IEC61850 过程层网络通信分析诊断工具设计

李忠安[1]，王 娇[2]，张惠刚[2]，唐 琳[2]

(1.南瑞继保电气有限公司，江苏 南京 211100；2.南京工程学院电力工程学院，江苏 南京 211167)

摘要：在智能化变电站中，过程层网络通信是其信息共享和信息传输的基础。为了保证电力系统的安全、可靠性，实现过程层网络通信异常的分析、诊断是目前研究的热点。采用特殊的智能DAG网卡，其具有结构简单、零包丢失、高精度时间戳等优势，然后配合扩展的Wireshark分析软件，设计了一套软硬件结合的网络分析诊断软件。同时详细阐述了报文异常检查、网络状态统计以及故障波形记录等功能实现步骤，展示网络分析、诊断系统的应用效果以及提出未来亟待改进的地方。该设计将故障录波器和网络通信记录分析系统集成一体化，对减少变电站内设备、降低投资、简化运行维护具有重大的变革意义。

关键词：Wireshark；DAG；网络分析；一体化；IEC61850；过程层

Design of process layer network communication fault diagnosis and analysis tool based on IEC61850

LI Zhongan[1], WANG Jiao[2], ZHANG Huigang[2], TANG Lin[2]

(1. Nari-Relays Electric Co., Ltd., Nanjing 211100, China; 2. School of Electric Power Engineering, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract: In the intelligent substation, the process layer network communication is the basis of information sharing and information transmission. To ensure safety and reliability of power system, diagnosing and analyzing process layer network communication is currently a hot research. This paper uses a special smart DAG card, which has simple structure, zero packet loss, high-precision timestamp and other advantages. Then it combines expanded Wireshark analysis software. At last, a network communication fault diagnosis and analysis tool is designed. Meanwhile, it also elaborates three functions with abnormal packet inspection, network status statistics and fault waveform recording. Then this paper displays the strengths and weaknesses of the network communication analysis tool. This design is an integration between fault recording and network traffic records analyzing system. It provides signification in reducing the substation devices and investment, simplifying operation and maintenance.

Key words: Wireshark; DAG; network diagnosis; integration; IEC61850; process level

中图分类号： TM73 文献标识码：A 文章编号： 1674-3415(2015)01-0093-05

0 引言

IEC 61850标准提出“三层两网”通信体系中，过程层网络主要负责传输智能开关相关状态量，控制量以及模拟量信息[1]。过程层网络通信是智能变电站信息传输和信息共享的基础，对电网运行的安全性、可靠性起着至关重要的作用[2]。目前网络运行状况和IED设备之间通信过程的实时分析、监测与诊断已经成为智能变电站安全运行的迫切要求[3]。因此如何实现过程层网络通信异常的分析、诊断，是亟待研究解决的关键课题[4-5]。

现阶段，对于过程层网络报文的分析与诊断，国内外各个二次设备厂家有了相应的一些测试仪器与工具[6-9]。而这些产品或工具一定程度上满足电力系统故障诊断的要求[10]。但它们都有共同的缺陷：1) 经济性上，变电站配置这些仪器需要从自动化厂家购买，价格昂贵；2) 实用性上，这些仪器设备需携带到现场进行分析，携带不便。3) 可拓展性上，这些报文分析仪器升级无论从硬件还是软件角度看，工序较为复杂。

本文以硬件DAG网卡为支撑，在Wireshark开源软件基础上，采用 c++语言设计了一款过程层网络通信分析诊断工具。

1 开发环境介绍

1.1 Wireshark简介

Wireshark 是一款免费开源的应用较为广泛的网络协议分析软件。它具有简洁友好的用户界面，

能够实现协议解析器的二次开发、网络故障的定位查找、网络流量测量与分析功能[11]。其中 Wireshark 中最重要的模块为 epan，它负责具体的协议解析，并以协议树的方式逐层处理。另外 Tap 是 wireshark 中一个强大且灵活的运行机制。它通过事件驱动获得某个特定协议的每一帧报文，一方面，利用回调函数 tap_packet_cb 实现特定协议的数据分析。另一方面，以定时方式，即采用定时回调函数 tap_draw_cb 展示监测数据界面。该机制为后续开发提供了借鉴意义。

