Electrical Power and Energy Systems 90 (2017) 124–133

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

Real-time cyber physical system testbed for power system security and control

Shiva Poudel, Zhen Ni*, Naresh Malla

Department of Electrical Engineering and Computer Science, South Dakota State University, Brookings, SD 57007, USA

ARTICLE INFO

Article history:
Received 28 June 2016
Received in revised form 3 November 2016
Accepted 21 January 2017

Keywords:
Cyber-physical system testbed
Power grid security
Real-time adaptive control
Optimal power flow (OPF)
Intelligent electronic devices (IEDs)

ABSTRACT

The existing electric power grid is upgraded into a smart grid through an intelligent communication infrastructures, layers of information, extensive computing and sensing technologies. These cyber and physical components of grid together constitute a complex cyber-physical system (CPS), and this integration increases the risk from cyber attacks and introduces new vulnerabilities to the power system. Researchers need a power system testbed which can provide a platform for realistic experiments. This paper presents the development of a real-time cyber-physical system testbed for cyber security and stability control. We use SEL 351S protection system with OPAL-RT including control functions and communications to build a cyber-physical environment. In this testbed, we conducted power grid security experiment by knocking down two transmission lines in a row and analyzed the impact of failures. Meanwhile, we provided two mitigation strategies for this failure using optimal power flow. In addition, we conducted load fluctuations for multimachine power system, and provide timely adaptive control strategies.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Smart grid is a modernized electrical grid and is generally referred as the next generation power system. For the purpose of sensing, monitoring, protection and control, information and communication technology system are being deployed in modern power system. With this integration, smart grid is expected to greatly enhance efficiency, reliability and economy of power production and consumption along with the integration of renewable energy resources, as well as demand response and distributed intelligence [1]. Although the current smart grid initiatives are expanding the use of information technologies to modernize the existing grid, their adoptions in cyber physical systems (CPS) have introduced power system security issues [2,3]. Attacks on either cyber or physical part of the smart grid will possibly impact the stability of the entire system.

Recent research in cyber attack against smart grid has shown that these intentional attacks can have an impact on power system operation in terms of stability and economy. For example, authors in [4] commented that cyber attack in measurements of static var compensator (SVC) or static synchronous compensator (STATCOM) can degrade the system's stability margin. Cyber attacks including false data injection attacks can mislead the state estimating process [5] or even can impact the economic operation of electric power market operations by manipulating the nodal price [6]. Similarly, denial of service (DoS) attacks in the cyber layer of smart grids can affect the dynamic performance of physical power system [7]. It is also important to verify the device settings, algorithms and application before they are deployed in real power system to avoid any unfortunate incident. For example, malfunctioning of relays can lead to false tripping of breakers which can cause cascading failures. In this case, cyber-physical testbeds can serve as a tool for simulating the power system model accurately and also helps to understand the complex relation between cyber and physical domains. Although United States Department of Energy (DoE) is giving considerable attention to the security enhancements of cyber-physical power system, the research related to cyber attack and impacts are constrained by the availability of realistic cyber-physical system testbed.

In many cases, cyber and/or physical attacks also result in the stability issues in smart grid and microgrid. There are several dynamic events happening in power system, e.g., a sudden change in load, fault in transmission lines or buses, and generator out of service. These events will impact the system's stability and can ultimately lead to loss of synchronism. The stability control is also an important piece in cyber-physical system [8]. Computational

* Corresponding author.
E-mail addresses: shiva.poudel@wsu.edu (S. Poudel), zhen.ni@sdstate.edu (Z. Ni), naresh.malla@sdstate.edu (N. Malla).

http://dx.doi.org/10.1016/j.ijepes.2017.01.016
0142-0615/© 2017 Elsevier Ltd. All rights reserved.

intelligence (CI) based supplementary adaptive control approaches for microgrid have been investigated in simulation platforms with the consideration of different faults [9–11]. For example, researchers reported their computational cost in seconds based on adaptive dynamic programming (ADP) controller, and the controller usually generated the instant actions within the sampling interval [9,12]. However, none of them implements this type of computational intelligence based controller on a real-time platform. This motivates us to conduct the adaptive control experiment based on CI for power system on the developed platform. The contributions of this work are summarized as:

- A real-time cyber-physical system testbed is developed based on OPAL-RT, SEL 351S protection system, high-performance computers and communication networks. The testbed capability is then investigated in terms of power system protection and control.
- The impact of a real-time cyber attack on the multimachine power system is studied in terms of voltage stability and generation loss. The post-contingency results after the successful coordinated attack are observed through bus voltage fluctuations and generator transients.
- Two different mitigation strategies are studied off-line using optimal power flow for system reconfiguration in order to restore normal or next steady state operating condition after failures. Different reconfiguration plans are suggested for avoiding the cascading failures following any kind of cyber attack.
- The ADP based real-time adaptive control is conducted for multimachine power system during the load fluctuations based on this proposed cyber-physical system platform.

