



数字化变电站实战篇

学会看报文

V1.00

工程服务中心
内部培训资料



修订历史

日期	版本	描述	编写、维护人员
2010-6-3	V1.00	首次建立文档：《数字化变电站实战篇—学会看报文》	数字化项目小组

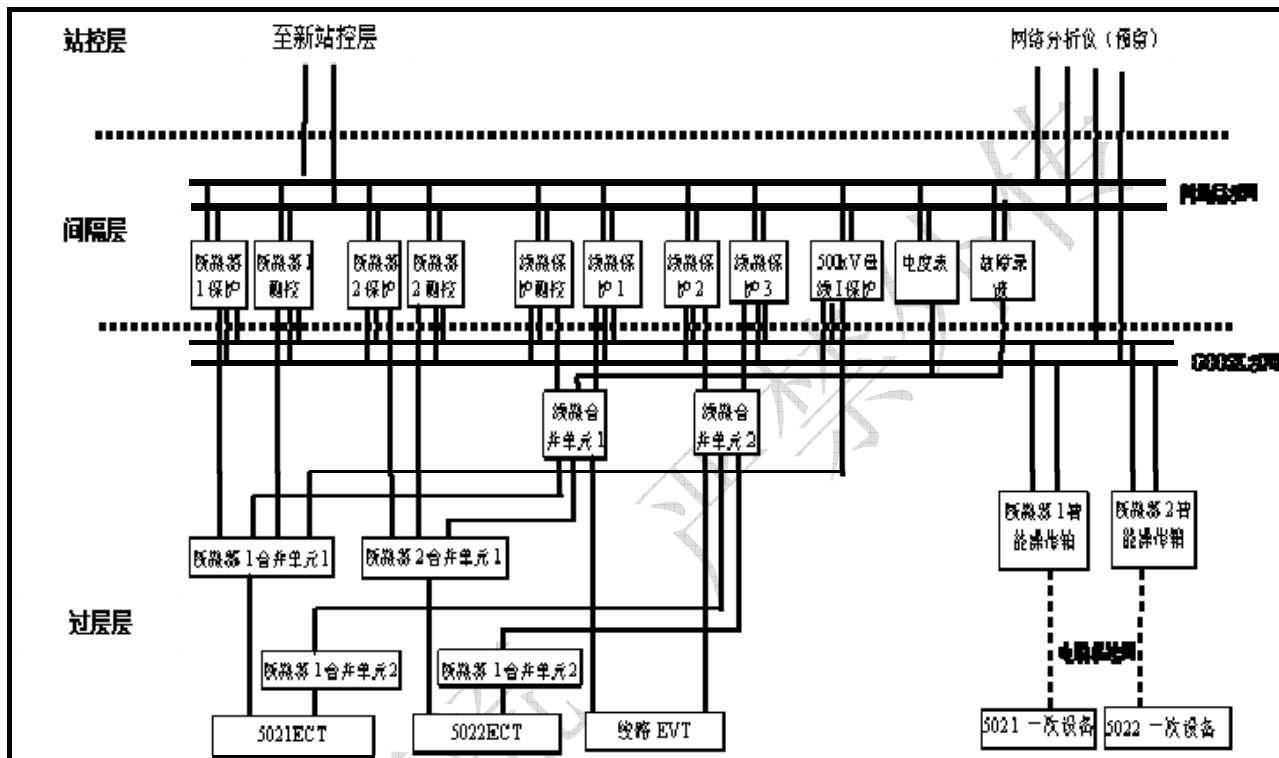
内部交流 严禁外传

一、 概述	- 1 -
1. 网络拓扑结构	- 1 -
2. 通讯子网	- 1 -
3. 子网通讯规约	- 1 -
4. 抓包工具	- 1 -
二、 如何看 MMS 报文	- 2 -
1. 通讯初始化	- 2 -
1.1. ACSI 中的通讯初始化	- 2 -
1.2. MMS 中的通讯初始化	- 2 -
1.3. 建立 TCP 连接	- 2 -
1.4. 释放 TCP 连接	- 3 -
1.5. 初始化请求	- 3 -
1.6. 读模型	- 4 -
1.7. 写控制块	- 8 -
1.8. 常见问题	- 9 -
2. 报告	- 9 -
2.1. ACSI 中的报告	- 9 -
2.2. MMS 中的报告	- 10 -
2.3. 常见问题	- 12 -
3. 控制	- 12 -
3.1. ACSI 中的控制报文	- 12 -
3.2. MMS 中的控制报文	- 13 -
3.3. 常见问题	- 16 -
三、 如何看 GOOSE 报文	- 16 -
1. GOOSE 报文传输机制	- 16 -
2. GOOSE 信号传输	- 17 -
3. 常见问题	- 19 -
四、 如何看 SMV 报文	- 19 -
1. 9-2 报文	- 19 -
2. 常见问题	- 22 -

