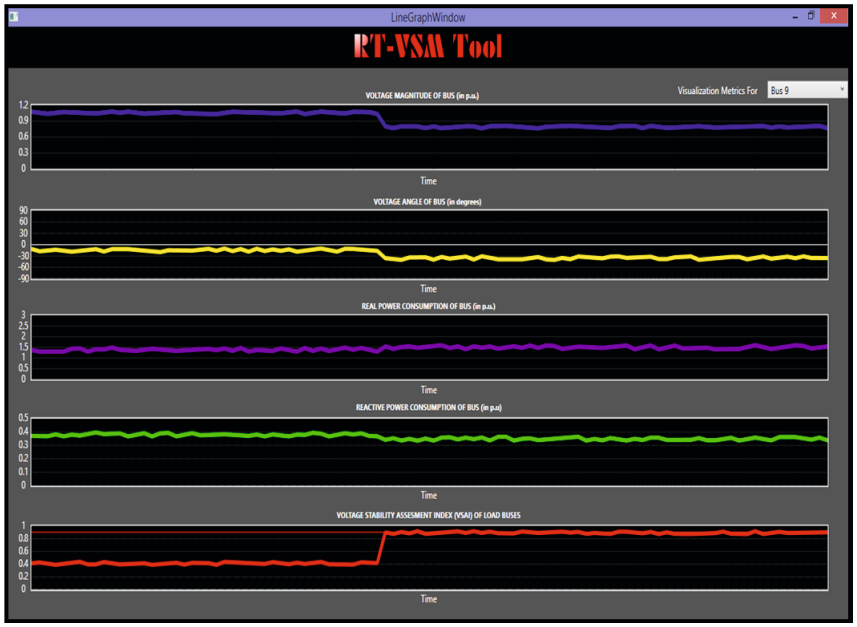

Fig. 18 Real time visualization window of the RT-VSM Tool

XAML have been used to build this tool. Fig 16 shows the visualization window of the RT-VSM Tool when the loading at the load buses in the IEEE 14 bus test case is increased. The increase in load leads to an increase in the voltage stability assessment index indicating a stressed system. The visualization windows of the RT-VSM Tool show that during the stressed case, VSAI of all the load buses increase indicating deterioration of voltage stability. It is found that buses 9 and 14 have VSAI values above the set alarm value of 0.9, as has been indicated in the Fig 17. Fig 18 shows the visualization window of the RT-VSM Tool that tracks the changes in the critical system metrics during the change in system loading. The VSAI of the weakest bus under the given system conditions i.e. Bus-9 changes from 0.44 to 0.94. Further details related to the use of the test bed for this application can be found in reference [26].

4.3 Shipboard Power System Reconfiguration

The Shipboard Power System Reconfiguration Algorithm (SPSRA) implemented in the test bed is a genetic algorithm based application [28]. The algorithm is coded in structured text and implemented in the SEL 3530 RTAC. Power generation, load on the system and breaker status data in the system are the data required in addition to load priority information. DNP data communication is implemented between all devices in the network. Fig 19 shows the test bed setup for SPSRA. The algorithm monitors the state of the power system continuously. In the event of generation loss due to a contingency, the RTAC computes the most effective solution through the

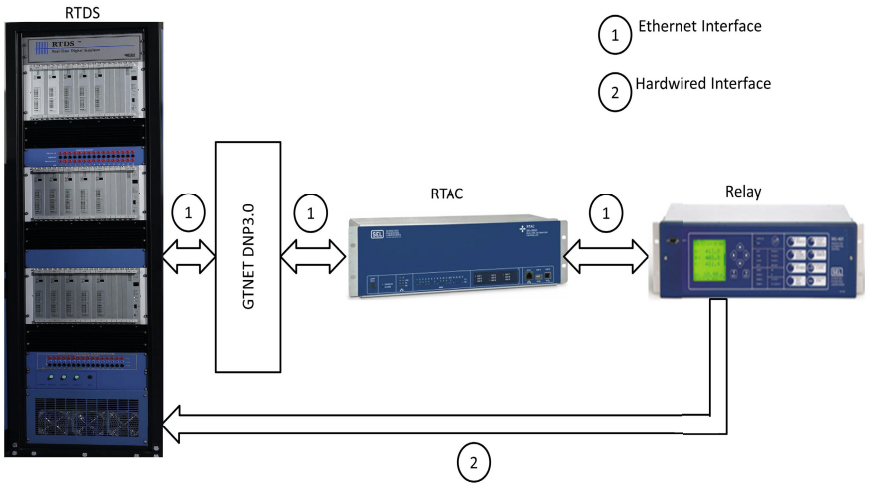

Fig. 19 Test bed setup for testing SPSRA

use of genetic algorithm and performs a reconfiguration of the system based on load priority, restoring power very quickly.

