Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 145 (2018) 9–14

Energy Procedia

www.elsevier.com/locate/procedia

Applied Energy Symposium and Forum, Renewable Energy Integration with Mini/Microgrids, REM 2017, 18–20 October 2017, Tianjin, China

Reliability analysis of the security and stability control device based on the Monte Carlo method

Xueming Li[a], Zengji Liu[b]*, Yi Tang[b] Xu Gao[c], Yingxin Ma[c], Sumeng Tao[b]

[a]*NARI Technology Co., Ltd, #19,Chengxin Street, Jiangning District, Nanjing 210000, China*
[b]*School of Electrical Engineering, Southeast University, #2 SiPailou Street, Xuanwu District, Nanjing 210000, China*
[c]*Northern Hebei Electirc Power Co., Ltd, #32,ZaoQianlin Street, Xicheng District, Beijing 100053, China*

Abstract

Security and stability control device plays a significant role in ensuring the reliable operation of power system. However, fault-operation, fail-operation, under-control and over-control could be caused by the failure of stability control devices and system. Taking SCS-500E, one kind of security and stability control device, the failure of hardware and software are discussed in this paper. According to device structure and failure data, the failure model of the device is established. The advantages of the Monte Carlo method are analyzed, and the failure probability of the device is calculated by this method. It is proved that the results worked by the method proposed in the paper are matched with the actual condition.

Selection and peer-review under responsibility of the scientific committee of the Applied Energy Symposium and Forum, Renewable Energy Integration with Mini/Microgrids, REM 2017

Keywords: Security and stability control device, Failure rate, Monte Carlo method;

1. Introduction

The fundamental task of the power system is to supply electricity to the user safely, reliably and economically. As the second and third line of defense, the security and stability control device plays a key role on the reliable operation of power system [1]. The stability control device can be classified as regional security and stability control device, out-of-step splitting device, frequency and voltage control device and standby power supply device [2]. These devices are usually based on the unified platform [3]. The hardware of the stability control device can be divided into five parts: I/O unit, AD unit, calculation unit, man-machine interface unit and communication unit [4]. With the construction of intelligent substation, stability control device has been fully support IEC61850 standard [5]. It can get

* Corresponding author. Tel.: +86-15151838703; fax: 025-81093767.
E-mail address: liuzengji@seu.edu.cn

Selection and peer-review under responsibility of the scientific committee of the Applied Energy Symposium and Forum, Renewable Energy Integration with Mini/Microgrids, REM 2017
10.1016/j.egypro.2018.04.003

analog data through the SV net, communicate with intelligent operation box through GOOSE net and monitor the control layer management background through MMS net. Therefore, the reliable operation of the stability control device is exceedingly important for the security of the power system [6].

With the development of the smart grid, the stability control device is also constantly upgrading. But there are still some loopholes and problems. The stability of the power grid depends on the reliable operation of the device, so it is paramount to analyze the stability control device [7].The failure of the device consists of hardware failure, software failure, communication failure and human error [8]. These faults can be divided into dominant fault and hidden fault. The impact of hidden fault is more serious [9]. There are more researches on the relay protection device rather than the stability control device, and examine of hidden faults has just started. The methods of reliability analysis include Monte Carlo method, fault tree method, key sampling method, Markov state space method, etc. [10]. Some works incorporate these methods and summarize innovative approaches with the advantages of each method. The reliability analysis method of the device is proposed based on the Monte Carlo method in this paper.

2. The hardware system structure of the security and stability control device

The security and stability control device consists of three parts: control unit, input/output (I/O) unit and communication unit. There are differences in diverse set of devices. Taking SCS-500E as an example, the structure of the security and stability control device is shown in Fig. 1.

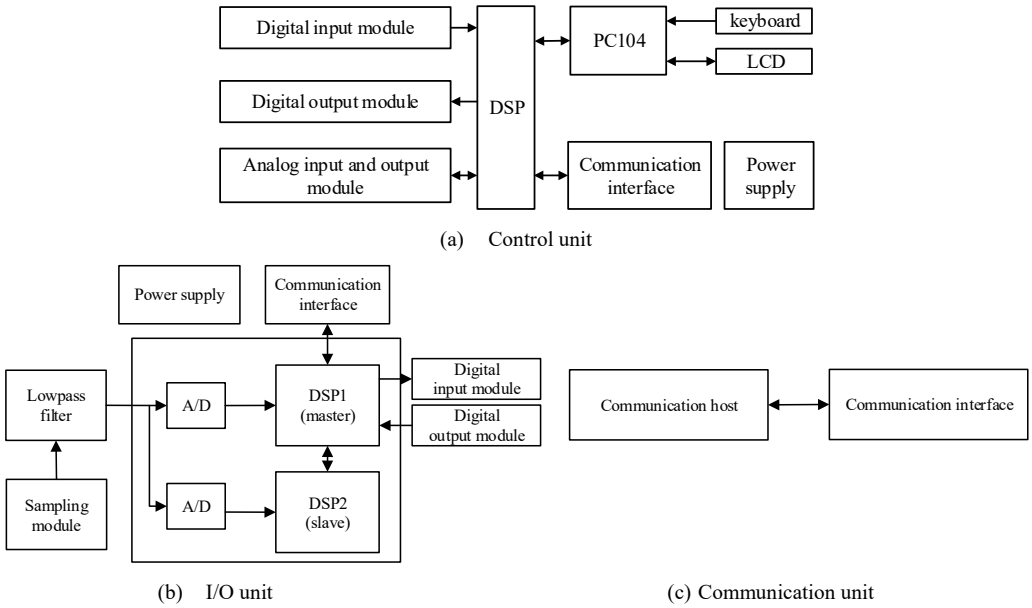

Fig. 1. Structure of the security and stability control device: (a) Control unit; (b) I/O unit; (c) Communication unit

In SCS-500E, the modules are divided into control unit, I/O unit and communication unit by functions. Control unit is the center of the device. Its key responsibilities include analyzing, decision making and output controlling. It provides man-machine interface and communication management in addition. I/O unit is the direct interface between device and external systems. Its main responsibilities include collection and calculation of the data, port output and fault diagnosis. Communication unit converts the data of fiber to E1/64K to access SDH or PCM. The hardware of communication unit is designed based on complex programmable logic device (CPLD). The entire logical function of the device is completed by using VHDL a kind of hardware description language.

Each unit of the security and stability control device consists of a series of modules. Control unit includes power supply module, interface management module, decision making module, communication extension module, digital output module, digital input module and analog input and output module. I/O module includes power supply module,