

基于扩展 103 规约的保护装置通信与调试系统设计

张磊, 陈宏君, 吴相楠, 冯亚东

(南京南瑞继保电气有限公司, 江苏 南京 211102)

摘要: 针对日益复杂的保护装置和受限的装置人机接口, 提出并实现了一种基于扩展 IEC60870-5-103 规约的保护装置通信与调试系统。该系统以 IEC60870-5-103 规约为基础, 并对其进行扩展, 除了具有 IEC60870-5-103 规约的全部功能外, 还支持装置菜单读取、权限控制、装置命令执行等功能, 有效地弥补了装置面板人机交互功能差、IEC60870-5-103 规约无菜单结构、无权限控制和无法支持装置全部接口功能的局限性。经过在保护装置中的实际工程应用, 表明本系统通信稳定可靠, 调试功能全面丰富, 支持了装置所有的接口功能, 提高了保护装置的开发和调试效率。

关键词: IEC60870-5-103 规约; 保护装置; 通信与调试; 人机接口; 嵌入式系统

Design of communication and debugging system for protection device based on extended 103 protocol

ZHANG Lei, CHEN Hongjun, WU Xiangnan, FENG Yadong

(NR Electric Co., Ltd., Nanjing 211102, China)

Abstract: To settle the ever profound protection device and its limited human-machine interface, this paper promotes and implements a communication and debugging system extended from the IEC60870-5-103 protocol. The system extends IEC60870-5-103 protocol by supporting device menu reading, access control, device command execution and other functions besides its pre-existing functionality, which makes up the protocol's limitations such as weaker human-machine interface of device panel, lacking of menu structure and access control, and incomplete supporting of all interface functions, etc. Engineering application in protection devices demonstrates the system has high communication stability and comprehensive debugging functions, as well as supports all interface functions of the device, thus effectively increases the development and debugging efficiency for protection device.

Key words: IEC60870-5-103 protocol; protection device; communication and debugging; human-machine interface; embedded systems

中图分类号: TM73

文章编号: 1674-3415(2015)21-0126-05

0 引言

随着嵌入式技术的发展, 保护装置的功能日益强大, 其通信、调试与维护也越发复杂。一般的保护装置都采用由国际电工委员会(IEC)于 1997 年定义的 IEC60870-5-103《继电保护设备信息接口配套标准》(下称 103 规约)来完成与上位机调试系统的通信^[1]。利用 103 规约, 上位机可以获得保护装置的状态量、定值等信息, 相关技术已经非常成熟^[2]。但 103 规约存在着无法获得装置菜单结构, 无法读取装置报告, 无法执行命令, 无权限控制等问题。

许多学者针对 103 规约存在的问题做了大量研究。文献[3]基于 103 规约设计并实现了一种嵌入式

通信管理系统, 该系统实现了一个标准 103 规约。文献[4]提出了一种基于 103 规约的冗余网络通信设计方案, 提高了系统的稳定性。文献[5]提出了一种利用统一编码表实现 103 规约通信报文便利统一传送的方法, 解决了各厂家的 FUN 与 INF 不一致问题。文献[6-7]分别指出电力系统信息安全关系着电力系统的可靠运行。

针对目前存在的问题, 结合 103 规约的成熟性, 本文提出了一种基于扩展 103 规约的保护装置通信与调试系统协议。该协议以 103 规约为基础, 除实现通用数据分组相关的读写、浏览功能外, 通过对 103 规约进行扩充, 还具有以下优点。

(1) 可以上送装置液晶菜单, 做到液晶内容与上

位机显示内容一致。

(2) 拥有权限控制功能, 可以有效防止非法操作。

(3) 支持装置信号灯状态读取, 装置报告读取, 执行出口传动等装置命令。

1 规约设计

1.1 基本格式

规约基本单元为 APDU(应用规约数据单元), 每个 APDU 含有 1 个或多个 APCI(应用规约控制信息), 每个 APCI 后面跟随 0 个或 1 个 ASDU(应用服务数据单元)。其中, APCI 包含 ASDU 校验和, ASDU 序号等必要信息, ASDU 为标准 103 规约应用服务数据单元, 如图 1 所示。

