The Journal of CPRI,
Vol. 12, No. 4, December 2016 pp. 731-736

Need for Real Time Simulation in cyber security Applications

Sreedevi J*, Noorcheshma P**, Ashwin N**and Meera K S***

Various sophisticated technologies have been deployed in the modern power system to facilitate the notion of smart grid, integrating the power system, associated IT infrastructure and the communication network into a Cyber-Physical System (CPS). The increasing coupling between a physical power system and its communication network necessitates a Cyber-Physical test environment to investigate and guarantee the grid's stability and reliability. A Cyber-Physical Testbed consists of four components – a Physical power systems layer, a power systems monitoring layer, a Communication Network layer and an Energy Management Systems layer. In this paper, the need of a Cyber Security testbed is detailed along with an architecture of a typical Cyber Security Testbed and the role of a Real Time Simulator in the Testbed.

Keywords: *Cyber-Physical System (CPS), Cyber-Physical Testbed, Phasor Measurement Units (PMU), Real Time Digital Simulator*

1.0 INTRODUCTION

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 system study for analysis. [1, 2] Most smart grid technologies enable bidirectional data communications, hence potentially introduce cyber security issues. Numerous access points that are distributed over the smart grid become possible victims that can be compromised by potential cyber-attacks [3]. Recent research has shown that an intentional cyber-attack can cause significant impact on power systems in terms of stability and economical operation [4].

Therefore, cyber security of smart grid is a big concern that is getting more and more attention along with the deployment of smart grid applications.

In this paper, the various components of a typical Cyber-Physical test bed and its applications are explained. Further, the role of Real Time Simulators in testing and analysing the cyber physical system is examined.

2.0 NEED FOR A CYBER-PHYSICAL TESTBED

Cyber security in smart grids is becoming increasingly important due to adoption of smart grid technologies. Smart grid technologies like Wide Area Monitoring Systems (WAMS) are implemented based on bi-directional data communication. Measurement data, control commands and other types of data are transmitted between control centres and end users through an interconnected communication network. On one hand these technologies greatly facilitate

*Joint Director, PSD, Central Power Research Institute, Bengaluru, Karnataka, 560080.E-mail: sreedevi@cpri.in
**Senior Research Fellow, PSD, Central Power Research Institute, Bengaluru, Karnataka, 560080. E-mail: ashwin-srf@cpri.in
***Additional Director, PSD, Central Power Research Institute, Bengaluru, Karnataka, 560080.E-mail: meera@cpri.in `

smart grid in terms of reliability, stability and economic operation. On the other hand cyber security issues are introduced inevitably due to numerous accessing points that are exposed to potential hazards. An attacker with knowledge of communication, networking and power system can easily launch cyber-attacks [3].

Simulation-based evaluation of the behaviour of the electric grid is complex, as it involves multiple heterogeneous, interacting domains. Each simulation domain has sophisticated tools, but their integration into a coherent framework is a very difficult, time-consuming, labour intensive, and error-prone task. These types of computational studies have to be done in real time to provide timely answers to the planners, operators and policy makers are necessary. Further electric grid behaviour has to be tested against a number of scenarios and situations, which may occur due to changes in generation and load scenarios. So, a huge number of real time simulations must be executed covering all possibilities while testing cyber physical system.

A Real Time Simulator works on the parallel processing technique of digital signal processors and executes the program developed on its processors in real time[5]. Interfacing and testing of SCADA, relays and PMU hardware is only possible with Real Time Simulators by simulating the actual system to be connected for this hardware in simulator. This setup helps in monitoring the power system in closed loop with SCADA, Relays and PMUs.

3.0 CYBER-SECURITY TEST BED APPLICATIONS

Following are a set of test bed applications and benefits [6, 7].

i) *Vulnerability Research*: The Testbed can be used to inspect weakness in the industry standards, software platforms, network protocols and system configurations.

ii) *Impact Analysis*: The test bed can be used to explore and quantify physical system impacts from various cyber-attacks. Test beds help to capture the risk posed by a particular security event through the ability to determine impact on grid stability and power flow.

iii) *Mitigation Research*: Test beds present a useful environment to explore the effectiveness of various mitigation strategies. Mitigation efforts are attempts to reduce the vulnerabilities of the cyber infrastructure while increasing the robustness of the power systems.