4.4 Aurora Attack Simulation

In 2007, Idaho National Laboratories (INL) demonstrated the Aurora attack involving the opening and closing of breaker associated with the generator in fixed intervals. The assumption is that the sync check element (25) is disabled in the relay

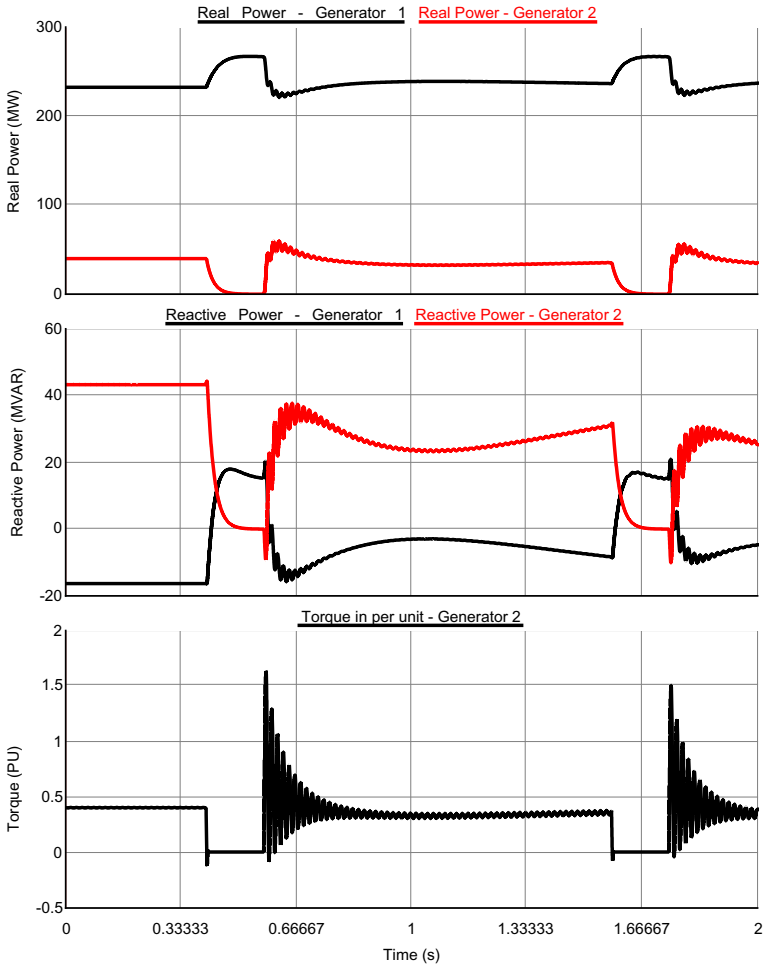

Fig. 20 Plot showing swing in real, reactive power, and electrical torque at Gen 2

leading to the possibility of re-closing the generator without a synchronism check leading to a out-of-sync close.

Aurora attack was re-simulated using the developed cyber-power test bed. The ranking of critical generators for the IEEE 14 bus system is computed based on the generator contingency ranking with incomplete information and cyber vulnerability index for relays [29]. For the purpose of simulating the attack in the test bed, it is assumed that the attacker has access to the network information and IEDs by compromising the private network. The attacker gets access through engineering access to the IED used to control the breaker at Bus 2 of the IEEE 14 bus system. This means that the attacker now has access to the IED settings, which can be modified maliciously. The IED settings is reprogrammed by the attacker to open the breaker for 10 cycles, causing the generator to spin faster upon loss of the load, and reclose the breaker after one second. The one second intervals gives enough time for the system to recover and not cause tripping due to any other relays picking up the induced fault condition in the system. The simulation of this attack can be made realistic by overlaying a security model on the communication network. This requires implementation of a security module that can be integrated with NS3. The impact on the machine due to the attack is depicted in Fig 20. It can be seen that the machine is subjected to high mechanical stress due to the out of sync reclosing and will suffer physical damage if attack is repeated.

5 Summary

In this chapter, the cyber-physical characteristics of the smart grid and need for a cyber-power system analysis using a real time test bed is presented. The different layers of the smart grid and the coupling between these layers are discussed. The modeling and simulation of the power system layer, communication network layer, measurement and data collection layer, and EMS layer using real time digital simulator (RTDS), network simulator-3 (NS3), hardware sensors, and controllers have been presented. Challenges involved in developing such a test bed and guidelines have also been discussed. Additionally, example applications using the developed cyber-power test bed have been successfully implemented and presented. The next step in the test bed development process is to add a security layer, which would reflect a real world scenario. By defining access policies and firewall rules for each private network, the attack-defense mechanism testing can be made possible. Recent developments in NS3 in the implementation of network address translation (NAT) and Netfilter provide basic framework for the implementation of a security layer. These improvements are still in development and need validation and testing before deployment in the test bed.