The rest of the paper is organized as follows. Section 2 describes the research work related to cyber-physical system for security and control. Section 3 describes the application areas of real-time cyber-physical system testbed. Section 4 provides the implementation of proposed testbed. Sections 5 and 6 shows experimental studies on cyber-security and control respectively. Finally, Section 7 concludes the work with possible future directions.

2. Related work

Suitable power system testbeds are needed in order to accurately capture the attack effects, attack impacts in the physical system, and possible mitigation strategies as well as control algorithms to ensure stability and security of power grid. Several cyber defense testbeds have been developed at various entities such as national labs, universities and research centers for purpose of studying the consequences associated with these cyber-physical threats and mitigate those consequences. The researchers at national SCADA testbed at Idaho National Laboratory investigated how a cyber attack can cause damage to a physical system through an aurora generator test [13]. In the experiment, the researcher used a computer program to open and close the breaker out of phase from the grid to maximize the stress. Virtual control system environment (VCSE) was developed at Sandia National Laboratory which uses hybrid modeling and simulation architecture in order to understand the possible impact of particular cyber threats, cyber defense training and exploring power system vulnerabilities [14].

Beside national labs, universities and research institutes are also focusing research in the development of a CPS testbed for cyber security issues. A testbed has been developed at University of Arizona using PowerWorld and MODBUS protocol to detect cyber attacks on SCADA system [15]. In this work, authors presented compromised human machine interface (HMI) and denial of service as different attack scenarios. Authors in [16] suggested various applications of testbed developed at Mississippi State University. The proposed testbed was used for simulation of common power system contingencies (generator loss, transmission loss and sudden load loss), and event detection using data mining of phasor measurement unit data. Similarly, a power system cyber-physical testbed was developed for intrusion detection and it also provides the platform for hardware in the loop (HIL) simulation, cyber-attack and generated data sets for developing and validating an intrusion detection system for monitoring power system events [17]. The SCADASim testbed has been developed at Royal Melbourne Institute of Technology University for building SCADA simulations which support combination of network simulation and real device connectivity [18]. It helps to analyze the effects of malicious attacks, e.g., denial of service, eavesdropping, man-in-the-middle and spoofing on the devices and simulated network. Emerging smart grid distributed control algorithms were examined in the developed smart-grid cyber-physical system testbed where authors highlighted the impacts of different interactions in the operation of micro-grid [19]. A cyber-physical security testbed at University College Dublin [20] provides an accurate tool for analyzing cyber-physical vulnerabilities, allows monitoring of the dynamic behavior of power system as response to cyber attacks (impact analysis), and mitigation of cyber attacks. For analyzing the physical impact due to compromise in cyber network, a cyber-physical contingency analysis framework was introduced in [21] for both accidental contingency and malicious compromise. The impact of three different types of real-life cyber attacks namely, communication line outage, denial of service and man-in-the-middle attack in physical power grid was studied through the proposed testbed developed at Washington State University [22]. Other related CPS power testbed research has been discussed in [23–25].

Research efforts have been made worldwide from industry, academia and national laboratories for the development of real time cyber-physical testbed. The realistic cyber-physical environment achieved from these testbeds is helpful for investigating power system vulnerabilities, mitigation strategies and system behavior during different kinds of conditions for our research in this paper.

3. CPS testbed application areas

A CPS testbed needs to have certain capabilities to provide realistic cyber physical environment. This section provides the various research applications of a cyber-physical power system testbed. The main application areas are shown in Fig. 1 and are elaborated below in detail.

3.1. Vulnerability analysis

Vulnerability is any weakness that an intruder takes benefit of in order to compromise the security goals (confidentiality, integrity, availability or authenticity) of smart grid [26]. In the cyber security context, it is equally important to incorporate both cyber and physical layers of power system for vulnerability analysis [20]. Vulnerability might be associated with communication protocols, firewall or VPNs, sensing and monitoring devices in substation or even in control centers. However, unavailability of these technologies publicly is the main constraint for vulnerability assessment. A real-time cyber-physical testbed provides the environment to analyze the weakness as well as testing of these platforms and architectures.

3.2. Disturbance scenarios

Different disturbances can be simulated in a real-time CPS testbed. They might be an attack or any dynamic events within

Download English Version:

https://daneshyari.com/en/article/4945622

Download Persian Version:

https://daneshyari.com/article/4945622

Daneshyari.com