

文章编号: 1001 - 893X(2012)10 - 1675 - 06

Power-One 通信电源监控系统通信协议破解^{*}

于友成

(西安邮电学院 通信与信息工程学院, 西安 710121)

摘 要:根据数据链路层通信协议的一般格式,对串口监听工具截取的 Power-One 通信电源监控系统的通信信息进行了逻辑推理和分析,破解了其通信协议的格式和各种通信命令。实际验证表明,破解结果正确无误。研究结果对于我国通信电源分布式监控系统通信协议的设计和实现,具有一定的借鉴意义。

关键词:通信电源;分布式监控系统;通信协议;解析

中图分类号:TN86 **文献标志码:**A doi: 10.3969/j.issn.1001 - 893x.2012.10.023

Decipherment of Communication Protocol for Power-One Communication Power Supply Monitoring System

YU You-cheng

(School of Telecommunications and Information Engineering, Xi'an University of
Posts and Telecommunications, Xi'an 710121, China)

Abstract: According to the general format of communication protocol of data link layer, logical reasoning and analysis are conducted of the communication information of Power-One communication power supply monitoring system intercepted through the serial port trace tool. The communication protocol format and various communication commands of Power-One communication power supply monitoring system are deciphered. The practical verification shows that, the reasoning and analytical results are correct. The research in this paper has a certain referential significance for the design and implementation of communication protocol for distributed monitoring system of China's communication power supply.

Key words: communication power supply; distributed monitoring system; communication protocol; decipherment

1 引 言

通信电源通常被称为通信系统的“心脏”,其工作不正常,将会造成通信系统故障,甚至导致整个系统瘫痪。因此,为了保证整个通信系统的畅通,节约人力成本和能源损耗,通信电源监控系统应运而生。通信电源监控系统对分布的通信电源设备和空调机房进行遥测、遥信和遥控,能实时监视和显示其运行参数,能自动监测和处理系统内各种设备的故

障^[1-2]。

鉴于国外发达国家通信电源监控系统的研发工作比较早而且产品比较成熟,我国的相关研究工作通常是先借鉴国外的经验,然后研发具有自主知识产权的系统。其中,最关键的问题就是通信协议的破解。一般的破解思路是通过不断试探,截获通信信息,分析其规律性,进而推测得到通信协议,然后按此协议发送指令进行验证^[3]。这种方法具有一定的盲目性,工作量比较大,而且具有一定的局限性。

本文在破解美国 Power-One 通信电源监控系统

^{*} 收稿日期:2012 - 04 - 13;修回日期:2012 - 05 - 10

时,以数据链路层通信协议的一般格式为指导,结合监控系统生成的各种文件,通过合理的逻辑推理和分析,破解通信规约和通信命令,并利用破解的通信命令直接对电源系统实施监控,实际验证其正确性。这种方法准确性高,通用性强,而且节省时间和精力。

2 通信协议解析

2.1 解析思路

通信协议(Communication Protocol)是两个实体完成通信或服务所必须遵循的规则和约定。协议定义了数据单元使用的格式,信息单元应该包含的信息与含义,连接方式,信息发送和接收的时序,从而确保网络中数据顺利地传送到确定的地方。以下对 Power-One 通信电源监控系统所采用的通信协议进行破解。

破解时,运行上位机软件 PowCom,并利用免费的串口监听工具,截获 Power-One 通信电源监控系统上位机(PC)与下位机(即电源控制模块 PCU)之间的通信信息,即捕获下行(PC→PCU)和上行(PCU→PC)数据帧。对于截获的上下行数据帧,首先根据高级数据链路控制规程(HDLC)帧结构(图 1),推理出对通信协议的格式和各种功能命令;然后根据菜单界面和监控系统生成的各种文件,如配置文件(.pcg)、参数文件(.prm)、测试文件(.tst)和告警历史文件等,推理出各种功能命令中数据字段的格式。

标志(F)	地址(A)	控制(C)	信息(I)	帧校验序列 FCS)
-------	-------	-------	-------	------------

图 1 HDLC 帧结构
Fig.1 HDLC frame structure

2.2 协议破解

基于上述思路,就可以进行具体的解析。

首先,将 Power-One 通信电源监控系统上位机(PC)通过串口 Com1 与 PCU 相连,运行上位机软件 PowCom,选择 Communication(通信)菜单下的菜单项 Port setup(端口设置),选择 COM1 口,波特率9 600(图 2),然后选择该菜单下的菜单项 Direct communication(直接通信)实现与 PCU 连接(图 3)。注意,通信采用 10 bit异步方式:起始位 1 bit,数据位 8 bit,停止位 1 bit,无校验,波特率9 600,必须与 PCU 设置相同。

