Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 142 (2017) 2021–2026

Energy Procedia

www.elsevier.com/locate/procedia

9th International Conference on Applied Energy, ICAE2017, 21-24 August 2017, Cardiff, UK

Reliability Assessment of Cyber Physical Distribution System

Jie Liu[a], Diangang Wang[a], Cheng Zhang[a], Zhenyu Tang[a], Zhuozhen Jiang[b]*, Junyong Liu[b], Yue Xiang[b]

[a]*State Grid Information&Telecommunication Co.Lid of Sichuan,Chengdu610041,China*
[b]*School of Electrical Engineering and Information ,Sichuan University,Chengdu610065,China*

Abstract

The traditional distribution network is gradually evolving into the cyber physical distribution system (CPDS) to suit the new characteristics of the distribution network. Distribution network plays an important role of risk source and vulnerable sector. Therefore, it is necessary to do some research on the reliability assessment for CPDS. The key factors of reliability assessment for the distribution network mainly including network components, cyber medium, network topology are firstly analyzed. Reliability assessment index is then summarized in terms of traditional physical system, common cyber system and the CPDS from extensive literature. This is followed by a review of reliability assessment methods in CPDS, which is mainly categorized into two aspects. Finally, the future research emphases are discussed.

Peer-review under responsibility of the scientific committee of the 9th International Conference on Applied Energy.

Keywords: Cyber physical system; distribution system; reliability assessment; review

1. Introduction

With the development of active distribution network, a large number of electrical equipment, data acquisition equipment and computing devices connect to the power system. And the scale and complexity of the distribution network are becoming unprecedentedly as the increase of demand. The traditional distribution network is gradually developing into highly coupled cyber physical distribution system [1-4].The CPDS is a specific application form in power system from cyber physical system (CPS). It is said that more than 80% of users suffered from interruption because of distribution system failure. Therefore, it is necessary to assess the reliability of the distribution network to ensure the safe operation of the power system. In the CPDS, power system is monitored and controlled by cyber system in a reliable way. Though the advanced information technology can improve the operation of the power system, it brings the potential negative impact to the power system [5]. These security risks of the cyber system may lead to feared blackouts. Comparing with transmission network, the analysis of distribution system need to take

* Corresponding author. Tel.: +86-182-0280-7247; fax: +86-028-85465996.
E-mail address :jiangzhuozhen@stu.scu.edu.cn

1876-6102
Peer-review under responsibility of the scientific committee of the 9th International Conference on Applied Energy.
10.1016/j.egypro.2017.12.405

more flexible factor into consideration, such as distribution renewable sources, electric vehicles and so on. Owing to the fact that the intelligent terminal equipment is lack of perfect protection, the distribution network can be attacked easily. Cyber threats should not be ignored in CPDS. Therefore, it is necessary to study the reliability assessment for CPDS.

The remainder of this paper is organized as follows. The key factors of reliability assessment in CPDS are described and analyzed in Section 2. In Section 3 and 4, the common reliability assessment Index and reliability assessment methods for CPDS are reviewed. Furthermore in Section 5, the prospects are discussed, and this paper is concluded in Section 6.

2. Key factors in reliability assessment

With the development of distributed generation equipment and energy storage technology, the structure of power system changes gradually. In the future CPDS, more and more intelligent electronic devices with the abilities of communication and information processing will be installed in all sectors of power system, so it is necessary for the cyber system to collect, transmit and deal with mass heterogeneous information. And the information of the power system is growing up explosively [6].

The reliability of cyber system is related to the network components, cyber medium, network topology, routing protocol and business objects [7-10]. Moreover, factors in terms of these aspects have become the main obstacles of reliability management and control. For example, opening protocols (such as IEC 61850 standard) improves the availability of communication equipment, but brings cyber system more security risks. In the CPDS, the security risks of cyber system cannot be ignored. Therefore, cyber risks are likely to be transmitted to the physical power system, even lead to the failure of the power equipment.

Some scholars have simplified the function of the cyber system to the physical system, which is divided into the direct action type and the indirect action type [11-12]. The former refers to the equipment failure in cyber system will directly lead to a relevant power equipment failure, for example, the failure of the intelligent terminal controller causes the circuit breaker to malfunction and even load cut off. The latter refers to the equipment fault of cyber system does not directly lead to a failure of power equipment, such that monitoring failure may make the operating staff can not identify potential risk timely, which does not immediately lead to power system fault.

The physical system can be affected by the cyber system. For example, Vulnerabilities of SCADA communication links can be exploited by an attacker to gain higher privilege level and compromise the system. Having gained higher privilege level, an attacker can create a fake outage scenario and send false trip signals to remote controlled switches. In order for a fake outage to seem authentic, an attacker should imitate a real outage scenario of a power distribution system. Finally, the users suffered from power interruption.

The cyber system can be affected by the physical system in some aspects including equipment, transmission medium, operational environment. Besides, it is worth mentioning that the interaction between the cyber system and the physical system is tight indeed. The reliability may be change along with some factors (delay of data transmission, packet loss rate and throughput). For example, the corresponding packet loss rate would be higher at the longer the communication distance, which lead to decrease the reliability for the cyber system more easily [13].

3. Reliability assessment index for the CPDS

3.1. Reliability assessment index for distribution network

The common reliability assessment index [14-16] for distribution network could be grouped into three categories, as listed in Table 1.

Table 1.Reliability assessment index for distribution network.

Category	Name	Acronym	Definition (“/”means divide)
Equipment	Equipment shutdown rate per year	-	Times of failure/years
	Equipment interruption time per year	-	Time of failure statistics /years