



面向继电保护装置的嵌入式软件安全性检测技术

丁伟, 蒙家晓, 戴涛, 陈华军

(南方电网科学研究院有限责任公司, 广东 广州 510663)

摘要: 继电保护装置作为电网安全的第一道防线, 其正确动作能够最大限度地降低系统或设备故障对电力系统安全的影响。在对继电保护装置检验规程以及电力行业企业标准研究的基础上, 从功能检测、性能检测以及故障注入检测等方面对继电保护嵌入式软件检测内容和技术进行研究, 以保证继电保护嵌入式软件检测的完整性和正确性。

关键词: 继电保护装置; 功能测试; 性能测试; 软件故障注入

中图分类号: TP39

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018150

Embedded software security testing technology for relay protection devices

DING Wei, MENG Jiaxiao, DAI Tao, CHEN Huajun

China South Power Grid International Co., Ltd., Guangzhou 510663, China

Abstract: As the first defensive line of power grid security, the right actions of relay protection devices can minimize the influence to the electric power system security caused by system or equipment failures. Based on the research of relay protection device inspection procedures and enterprise standard of electric power industry, the embedded software testing content and technologies of relay protection device were studied, including functional testing, performance testing and fault injection testing. This research contributes to the completeness and correctness of the embedded software testing about relay protection device.

Key words: relay protection device, functional testing, performance testing, software fault injection

1 引言

随着电力需求量的不断增大, 保障电力传输、供应的安全尤为重要。当电力系统中的电力元件(如发电机、线路等)或电力系统本身发生了故障危及电力系统安全运行时, 继电保护装置能够向运行值班人员及时发出警告信号, 或直接向其控

制的断路器发出跳闸命令, 以终止这些事件的发展。因此, 继电保护装置是否正常运行直接关系到电网的运行安全。为了保证继电保护装置的稳定运行, 需要对其进行安全性检测, 包括硬件检测和软件检测^[1]。

继电保护装置嵌入式软件对电力系统的安全稳定运行起着至关重要的作用。如果电力系

统继电保护软件出现设计失误、编码错误,会造成电力系统继电保护功能的不稳定,进而会影响电力系统继电保护的作用发挥。本文主要对继电保护嵌入式软件的检测技术进行研究。根据我国对继电保护装置制定的检验规程以及电力企业制定的企业标准要求,从功能检测、性能检测以及故障注入检测等方面,检测继电保护嵌入式软件能否正确实现要求的功能、是否满足性能指标要求以及是否存在软件故障,从而监测继电保护软件设备是否在电网中安全、稳定、可靠地运行^[2-4]。

2 继电保护装置概述

2.1 继电保护装置组成

继电保护装置主要由3部分组成:测量部分、逻辑部分和执行部分^[5],如图1所示。

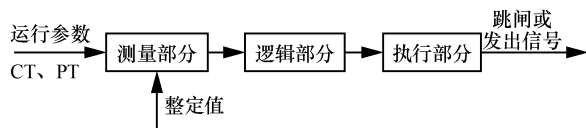


图1 继电保护装置基本结构

- 测量部分主要根据对象输入的有关电气量与给定的整定值进行比较,判断保护是否启动。
- 逻辑部分主要确定是否应该使断路器跳闸或发出信号,将命令传送给执行部分。
- 执行部分根据接收到的命令完成保护装备相应任务。如出现故障时,使断路器跳闸;不正常运行时,发出信号;正常运行时,不动作。

从图1中可以看出,继电保护装置基本结构的各个部分出现问题都会影响保护装备的正常运行。为了保证继电保护正常运行,需要对每个部分进行检测。

2.2 继电保护装置安全需求

继电保护装置是由多个继电器组成的自动装

置,类型多样,包括零序继电保护装置、过流保护装置、过压保护装置、差动保护装置、方向高频保护装置^[6]等(如图2所示)。一般要求其在合理的电网结构前提下,保证电力系统和电力设备的安全运行,并且应符合可靠性、选择性、灵敏性和速动性的要求。