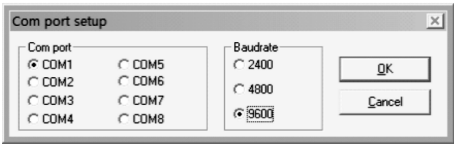


图 2 端口设置界面
Fig.2 Port setup menu window

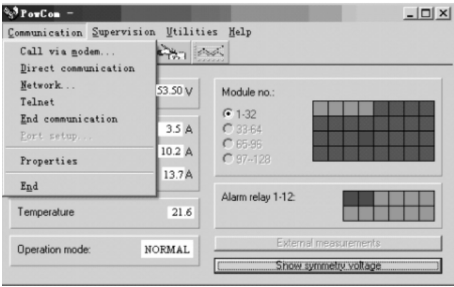


图 3 通信菜单
Fig.3 Communication menu

依次选择 PowCom 各个菜单下的各种监控功能,包括 Communication(图 3)、Supervision(图 4)和 Utilities(图 5)菜单下的各种监控功能。参考图 1 的一般格式,分析用 SUDT SerialTrace Monitor 截获的上下行数据帧,推断通信协议的格式如下:每个数据帧的第一个字节均为 FFH,由此推断为标志字段。最后一个字节可能是校验和字段,经过计算,它是帧中其他字段的校验和。第二个字节很显然是帧长字段。第三和第四个字节在上下行数据帧中数值总是颠倒,初步推断为发送地址字段和接收地址字段,选择对不同整流模块进行监控操作,证明了上述推断,其中,上位机的地址始终为 00H,下行接收地址为整流模块的地址。第五个字节在下行数据帧时为 01H,而在上行数据帧时为 00H,推断为应答字段,即 00H 表示无需应答;01H 表示必须应答。第六个字节始终为 01H,可能是结构控制字段。第七个字节对每个监控功能而言都是唯一的,而在每对上下行数据帧中相同,故此推断为功能码或命令字段。最后,第七个字节与最后一个字节之间的部分显然为数据字段,其长度为(帧长-8)。

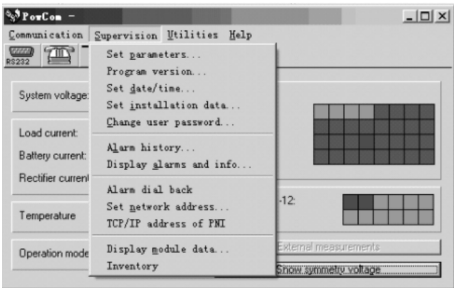


图 4 监控菜单
Fig.4 Supervision menu

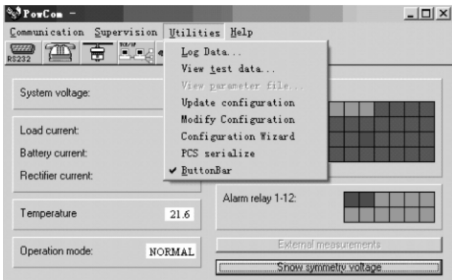


图 5 实用工具菜单
Fig.5 Utilities menu

综合以上的分析推理结果,得到 Power-One 通信电源上下位机间通信协议的格式,如表 1 所示。其中,标志字段表示每一帧的开始,取值恒为 FFH。帧长字段为帧中所有字段的字节数,取值范围为 08H ~ FFH。发送地址和接收地址字段分别表示数据的发送者和接收者的地址,上位机监控系统地址始终为 00H,整流模块的地址为 01H ~ FFH。应答字段表示接受者是否需要对接收的数据进行回复:00H 表示无需回复;01H 表示必须回复。结构控制

字段恒为 01H。功能码字段为请求或响应数据帧的功能编码,取值范围为 00H ~ FFH。数据字段为请求或应答数据,数据格式取决于具体的监控功能。校验和字段对帧中其他字段按字节计算的校验和,用于检测数据帧在传输中是否出现差错。

表 1 Power-One 通信协议格式		
Table 1 Power-One communication protocol format		
序号	字节数	格式字段
1	1	标志
2	1	帧长
3	1	发送地址
4	1	接收地址
5	1	应答
6	1	结构控制
7	1	功能码
:	$n - 8$	数据
n	1	校验和

