Design and Implementation of Distribution Automation Terminal Test Software Based on IEC 104 Protocol

Wei Si Mingyang Liu* Chenglin Li Shixiong Zhai Lichao Han

State Grid Tianjin Electric Power Company Binhai Power Supply Branch, Tianjin, 300450, China

Abstract

With the rapid development and wide application of smart grid, distribution automation terminal as an important part of smart grid, its stability and efficiency for the reliable operation of the entire power system is crucial. This paper designs the test software of distribution automation terminal based on IEC 104 protocol. First, it introduces the overall architecture and design ideas of the software, including module division and interface design, and describes the functions and implementation methods of key modules. Finally, it introduces the environment and tools of software development, as well as the organizational structure of the code, and describes the implementation process of key modules in detail. Including code implementation, testing methods. The debugging software solves the problem that users use multiple software to debug the equipment of multiple manufacturers, and improves the debugging efficiency.

Keywords

distribution automation terminal; IEC104; agreement; software testing

基于 IEC 104 规约的配电自动化终端测试软件设计与实现

司威 刘明阳* 李承霖 翟世雄 韩立超

国网天津市电力公司滨海供电分公司，中国 · 天津 300450

摘 要

随着智能电网的快速发展和广泛应用，配电自动化终端作为智能电网的重要组成部分，其稳定性和高效性对于整个电力系统的可靠运行至关重要。论文设计了基于IEC 104规约的配电自动化终端测试软件，首先介绍软件的整体架构和设计思路，包括模块划分、接口设计，并描述关键模块的功能和实现方法，最后介绍软件开发的环境和工具，以及代码的组织结构，并详细描述关键模块的实现过程，包括代码实现、测试方法。调试软件解决了用户调试多个厂家设备使用多套软件的问题，提高了调试效率。

关键词

配电自动化终端；IEC104；协议；软件测试

1 项目背景

1.1 配电自动化终端介绍

在传统的电力系统中，配电网主要负责电力的分配与输送，随着科技的不断进步以及能源需求的增长，配电网面临着前所未有的挑战。为应对这些挑战，智能电网应运而生且已成为现代电力系统的重要发展方向。在此背景下，配电自动化终端作为智能电网架构中的重要一环，扮演着关键角色。配电自动化终端是一种集成多种功能于一身的智能设备，能够实现数据采集、处理、传输以及控制等功能。其主要作用是通过集成传感器、处理器、通信模块等硬件组件，对配电网进行实时监测和分析，从而提供准确、及时的信息支持，促进电网的高效、安全运行 [1]。

1.2 配电自动化终端软件介绍

为了确保终端能够满足电力系统的需求，对其进行严格且全面的测试变得至关重要。现有的配电自动化终端测试方法往往侧重于硬件或软件层面的个别功能测试，而忽略了系统层面的综合性能评估。因此，开发一种能够集成多种测试场景、全面模拟实际通信环境的测试软件，成为当前行业内的迫切需求。基于 IEC 104 规约的配电自动化终端测试软件设计与实现，旨在提供一个全面、高效且可扩展的测试平台，支持终端的通信功能、数据处理能力和系统集成度量，还能评估其对复杂网络环境的适应性，为设备制造商和运维人员提供技术支持，从而提升整体系统的安全性和稳定性 [2]。

【作者简介】司威（1991–），男，中国河北张家口人，硕士，工程师，从事智能配电网及储能研究。

【通讯作者】刘明阳（1992–），男，中国辽宁朝阳人，硕士，工程师，从事配电自动化研究。

2 IEC104 规约

2.1 IEC104 规约介绍

IEC 104 规约全称为“Substation Automation Systems ——Protocol for Communication with Stand-alone Control and Protection Devices”，简称“Ethernet/IP”。IEC104 规约协议是一种国际规范的标准，用来定义电力远动方面，该规约基于开放的工业以太网，采用 TCP/IP 协议族实现通信，支持多种应用层协议，如 MODBUS、DNP3、CIP 等，使得其具备良好的通用性和灵活性。协议一般规则：平衡方式传输——也就是说每一个过程的会话，没有规定谁从头发起，双方均可；一般情况下配电主站作为 TCP 的客户端，配电自动化终端作为 TCP 的服务器；TCP 的默认端口号是 2404[3]。