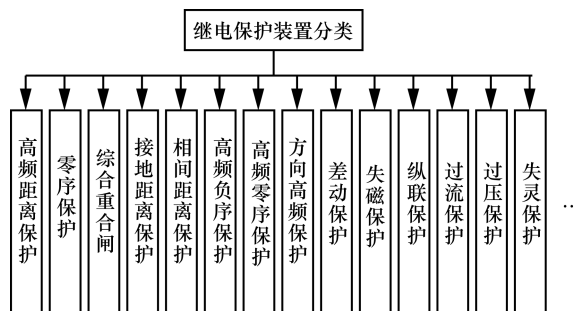


图2 继电保护装置分类

- 可靠性是继电保护最根本的要求。可靠性是指在保护范围内发生故障时,保护装置动作,而在任何不应动作的情况下,保护装置不应误动。出现过载、短路时,如果拒动,过热的电力设备或电缆会导致起火,某些情况下甚至发生爆炸,继电保护的误动作和拒动作都会给电力系统带来严重危害,甚至会导致人身伤害。因此,继电保护装置对于安全性是有明确的需求的,并且比较重要的是,继电保护装置在维护时,其保护功能并不可用,对于可用性和安全性都有影响^[7,8]。
- 选择性就是指当电力系统中的设备或线路发生短路时,其继电保护仅将故障的设备或线路从电力系统中切除,当故障设备或线路的保护或断路器拒动时,应由相邻设备或线路的保护将故障切除。
- 灵敏性是指在设备或线路的被保护范围内发生故障时,保护装置的反应能力。
- 速动性是指继电保护装置应能尽快地切除故障,以减少设备及用户在大电流、低电



压运行的时间,降低设备的损坏程度,提高系统并列运行的稳定性,减轻故障设备和线路的损坏程度,缩小故障波及范围。

故障切除时间包括保护装置和断路器动作时间,一般快速保护的动作为 $40\sim 80\text{ ms}$,最快的可达到 $10\sim 40\text{ ms}$,一般断路器的跳闸时间为 $60\sim 100\text{ ms}$,最快的可达 $20\sim 60\text{ ms}$ 。对 220 kV 及以上电压等级的线路,其近故障点侧与远故障点侧的故障切除时间(即从故障发生开始到断路器断开故障为止)应分别不大于 100 ms 与 $100\sim 150\text{ ms}$ 。

2.3 嵌入式软件主程序流程

继电保护装置软件主程序流程如图3所示。通过保护装置上电或按下复位键后,要进行“初始化(一)”处理,它主要通过对单片机(CPU)及可编程扩展芯片的初始化,使得各个参数保持正常值,保证出口继电器均不动作。若人工选择“运行”工作方式,需要对保护装置进行“初始化(二)”处理,它包括采样定时器的初始化,控制采样间隔时间、对RAM区中所有运行时要使用的软件计数器及各种标志清零等程序。初始化完毕后,接下来进行保护装置自检,如果自检不通过,显示装置故障信息,然后开放串行口中断,把管理系统CPU查询到的自检结果通过串口发送到保护装置监控系统。开放中断也就是开放采样中断,使采样定时器开始计时,并每隔 T_s 时间发出一次采样中断请求信号。自检循环包括查询检测报告、专用及通用自检等内容^[6]。