在推断通信协议的同时,根据菜单功能与上下行数据帧的对应关系,可以解析出 Power-One 通信电源上下位机间的各种通信命令,如表 2 所示。

表 2 Power-One 通信命令							
Table 2 Power-One communication commands							
序号	功能命令	功能码 (Hex)	发送 方向	序号	功能命令	功能码 (Hex)	发送 方向
1	请求系统数据(request system data)	00	PC→PCU	23	请求系统信息(request system information)	0B	PC→PCU
2	发送系统数据(send system data)	00	PCU→PC	24	发送系统信息(transmit system information)	0D	PCU→PC
3	请求设置点(request set points)	01	PC→PCU	25	请求告警历史数据(request alarm history data[1-20])	0E	PC→PCU
4	发送设置点(transfer set points)	01	PCU→PC	26	发送告警历史数据(send alarm history data[1-20])	0E	PCU→PC
5	更新设置点(update set points)	02	PC→PCU	27	请求告警历史数据(request alarm history data[21-40])	0F	PC→PCU
6	设置点更新完成(set points updated)	02	PCU→PC	28	发送告警历史数据(send alarm history data[21-40])	0F	PCU→PC
7	请求测试数据报头(request testdata header)	03	PC→PCU	29	请求额外数据(request extra information)	10	PC→PCU
8	发送测试数据报头(transfer testdata header)	03	PCU→PC	30	发送额外数据(transmit extra information)	10	PCU→PC
9	请求测试电压(request test voltages)	04	PC→PCU	31	设置额外数据(set extra data)	11	PC→PCU
10	发送测试电压(transmit test voltages)	04	PCU→PC	32	设置额外数据完成(extra data set)	11	PCU→PC
11	请求测试电流(request test current)	05	PC→PCU	33	请求系统配置(request system configuration)	12	PC→PCU
12	发送测试电流(transmit test current)	05	PCU→PC	34	系统配置完成(transmit system configuration)	12	PCU→PC
13	请求测试安时(request test amphour)	06	PC→PCU	35	设置配置(set configuration)	13	PC→PCU
14	发送测试安时(transmit test amphour)	06	PCU→PC	36	配置设定(configuration set)	13	PCU→PC
15	设置日期/时间(set date/time)	07	PC→PCU	37	请求设备清单(request inventory)	1F	PC→PCU
16	日期/时间设置完成(date/time set)	07	PCU→PC	38	发送设备清单(transmit inventory)	1F	PCU→PC
17	设置/更改密码(set/change password)	08	PC→PCU	39	请求外部测量(request external measurements)	2B	PC→PCU
18	密码设置完成(password set)	08	PCU→PC	40	发送外部测量(transmit external measurements)	2B	PCU→PC
19	验证密码(check password)	09	PC→PCU	41	请求 PNI 的 TCP/IP 地址(request TCP/IP address)	2F	PC→PCU
20	密码确认(password confirmation)	09	PCU→PC	42	发送 PNI 的 TCP/IP 地址(transmit TCP/IP address)	2F	PCU→PC
21	设置系统信息(set system information)	0A	PC→PCU	43	设置 PNI 的 TCP/IP 地址(set TCP/IP address)	30	PC→PCU
22	系统信息设定(system information set)	0A	PCU→PC	44	PNI 的 TCP/IP 地址设定(TCP/IP address set)	30	PCU→PC

2.3 数据字段解析

在解析出表 2 中所列出的功能命令以后,下一步的工作就是解析出每一种命令数据字段的格式。这本来是一个非常耗时而且繁琐的不断比对和尝试的过程,但是,只要掌握本文的基本分析方法,特别是有效地利用监控系统生成的各种文件,最终还是能够获得令人满意的结果。限于篇幅,以下只简单介绍部分命令的数据字段的解析过程和解析结果。另外,为清晰起见,功能码均以粗斜体字表示,数据字段均以下划线示出。

2.3.1 设置日期/时间(set date/time)、日期/时间设置完成(date/time set)

当通过上位机 PowCom 菜单命令将日期和时间设置为 2011 年 3 月 15 日 15 时 13 分时(图 6),截获如下的设置日期/时间(set date/time)下行数据帧:FF 0D 01 00 01 0107 0B 03 0F 0F 0D 4F,将数据字段与预设定的日期和时间比对后,推断数据字段的格式如表 3 所示。其中,YY 为年份(0~99),MM 为月份(1~12),DD 为日(1~31),hh 为小时(0~23),mm 为分钟(0~59),所有数据字节以十六进制表示。注意应答字段为 01H,表示 PCU 必须回复。