一、概述

1. 网络拓扑结构

通讯网拓扑结构一般有总线型、星型、环形、树形、网型等，工程中常用总线型或环形拓扑结构。



2. 通讯子网

在准数字化变电站中，按照通讯网络层次结构，可划分为站控层通讯网、过程层通讯网两大类，其中过程层通讯网又可分为 GOOSE 通讯子网和 SMV 通讯子网，GOOSE 通讯子网和 SMV 通讯子网可共网，也可各自独立组网，在最新的国网数字化变电站实施标准中，推荐 GOOSE 子网与 SMV 子网各自独立组网，以减少交换机的数据传输延时。

3. 子网通讯规约

站控层主要使用 IEC61850 标准体系中的 MMS 通讯服务规范，过程层主要使用 IEC61850 标准体系中的 GOOSE 及 SMV 通讯服务规范。

4. 抓包工具

为便于分析现场异常问题，常需要抓取现场通讯报文，常用的工具有 MMS Ethereal 和 EPT61850，MMS Ethereal 可将报文按 MMS 规范予以完整分析；EPT61850 可将报文分别按 MMS 规范和 ACSI 规范

进行分析，但其对 MMS 分析有遗漏问题，故一般两种工具需要配合使用。

二、 如何看 MMS 报文

1. 通讯初始化

1.1. ACSI 中的通讯初始化

在 ACSI 中，通讯初始化服务主要包括：关联、放弃、释放、读逻辑设备目录、读逻辑节点目录、读数据目录、读所有数据值、写报告控制块值、读文件等。

1.2. MMS 中的通讯初始化

ACSI 中的通讯初始化过程映射到 MMS 中，主要包含建立 TCP 连接、释放 TCP 连接、初始化请求、读模型、读控制块、写控制块等。

1.3. 建立 TCP 连接

建立 TCP 连接，分三次握手，第一步客户端向服务器端发起同步请求，第二步服务器端响应，同时也向客户端发起同步，第三步，客户端响应确认，三步过后即完成 TCP 建立连接。

第一步：客户端向服务器端发起同步请求，服务器侧端口固定为 102，客户端端口由 socket 随机产生

```
Transmission Control Protocol, Src Port: 36295 (36295), Dst
Source port: 36295 (36295)
Destination port: iso-tsap (102)
Sequence number: 0 (relative sequence number)
Header length: 32 bytes
Flags: 0x0002 (SYN)
  0... .... = Congestion window Reduced (CWR): Not set
  .0.. .... = ECN-Echo: Not set
  ..0. .... = Urgent: Not set
  ...0 .... = Acknowledgment: Not set
  .... 0... = Push: Not set
  .... .0.. = Reset: Not set
  .... ..1. = Syn: Set
  .... ...0 = Fin: Not set
window size:49640
Checksum: 0x0000 [checksum offloaded]
Options: (12 bytes)
```

第二步：服务器端详客户端响应，同时也想客户端发起同步请求

```

Transmission Control Protocol, Src Port: iso-tsap (102), Dst
Source port: iso-tsap (102)
Destination port: 36295 (36295)
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 32 bytes
Flags: 0x0012 (SYN, ACK)
  0... .... = Congestion window Reduced (CWR): Not set
  .0.. .... = ECN-Echo: Not set
  ..0. .... = Urgent: Not set
  ...1 .... = Acknowledgment: Set
  .... 0... = Push: Not set
  .... .0.. = Reset: Not set
  .... ..1. = Syn: Set
  .... ...0 = Fin: Not set
Window size: 5840
Checksum: 0x40a6 [correct]
Options: (12 bytes)

```

第三步：客户端予以确认

```

Transmission Control Protocol, Src Port: 36295 (36295), Dst
Source port: 36295 (36295)
Destination port: iso-tsap (102)
Sequence number: 1 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x0010 (ACK)
  0... .... = Congestion window Reduced (CWR): Not set
  .0.. .... = ECN-Echo: Not set
  ..0. .... = Urgent: Not set
  ...1 .... = Acknowledgment: Set
  .... 0... = Push: Not set
  .... .0.. = Reset: Not set
  .... ..0. = Syn: Not set
  .... ...0 = Fin: Not set
Window size: 49640
Checksum: 0x0000 [checksum offloaded]

```

1.4. 释放 TCP 连接

释放 TCP 连接，分四次挥手，这是由于 TCP 通讯为全双工通讯，发起关闭连接的一方只能关闭己方的发送通道，而接收通道还允许继续接收对侧的数据，除非对侧也发起关闭连接；第一步发起方向对侧端发起结束请求，第二步接收方向发起方做确认响应，第三步，接收方也向发起方发起关闭连接请求，第四步，发起方对收到的结束请求予以确认响应，四步过后即完成 TCP 关闭连接。