1.2 DAG 卡简介

DAG 网卡是 Endace 公司生产的数据采集卡，专门为网络监控和安全应用所设计的高精产品。DAG 卡与传统网卡相比，具有极大的优势：1) 数据访问路径短；DAG 卡直接将数据捕获并存储到用户空间存储器中，减少了常规网卡的数据搬迁次数。2) I/O 内存占用率低；DAG 卡采用 I/O 虚拟化及 DMA 技术，将网络流量 100%捕获到主机内存，极大地减少了 CPU 资源。3) 存储容量大，由于一体化结构，网络数据极易从内存直接复制到磁盘，存储不受限。这对于智能变电站过程层海量数据具有极大意义。4) 时标精度高；DAG 卡支持 IRIGB 或 PPS 对时，可以为每个收到的数据包产生一个高精度时间戳(通过硬件)，精度可达 7.5 ns。

2 设计与实现

2.1 系统架构与主要流程

2.1.1 系统架构

基于 Wireshark 的网络分析诊断软件基本结构逻辑上是由以下五部分组成。1) DAG 卡捕获的网络数据通过 winpcap 驱动 NPF 及其用户级接口库 packet.dll 和 wpacp.dll 将数据传输给 Capture；2) Capture 将捕获的数据储存在 Wiretap 部分；3) GTK 提供图形窗口工具，将用户的输入消息传递出去；4) Core 综合协调用户传入、传出的消息；5) Epan 接收来自 Core 传达的命令，指挥协议解析器，将结果传送到 Core，最后调用 GTK 库文件在界面上显示。如图 1 所示。

DAG 有专门的接口 API，也支持 Winpcap 的 NPF 驱动相关的 packet.dll 和 wpacp.dll 接口。因此 Wireshark 基本兼容 DAG 卡，可将 DAG 卡作为普通网卡使用，Wireshark 原有接口基本不用更改。但实际应用时需要注意的是 DAG 卡传送的数据比一般网卡多带有 4 字节校验和，因此 Wireshark 处理 DAG 数据时需要为此特殊处理。

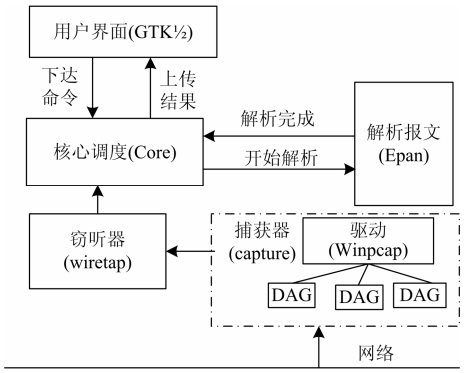

图 1 软件系统架构

Fig. 1 Basic framework of system

2.1.2 系统流程

分析诊断工具对过程层报文的解析、分析、诊断功能基本都在 Epan 模块完成，并结合 tap 的两类回调函数实现的。其主要流程为：对于每帧报文 Epan 判别出 GOOSE 或 SV 报文类型后，分别调用各自的基本解析器解析出基本信息，然后调用协议分析模块检查分析报文的异常情况，最后根据是否存在对应统计 tap，进行状态统计量的计算，对于 SV 数据还要进行波形数据的记录。具体流程如图 2 所示。

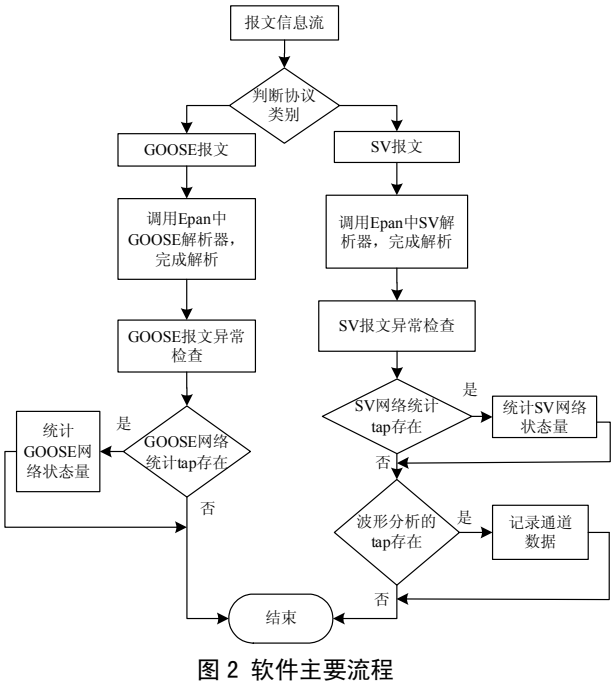

图 2 软件主要流程

Fig. 2 Main flowchart of the software

2.2 分析功能实现

2.2.1 报文异常检查

1) SV 异常检查。其异常状态主要包括断链、跳变、失步、品质变化等。根据 IEC 61850-9-1 标

准，报文中各字节有严格的规范定义。①在规定时间内(一般 10 ms)没有收到下一帧 SV 报文则判断通信中断。②SV 报文中的 smpCnt 为采样计数器，用于检查数据内容是否被刷新。如果该计数器发生跳变、越限、重复、错序、翻转异常等，说明合并单元发生故障。③SV 报文中的 smpSync 为同步标识位，反映了合并单元的同步状态。根据报文中该位的值判断合并单元是否出现失步。④SV 主要有三个品质标志：validity，test，derived。validity 为状态标志位置，如果一个电子式互感器内部发生故障，那么相应的通道的状态有效位置为无效。