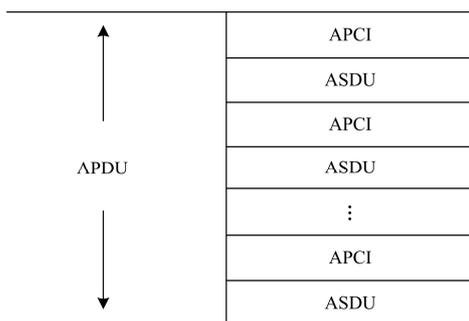


图 1 基本单元结构图

Fig. 1 Diagram of basic unit

1.2 菜单结构

主菜单为树形结构, 其特点为: 有且只有一个根菜单, 除叶菜单外, 每个菜单都有至少一个子菜单, 叶菜单用于实现某种功能, 如显示状态量、显示定值、执行出口传动命令等。

每个菜单分配一个通用分类条目, 根菜单的公共地址和 GIN 为固定值。每个菜单对应的条目中, 条目描述(KOD = 10)表示该菜单的描述, 数据类型为字符串; 相关联条目(KOD = 23)表示该菜单的所有子菜单, 数据类型为 32 位无符号整数(格式 {uint8_t entry_id, uint8_t group_id, uint8_t addr, uint8_t reserve}), 数据数量可以为一个或多个; 实际值(KOD = 1)表示该菜单实现的功能、读写或执行该功能需要的权限条目以及该功能实际数据条目。显而易见, 叶菜单对应的条目没有相关联条目数据, 而其他菜单对应的条目没有实际值数据。菜单数据结构如图 2 所示。

菜单实际值的解析分为三个步骤^[8]: 1) 确定菜单种类; 2) 按菜单种类执行实际值解析操作; 3) 解析结果类型存储供其他系统使用。

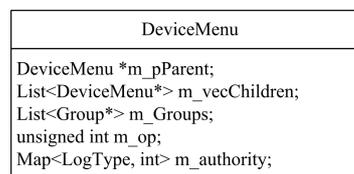


图 2 菜单数据结构图

Fig. 2 Diagram of data structure for menu

1.3 权限控制

针对 103 规约无权限控制的问题, 本文规约为每个菜单增加权限校验机制。权限分为读取, 写入与执行三种, 每种权限对应一个条目。每个菜单的权限信息通过该菜单的对应条目的实际值(KOD=1)上送给上位机客户端。若未上送权限信息, 则表明该菜单无需权限校验。

当要读写或执行该菜单的功能时, 客户端首先向相应的权限条目写入用户名及口令, 装置根据用户名及口令, 向客户端回复密码正确且有权限、密码正确但无权限、密码错误三种情况。只有客户端收到密码正确且有权限的回复后, 才能继续进行相应的读写或执行操作。

1.4 命令执行

与模拟量, 定值展示不同, 装置命令需要装置做出相应动作, 例如出口传动, 清除报告等。一般而言, 命令均带有执行参数, 这些参数使用命令条目的相关联条目(KOD=23)表示, 数据类型为 32 位无符号整数(格式 {uint8_t entry_id, uint8_t group_id, uint8_t addr, uint8_t reserve}), 数据数量可以为零个或多个。每个参数条目包含描述(KOD = 10)、范围和步长(KOD=3, 可选)、单位(KOD=9, 可选)、默认值(KOD=2)、枚举值(KOD=8, 可选)等等。客户端在执行某条命令前, 先向所有参数条目写入数据, 然后再向命令条目写入数据。

命令执行进度和结果由装置命令条目的实际值(KOD = 1)上送给客户端。

2 系统设计

2.1 硬件设计

本设计应用于 PCS 系列保护装置中, 该系列装置采用双 CPU 架构, 其硬件架构图如图 3 所示。

其中, DSP 分为保护 DSP 和启动 DSP, 具有独立的采样和出口电路, 采用“与门”出口方式。完成模拟量数据采集、与对侧交换采样数据、保护逻辑计算和跳闸出口等功能。CPU 实现对整个装置的管理、人机界面、打印、对时、通信和录波等功能。

