Electric Power Systems Research 129 (2015) 160–169

Contents lists available at ScienceDirect

Electric Power Systems Research

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

Power system reliability evaluation considering cyber-malfunctions in substations

Hangtian Lei*, Chanan Singh

Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA

ARTICLE INFO

Article history:
Received 22 April 2015
Received in revised form 3 August 2015
Accepted 5 August 2015

Keywords:
Cyber-physical interface matrix
Hidden failure
Protection system
Reliability
Switching

ABSTRACT

Protection system failures have been recognized as major causes of expanded outages and thereby affect bulk power system reliability. With the rapid progress of smart grid technologies, legacy protection systems with hardwired architecture are being gradually replaced by computer and communication networks consisting of multi-functional and smart Intelligent Electronic Devices (IEDs). In this paper, a systematic methodology for considering the effect of cyber-malfunctions in substations on power system reliability is proposed by extending the concepts we previously presented. The Roy Billinton Test System (RBTS) is extended to include substation protection systems with modern architecture, which is an important step as a test system like this is currently unavailable. The proposed approach is then demonstrated on this test system. The quantitative relationship between switching time and system-wide energy unavailability is studied. The results of our study clearly indicate the impact of protection system failures on system-wide reliability indices and signify the importance of accelerating line switching process. Furthermore, the overall methodology used in this paper provides a tractable and scalable option for the reliability evaluation of large cyber-physical power systems.

1. Introduction

The quantitative reliability indices of bulk power systems are important to utility companies, vendors, and regulators for planning, operation, maintenance, and regulatory purposes. Studies of bulk power system reliability evaluation have been mostly focusing on the current-carrying part. The pertinent theories and methodologies are well established and documented [1–3].

In bulk power system reliability evaluation, protection systems are typically assumed to be perfectly reliable so that the failure of a current-carrying component will result in the isolation of that component only. This assumption may neglect the impact of protection system failures on system-wide reliability indices. It has been recognized that protection system hidden failures are common causes of multiple or cascading outages [4–7]. Some studies [6–10] have been done to consider protection system failures and the results show that protection system failure modes have significant effects on evaluated reliability indices.

A protection system consists of circuit breakers, current and voltage transformers, communication cables, protective relays, and possibly some auxiliary devices [11–13]. With the advent of microprocessor-based relays and the rapid progress of communication technologies, modern protection panels are equipped with multifunctional Intelligent Electronic Devices (IEDs) that are connected to communication networks [14–17].

In composite power system reliability evaluation, due to the variety of protection system architectures as well as the diversity of control and communication mechanisms, it is hard to explicitly model protection systems with detailed configurations. As a result, in most of the previous work, protection system failures were either concentrated on circuit breaker trip mechanisms [6] or represented abstractly by multistate models [7–10] without showing the technical details regarding protection system elements as well as their connections. Due to the absence of such details, the interdependencies between protection elements and power equipment were not covered in those publications. In [18,19], to study the direct and indirect cyber-physical interdependencies, some mathematical terms and operations were defined and proposed with applications on small test systems including monitoring, control, and protection features. The results in [18,19] provide valuable information that indicates the impact of cyber element failures on physical system reliability indices. However, excessive self-defined

* Corresponding author. Tel.: +1 979 571 0474.
E-mail addresses: hlei7@tamu.edu (H. Lei), singh@ece.tamu.edu (C. Singh).

http://dx.doi.org/10.1016/j.epsr.2015.08.010
0378-7796/

reliability terms and tedious mathematical operations were introduced in [18,19]. These terms are hardly available from engineering practice, making it difficult to implement the overall methodology in practical applications. Reference [20] proposed a more systematic and scalable methodology of performing the overall analysis in a tractable fashion with the use of *Cyber-Physical Interface Matrix* (*CPIM*). In [20], a typical substation protection system with detailed architecture was designed and analyzed as an example to illustrate the procedures of obtaining a CPIM. The steps on how to use a CPIM in composite power system reliability evaluation were also formulated.