1.5. 初始化请求

在 TCP 连接建立之后，客户端将向服务器端发起初始化请求，服务器端在收到请求后，将予以初始化响应，如下图所示，

14	2010-03-26 16:04:30.730260	198.120.0.184	198.120.0.93	MMS	Initiate Request
15	2010-03-26 16:04:30.748198	198.120.0.93	198.120.0.184	MMS	Initiate Response

初始化请求内容分析如下：

初始化请求主要用于通知服务器端，客户端所支持的服务类型，服务类型后括号中的数字为服务的编码，例如支持身份识别、文件服务（打开、读、关闭共同配合完成）、报告服务。

```

ISO/IEC 9506 MMS
Initiate Request (8)
Proposed MMS PDU Size: 32000
Proposed Outstanding Requests Calling: 30
Proposed Outstanding Requests Called: 250
Proposed Data Nesting Level: 5
Initiate Request Detail
MMS Version Number: 1
  Proposed Parameter CBBs:
    Proposed Parameter CBBs:
      Array Support [STR1] (0)
      Structure Support [STR2] (1)
      Named Variable support [VNAME] (2)
      Alternate Access Support [VALT] (3)
      Addressed Variable Support [VADR] (4)
      Third Party Service Support [TPY] (6)
      Named Variable List support [VLIS] (7)
  Services Supported Calling:
    Services Supported Calling:
      identify (2)
      fileopen (72)
      fileRead (73)
      fileClose (74)
      informationReport (79)

```

初始化响应内容分析如下：

初始化响应主要用于服务器端，为服务器端收到初始化请求后，通知服务器端所支持的类型，例如状态现报告服务、身份识别、读模型服务（读名称列表、读变量访问属性、读有名变量列表属性、读域名属性服务等）、读服务、写服务、文件服务（包含打开、读、关闭、重命名、删除、读文件列表等）、报告服务、终止服务、取消服务等等。

```

ISO/IEC 9506 MMS
Initiate Response (9)
Negotiated MMS PDU Size: 32000
Negotiated Max Outstanding Requests Calling: 5
Negotiated Outstanding Requests Called: 5
Negotiated Data Nesting Level: 5
Initiate Response Detail
MMS Version Number: 1
  Negotiated Parameter CBBs:
  Services Supported Called:
    Services Supported Called:
      status (0)
      getNameList (1)
      identify (2)
      read (4)
      write (5)
      getVariableAccessAttributes (6)
      defineNamedVariableList (11)
      getNamedVariableListAttributes (12)
      deleteNamedVariableList (13)
      getDomainAttributes (37)
      obtainFile (46)
      readJournal (65)
      initializeJournal (67)
      reportJournalStatus (68)
      getCapabilityList (71)
      fileopen (72)
      fileRead (73)
      fileClose (74)
      fileRename (75)
      fileDelete (76)
      fileDirectory (77)
      informationReport (79)
      conclude (83)
      cancel (84)

```

1.6. 读模型

读模型由多种服务配合完成，一般过程为读 VMD 下 LD 列表，读所有 LD 中的所有的名称列表，逐个 LN 的读变量访问属性，逐个 LN 的读值、读数据集。

读 LD 列表采用 GetNameList 服务，客户端发起读 VMD，服务器端以 LD 列表响应，如下图示：

读

响应

```

ISO/IEC 9506 MMS
  Conf Request (0)
  GetNameList (1)
  InvokeID: InvokeID: 1
  GetNameList
    extendedObjectClass
      OBJECT Class: Domain (9) 9
    objectScope
      vmdspecific

```

```

ISO/IEC 9506 MMS
  Conf Response (1)
  GetNameList (1)
  InvokeID: InvokeID: 1
  GetNameList
    ListofIdentifier
      PL2202BPROT1
      PL2202BCTRL1
      PL2202BPROT2
      PL2202BCTRL2
      PL2202BPROT3
      PL2202BCTRL3
      PL2202BPROT4
      PL2202BCTRL4
      PL2202BPROT5
      PL2202BCTRL5
      PL2202BSYNC1
      PL2202BGOLD1
      PL2202BGOLD2
    MoreFollows FALSE

```

读 LD 中有名列表页采用 GetNameList 服务，客户端发起读哪个 LD，服务器端响应，如下图示：

读

响应

```

ISO/IEC 9506 MMS
  Conf Request (0)
  GetNameList (1)
  InvokeID: InvokeID: 2
  GetNameList
    extendedObjectClass
      OBJECT Class: NamedVariable (0) 0
    objectScope
      PL2202BCTRL1