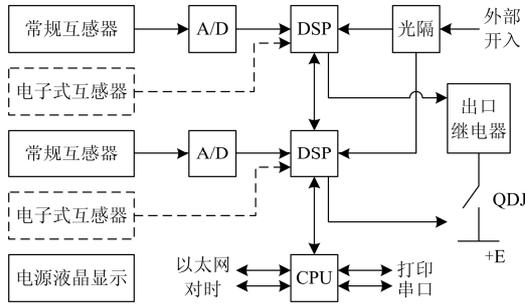


图 3 硬件结构图

Fig. 3 Diagram of hardware structure

2.2 软件设计

2.2.1 软件架构设计

上位机客户端逻辑设计采用经典的三层架构方式^[9-10]，从下自上依次为网络层，数据处理层与展示层。如图 4 所示。

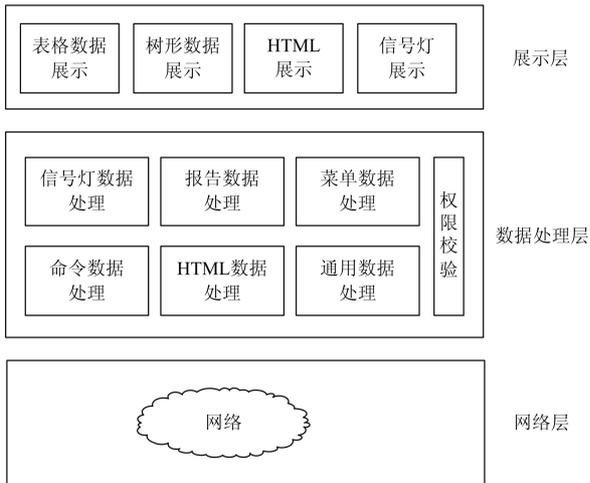


图 4 软件逻辑视图

Fig. 4 Diagram of software's logical view

网络层为最底层，其主要功能是从网络接收装置的数据以及通过网络将数据发送至装置。同时，网络层还需要负责将接收到的数据送给数据处理层进行处理，并将数据处理层生成的数据发送到网络。

数据处理层为核心层，负责将网络层上送的流数据进行解析，并组织为结构化的数据。同时需要将结构化数据组织为流数据，交给网络层。

展示层为最上层，该层负责将结构化的数据按照一定的格式展示，并响应用户操作。

由于报文的接收、发送、用户操作有可能同步进行，为了避免接收报文与发送报文同时出现，为了使得客户端在处理报文时能够及时响应用户操作，上位机客户端运行设计采用多线程方式，分别为 UI 线程，发送线程与接收线程，如图 5 所示。

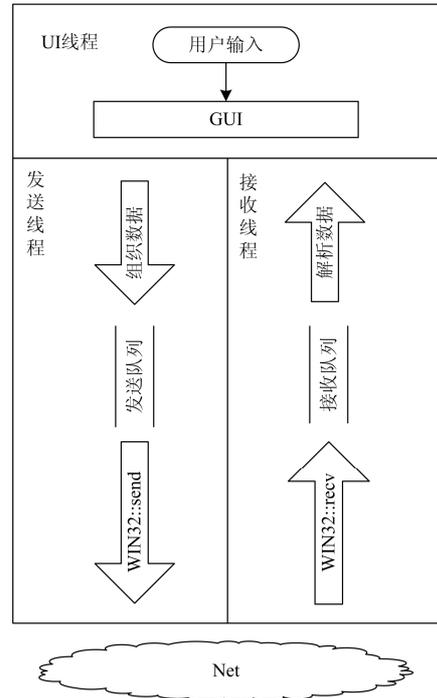


图 5 软件运行视图

Fig. 5 Diagram of software's runtime view

UI 线程负责刷新用户界面，响应用户操作。接收线程负责从网络接收流数据，并将流数据解析为结构化数据。发送线程负责将结构化数据组织为流数据，并发送到网络。

2.2.2 关键模块设计

数据处理层是本软件的核心业务层，该层的主要作用是解析和生成与保护装置通信的 103 规约报文，包括装置菜单解析，权限校验，通用分类服务数据解析，生成通用分类服务数据，请求执行装置命令，读取命令执行结果等。

成功连接到装置后，上位机客户端发起读取菜单报文。首先构造一个 ASDU21，GIN 为根菜单 GIN，KOD 为描述与相关联条目。装置回复一个 ASDU10，包含菜单描述与子菜单 GIN。上位机对于每个子菜单再次使用 ASDU21 读取其内容，直到所有菜单读取完毕。如图 6 所示。