3 安全检测技术

在对继电保护装置的主程序流程进行分析的基础上,针对继电保护嵌入式软件安全性检测技术进行研究,包括功能检测、性能检测和软件故障注入检测。

3.1 功能检测

功能检测主要测试嵌入式软件是否实现要求

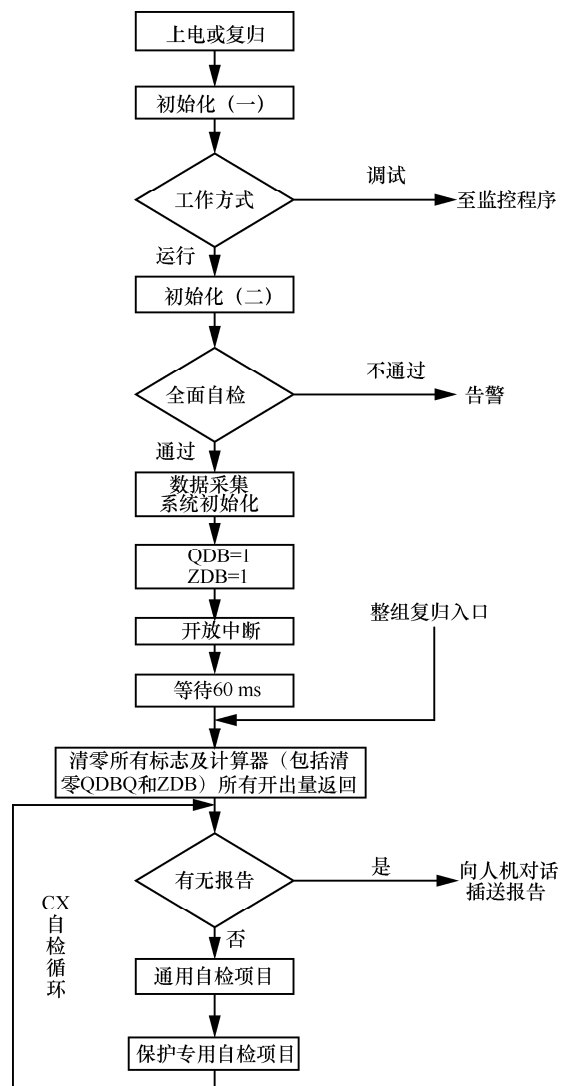


图3 继电保护装置主程序流程

的功能、功能是否完善。不同类型的继电保护嵌入式软件实现的保护功能也不一样。例如,过流保护也称为电流三段式保护,主要实现无时限电流速断保护、带时限电流速断保护和定时限电流速断保护^[9]。

通过对继电保护嵌入式软件程序进行分析,并结合继电保护校验规范、中国南方电网安全稳定控制系统入网管理及试验规定等标准,可以得出继电保护嵌入式软件实现的功能应包括输入量校验功能、动作标志清零功能、自动复归功能、在线自检功能、闭锁及报警功能等^[10-12],具体见表1。

表1 继电保护嵌入式软件功能检测内容

项目	描述
输入量校验功能	软件需用输入量的物理含义校核输入量的正误,防止装置误动
动作标志清零功能	软件在判别和动作过程中一般设有多个动作标志,装置应确保及时全部清零,需要记录的信息应保留在另外的记录区
自动复归功能	当软件处于“死循环”时,软件判断出异常并且发出自动复归信号,使软件处于正常运行状态
故障判断及自动打印功能	识别故障模式、打印故障记录
异常报警功能	软件发生异常时,自动发出异常信号

3.2 性能检测

性能检测主要测试嵌入式软件是否达到要求的性能指标。根据继电保护装置的结构原理,需要设定整定值,将测量值与之进行比较,从而装置做出响应^[13]。因此测量值应达到一定要求,继电保护装置才会做出合理的判断。

软件性能应包括交流电压有效值测量误差、交流电流有效值测量误差、功率测量精度、频率测量精度、相位角测量精度等,具体见表2。

表2 继电保护嵌入式软件性能要求

项目	要求
通信软件原理校验等级校验	具备四级以上
交流电压有效值测量误差	$\leq \pm 1\% (0.2 \sim 1.2 U_N)$
交流电流有效值测量误差	$\leq \pm 1\% (0.2 \sim 1.5 I_N)$
功率测量精度	$\leq \pm 1\%$
故障判断时间	线路故障跳闸判出时间 $\leq$ 收到保护动作信号或开关位置变为信号后 10 ms 线路无故障判出时间 $\leq$ 线路实际跳开后 20 ms
装置动作时间	本地装置整组动作时间 ≤ 30 ms
装置采样频率	不应低于 200 Hz
其他	/

3.3 基于故障注入的安全性检测

继电保护嵌入式软件功能性能测试可以保证系统实现功能的正确性和完整性,而故障注入检测是加速验证系统容错机制的重要方法^[14]。故障注入检测^[15,16]是指在收集测试对象故障模式的基础上,采用一定的策略和合适的故障注入方法将

故障引入测试对象中,观察故障注入后测试对象的行为,为分析测试对象容错性、可靠性和安全性提供所需的评价依据和结果。

在对继电保护装置现有故障模式分析的基础上,介绍其嵌入式软件故障注入检测方法。继电保护嵌入式软件故障检测基本步骤包括继电保护嵌入式软件故障分析(可以采用 FMEA、FTA 故障分析方法)、继电保护装置故障模式库建立、故障注入框架和工具研发及试验。

根据对继电保护装置的组成介绍,通过分析得出继电保护嵌入式软件故障因素主要包括内存使用问题、逻辑遗漏与执行错误、计量相关的错误、软硬件接口的错误、数据操作错误、数据问题等,具体见表3。

根据表3分析得出的继电保护嵌入式软件故障分类和原因,可以建立继电保护装置故障注入模型,并采用形式化方法表达。本文介绍的继电保护嵌入式软件故障注入模型由一个六元组成: $SFI=(FL, FT, FM, FK, FC, FD)$ 。其中,FL 为故障注入的位置,FT 为故障触发方式,FM 为故障注入方式,FK 为故障类型、FC 为故障附加控制参数,FD 为故障附加数据参数。