2.2 IEC 104 的设计原理及特点

IEC 104 规约采用客户—服务器架构，具备如下特点：可靠性与容错性：IEC 104 采用确认机制、超时重传等手段保证数据传输的可靠性；可扩展性：支持多种应用层协议，适应不同场景下的需求；实时性：通过合理的帧结构和优化的传输算法，保证数据的及时传递；安全性：采用加密、认证等技术保护数据传输过程中的信息安全；兼容性：与多种工业标准和协议兼容，易于集成到现有系统中。

3 软件测试需求与挑战：

配电自动化终端的软件测试需求主要围绕以下几个方面展开，以确保终端系统在各种环境下稳定、安全且高效地运行：

功能测试：①基本功能验证：确认软件能够正常执行其设计任务，如数据采集、设备控制、通信、故障检测等。②边界条件测试：模拟终端在不同负荷、环境条件下（如高温、低温、高海拔等）的性能，确保软件在极限情况下仍能保持稳定运行。

异常情况测试：模拟系统可能出现的故障或错误输入，检查软件的容错能力和恢复机制。

性能测试：负载测试：评估软件在高并发请求、大容量数据处理等情况下的性能表现，确保系统的响应时间和处理效率满足需求。

压力测试：测试软件在持续高负载下的稳定性，评估系统在长时间运行下的性能变化。

稳定测试 ：通过长时间运行和反复操作，验证软件的长期稳定性和可靠性。

安全测试：①安全性评估：包括权限管理、数据加密、防火墙配置等，确保终端系统的数据传输和存储安全。②渗透测试：模拟、查找并修复可能的漏洞和安全风险。

兼容测试：①硬件兼容性：验证软件与不同型号的硬件设备（如传感器、执行器等）之间的兼容性。②系统兼容性：确保软件能够与多种操作系统和网络协议无缝对接。

用户界面与用户体验测试：①界面易用性：测试用户界面的直观性、友好性，确保非技术用户也能轻松操作。②交互流畅性：评估软件在用户操作过程中的响应速度和流畅度。

故障诊断与恢复测试：①故障注入：人为模拟各种故障情况，测试软件的故障诊断能力和自恢复机制。②维护便利性：测试软件的可维护性，包括日志记录、错误报告、远程更新等功能。

基于上述需求软件测试面临许多挑战，主要挑战包括：确保通信的可靠性和稳定性；模拟复杂网络环境，包括丢包、延迟和重传等情况；验证终端设备的性能，如响应时间、数据吞吐量等；鉴定安全性和隐私性问题，包括认证、加密和完整性保护 [4]。

4 软件设计

基于上述需求，测试软件的系统架构应包括厂家选择模块、设备连接模块、报文通讯模块、报文接收模块、报文发送模块和人机交互界面，各模块实现方法如下：

厂家选择模块：用代码实现了一个对话框，用于让用户选择设备厂家。对话框中包含一个标签、一个下拉组合框和一个确定按钮。标签提示用户“请选择设备厂家，下拉组合框提供了厂家名称选项供用户选择。确定按钮用于提交用户的选择。当用户点击确定按钮后，对话框将关闭，并根据用户选择的设备厂家设置相应的配置文件路径。如果用户选择了对应的厂家名称，则 display 与 protocol 变量设置为厂家对应的 xml 文件路径。如果用户未选择设备厂家直接关闭对话框，程序将返回 1，表示程序退出。