装置菜单读取完毕后，此时用户可以点击菜单，进行各项操作。例如，用户可以点击状态量菜单，查看装置各个模拟量组，也可以点击出口传动菜单，对装置进行出口传动试验。其中涉及到遥控、定值整定、报告清除等关键操作，需要输入用户名和密码，进行权限校验。

以定值整定为例，其逻辑处理流程如图 7 所示。

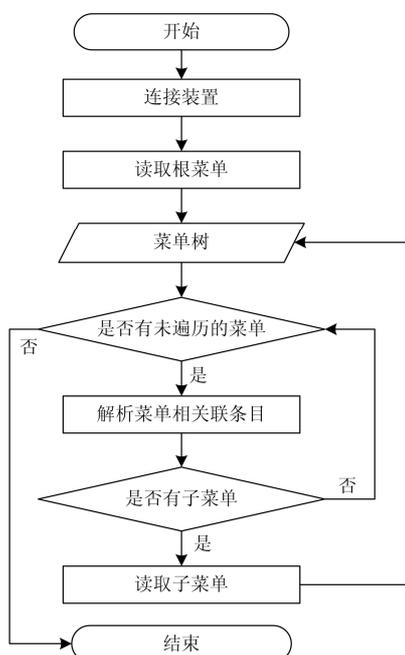


图 6 读取装置菜单流程图

Fig. 6 Flow chart of reading device menu

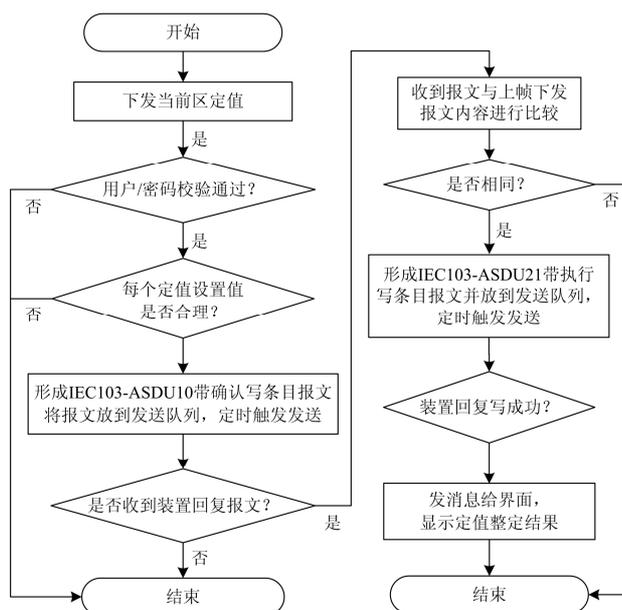


图 7 定值整定流程图

Fig. 7 Flow chart of fixed value setting

3 系统实现

本系统底层硬件采用双 CPU 架构, 运行嵌入式系统。上位机客户端软件运行于 Windows 平台, 采用 C++ 编写, 软件主界面如图 8 所示。

界面左侧为信号灯与资源管理器窗体, 分别用于展示装置信号灯与装置菜单。界面右侧为工作区, 使用标签页形式展示各项菜单内容。

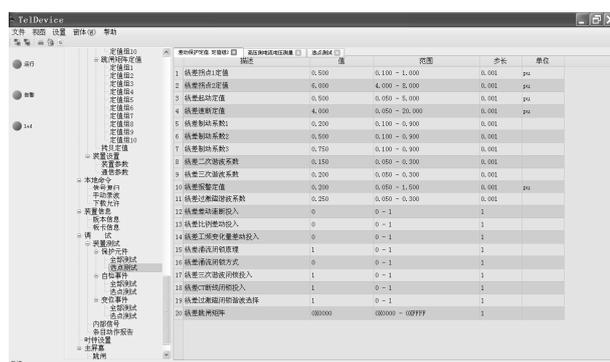


图 8 软件主界面

Fig. 8 Main interface of the software

4 结论

本文基于扩展 103 规约, 设计与实现了保护装置通信与调试系统。该系统以 103 规约为基础, 不但具有 103 规约的全部功能, 还可以实现装置菜单读取, 权限控制, 装置命令执行等功能。目前本系统已经在基于 UAPC 平台的 PCS 系列装置中广泛应用, 并得到多个国家和地区的用户高度认可。