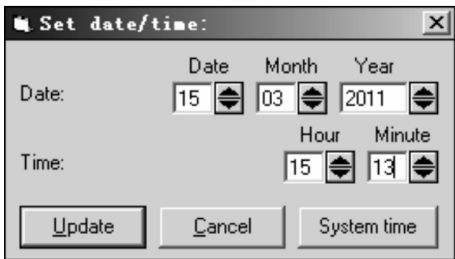


图 6 设置日期/时间界面
Fig.6 Set date/time window

表 3 设置日期/时间命令数据字段的格式
Table 3 Set date/time data format

序号	字节数/byte	格式字段
1	1	YY
2	1	MM
3	1	DD
4	1	hh
5	1	mm

此时,截获到 PCU 回复日期/时间设置(FF 08 00 01 00 01 07 10)完成(date/time set)数据帧,表示日期/时间设置成功。注意应答字段为 00H,表示 PC 无需回复。

2.3.2 设置/更改密码(set/change password)、密码设置完成(password set)

当通过上位机 PowCom 菜单命令将密码设置或更改为 8888 时(图 7),截获如下的设置/更改密码(set/change password)下行数据帧:FF0C 01 00 01 01 08 38 38 38 38 F6,显然,数据字段为密码数字的 ASCII 码,因为十进制 0~9 对应的 ASCII 码 30H~39H。注意应答字段为 01H,表示 PCU 必须回复。



图 7 设置/更改密码界面
Fig.7 Set/change password window

此时,截获到 PCU 回复的密码设置(FF 08 00 01 00 0108 11)完成(password set)上行数据帧,表示密码设置成功。注意应答字段为 00H,表示 PC 无需回复。

2.3.3 验证密码(check password)、密码确认(password confirmation)

当通过上位机 PowCom 菜单命令输入错误密码 5678 时,截获如下的验证密码(check password)下行数据帧:FF0C 01 00 01 01 09 35 36 37 38 F1,注意,应答字段为 01H,表示 PCU 必须回复。此时截获到 PCU 回复如下的密码确认(password confirmation)上行数据帧:FF 09 00 01 00 0109 00 13,根据 PowCom 此时的显示界面(图 8),推断数据字段 00H 表示密码错误。同样,应答字段为 00H,表示 PC 无需回复。



图 8 密码错误界面
Fig.8 Wrong password window

当通过上位机 PowCom 菜单命令输入正确的密码 8888 时,截获如下验证密码(check password)下行数据帧:FF0C 01 00 01 01 09 38 38 38 38 F7,注意,应答字段为 01H,表示 PCU 必须回复。此时截获到 PCU 回复如下的密码确认(password confirmation)上行数据帧:FF 09 00 01 00 0109 01 14,数据字段 01H

表示密码正确。同样,应答字段为 00H,表示 PC 无需回复。

2.3.4 其他

由于篇幅所限以及很多数据帧数据字段过长等原因,在此无法一一列举各种数据帧的推理过程和推理结果。

对于其他数据帧的解析,只说明大致的解析方法和过程:在相关菜单运行相应的菜单项监控功能,将截获的数据帧与菜单项的参数、配置数据等进行比对,推理出数据字段的格式。另外,在解析很多数据帧的数据字段时,参考了系统生成的相关文件。这样,既节省了大量的时间,又提高了推理的准确性。

- (1)借助于配置文件(.pcg),解析了与配置相关的数据帧(如表 2 中序号 33~36 和 39~44);
- (2)借助于参数文件(.prm),解析了与参数相关的数据帧(如表 2 中序号 1~6);
- (3)借助于测试文件(.tst),解析了与测试相关的数据帧(如表 2 中序号 7~12);
- (4)借助于告警历史文件,解析了与告警相关的数据帧(如表 2 中序号 25~28)。

3 实际验证

对于以上的破解结果,必须验证其正确性。验证过程如下:首先利用串口调试工具(如串口调试助手)替代 PowCom 上位机软件,直接与下位机 PCU 通信;然后将以上解析得到的下行(PC→PCU)数据帧逐一经串口调试工具发出,检查 PCU 是否正确响应,返回正确的上行(PCU→PC)数据帧,并正确无误地完成监控工作。

图 9~13 分别是设置日期/时间、设置密码、请求系统信息、请求历史告警数据和请求系统信息的测试截图。测试截图显示,利用破解的通信命令可以直接与 PCU 通信,并正确地完成监控工作。