设备连接模块：连接过程基于 QT 平台实现，采用 IEC104 协议与从站进行通信。在连接处理函数 IEC104 Master::cs104_connectionHandler 中，根据不同的连接事件，进行相应的处理。当连接事件为 CS104_CONNECTION_OPENED 时，表示设备与 IEC104 从站成功建立连接。此时，设备将初始化相关参数，并将连接状态设置为 IEC104_CONNECTED。同时，设备会发出一个信号，通知其他模块当前连接状态。若为首次连接，则记录连接成功的日志信息；若为重连，则记录重连成功的日志信息。当连接事件为 CS104_CONNECTION_CLOSED 时，表示设备与 IEC104 从站的连接已断开。此时，设备将连接状态设置为 IEC104_IDLE，并发出一个信号，通知其他模块当前连接状态。同时，设备将活动标志设置为 false，并记录连接断开的日志信息。

报文通讯模块：本系统的通讯模块通过集成的库函数实现与 IEC104 从设备的高效通信。在发送请求和接收响应的过程中，模块采用了 CS101_Master_sendASDU 和 CS104_Connection_sendASDU 函数来发送应用层消息（ASDU）。这些函数支持发送系统命令或过程命令，并有助于构建符合 IEC 标准的数据单元。为了处理接收到的 ASDU，系统实现了一个回调函数 asdu Received Handler，该函数会在接收到

ASDU 时被触发。在回调函数中，系统会根据 ASDU 的类型进行相应的处理，此外，通讯模块还通过 CS101_Master_setASDUReceivedHandler 函数将 asduReceivedHandler 回调函数安装到系统中，确保所有接收到的 ASDU 都能得到及时处理。

报文发送模块：构造对时、总召、遥调、遥测的 IEC104 报文并控制报文的发送过程。

报文接收模块：通过通信模块接收终端上送的 IEC104 报文，并将 IEC104 报文送至报文解析函数进行报文解析，实现数据接收并更新界面。

报文解析模块：报文解析模块的核心由 respondSetMassPointCmd 函数构成，该函数针对自定义批量装载命令进行响应处理。函数首先确定 ASDU（应用服务数据单元）的有效载荷大小，并根据特定的页面类型提取报文中的数据。数据提取过程中，函数将字节数据按照特定的顺序组合成完整的值数组，以便后续处理。在解析过程中，模块会根据报文中的地址信息来定位对应的 C_SE_NB 对象，该对象代表了一个具体的监视或控制点。一旦定位到对象，模块将调用 updateData 方法来更新数据。updateData 方法根据不同的数据类型对提取的数据进行格式化处理，并将其转换为用户友好的显示格式。在 updateData 方法中，数据类型的识别是通过一个 switch 语句实现的，每种数据类型都有相应的处理逻辑。

人机交互界面：提供人机交互界面，对各个模块功能的集中展示，测试人员能够通过交互界面，读取收发的报文信息同时可以通过写定值功能实现参数的修改。最终，更新后的数据显示在界面对应的元素上，实现了数据的实时反馈和展示。

5 软件实现

104 规约测试软件主要是链接底层的设备，电闸之类的底层设备信号被接入继电保护装置，然后装置转换成信号，显示在继电保护装置中，并通过 104 规约测试软件传输到后台，把底层装置的数据读到软件里面，软件可以读取报文并且解析出来，而且还能通过软件去对底层装置进行遥控。

①将设备与电脑通过网线连接后，设置电脑 ip，确保电脑 ip 与装置 ip 在同一网段内，以保证正常的通信。

②打开软件，选择对应的设备厂家，如图 1 所示，等待驱动程序加载后，自动进入下一个界面

③进入软件后，点击左上角端口设置，配置软件对应装置的 ip 地址，如图 2 所示。

④点击“连接设备”，连接状态信息可从左下方“告警信息“一栏出得知，如连接成功则”状态“一栏会显示绿色圆形，连接失败则显示红色圆形，如图 3所示。

⑤对于遥测、遥信、遥调中对应的数据值都是默认的，连接成功后如需查看某一项的值比如“终端硬件版本”，可以点击对应项，再点击上方“定值”框内的“读单定值”，即可在“值”中显示对应数据。如果需查看当前页面内表项的所有值，可点击“读多定值”，下方会产生新的警报信息，对应“状态”一栏显示绿色圆形则代表读取成功，页面内各表项的值都会依次显示出来。

