工程与管理科学
Engineering and Management Science
第 7 卷◆第 12 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

适用于二次设备通信安全测试场景的自动测试系统开发与应用

程晓　张玮　董彦　胡良生
南京国电南自软件工程有限公司　江苏南京　211100

DOI:10.12238/ems.v7i12.16450

[摘　要] 在现代电力系统中，保护装置、测控装置等二次设备担负着对一次设备进行监测、控制以及保护等重要任务，也为电网安全稳定运行提供了重要保障。这些二次设备相互之间以及和监控系统之间需要开展大量的数据通信工作，以此实现信息的交互与共享，不过，随着信息技术不断发展以及网络攻击手段日益多样化，二次设备的通信安全正面临十分严峻的挑战，一旦二次设备的通信遭遇攻击或者受到干扰，就会造成保护误动作、控制指令错误执行等严重后果，进而危及电网的安全稳定运行。本研究旨在开发一套适用于二次设备通信安全测试场景的自动测试系统，以解决传统人工测试的弊端。通过分析人工手动测试存在的问题与不足、现有的测试工具以及固有的测试用例，该系统能够实现一键执行测试任务，测试任务执行过程中，实时展示测试进度、测试结果、执行失败报错等信息，任务执行完毕生成报告等功能。实验结果显示，该自动测试系统在测试效率、测试规范化及用户反馈方面表现优于传统人工测试方式。

[关键词] 二次设备；通信安全；自动测试系统；应用

电力系统中，二次设备主要用来对一次设备开展监测、控制、保护和调节工作，其通信网络承担着传输各类关键数据以及指令的重要任务，通信安全是保障二次设备正常运行与电力系统稳定的基础条件，一旦通信遭受干扰或者攻击就可能造成保护误动、拒动甚至引发大面积停电事故，所以对二次设备通信安全进行全面且高效的测试十分关键，目前二次设备通信安全测试如网络风暴、协议攻击类等，主要依靠人工手动测试这种方式，测试人员手动执行测试用例，通过人为逻辑判断校验当前步骤是否正确实现，该方式不仅测试周期长、效率低下而且易受测试人员经验和技能水平的限制。为了解决这些问题，开发一套适用于二次设备通信安全测试场景的自动测试系统具有重要的现实意义。

一、二次设备通信安全的重要性

从系统稳定运行这个角度来看，二次设备借助通信达成数据交互与指令传输，要是通信存在不安全的情况，就可能致使数据出现错误或者丢失，进而会让保护装置出现误动作或者拒动作的问题，就像在电网发生故障的时候，保护装置没办法准确接收故障相关信息，不能及时对故障线路进行切断操作，如此便会扩大停电范围，严重威胁到电力系统的稳定运行。从经济层面来考量，通信安全问题所引发的系统故障会造成设备损坏以及生产停滞的后果，修复故障设备、恢复生产等各个环节都需要耗费大量的人力、物力以及财力，给企业带来非常巨大的经济损失。在信息安全方面而言，二次设备存储着数量众多的敏感信息，一旦通信遭受攻击，这些信息就有可能被窃取或者篡改，还可能被不法分子加以利用，从而引发一系列的安全风险，甚至会对国家安全造成影响。因此，通过保护二次设备通信安全能够增强用户对系统可靠性的信心，推动相关产业实现健康发展[1]。

二、自动测试系统开发

（一）系统架构设计

本系统架构主要分三层：数据采集层、测试控制层和结果展示层（如图 1）。数据采集层负责收集二次设备的物理信息，需通过网络接口接入；测试控制层属于本系统的核心部分，依据预设的测试策略和流程，对采集到的数据开展自动化测试工作；结果展示层在测试过程中，以直观的界面来呈现测试进度以及简要测试结果，测试执行完毕后，将自动生成测试报告，方便用户快速了解被测设备的通信安全状况。

本系统采用模块化设计，将系统分解为独立模块，可进行功能复用、个性化定制，便于后续进行功能的扩展和维护，增强系统的灵活性，例如添加新的测试用例或者适配不同型号的被测设备[2]。