图 10 设置密码测试截图
Fig.10 Set password test screenshot



图 11 请求系统信息测试截图
Fig.11 Request system information test screenshot

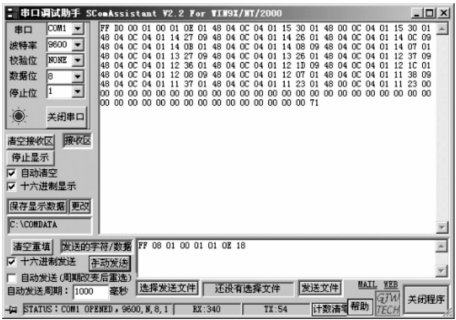


图 12 请求历史告警数据测试截图
Fig.12 Request alarm history data test screenshot

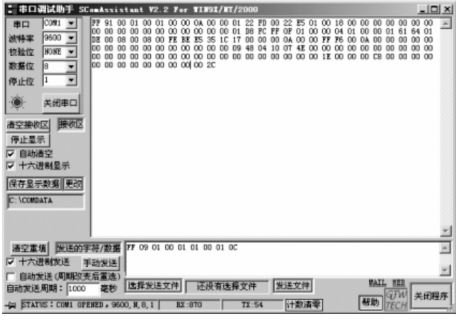


图 13 请求系统信息测试截图
Fig.13 Request system information test screenshot



图 9 设置日期/时间测试截图
Fig.9 Set date/time test screenshot

4 结 论

本文基于数据链路层通信协议一般格式的破解方法,对于各种数据链路层通信协议的破解具有通用性,具有实际的指导意义。但是,本文的破解结果具有一定的局限性,原因是 Power – One 通信协议的格式和通信命令并不是开放的和通用的。尽管如此,对于通信电源的监控管理人员以及通信电源监控系统的设计人员仍然具有一定的理论指导意义。破解是手段而不是目的,下一步的工作是在此基础上设计适合中国国情而且适应通信电源发展的监控系统和通信协议。通信电源地理上的分散化,必然要求监控的分布式^[4-6],而分布式电源监控系统必然要求通信协议的规范化和统一化^[7]。因此,研究工作的重点是我国通信电源分布式监控软件的设计和实现。

参考文献:

- [1] 徐小杰,侯振义. 通信电源集中监控系统发展浅析[J]. 电源世界,2006(5):13 – 15.
XU Xiao-jie, HOU Zhen-yi. Development of Centralized Supervision and Control System of Communication Power Supply[J]. The World of Power Supply, 2006(5): 13 – 15. (in Chinese)
- [2] 刘兴纲,康洪波. 基于 B/S 结构的通信电源监控系统的设计与研究[J]. 河北北方学院学报,2010,26(3):43 – 46.
LIU Xing-gang, KANG Hong-bo. Research and Design of the Power Monitoring System of Communication Based on B/S Structure[J]. Journal of Hebei North University, 2010, 26(3): 43 – 46. (in Chinese)
- [3] 张洪生,杨三民,吴莹. 串行通信协议的破解和控制系统的功能扩展[J]. 电气自动化,2008,30(5):44 – 45.
ZHANG Hong-sheng, YNAG San-min, WU Ying. The Deci-

pherment of Serial Communicaton Protocol and The Function Extension of Control System[J]. Electrical Automation, 2008, 30(5):44 – 45. (in Chinese)

- [4] 杨永标,王双虎,王余生,等. 一种分布式电源监控系统设计方案[J]. 电力自动化设备,2011,31(9):125 – 128.
YANG Yong-biao, WANG Shuang-hu, WANG Yu-sheng, et al. A Distributed Power Monitoring System Design[J]. Electric Power Automation Equipment, 2011, 31(9): 125 – 128. (in Chinese)
- [5] 李玲,王欢欢,谢利理. 基于集散控制的分布式电源并网监控系统研究[J]. 计算机测量与控制,2010, 18(3):580 – 582.
LI Ling, WANG Huan-huan, XIE Li-li. Research of Grid Connection of Monitor System of Distributed Power Supply-Based on Distributed Control System[J]. Computer Measurement and Control, 2010, 18(3): 580 – 582. (in Chinese)
- [6] 郑家庆. 通信电源监控系统的发展与完善[J]. 硅谷, 2011(12): 25 – 25.
ZHENG Jia-qing. The Development and Perfection of Communication Power Supply Monitoring System[J]. Silicon Valley, 2011(12): 25 – 25. (in Chinese)
- [7] 杨耿杰,郭谋发,张书芳,等. 厂站直流电源分层分布式监控系统[J]. 福州大学学报,2009(4): 536 – 541.
YANG Geng-jie, GUO Mou-fa, ZHANG Shu-fang, et al. Station DC Power Supply Distributed Monitoring System[J]. Journal of Fuzhou University, 2009(4): 536 – 541. (in Chinese)

作者简介:

于友成(1963—),男,山东威海人,硕士,高级工程师,主要研究方向为现代通信网优化和通信电源监控系统。

YU You-cheng was born in Weihai, Shandong Province, in 1963. He is now a senior engineer with the M. S. degree. His research interests include network optimization and communications power supply monitoring system.

Email: yuyoucheng@sina.com