由于 Wireshark 中 epan 含有的 SV 协议解析器只能完成基本数据解析，因此需要增加异常数据分析功能，根据解析器解析出来的 SV 数据包括 smpCnt、smpSync 以及报文时间，分析判断 SV 报文异常状况。

以下为采样计数器的判断过程：比较本帧计数器(data->smpCnt)与上一帧计数器(svd->smp_cnt)的代数关系。代码如下：

```
q = 0; //计数跳跃统计量
if(data->smpCnt !=((svd->smp_cnt+1) % 4000 ))
{
q =1; //计数跳跃,标记
svd->smp_qflags_1 = svd->smp_qflags_1 | (1   <<
    RS_CNT_ABN);
}
```

2) GOOSE 报文异常检查。其异常状态包括通信中断、重复、丢帧、错序等。其判断依据为：①在 GOOSE 报文的生存时间的 2 倍时间内没有收到下一帧 GOOSE 报文则判断通信中断。②顺序计数 sqNum 以及报文内容与上一帧 GOOSE 报文完全相同，则为重复。③状态计数 stNum 小于上一帧 GOOSE 报文的 stNum，且 stNum 不等于 1。顺序计数 sqNum 小于上一帧 GOOSE 报文的 sqNum，且 sqNum 不等于 1，则为错序。④当 stNum 不变、sqNum 跳变或 stNum 跳变，则报文出现丢帧现象。

同 SV 类似，Wireshark 中 epan 原有的 GOOSE 协议解析器只能完成基本数据解析，也需要增加异常数据分析功能。根据解析器解析出来的 GOOSE 数据，对其内部的计数器 stCnt、sqNum，标志 test 以及报文时间等进行分析判断。

以下为检修标志变化的判断过程：本帧检修标志(data->test)，根据其值确定检修状态量。代码如下：

```
q = data->test ==0 ? 0 :1;
if( q != ((god->go_qflags >> RS_TEST) & 1))
{
        god->go_qflags_1 = god->go_qflags_1 | (1 <<
    RS_TEST);//检修变化,标记
}
```

2.2.2 网络状态统计

网络的状态统计包括以太网流量、速率、广播风暴以及 SV 报文的抖动、延时等数据的统计。流量是指单位时间内捕捉的报文位数；广播风暴判断依据是在单位时间内接收重复报文超过一定的阀值；SV 抖动是相邻两个报文的时间间隔变化量，对于 4 k 采样率而言，其相邻两个报文间隔为 250 μs；SV 延时指当 smpCnt 为 0 时发送报文时刻与同步脉冲发生时刻(0 时刻)的时间差。

GOOSE、SV 网络的状态统计均采用 tap 机制，但相互独立。GOOSE、SV 采用各自的报文处理回调函数分析状态统计量，并将统计信息存储到数据结构中，供定时回调函数在界面显示使用。

例如 SV 信息流的数据定义如下所示：

```
typedef   struct _sv_stream_info {
      address   src_addr;    //源地址
      address   dest_addr;   //目的地址
      guint16   appid;       //应用标识符
      guint32   npackets;    //总报文
      guint32   apackets;    //报文速率
      float     average_bw; //平均带宽
      gint64    asyn_cnt;    /失步
      gint32    delay;        //延时
      gint32    jitter;       //抖动
      …….
 } sv_stream_info;
```

初始化信息流中的数据后，epan 处理完每一帧 SV 报文后，利用 tap 报文处理回调函数 sv_stat_packet( )更新信息流中数据，归纳相同目的地址和源地址的信息流，计算报文速率、带宽等变量，例如下计算方式：

```
sinfo->apackets=(guint32)(sinfo->npackets/
deltatime);//报文速率
sinfo->average_bw=((float)(sinfo->total_bytes*8)/
deltatime)/1000000;//带宽 Mbit/s
```