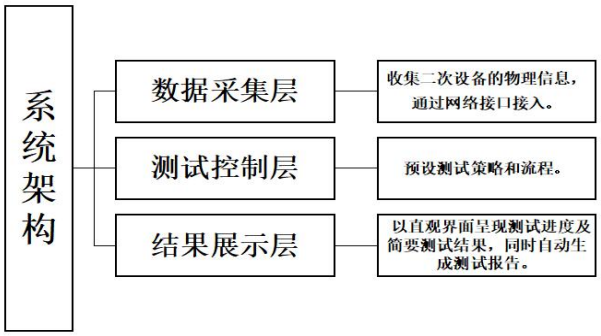

图 1　二次设备通信安全自动测试系统架构设计图

（二）测试用例生成

本系统的固定测试用例，是基于对二次设备抗拒绝服务及网络协议健壮性要求的深入分析而生成的。抗拒绝服务，是被测设备对于拒绝服务攻击的抵御能力。拒绝服务攻击，是攻击者想办法让攻击目标无法提供原有服务，包括消耗网络带宽、内存、占满 CPU，以至服务暂停甚至目标死机重启等。拒绝服务攻击一直得不到合理解决的原因在于网络协议本身的缺陷，常见的拒绝服务攻击有：SYN Flood 攻击、ICMP Flood 攻击、Ping of death 等。网络协议健壮性，是被测设备对于异常数据包的处理能力。我们对以太网、ARP、TCP、UDP、MMS 等协议进行分析，构造风暴报文以及非法报文，模拟攻击者攻击系统的方式，测试被测设备能否及时发现网络攻击并做出正确响应，保障系统正常运行。

生成的测试用例具备可重复性和可维护性，方便后续测试执行与更改，同时为每个测试用例设定明确的预期结果，

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

用以准确判断测试是否通过[3]。

（三）测试执行与结果分析

在测试执行阶段，测试人员可以自由选择需要执行的测试用例，选定以后可以一键执行测试，测试执行过程中，系统界面会将测试进度、测试结果、执行失败报错等进行实时展示。

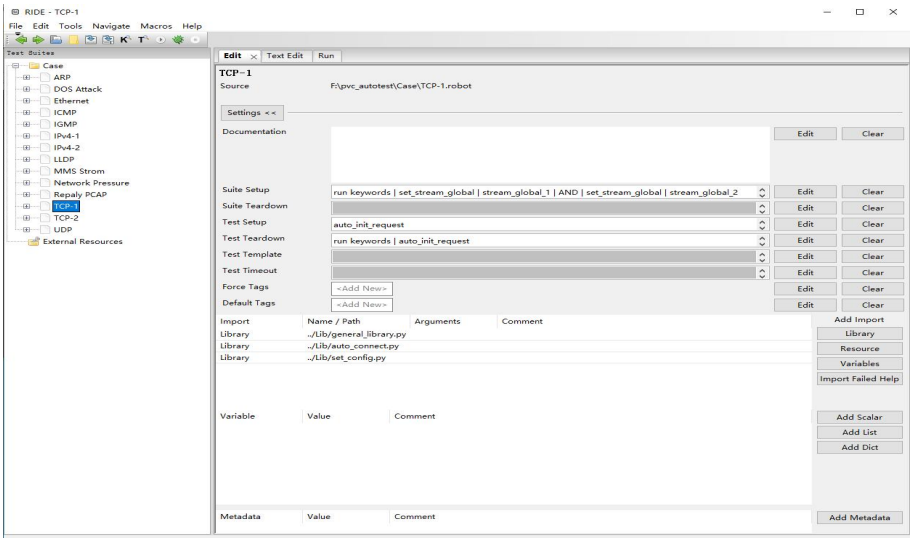

图 2　二次设备通信安全自动测试系统用例执行界面

每个测试步骤执行完毕后系统会自动与预期结果比对，以此判断测试是否能够通过，若出现测试不通过的情况，系统会记录相关信息，例如：错误代码和异常报错等，便于测试人员后续进行问题排查。