```



```

ISO/IEC 9506 MMS
Conf Response (1)
GetNameList (1)
InvokeID: InvokeID: 2
  GetNameList
    ListOfIdentifier
      LLNO
      LLNO$ST
      LLNO$ST$Mod
      LLNO$ST$Mod$stval
      LLNO$ST$Mod$q
      LLNO$ST$Mod$t
      LLNO$ST$Beh
      LLNO$ST$Beh$stval
      LLNO$ST$Beh$q
      LLNO$ST$Beh$t
      LLNO$ST$Health
      LLNO$ST$Health$stval
      LLNO$ST$Health$q
      LLNO$ST$Health$t
      LLNO$ST$Loc

```

读 LN 中变量访问属性采用 GetVarAccessAttributes 服务，客户端发起读哪个 LN，服务器端以变量访问属性响应，如下图所示：

读

响应

```

ISO/IEC 9506 MMS
Conf Request (0)
GetVariableAccessAttributes (6)
InvokeID: InvokeID: 3543
  GetVariableAccessAttributes
    Object Name
      Domain Specific
        DomainName:
          DomainName: PL2202BGOLD1
        ItemName:
          ItemName: GGIO40

```

```

ISO/IEC 9506 MMS
Conf Response (1)
GetVarAccessAttributes (6)
InvokeID: InvokeID: 3543
  GetVarAccessAttributes
    MMSDeletable FALSE
    TypeSpecification
      structure
        components
          ST
            typespecification
              structure
                components
                  Mod
                    typespecification
                  Beh
                    typespecification
                  Health
                    typespecification

```

读值采用 read 服务，客户端发起读哪个 LN 的哪个 FC，服务器端以值响应，如下图所示：

读

响应

```

ISO/IEC 9506 MMS
Conf Request (0)
Read (4)
InvokeID: InvokeID: 285
Read
  List of Variable
    VariableSpecification
      Object Name
        Domain Specific
          DomainName:
            DomainName: PL2202BCTRL1
          ItemName:
            ItemName: CKGGIO1$ST

```

```

ISO/IEC 9506 MMS
Conf Response (1)
Read (4)
InvokeID: InvokeID: 285
Read
  STRUCTURE
    STRUCTURE
      INTEGER: 1
    BITSTRING:
      BITSTRING:
        BITS 0000 - 0015: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    UTC
      UTC 2010-05-23 23:29.55.170000 Timequality: 0a
    STRUCTURE
    STRUCTURE

```

读数据集采用 GetNamedVariableListAttributes 服务，客户端发起读哪个 LD 的哪个数据集，服务器端以 FCDA 响应，如下图所示：

读

响应

```

ISO/IEC 9506 MMS
Conf Request (0)
GetNamedVariableListAttributes (12)
InvokeID: InvokeID: 8890
GetNamedVariableListAttributes
  Domain Specific
    DomainName:
      DomainName: PL2202BCTRL1
    ItemName:
      ItemName: LLN0$dsAin

```

```

ISO/IEC 9506 MMS
  Conf Response (1)
    GetNamedVariableListAttributes (12)
      InvokeID: InvokeID: 8890
      GetNamedVariableListAttributes
        MMS Deletable: FALSE
        List of Variable
          Object Name
            Domain Specific
              DomainName:
                DomainName: PL2202BCTRL1
              ItemName:
                ItemName: CKMMXU1$MX$HzBus$mag$f
          Object Name
          Object Name
          Object Name

```

1.7. 写控制块

在模型读取完毕后，将进入写控制块过程，其中最重要的一个就是控制块使能，这关乎到服务器端是否以报告形式响应客户端。

控制块使能，一般是先写取消使能，再写使能，如果写成功，将以肯定确认，如果写失败，将以否定确认，如下图示，

```

ISO/IEC 9506 MMS
  Conf Request (0)
    Write (5)
      InvokeID: InvokeID: 8986
      Write
        List of Variable
          Object Name
            Domain Specific
              DomainName:
                DomainName: PL2202BCTRL1
              ItemName:
                ItemName: LLN0$BR$brcbdIn0101$RptEna
        Data
          BOOLEAN: FALSE

```

```
ISO/IEC 9506 MMS
Conf Request (0)
write (5)
InvokeID: InvokeID: 8999
Write
List of Variable
Object Name
Domain Specific
DomainName:
DomainName: PL2202BCTRL1
ItemName:
ItemName: LLN0$BR$brcbdin0101$RptEna
Data
BOOLEAN: TRUE
```