References

1. Singh, S.N.: Electric Power Generation, Transmission and Distribution. Prentice Hall India Pvt. Limited (2004) ISBN: 9788120321922

2. Padiyar, K.R.: HVDC Power Transmission Systems: Technology and System Interactions, New Age International (1990) ISBN: 9788122401028
3. Bose, A.: Power System Stability: New Opportunities for Control. In: Liu, D., Antsaklis, P.J. (eds.) Stability and Control of Dynamical Systems and Applications. Birkhäuser, Boston (2003)
4. Gungor, V.C., et al., Smart Grid Technologies: Communication Technologies and Standards. IEEE Trans. Ind. Informat. (2011), doi: 10.1109/TII.2011.2166794
5. National Institute of Standards and Technology, NIST framework and roadmap for smart grid interoperability standards 2.0 (2012), http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf
6. Smith, R.: Assault on California Power Station Raises Alarm on Potential for Terrorism (2014)
7. Govindarasu, M., et al.: Cyber-Physical Systems Security for Smart Grid. PSERC (2012), http://www.pserc.wisc.edu/documents/publications/papers/fgwhitepapers/Govindarasu_Future_Grid_White_Paper_CPS_Feb2012.pdf
8. Meserve, J.: Stage cyber attack reveals vulnerability in power grid (2007), http://www.cnn.com/2007/US/09/26/power.at.risk/
9. Bou-Harb, E., et al.: Communication security for smart grid distribution networks. IEEE Commun. Magazine (2013), doi:10.1109/MCOM.2013.6400437
10. Yilin, M., et al.: Cyber-Physical Security of a Smart Grid Infrastructure. Proceedings of the IEEE (2011), doi: 10.1109/JPROC.2011.2161428
11. Khaitan, S.K., McCalley, J.D., Cyber physical system approach for design of power grids: A survey. In: IEEE Power and Energy Society General Meeting (PES) (2013), doi:10.1109/PESMG.2013.6672537
12. Khaitan, S.K., McCalley, J.D.: Design Techniques and Applications of Cyberphysical Systems: A Survey. IEEE Systems Journal (2014), doi:10.1109/JSYST.2014.2322503
13. Gurusinghe, D.R., et al.: Modeling of a synchrophasor measurement unit in an electromagnetic transient simulation program. In: Proc. Int. Conf. on Power Syst. Transients (2012), doi:10.1109/PESGM.2012.6343954
14. Menike, S., et al.: Implementation of communication network components for transient simulations in PSCAD/EMTDC. In: Int. Conf. on Power Syst. Transients (2013)
15. Anderson, P.M., Fouad, A.A.: Power System Control and Stability, p. 450. Iowa State University Press, Ames (1977)
16. Premerlani, M., Kasztenny, B.: Synchrophasors: Definition, Measurement, and Application (2006), http://www.gedigitalenergy.com/SmartGrid/Sep06/Synchrophasors_Paper.pdf
17. Lin, H., et al.: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network. IEEE Trans. Smart Grid (2012), doi:10.1109/TSG.2012.2191805
18. Mallouhi, M., et al.: A testbed for analyzing security of SCADA control systems. In: IEEE PES Innovative Smart Grid Technologies (2011), doi:10.1109/ISGT.2011.5759169
19. Davis, C.M., et al.: SCADA cyber security testbed development. In: North American Power Symp., Carbondale, Illinois (2006)
20. McDonald, M.J.: Modeling and simulation for cyber-physical system security research. Sandia National Laboratories Development and Applications, SAND2010-0568 (2010)

21. Bergman, D.C., et al.: The virtual power system testbed and inter-testbed integration. In: Proceedings of Cyber Security Exp. Test (August 2009)
22. Vellaithurai, C., et al.: Development and Application of a Real Time Cyber-Power Test Bed. IEEE Trans. on Industrial Informatics (in Review)
23. Biswas, S.S., et al.: Development of a smart grid test bed and applications in PMU and PDC testing. In: North American Power Symp., Champaign, Illinois (September 2012)
24. Biswas, S.S., et al.: Development and real time implementation of a synchrophasor based fast voltage stability monitoring algorithm with consideration of load models. In: IEEE Ind. Applicat. Soc. Annual Meeting (October 2013), doi:10.1109/IAS.2013.6682584
25. Biswas, S.S., et al.: RT-VSMAP: A Real Time Voltage Stability Monitoring and Prediction Algorithm for Electric Power Grids, Patent filed, USPTO: 27158.8052.US01 (2014)
26. Srivastava, A., et al.: Real Time Cyber-Power System Analysis. In: TCIPG Annual Ind. Day Workshop (2013), http://www.youtube.com/watch?v=_wfbcOWckmM
27. Dommel, H.W.: Digital Computer Solution of Electromagnetic Transients in Single- and Multiphase Networks. IEEE Trans. on Power Apparatus and Systems (1969), doi:10.1109/TPAS.1969.292459
28. Shariatzadeh, F., et al.: Real-Time Implementation of Intelligent Reconfiguration Algorithm for Microgrid. IEEE Trans. Sustain. Energy (2013), doi:10.1109/TSTE.2013.2289864
29. Srivastava, A., et al.: Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information. IEEE Trans. Smart Grid (2013), doi:10.1109/TSG.2012.2232318