结合上述建立的故障注入模型,设计了由继电保护嵌入式软件故障注入主控器、故障注入脚本生产者、故障注入脚本执行器、负载生成器、监视器和数据收集器组成的继电保护嵌入式软件故障注入器框架,如图4所示。

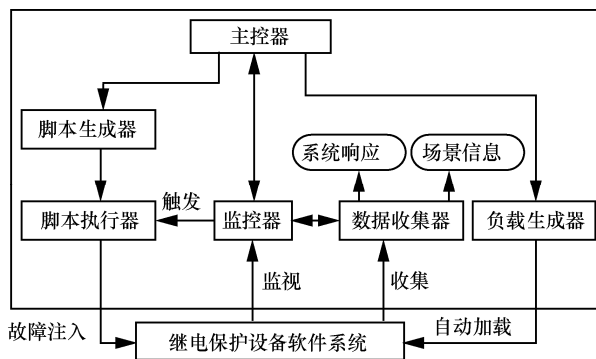


图4 继电保护装置入网软件故障注入器结构



表 3 继电保护嵌入式软件故障分类

软件故障分类		故障原因	
逻辑遗漏与执行错误	不必要的功能	/	
	逻辑重复	/	
	忽略极限条件	/	
	遗忘细节或步骤	/	
	需求的错误表述	/	
	未进行条件测试	/	
	检查错误变量	/	
	循环错误	/	
	未对异常情况进行处理	/	
	功能实现没有覆盖整个问题域	/	
	定义域处理不完全	/	
	功能运行的前提条件不满足	/	
	时钟不一致	/	
	计算相关的错误	等式不完整或不正确	部分计算缺失
			操作数错误
		操作符错误	
		括号错误	
精度损失		混合类型计算	
		舍入或舍去错误	
符号约定错误		/	
除零操作		/	
开方为负数		/	
浮点数做相等比较		/	
软硬件接口错误	中断句柄错误	/	
	I/O 时序错误	/	
	时序错误导致数据丢失	/	
	子函数调用不当	/	
	子函数调用位置错误	/	
	调用不存在的子函数	/	
	数据操作错误	数据存取错误	/
数据初始化错误		标志或索引设置错误	
数据缩放比例或单位不正确		/	
数据的维度不正确		变量类型错误	
		变量的下标错误	
		下标变量使用前未定义	
数据的作用域不正确		/	
局部变量与全局变量重名		/	
变量两次赋值间未使用		/	
数据问题		输出数据错误或丢失	/
	传感器数据错误或丢失	/	
	操作数据错误或丢失	/	
	嵌入表中的数据错误或丢失	/	
	外部数据错误或丢失	/	
	输入数据错误或丢失	/	
	内存使用问题	内存单元耦合错误	/
除法运算溢出		/	
内存分配空间未及时释放		/	

通过上述介绍的软件故障注入设计和实现方法,可以实现继电保护嵌入式软件故障注入检测,对继电保护嵌入式软件进行故障分析,保证继电保护嵌入式软件的可靠性和安全性。

4 结束语

本文通过对继电保护装置的安全需求以及嵌入式软件主程序进行分析,并结合检验规程和行业标准进行研究,从软件的功能、性能和软件故障注入 3 个方面研究了继电保护嵌入式软件检测的内容和方法,为保证继电保护嵌入式软件检测的正确性和全面性提供参考,同时为电力系统的安全稳定运行提供重要的技术支撑。

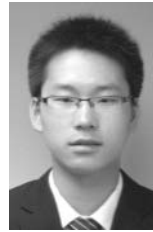
参考文献:

- [1] 马彩霞. 探讨智能电网发展[J]. 信息通信, 2015, 29(6): 286.
MA C X. Exploring the development of smart grid[J]. Information and Communication, 2015, 29(6): 286.
- [2] 郭春梅, 马骏, 郭昊, 等. 软件定义安全模型与架构浅析[J]. 电信科学, 2017, 33(6): 186-192.
GUO C M, MA J, GUO H, et al. Analysis of software defined security model and architecture[J]. Telecommunications Science, 2017, 33(6): 186-192.
- [3] 郭江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 2-7.
WU J X. Meaning and vision of mimic computing and mimic security defense [J]. Telecommunications Science, 2014, 30(7): 2-7.
- [4] 王崇霞, 高美真, 刘倩, 等. 混合云联合身份认证与密钥协商协议设计[J]. 电信科学, 2014, 30(4): 95-99, 108.
WANG C X, GAO M Z, LIU Q, et al. Design of united identity authentication and key agreement protocol for hybrid cloud[J]. Telecommunications Science, 2014, 30(4): 95-99, 108.
- [5] 周怡. 智能网设备的入网测试[J]. 电信网技术, 2004, 3(3): 53-56.
ZHOU Y. Network testing of intelligent network equipment[J]. Telecommunications Network Technology, 2004, 3(3): 53-56.
- [6] 刘帅. 继电保护综合测试系统软件平台开发[D]. 武汉: 华中科技大学, 2013.
LIU S. The development of software platform for relay protection test system[D]. Wuhan: Huazhong University of Science and Technology, 2013.
- [7] MOORE P J, BO Z Q, AGGARWAL R K. Digital distance protection for composite circuit applications[J]. IEEE Proceedings-Generation, Transmission and Distribution, 2005, 152(2):