其余写 RptID、EntryID 等过程与写 RptEna 过程一致，不再赘述。

1.8. 常见问题

①读模型不成功

分析：可在读失败的地方，查看是什么引起的失败，一般情况下，都是装置内模型有异常引起，例如，某个数据集中无 FCDA，即空数据集，此时可能引起模型读取失败；

②控制块使能不成功

分析：使能不成功可能是由于该实例已经被占用，例如某个客户端在未指定实例号的情况下，将会把服务器端所有实例注册掉，引起其他客户端不能注册实例；

③写完 EntryID 后，装置将缓存的历史信息又上送一遍

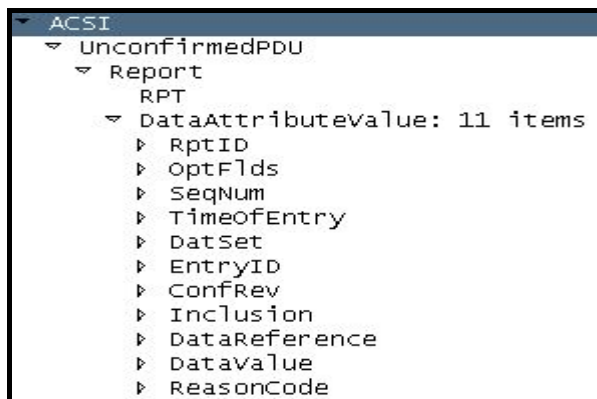
分析：写 EntryID 的目的，是在通讯恢复后补采集该 EntryID 之后的报告，但如果写下去的 EntryID 得值为全 0，那势必引起服务器端将所有缓存中的报告上送一遍；

2. 报告

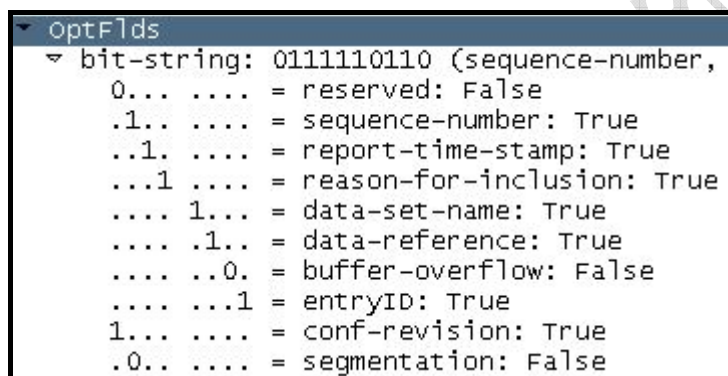
2.1. ACSI 中的报告

在 ACSI 中，server 端以报告的形式来传递信息，诸如状态值、测量值、控制的返回信息等等，一个报告包含必选项及可选项，必选项有 RptID、OptFlds、Inclusion、DataValue，可选项由必选项中的 OptFlds 内容决定。

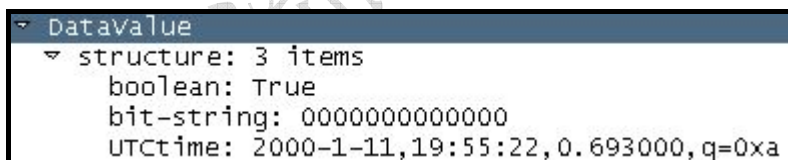
下图为 ACSI 中的一个报告，在数据属性值中包含 11 个属性值，属性值的个数随 OptFlds 中的值变化而变化。



OptFlds 共包含十个选项，分别为（保留项、序号、时标、传输原因、数据集名称、数据引用名、缓冲区满、入口标识、配置版本、分段），如下图所示：



数据值一般为结构体，包含数据值、品质、UTC 时间等如下图



2.2. MMS 中的报告

ACSI 中的报告是基于抽象通讯的，不具有实际通讯手段，故在 8-1 中，将 ACSI 模型一一映射到现有的工业自动化系统《制造报文规范（MMS）》中，通过现有的 MMS 通讯来实现抽象通讯。

下图为 MMS 中的一个报告，ACSI 中的 Report 映射为 MMS 中的 informationReport，数据属性值映射为访问结果列表，

```

ISO/IEC 9506 MMS
Unconfirmed (3)
  InformationReport
    VariableList
      RPT
    AccessResults
      VSTRING:
        brcbCommState04
      BITSTRING:
        BITSTRING:
          BITS 0000 - 0015: 0 1 1 1 1 1 0 1 1 0
          UNSIGNED: 2
      BTIME
        BTIME 2000-01-11 19:55:22.038 (days=5854 msec= 71722038)
      VSTRING:
        PCS31ACTRL4/LLN0$dsCommState
      OSTRING:
        OSTRING: 01 00 00 00 00 00 00 00
        UNSIGNED: 1
      BITSTRING:
        BITSTRING:
          BITS 0000 - 0015: 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
          BITS 0016 - 0031: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
          BITS 0032 - 0047: 0
      VSTRING:
        PCS31ACTRL4/GGIO27$ST$A1m6
      STRUCTURE
        BOOLEAN: FALSE
      BITSTRING:
        BITSTRING:
          BITS 0000 - 0015: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
          UTC

```

访问结果列表内容如下：

条目 1: RptID, 报告 ID, 表示该报告的报告控制块 ID

条目 2: OptFlds, 选择域, 用以标识该报告包含哪些可选项, 该值一般由客户端程序统一写入服务器;