参考文献

- [1] 吴晓辉, 陈泽文. 基于 DSP 的以太网 103 规约在电力监控系统中的应用[J]. 计算机应用与软件, 2009, 26(10): 235-238.
WU Xiaohui, CHEN Zewen. The applications of Ethernet 103 protocol in power control system based on DSP[J]. Computer Applications and Software, 2009, 26(10): 235-238.
- [2] 柏嵩, 陈斌, 唐涛, 等. IEC870-5-103 规约的应用经验[J]. 电力系统自动化, 2000, 24(13): 68-70.
BAI Song, CHEN Bin, TANG Tao, et al. Analysis and usage of IEC870-5-103 standard[J]. Automation of Electric Power Systems, 2000, 24(13): 68-70.
- [3] 徐伟国, 杨锁红, 姜勇. 应用 IEC60870-5-103 规约的嵌入式通信管理系统设计[J]. 电力系统保护与控制, 2009, 37(7): 67-70.
XU Weiguo, YANG Suohong, JIANG Yong. Application of IEC60870-5-103 transmission protocol in embedded correspondence management system design[J]. Power System Protection and Control, 2009, 37(7): 67-70.
- [4] 郑飞, 路建涛, 高莉, 等. 基于 IEC60870-5-103 规约的保护装置冗余网络通信设计[J]. 电力系统保护与控制, 2010, 38(24): 168-171.
ZHENG Fei, LU Jiantao, GAO Li, et al. Design of redundant network communication of microcomputer-

based relay protection devices based on IEC60870-5-103 transmission protocol[J]. Power System Protection and Control, 2010, 38(24): 168-171.

[5] 李钢, 郑徐华, 石秋生, 等. 103 协议通信报文便利统一传送的实现[J]. 电力系统自动化, 2007, 31(增刊): 307-309.
LI Gang, ZHENG Xuhua, SHI Qiusheng, et al. Realizing convenient and unified transfer for IEC 60870-5-103 communication message via a unified coding table[J]. Automation of Electric Power Systems, 2007, 31(S): 307-309.

[6] 李文武, 游文霞, 王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制, 2011, 39(10): 140-147.
LI Wenwu, YOU Wenxia, WANG Xianpei. Survey of cyber security search in power system[J]. Power System Protection and Control, 2011, 39(10): 140-147.

[7] 镐俊杰, 王丹, 杨东海. 电力信息系统网络安全态势在线评估框架与算法研究[J]. 电力系统保护与控制, 2013, 41(9): 116-120.
HAO Junjie, WANG Dan, YANG Donghai. Research of security situation online-assessing framework and algorithm in electric power information system[J]. Power System Protection and Control, 2013, 41(9): 116-120.

[8] 蒋湘涛, 贺建飏, 李楠. 电力信息采集的通用型通信规约解析系统研究与设计[J]. 电力系统保护与控制, 2012, 40(9): 118-122.
JIANG Xiangtao, HE Jianbiao, LI Nan. Research and design on general communication protocol analysis system for power information collecting[J]. Power System Protection and Control, 2012, 40(9): 118-122.

[9] 马银戌, 刘庆东, 鲍慧. 变电站智能巡视后台管理系统的设计与实现[J]. 电力系统保护与控制, 2014, 42(10): 125-129.
MA Yinxu, LIU Qingdong, BAO Hui. Design and implementation of substation intelligent patrol background management system[J]. Power System Protection and Control, 2014, 42(10): 125-129.

[10] 陈海宏, 张静, 万书亭. 基于 GIS 的电力通信线路管理系统开发与应用[J]. 电力系统及其自动化学报, 2013, 25(2): 26-30.
CHEN Haihong, ZHANG Jing, WAN Shuting. Development and application of electric power communication line management system based on GIS[J]. Proceedings of the CSU-EPSA, 2013, 25(2): 26-30.

收稿日期: 2015-01-26; 修回日期: 2015-04-27

作者简介:

张磊(1985-), 男, 硕士, 工程师, 研究方向为保护测控配置软件开发; E-mail: zhangll@nrec.com

陈宏君(1981-), 男, 硕士, 高级工程师, 研究方向为可视化编程调试软件开发。

(编辑 姜新丽)