The composite power system displayed in [20] is simple and is used for illustration only. The overall methodology with the use of CPIM needs to be further demonstrated with its implementation on a standard test system so that the impact of protection failures on system-wide reliability indices can be numerically validated. Also, the scalability of the overall methodology needs further illustration as this is very important to its application for large power systems. Moreover, the unavailability of standard reliability test systems containing practical protection features is an obstacle for validation of the impact of protection failures on system-wide reliability indices. The extension of the Roy Billinton Test System (RBTS) [21] performed in this paper provides valuable information for developing standard reliability test systems including protection features and will thereby benefit future studies in this area. With these objectives, this paper continues and enhances the work that has been performed in [20]. The remainder of this paper is organized as follows. Section 2 outlines the overall methodology. Section 3 presents the test system configuration and parameters. In Section 4, the overall analysis, including the reliability analysis at the substation level and the reliability evaluation at the composite system level, is performed. Also, the results are presented and summarized. The scalability of the overall methodology performed in this paper is illustrated in Section 5. Some major considerations in software implementation for large power systems are discussed in Section 6. Finally, the conclusions are made in Section 7.

2. Methodology outline and objectives

The cyber-physical interdependencies exist in many aspects of power systems, including but not limited to supervisory control, protection, monitoring, metering, etc. This paper focuses on the aspect of protection since protection hidden failures are recognized as common causes of expanded outages and have significant impact on power system reliability [4–10].

In this paper, reliability evaluation is performed in a composite power system consisting of current-carrying components and protection systems. The Roy Billinton Test System (RBTS) [21] is used as the test system with extensions at load buses to include detailed configuration in terms of protection system elements.

The size of this system is small to permit reasonable time for extension of cyber part and development of interface matrices but the configuration of this system is sufficiently detailed to reflect the actual features of a practical system [22]. The methodology performed in this paper also applies for large systems. For large systems, in spite of more efforts needed in detailed analysis of cyber failure modes as well as effects on the physical side, the main procedures are identical to those performed in this paper. In short, the selected system is adequate to illustrate the methodology and extension to larger systems is more mechanical effort rather than illustrating the validity of the technique.

The overall analysis mainly consists of two stages: (1) reliability analysis of protection systems at the substation level and (2) reliability evaluation from the system-wide perspective.

2.1. Reliability analysis at the substation level

The failure modes of protection systems in terms of basic cyber elements and their relationships to transmission line tripping scenarios are analyzed in this stage. The CPIMs, which depict the interdependencies among the failures of physical components due to various cyber failure modes, are obtained at the end of this stage.

2.2. Reliability evaluation from the system-wide perspective

In this stage, a sequential Monte Carlo simulation is performed on the composite system to obtain system-wide reliability indices. The results of CPIMs obtained in the previous stage are directly utilized in this stage without the necessity of considering protection system configuration details. At the end of this stage, system-wide reliability indices, such as Loss of Load Probability (LOLP), Loss of Load Expectation (LOLE), Expected Energy Not Supplied (EENS), and Expected Frequency of Load Curtailment (EFLC), for each bus and for the overall system, can be obtained.

2.3. System-wide reliability indices

The following system-wide reliability indices [7,9,22] are defined and used in this paper.

2.3.1. Loss of load probability (LOLP)

$$\mathrm{LOLP} = \sum_{i=1}^{N_s} \frac{H_i t_i}{t_{\mathrm{total}}} \tag{1}$$

where,

N_s is total number of iterations simulated;

H_i equals 1 if load curtailment occurs in the ith iteration; otherwise it equals 0;

t_i is simulated time in the ith iteration, with the unit of year; and

t_{total} is total simulated time, with the unit of year.

2.3.2. Loss of load expectation (LOLE)

$$\mathrm{LOLE} = \mathrm{LOLP} \times 8760 \tag{2}$$

with the unit of hours/year.

2.3.3. Expected energy not supplied (EENS)

$$\mathrm{EENS} = \sum_{i=1}^{N_s} \frac{8760 R_i t_i}{t_{\mathrm{total}}} \tag{3}$$

with the unit of MWh/year,

where,

N_s is total number of iterations simulated;

R_i is load curtailment during the ith iteration, with the unit of MW;

t_i is simulated time in the ith iteration, with the unit of year; and

t_{total} is total simulated time, with the unit of year.

Expected frequency of load curtailment (EFLC)

$$\mathrm{EFLC} = \sum_{i=2}^{N_s} \frac{Z_i}{t_{\mathrm{total}}} \tag{4}$$

with the unit of (/year),

where,

N_s is total number of iterations simulated;

Z_i equals 1 if load curtailment does not happen in the $(i-1)$th iteration AND load curtailment happens at the ith iteration; otherwise it equals 0; and

t_{total} is total simulated time, with the unit of year.

3. Test system configuration

The Roy Billinton Test System (RBTS) [21] is used as the test system in this paper. The single line diagram of the RBTS is shown