条目 3: SeqNum, 同一报告控制块所对应报告的顺序编号

条目 4: TimeOfEntry, 报告产生时的时标

条目 5: DatSet, 该报告控制块所对应的数据集引用名

条目 6: EntryID, 入口标识, 同一 IED 下, 所有报告的顺序号, 每个报告均不重复

条目 7: ConfRev, 配置版本, 目前在 MMS 通讯中暂无用处, 固定填 1

条目 8: Inclusion, 数据集所包含 FCDA 个数, 一个 bit 对应一个 FCDA, 值为 1 的 bit, 表示报告中有该 bit 对应的 FCDA 值。值为 0 的 bit, 表示报告中, 不含该 bit 所对应的 FCDA 值

条目 9: DataReference, 数据引用名, 报告中值所对应的数据应用名

条目 10: DataValue, 数据值, 值为一个结构, 一般包含数据值、品质、UTC 时间等属性, UTC 时间为 FCDA 值变化时的时间, 可理解为 SOE 时间。

条目 11: ReasonCode, 传送原因, 表示报告上送某 FCDA 的原因, 常用的有数据变化、周期、总召三种, 所对应的编码, 6 个 bit 从左往右依次为: 预留、数据变化、品质变化、数据更新、周期、总召。不同的位为 1, 表示不同的原因, 多数情况下为单原因上送, 但也可能存在多原因上送。

2.3. 常见问题

①装置上有遥信、遥测变化、但后台、远动收不到

分析: 在网络上抓包, 看服务器侧是否发出相应报告, 如果有, 则需要查看报文中各条目的值与客户端中的值是否一致, 多数情况下, 都是因为报告中的部分条目值有误引起的;

3. 控制

3.1. ACSI 中的控制报文

在 ACSI 中, 最常用的控制类型是加强型选择控制, 由带值选择、取消、执行三种服务共同完成。

如下图所示: 带值选择服务报文, 如果服务器端支持该选择, 将以肯定确认响应, 否则将以否定确认响应, 并给出否定响应的原因, SBOW 模型的数据属性值为一个结构体, 共包含 6 个变量:

第一个变量值为控制值 (False 为分, True 为合);

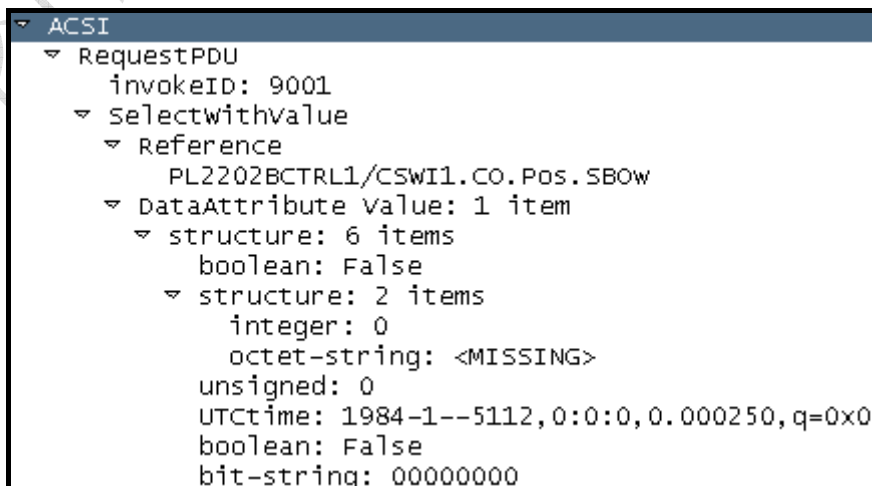
第二个变量为源发者, 是个结构体, 包含源发者类型及源发者标识;

第三个变量为控制序号, 标识该对象的控制次数, 每发起一次成功的控制过程, 该序号加 1;

第四个变量为发起控制时的 UTC 时标;

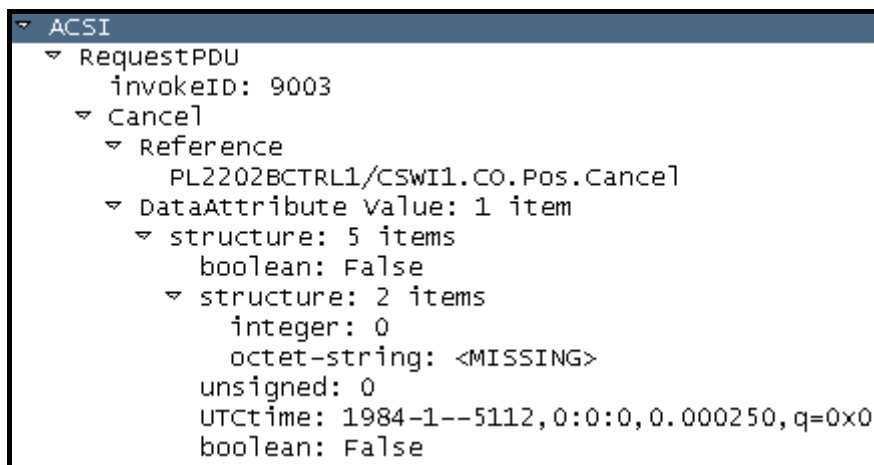
第五个变量为检修标识 (False 为非检修, True 为置检修)