最后 tap 定时回调函数 sv_stat_draw 在界面上显示信息流结构中的数据，如图 3 所示。

2.2.3 故障波形记录

故障波形记录是利用 epan 的 SV 解析器获得各通道瞬时值，结合 tap 机制，通过回调函数将各通道瞬时值存储到全局结构体中，定时使用图形方式实时显示数据波形。可用于分析电力系统现场故障

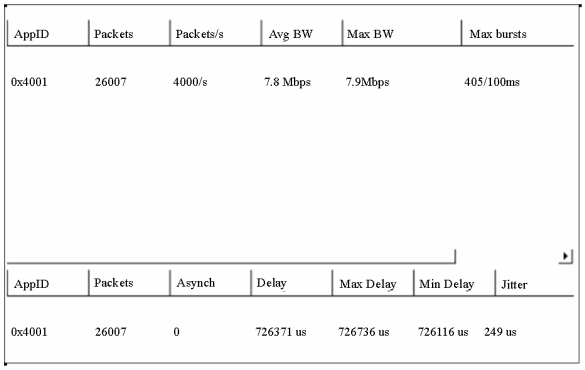

图 3 网络状态监测

Fig. 3 Network status supervision

状态，快速地定位故障源。具体实现步骤：先对波形变量数据初始化，定义 sv_osc_t 结构体，其结构如下：

```
typedef   struct _sv_osc_t {
          address       dest_addr;   //目的地址
          guint32             interval;    //每 ms 测量间隔
          guint32             last_interval; //最后展示间隔
          guint32             max_interval;
          guint32             num_items; //间隔的条目号
          struct _sv_chnl_t   chnls[8];      //8 路通道参数
}sv_osc_t;
```

初始化后，设置八路输出波形的格式、颜色。然后按照 Wireshark 中的 tap 机制，设置回调函数，其中报文处理回调函数 tap_sv_osc_packet( )用来获取报文的电压、电流值，采用 memcpy(&(it->phsMeas), &(svd->phsMeas[ch_idx]), sizeof(sv_phs_meas))拷贝报文中的具体数据值。若通道是电流量，需要除以 1 000；如果是电压量，需要除以 100，同时设置的二次变比，如果显示二次侧的电量值，还需要除以变比。最后 tap 定时回调函数 tap_sv_osc_draw 以图形的坐标的方式显示整体效果，如图 4 所示。

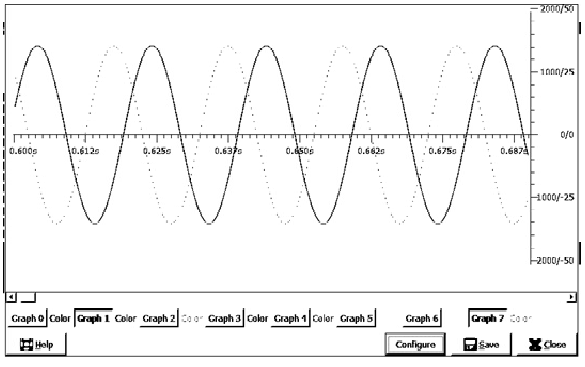

图 4 故障波形记录

Fig. 4 Fault waveform record

3 典型应用效果及其改进

本系统的典型应用效果有以下三点：

1) 软硬一体架构：采用一体化结构，减少了数据搬迁过程，千兆满流量捕获不丢包，存储容量不受限。

2) 通信过程预警：通过对报文流量、报文内容的实时分析，迅速评估通信品质和设备状况、提供通信故障的早期预警。

3) 波形再现：打破了传统单独使用故障录波器的格局，采用新型的网络报文分析仪和故障录播一体化的诊断工具软件，有效查看电网设备的运行状况。

同时，也存在一定不足。例如目前分析过程未与模型文件 CID 或 SCD 关联，需要下一步改进。

4 总结

本文开发了一个针对过程层网络通信自动化的诊断工具，解决了过程层通信故障分析目前过度依赖技术人员的人工分析，分析速度与自动化程度都不甚理想的问题，协助电力系统运维人员及时了解过程层通信网络的运行情况，并采取有效措施应对过程层通信网络出现的各种异常问题，也可将大量技术人员从浩瀚的报文分析中充分解放出来，提高电力系统自动化运维的管理水平。

参考文献

[1] 苏麟, 孙纯军, 褚农. 智能变电站过程网络构建方案研究[J]. 电力系统通信, 2010, 31(213): 10-13.
SU Lin, SUN Chunjun, CHU Nong. Study on the wireless temperature measuring system based on IEC61850 in digital substations[J]. Telecommunications for Electric Power System, 2010, 31(213): 10-13.