iv) *Cyber-Physical Standards*: Test beds help in producing an environment where controlled evaluations can be performed to support standards development and evaluation. On the physical side, standards can be evaluated based on impact to power flow, stability and even power markets.

v) *Data and Models Development*: Test bed environments help in developing models and data sets which can be disseminated to researchers to facilitate more accurate analysis and results. Models could incorporate power system models, network architecture, protocols and data.

vi) *Security validation*: The Test bed environment help to design methods to evaluate the security posture of a system for self-assessments and compliance requirements. Testbed environments that implement industry standard software and configurations can help understand both impacts and effectiveness of traditional security techniques while also presenting an environment where new methods can be explored.

vii) *Interoperability*: Testbeds also present a distinct opportunity to explore system interoperability within a realistic environment. It can be used to evaluate how products and technologies support and connect with real-world systems.

viii) *Cyber Forensics*: Cyber-attacks can be used to modify the operational logic of field devices, which depend heavily on embedded systems which utilize different operating systems and software platforms. Testbeds

play a key role in forensically analysing these devices specifically, whether they respond correctly to commands and return accurate measurements.

ix) *Operator Training*: Testbeds present the opportunity to analyse cyber incidents and demonstrate how a realistic attack would look to system operators. Testbeds may provide training applications to help identify differentiated failures from both cyber and physical aspects.

4.0 ARCHITECTURE OF A CYBER-PHYSICAL TEST BED

Integration of the following simulators/devices are required to realize a tightly coupled cyber-physical system: *power system layer*, *communication network layer*, *power system monitoring layer*, and *Energy Management System layer* [1].

i) *Power system layer*: The physical electrical network is modelled in a Real Time Simulator. It consists of libraries which can be used to model any type and any level of complex power system network.

ii) *Communication layer*: A network simulator is used to simulate the communication system for the simulated power system. Simulators such as Network Simulator 3 (NS3) [1] and OPNET [3] are widely used for simulating communication network.

iii) *Power Systems Monitoring layer*: It comprises of sensor devices such as potential transformers (PT) and current transformers (CT). Intelligent Electronic Devices (IED) like a Phasor Measurement Unit (PMU) also use the signals from these sensory devices. They are usually modelled inside the power system simulator.

iv) *Energy Management Systems (EMS) layer*: The EMS layer of the testbed is represented by the control centre. It consists of database, which is used to collect data from all other nodes for data archiving. Usually an OpenPDC software is used as a database.

5.0 ROLE OF REAL TIME SIMULATOR IN CYBER-PHYSICAL TESTBED

Advancements in the field of power system simulators have facilitated the real time simulation of the power system. Here the details on two Real Time Digital Simulators available at CPRI to test the cyber-security applications is provided:

5.1 Real Time Digital Simulator by RTDS Technologies:

It is a power system simulator designed for real time simulation with a typical time step of fifty microseconds, if no power electronic devices are modelled. This means that the mathematical model of the power system is solved and updated at less than 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 is close to the continuous time power system operation. The RSCAD draft software module of simulator includes accurate power system component models required to represent the complex elements of the physical power system. The network solution technique employed here is based on nodal analysis.

The basic model libraries provided can be extended to build up the actual network required. Hardware-in-loop (HIL) simulation can be enabled through signal interface devices. Analog and digital signals can be exported and imported into the simulation environment through these devices. Hence, both monitoring and control environments are supported inherently. DNP3, IEEE C37.118.1 standard compliant TCP/UDP, GOOSE messaging, and IEC 61850-9-2 sampled value protocols are supported by RTDS™ [2, 8, 9].

In any Cyber-Physical test bed, there are multiple substations that can be modelled in the simulator. In each of these modelled substations, several PMUs are used to measure the synchrophasor data and a Phasor Data Concentrator (PDC) is utilized to archive the data from PMUs. A small database is installed in each substation to temporarily store the synchrophasor data from PDC in case of data loss caused by communication failures. When

communication recovers, the database can also re-send the data automatically to control centre [10]. In order to synchronize the cyber-physical testbed, a high resolution time stamp is provided by satellite-synchronized clock to all the synchronized devices like PMU, PDC and simulator. In a developed testbed, it is not necessary that all buses (substations) should be connected with hardware PMU. Simulator provides software PMUs that are connected by Giga-Transceiver Analogue (GTAO) card to capture the phasor data from each bus. The hardware PMUs can also have a relay function, which can send the control command back to the Simulator through Giga-Transceiver Digital Input (GTDI) card for control action in the simulated power system [3].