第六个变量为校验位 check, 从左往右依次为检同期、检联锁、检无压、一般遥控、不检、其余位保留。IEC61850 标准中仅定义了 2 个 bit, 此处客户端进行了扩展, 扩展为 8 个 bit;

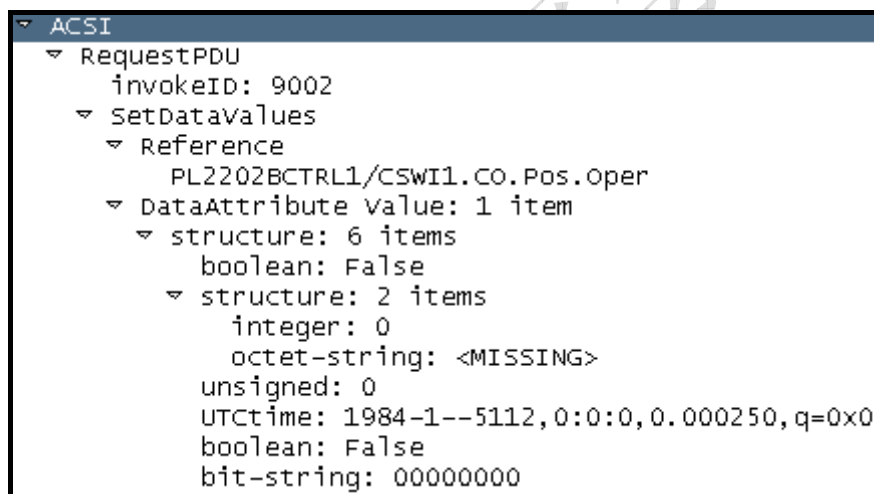


```
ACSI
  RequestPDU
    invokeID: 9001
    selectwithvalue
      Reference
        PL2202BCTRL1/CSWI1.CO.Pos.SBOW
      DataAttribute value: 1 item
        structure: 6 items
          boolean: False
          structure: 2 items
            integer: 0
            octet-string: <MISSING>
          unsigned: 0
          UTctime: 1984-1--5112,0:0:0,0.000250,q=0x0
          boolean: False
          bit-string: 00000000
```

如下图示，取消服务：Cancel 模型的数据属性值为一个结构体，共包含 5 个变量，仅比 SBOW 模型少了校验位，其余与 SBOW 模型一致



如下图示，执行服务：Oper 模型的数据属性值为一个结构体，共包含 6 个变量，仅与 SBOW 模型完全一致



3.2. MMS 中的控制报文

ACSI 中的控制服务也需要映射到 MMS 规范中，通过现有的 MMS 通讯体系来实现抽象通讯。

对于带值选择服务，若选择写成功，则可以继续发执行写；若选择写不成功，服务器端将以 LastAppError 报告响应客户端，控制过程结束；

对于执行服务，如果执行写成功，服务器端将以命令结束服务报告（Oper 的镜像报文）响应客户端；如果执行写不成功，服务器端将以 LastAppError 报告响应客户端，控制过程结束；

对于取消服务，如果取消写成功，则控制过程结束；如果取消写失败，服务器端将以 LastAppError 报告响应客户端，控制过程结束；

如下图：带值选择服务，MMS 控制报文由变量列表和数据两部分组成；变量列表有域名和项目

名两部分，组合起来确定控制对象；Data 则为对象的控制值，该值为一个复合结构体；该结构体成员数据的类型见报文所示，控制值为布尔量，源发者为结构体，控制序号为无符号单字节整型数据，检修标识为布尔量，时标为 UTC 时间（包含时间品质），check 位为位串数据。

```

ISO/IEC 9506 MMS
Conf Request (0)
write (5)
InvokeID: InvokeID: 9001
write
  List of Variable
    Object Name
      Domain Specific
        DomainName:
          DomainName: PL2202BCTRL1
        ItemName:
          ItemName: CSWI1$CO$Pos$SBOW
    Data
      STRUCTURE
        BOOLEAN: FALSE
        STRUCTURE
          INTEGER: 0
          OSTRING:
          UNSIGNED: 0
        UTC
          UTC 1970-01-01 00:00.0.000250 Timequality: 00
        BOOLEAN: FALSE
        BITSTRING:
          BITSTRING:
            BITS 0000 - 0015: 0 0 0 0 0 0 0 0
  