- 283-290.
- [8] 继电保护技术规程: GB14285-2006[S]. 北京: 中国标准出版社, 2006.
- Technical regulations of relay protection: GB14285-2006[S]. Beijing: China Standard Press, 2006.
- [9] 继电保护和电网安全自动装置检验规程: DL/T 995-2006[S]. 北京: 中国标准出版社, 2006.
- Inspection regulation for relay protection and power grid safety automatic device: DL/T 995-2006[S]. Beijing: China Standard Press, 2006.
- [10] 陈华军, 张宝林, 郭晓斌, 等. 功能安全在电力行业中的应用研究[J]. 网络安全技术与应用, 2016, 16(1): 44-45.
- CHEN H J, ZHANG B L, GUO X B, et al. Research on the application of functional security in electric power industry[J]. Network Security Technology & Application, 2016, 16(1): 44-45.
- [11] 陈华军, 张宝林, 黄晓昆, 等. 功能安全在电力行业的应用预案研究[J]. 电子产品可靠性与环境试验, 2016, 37(2): 52-57.
- CHEN H J, ZHANG B L, HUANG X K, et al. Application plan of functional safety in power industry[J]. Electronic Product Reliability and Environmental Testing, 2016, 37(2): 52-57.
- [12] 张宝林, 王剑亮, 陈华军, 等. 基于模糊层次法的继电保护装置安全性评估模型[J]. 现代计算机, 2015(11): 24-28.
- ZHANG B L, WANG J L, CHEN H J, et al. The safety assessment model of relay protection device based on fuzzy analytic hierarchy process[J]. Modern Computer, 2015, 32(11): 24-28.
- [13] 高海龙. 电力系统继电保护安全运行措施探讨[J]. 机电信息, 2011, 12(18): 29, 31.
- GAO H L. Discussion on safe operation of relay protection in power system[J]. Mechanical and Electrical Information, 2011, 12(18): 29, 31.
- [14] 孙峻朝, 王建莹, 杨孝宗. 故障注入方法与工具的研究现状[J]. 宇航学报, 2001, 22(1): 99-103.
- SUN J C, WANG J Y, YANG X Z. The present situation for research of fault injection methodology and tools[J]. Journal of Astronautics, 2001, 22(1): 99-103.
- [14] 饶翔, 王怀民, 陈振邦, 等. 云计算系统中基于伴随状态追踪的故障检测机制[J]. 计算机学报, 2012, 35(5): 856-870.
- RAO X, WANG H M, CHEN Z B, et al. Detecting faults by tracing companion states in cloud computing systems[J]. Chinese Journal of Computers, 2012, 35(5): 856-870.

- [15] 徐光侠. 分布式实时系统的软件故障注入及可靠性评测方法研究[D]. 重庆: 重庆大学, 2011.
- XU G X. Research of software-implemented fault injection and reliability evaluation methods in distributed real-time system[D]. Chongqing: Chongqing University, 2011.

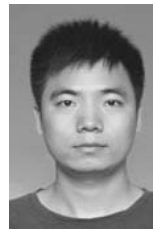
[作者简介]



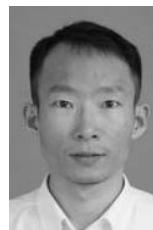
丁伟(1991-), 男, 南方电网科学研究院有限责任公司助理研究员, 主要研究方向为电力信息与通信、信息安全。



蒙家晓(1982-), 男, 南方电网科学研究院有限责任公司工程师, 主要研究方向为等级保护测评、信息安全、渗透测试。



戴涛(1990-), 男, 南方电网科学研究院有限责任公司助理研究员, 主要研究方向为信息安全、恶意代码分析。



陈华军(1980-), 男, 南方电网科学研究院有限责任公司高级工程师, 主要研究方向为信息安全。