5.2 Hypersim simulator by M/s Opal RT Technologies

This simulator provide a platform for simulation of virtual grids where the testing of multiple scenarios can take place simultaneously and in real-time. The FPGA based simulators include I/O signal modules with converters/conditioning units and multi-core processor computer which runs RT-LAB or HYPERSIM OPAL-RT's real-time simulation software platforms. Complex power grids, micro-grids, wind farms, hybrid vehicles, more electrical aircrafts, electrical ships and power electronic systems can be simulated in real-time with time step as low as 10 microseconds or less than 250 nanoseconds for some subsystem to achieve the best simulation accuracy [11].

Communication protocols supported by the simulator are DNP3, IEC 61850-9-2 Sampled values, Modbus, IEEE C37.118 standard compliant TCP/UDP.

6.0 CYBER SECURITY INITIATIVES IN INDIA

As cybersecurity is critical for Digital India and the Smart City Concept highlights smart grid to be resilient to cyber-attacks. The National Cyber Coordination Centre (NCCC) is being established by the Indian Government. It is a proposed cyber security and e-surveillance agency. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Also, National Cyber Safety and Security Standards has been started with a vision to safeguard the Nation from the current threats in the cyberspace.

The Bangalore Electricity Supply Company Ltd. (BESCOM) project in Bangalore envisaged a Smart Grid Pilot Project for integration of renewable and distributed energy resources into the grid, which is vital to meet growing electricity demands of the country, curb power losses, and enhance accessibility to quality power. To ensure security, BESCOM has come out with a separate IT security policy and dedicated trained IT professionals to safeguard its data and servers. BESCOM one of the few Discoms in India to take such measures for safeguarding the servers and data network from cybercrimes and threats [12].

7.0 CASE STUDY: SIMULATION OF CYBER ATTACKS ON SCADA SYSTEMS USING RTDS

If the power system's observability and controllability are compromised due to communication and cyber security problems, the grid can be exposed to catastrophic events. Hence there is a great need to model the interactions between information and communication technology(ICT) and power grids. The impact of cyber-attacks on power systems can be analyzed by means of computer simulations and system dynamics can be observed to quantify the seriousness of the problem. For this, it is necessary to model the electric grid and simulate the response due to cyber intrusions.

As part of this study a typical electrical substation is modeled in Real time simulator with incoming lines as generators and outgoing lines as loads.

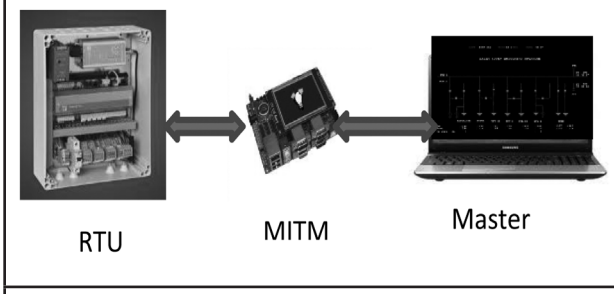

FIG. 1. SCADA SECURITY SYSTEM

The CDAC - SCADA system as shown in Figure 1, comprises of Remote Terminal Unit(RTU), Man In The Middle(MITM) and System Operator console(Master).

Closed loop working condition of SCADA system and RTDS is established by sending power flows, bus voltages and frequencies from RTDS to RTU. At the same time Breaker control signals are received from RTU to RTDS as shown in Figure 2. These signals while on further transmission to system operator (MASTER) are tampered by MITM.

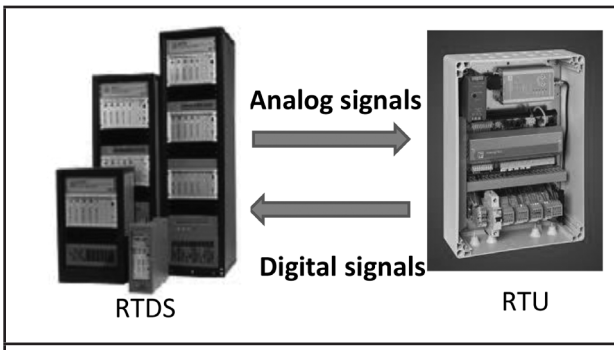

FIG. 2.: SIGNAL INTERFACE

Different Cyber Attacks are performed on the power system simulated on RTDS. Man in the Middle sending directly command to the breakers is simulated from SCADA system to RTDS. Tampering the Generator values, Load values, bus voltages and frequency by MITM and sending it to the operator for taking the wrong counter measures is also simulated. Impact analysis is carried out which is intended to analyze intrusions and determine the consequences of a cyber attack on the cyber physical system. A risk assessment approach that captures both power system vulnerabilities and the resulting impact on the real-time operation is studied[13].