⑥遥调操作需要选中对应表项的值，比如“L01 相 CT 一次额定”，点击对应“值”，并输入要修改的值，输入完成后点击“写单定值”，即可在下方状态栏里查看写入状态，也可再次点击”读单定值“查看是否写入成功。

⑦电脑和设备连接过程中产生的通讯报文都可在界面下方“通讯报文”一栏中查看，便于使用过程的调试和维护。

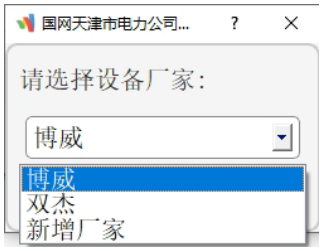

图 1 厂家选择界面

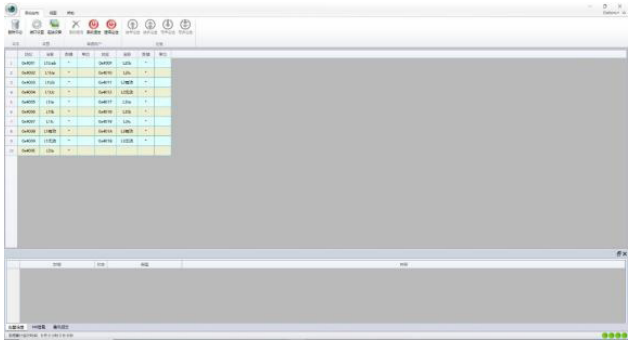

图 2 软件界面

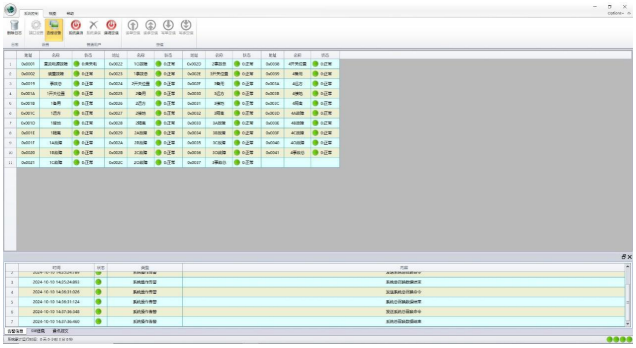

图 3 正常连接设备后的界面

6 结论与展望

基于 IEC 104 规约的配电自动化终端测试软件的设计与实现是一个复杂而精细的过程，涉及到通信协议的深入理解、软件架构的合理规划以及测试策略的有效设计。通过构建这样的测试工具，可以有效地验证配电自动化终端在实际

网络环境中的功能、性能和安全性，从而为电力系统的可靠运行提供坚实的技术保障。论文设计的基于 IEC 104 规约的配电自动化终端测试软件，能够接收终端设备上送的遥测、遥信报文，并同时记录调试日志。并且适配多个厂家，实现了使用同一个软件，调试不同厂家的终端设备。对于电力系统集成商、运维单位等用户来说，不需要为每个厂家的设备都购买专用的调试工具，只需要一个适配多个厂家的调试系统，就可以满足对不同设备的调试需求，从而降低工具采购成本。在实际应用中，当出现通信故障或设备异常时，适配多个厂家的调试系统可以快速对不同厂家的设备进行诊断和分析，帮助调试人员迅速定位问题所在，缩短故障排除时间。未来的研究方向可能包括集成更多高级测试技术，如自动故障注入、模糊测试和渗透测试，以及进一步提升测试软件的智能化水平，以适应不断发展的电力系统需求。

参考文献

[1] 钟加勇.配电物联网智能融合终端云边协同模型及应用研究[D].重庆:重庆大学,2021.

[2] 方洁.配电终端软件自动化测试系统的设计与实现[D].武汉:武汉理工大学,2010.

[3] 王莉.基IEC104规约的配电终端测试软件设计[J].科技资讯,2022,20(14):34-36.

[4] 王大法.基于软件测试过程模型的测试管理系统的研究与实现[D].青岛:青岛科技大学,2010.