测试过程中需保证测试环境处于稳定状态，防止外界因素对测试结果造成干扰。

选定测试用例全部执行完毕后，系统会自动生成一份报告文件、一份测试过程记录文件，为被测二次设备的安全评估和改进提供有利依据[4]。

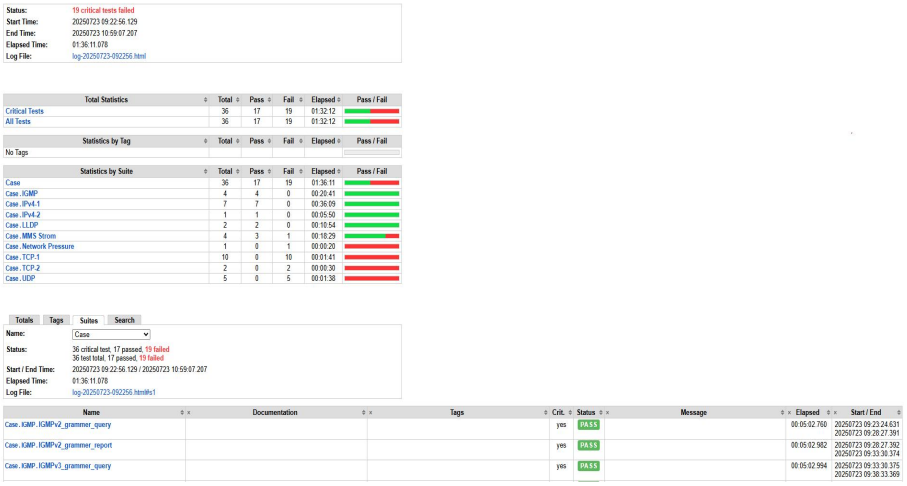

图 3　二次设备通信安全自动测试系统测试报告界面

Case Log

Generated
20250723 10:59:07 UTC+08:00
29 days 8 hours ago

Test Statistics

Total Statistics	Total	Pass	Fail	Elapsed	Pass / Fail
Critical Tests	36	17	19	01:32:12	
All Tests	36	17	19	01:32:12	

Statistics by Tag	Total	Pass	Fail	Elapsed	Pass / Fail
No Tags					

Statistics by Suite	Total	Pass	Fail	Elapsed	Pass / Fail
Case	36	17	19	01:36:11	
Case.IGMP	4	4	0	00:20:41	
Case.IPv4-1	7	7	0	00:36:09	
Case.IPv4-2	1	1	0	00:05:50	
Case.LLDP	2	2	0	00:10:54	
Case.MMS Strom	4	3	1	00:18:29	
Case.Network Pressure	1	0	1	00:00:20	
Case.TCP-1	10	0	10	00:01:41	
Case.TCP-2	2	0	2	00:00:30	
Case.UDP	5	0	5	00:01:38	

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

图 4　二次设备通信安全自动测试系统日志界面

三、自动测试系统关键技术

（一）网络攻击报文模拟技术

为了充分应对基于网络协议的恶意攻击，我们在深度解析这些协议后对设备进行模拟攻击测试，提前暴露问题并整改，保障设备在遭受各种异常攻击时的稳定性和可靠性。例如 TCP 协议，通信双方在数据传输之前首先要建立可靠的连接，也就是我们常说的三次握手，攻击者可通过监听、预测等手段，在通信双方的通信过程中插入或劫持数据包，从而控制通信会话。本系统基于 Python 开发环境，使用 Scapy 库发送 SYN、ACK 模拟报文，监听被测设备响应的 SYN-ACK 报文，在完成通信双方三次握手后，构造攻击报文（协议字段值遍历）进行攻击测试，具有发送、捕获、匹配请求和响应这些报文以及更多的功能。例如 MMS 协议，首先我们使用面向连接套接字 socket 函数模拟所需报文，其次我们使用线程池的方法来模拟同时使用不同 IP 地址的 MMS 客户端连接被测装置。

（二）自动化测试脚本技术

传统的手动测试方式，是通过人为操控测试仪器以及判断校验当前步骤是否正确实现，但是这种方式效率较低，耗时耗力，无法在短时间内完成大量测试用例的执行。本系统基于开源测试框架 RobotFramework，结合网络测试仪 API 接口进行二次开发，模拟人工操作测试仪器、执行测试任务、检查预期行为和结果、同步生成测试报告，形成适用于本单位产品的可视化一体测试框架。在自动测试系统中，测试人员可以根据需要自由选择测试用例，系统会依据预先设定好的测试脚本和流程，自动执行一系列的测试操作。