8.0 CONCLUSION

Cyber Physical Systems (CPS) offer coordination between different computational and physical resources, and thus, they are expected to play a major role in the design and development of next-generation smart grid. By the fusion of power, information and control, physical entities can be provided with functions of computation, communication, accurate control, coordination and autonomy, to improve the safety, reliability and efficiency of power system. CPSs enable data flow to be more regularized and available in internationally acceptable standards format. Data from various IEDs in the CPS such as, PMUs, RTUs, digital protective relays, etc. can be used for research, studies, industries and organizations to develop, airplanes, space vehicles, and smart homes. To guarantee the reliable operation of such infrastructure, a Cyber-Physical Testbed has been proposed by various authors. In this paper, an overall view of a Cyber-Physical Testbed, along with its need and architecture has been discussed in detail. Particularly, the role of a Real Time Simulator has been detailed, giving an idea to researchers and institutes about how to use Real Time Simulator to develop and design the Testbed.

ACKNOWLEDGMENTS

The authors wish to thank the authorities of CPRI for permitting to publish this paper. The authors wish to thank Rajesh Kalluri and Mahendra Lagineni for their support during the simulation work at RTDS.

REFERENCES

[1] C B Vellaithurai, S S Biswas, R Liu, and A Srivastava, “Real Time Modeling and Simulation of Cyber-Power System,” Power Systems, pp. 43-74, 2015.

[2] S K Khaitan and J D McCalley, "Design Techniques and Applications of Cyber

physical Systems: A Survey," in IEEE Systems Journal, Vol. 9, No. 2, pp. 350-365, June 2015.

[3] B Chen, K L Butler-Purry, A Goulart and D Kundur, "Implementing a real-time cyber-physical system test bed in RTDSTM and OPNET," North American Power Symposium (NAPS), 2014, Pullman, WA, pp. 1-6, 2014.

[4] B Chen, S Mashayekh, K L Butler-Purry, and D Kundur, "Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices," in Proc. 2013 IEEE/PES General Meeting, Vancouver, Canada, 2013.

[5] C B Vellaithurai, S S Biswas; A K Srivastava, "Development and Application of a Real-Time Test Bed for Cyber–Physical System," in *IEEE Systems Journal*, Vol.PP, No.99, pp.1-12, 2015.

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

[7] P S Kumar, W Emfinger and G Karsai, "A testbed to simulate and analyse resilient cyber-physical systems," 2015 International Symposium on Rapid System Prototyping (RSP), Amsterdam, pp. 97-103, 2015.

[8] Ram Mohan Reddi and A K Srivastava, "Real time test bed development for power system operation, control and cyber security," North American Power Symposium (NAPS), 2010, Arlington, TX, pp. 1-6, 2010.

[9] Real Time Digital Simulator user's Hardware and Software manual set.

[10] U Adhikari, T Morris, and S Pan, "WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining," in IEEE Transactions on Smart Grid , Vol.PP, No.99, pp.1-1, March 2016.

[11] T Kirk and D Manz, "Power Grid Cyber Security," Webinar, OPAL-RT Technologies, January 2016, https://www.youtube.com/watch?v=EHRE95AEd8M. Last accessed on Sep 16, 2016.

[12] E Hickok and V Rakesh, "Cyber Security of Smart Grids in India," in The Centre for Internet and Society, April 2016, http://cis-india.org/internet-governance/blog/dataquest-april-25-2016-vanya-rakesh-and-elonnai-hickok-cyber-security-of-smart-grids-in-india. Last accessed on Sep 19, 2016.

[13] Abhiram Amaraneni, Mahendra Lagineni, Rajesh Kalluri, Senthil kumar R K and Ganga Prasad G L, " Transient Analysis of cyber-attacks on Power SCADA using RTDS, The Journal of CPRI, Vol 11, No 1, March 2105, pp 79-91.