[2] 张智锐, 肖繁, 焦邵麟, 等. 不同过程层网络结构的保护系统可靠性分析[J]. 电力系统保护与控制, 2013, 41(18): 142-148.
ZHANG Zhirui, XIAO Fan, JIAO Shaolin, et al. Reliability evaluation of protective relay system based on process layer network[J]. Power System Protection and Control, 2013, 41(18): 142-148.

[3] 陈志光, 张延旭, 曾耿晖, 等. 变电站过程层网络特定通信服务映射(SCSM)及其对实时性的影响分析[J]. 电力系统保护与控制, 2012, 40(21): 96-101.
CHEN Zhiguang, ZHANG Yanxu, ZENG Genghui, et al. Real-time analysis of specific communication service mapping (SCSM) in process-level network of substation[J]. Power System Protection and Control, 2012, 40(21):

96-101.

[4] 丁修玲, 张延旭, 蔡泽祥, 等. 基于报文解析的变电站过程层网络信息流异常保护方法[J]. 电力系统保护与控制, 2013, 41(13): 58-63.
DING Xiuling, ZHANG Yanxu, CAI Zexiang, et al. A protection method of abnormal information flow in process layer network based on packet analysis[J]. Power System Protection and Control, 2013, 41(13): 58-63.

[5] 刘明慧, 赵晓东, 司梦, 等. 智能变电站过程层网络流量管理方式研究与应用[J]. 电力系统保护与控制, 2012, 40(23): 87-92.
LIU Minghui, ZHAO Xiaodong, SI Meng, et al. Research and application of process level network flow management in smart substation[J]. Power System Protection and Control, 2012, 40(23): 87-92.

[6] 黄欣, 白玉良, 贺春. 变电站报文监听系统设计[J]. 继电器, 2007, 35(11): 52-56.
HUANG Xin, BAI Yuliang, HE Chun. Implementation of message monitor system of communication protocol in substation[J]. Relay, 2007, 35(11): 52-56.

[7] 许伟国, 蒋晔, 张亮, 等. 数字化变电站中网络通信黑匣子的设计与应用[J]. 电力系统自动化, 2008, 32(17): 92-94.
XU Weiguo, JIANG Ye, ZHANG Liang, et al. Design and application of the network communication black box in digital substations[J]. Automation of Electric Power Systems, 2008, 32(17): 92-94.

[8] 王治民, 陈炯聪, 任雁铭, 等. 网络通信记录分析系统在数字化变电站中的应用[J]. 电力系统自动化, 2010, 34(14): 92-95.
WANG Zhimin, CHEN Jiongcong, REN Yanming, et al. Application of network communication recorder and analyzer in digital substations[J]. Automation of Electric Power Systems, 2010, 34(14): 92-95.

[9] 张劲松, 俞建育, 张勇, 等. 网络分析仪在数字化变电站中的应用[C] // 中国电机工程学会和中国电工技术学会 2010 输变电年会论文集, 2010 年 10 月 28 日, 南京, 2010: 89-92.
ZHANG Jinsong, YU Jianyu, ZHANG Yong, et al. Application of network communication recorder and analyzer in digital substations[C] // CSEE and China Electrotechnical Society Committee. 2010 Transmission Proceedings, Nanjing, October 28, 2010: 89-92.

[10] 张帆, 竹之涵, 刘之尧, 等. 面向通用对象的变电站事件 (GOOSE) 实时解析和预警系统[J]. 电力系统保护与控制, 2009, 37(23): 92-95.
ZHANG Fan, ZHU Zhihan, LIU Zhiyao, et al. Generic object oriented substation event (GOOSE) real-time analysis and surveillance system[J]. Power System Protection and Control, 2009, 37(23): 92-95.

[11] 罗青林, 徐克付, 臧文羽, 等. Wireshark 环境下的网络协议解析与验证方法[J]. 计算机工程与设计, 2011, 32(3): 770-773.
LUO Qinglin, XU Kefu, ZANG Wenyu, et al. Network protocol parser and verification method based on Wireshark[J]. Computer Engineering and Design, 2011, 32(3): 770-773.

收稿日期：2014-04-08；　修回日期：2014-04-24

作者简介：

李忠安(1975-)，男，硕士，工程师，主要研究方向为电力系统继电保护及自动化；E-mail: liza@nari-relays.com

王　娇(1989-)，女，通信作者，硕士研究生，主要研究方向为电力系统通信及标准，IEC61850，IEC62439 等；E-mail: jiaoseal@163.com

张惠刚(1957-)，男，教授，主要研究方向为电力系统调度自动化。