本系统利用 python 开发语言编写相应的测试脚本，对测试用例中的通信场景进行模拟，如正常通信、异常报文发送以及网络攻击等情况。测试过程中，脚本能够按照指定的顺序以及时间间隔来发送测试数据，同时还能实时监测二次设备的响应状况。当测试用例出现变化的时候，只需要修改脚本里面的参数或者逻辑，就能够快速适应新的测试需求。自动化测试脚本技术减少了人工干预的情况，降低人为错误出现的可能性，让测试过程变得更加标准化和规范化[5]。

（三）设备信息采集技术

本系统通过因特网包探索器 PING 被测设备后查询本地 ARP 缓存表来实现自动根据 IP 地址获取 MAC 地址的功能，测试人员只需在自动测试系统的配置文档中填写当前被测设备的 IP 地址。

四、自动测试系统应用

（一）两网检测

设备通过国/南网的检测，对于企业来说有重要意义，设备的安全性和可靠性直接关系到企业的运营效率和用户的使用体验。二次设备通信安全自动测试系统从无到有，覆盖用例的测试时间缩短至 1 天，时间成本节省 50%，人力成本节省 50%，测试便捷性大大提高。同时可根据国/南网检测标准，灵活调整测试用例，以快速满足针对两网检测的测试要求，在紧凑的时间内完成检测前的准备工作，尽早帮助送检人员发现问题解决问题，以充足的姿态应对两网的检测工作。

（二）新产品研发测试

在新产品研发的整个过程当中，二次设备通信安全自动测试系统能够对新产品通信安全性能开展全面且深入的测试工作，以此确保其满足相关标准以及实际应用方面的需求。对于通信协议的兼容性测试而言，系统会涵盖多种常见的协议来确保新产品能与不同类型的设备实现无缝通信，该系统能够有效检测新产品存在的安全漏洞，它会采用多种攻击模拟手段像拒绝服务攻击、数据篡改攻击等评估设备的抗攻击能力，一旦发现安全隐患，研发人员就可以及时进行改进和优化进而提高产品的安全性和可靠性。通过使用适用于二次设备通信安全测试场景的自动测试系统，能够大大缩短新产品的研发周期、降低研发成本并且提高产品的市场竞争力[7]。

五、结论

适用于二次设备通信安全测试场景的自动测试系统开发与应用是解决传统测试方法不足、提高二次设备通信安全测试效率及水平的有效途径。首先，我们通过对测试用例未覆盖的原因进行分析，探索新的测试方法，提高了安全测试的覆盖度；其次，在覆盖度得到提升的情况下，我们探索自动执行测试方法，旨在降低项目的时间、人力成本，提高测试便捷性。未来，随着技术的不断优化和完善，本系统将在保障电力系统通信安全方面发挥更加关键的作用，同时也将为通信安全测试领域的发展注入新的活力。

[参考文献]

[1]张灏.基于无线通信的电力系统二次设备运行状态自动监测方法[J].自动化应用，2025，66（02）：188-189+193.

[2]张章，王洪新，张旺旺，等.新形势下智能变电站二次设备的调试与检修分析[J].电工技术，2024，(S1)：73-75.

[3]陈福，路美杰.二次设备网络通信检测及故障诊断分析技术研究[J].电工技术，2024，(S1)：263-265.

[4]李楠，吕佩吾，葛雅川，等.智能变电站二次设备安全防护状态监控研究[J].电工技术，2022，(12)：76-78.

[5]雷宇，梁志豪.二次设备网络通信检测及故障诊断分析技术研究[J].网络安全技术与应用，2022，(04)：8-9.

[6]李玉敦，耿玉杰，管荑，等.基于边缘计算的二次设备动态诊断技术的研究与应用[J].电子器件，2021，44（05）：1176-1182.

[7]王堃，张立中，冯国礼，等.智能电网二次设备状态监测内容分析[J].中国设备工程，2021，(10)：6-8.

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.