```

如下图：取消服务，类似于 SBOW，仅在数据中无 check 位，因为取消选择可以不需要 check 位；

```

ISO/IEC 9506 MMS
Conf Request (0)
write (5)
InvokeID: InvokeID: 9003
write
  List of Variable
    Object Name
      Domain Specific
        DomainName:
          DomainName: PL2202BCTRL1
        ItemName:
          ItemName: CSWI1$CO$Pos$Cancel
    Data
      STRUCTURE
        BOOLEAN: FALSE
        STRUCTURE
          INTEGER: 0
          OSTRING:
          UNSIGNED: 0
        UTC
          UTC 1970-01-01 00:00.0.000250 Timequality: 00
        BOOLEAN: FALSE
  
```

如下图：执行服务报文结构与带值选择报文结构一致；

```

ISO/IEC 9506 MMS
Conf Request (0)
write (5)
InvokeID: InvokeID: 9002
write
  List of Variable
    Object Name
      Domain Specific
        DomainName:
          DomainName: PL2202BCTRL1
        ItemName:
          ItemName: CSWI1$CO$Pos$Oper
    Data
      STRUCTURE
        BOOLEAN: FALSE
        STRUCTURE
          INTEGER: 0
          OSTRING:
        UNSIGNED: 0
      UTC
        UTC 1970-01-01 00:00.0.000250 Timequality: 00
        BOOLEAN: FALSE
      BITSTRING:
        BITSTRING:
          BITS 0000 - 0015: 0 0 0 0 0 0 0 0

```

如下图时，当写失败时，服务器端响应的 LastAppError 报告，报告由变量列表和访问结果组成，变量列表定义了该报告为 LastAppError，访问结果是一个结构体，包含 5 个数据值，分别为控制对象、错误、源发者、控制序号、额外原因。

```

ISO/IEC 9506 MMS
Unconfirmed (3)
InformationReport (0)
InformationReport
  List of Variable
    Object Name
      LastAppError
  AccessResults
    STRUCTURE
      VSTRING:
        PL2202BCTRL1/CSWI1$CO$Pos$Cancel
      INTEGER: 1
    STRUCTURE
      INTEGER: 0
      OSTRING:
      UNSIGNED: 0
      INTEGER: 18

```

错误的数据类型为枚举类型，Error 的值分别为{(0) 正常、(1)未知、(2)超时测试失败、(3)操作测试失败}。

额外原因的数据类型为枚举类型，AddCause 的值编码见下表

MMS 值	ACSI 值
0	未知原因 (Unknown)

1	不支持 (not-supported)
2	被开关闭锁 (Blocked-by-switching-hierarchy)
3	选择失败 (Select-failed)
4	无效的位置 (Invalid-position) (例如对控制对象的属性值为无效时)
5	位置达到 (Position-reached) (例如对已在合位的开关进行合操作)
6	执行中参数改变 (Parameter-change-in-execution) (例如执行过程中参数发生变化,)
7	步限制 (Step-limit) (例如档位值已到最大或最小值)
8	被模型闭锁 (Blocked-by-Mode) (例如模型中 LN 的 ctlModel 值为非控制值)
9	被过程闭锁 (Blocked-by-process) (例如过程层异常)
10	被联锁闭锁 (Blocked-by-interlocking) (例如联锁条件不满足)
11	被检同期闭锁 (Blocked-by-synchrocheck) (例如检同期合闸时, 同期条件不满足)
12	命令已经在执行中 (Command-already-in-execution) (例如在发遥控执行后, 又发遥控取消)
13	被健康状况所闭锁 (Blocked-by-health) (例如 health 值异常引起闭锁,)
14	1 对 n 控制 (1-of-n-control)
15	被取消终止 (Abortion-by-cancel) (例如取消引起的终止)
16	时间限制结束 (Time-limit-over) (例如遥控执行超时后)
17	被陷阱异常中止 (Abortion-by-trip) (例如在遥控选择之后执行之前发生跳闸, 跳闸后再执行)
18	对象未被选择 (Object-not-selected) (例如未选择对象, 直接控制)

3.3. 常见问题

①在控制不成功时的分析思路

分析：当选择或执行不成功时，应根据 LastAppError 中 AddCause 的值予以分析，如果 AddCause 的值为 0，那么多数情况下为装置内部原因，此时需查看装置上操作记录中的失败原因。

三、 如何看 GOOSE 报文

1. GOOSE 报文传输机制

IEC61850-7-2 定义的GOOSE 服务模型使系统范围内快速、可靠地传输输入、输出数据值成为可能。在稳态情况下，GOOSE服务器将稳定的以T0时间间隔循环发送GOOSE报文，当有事件变化时，

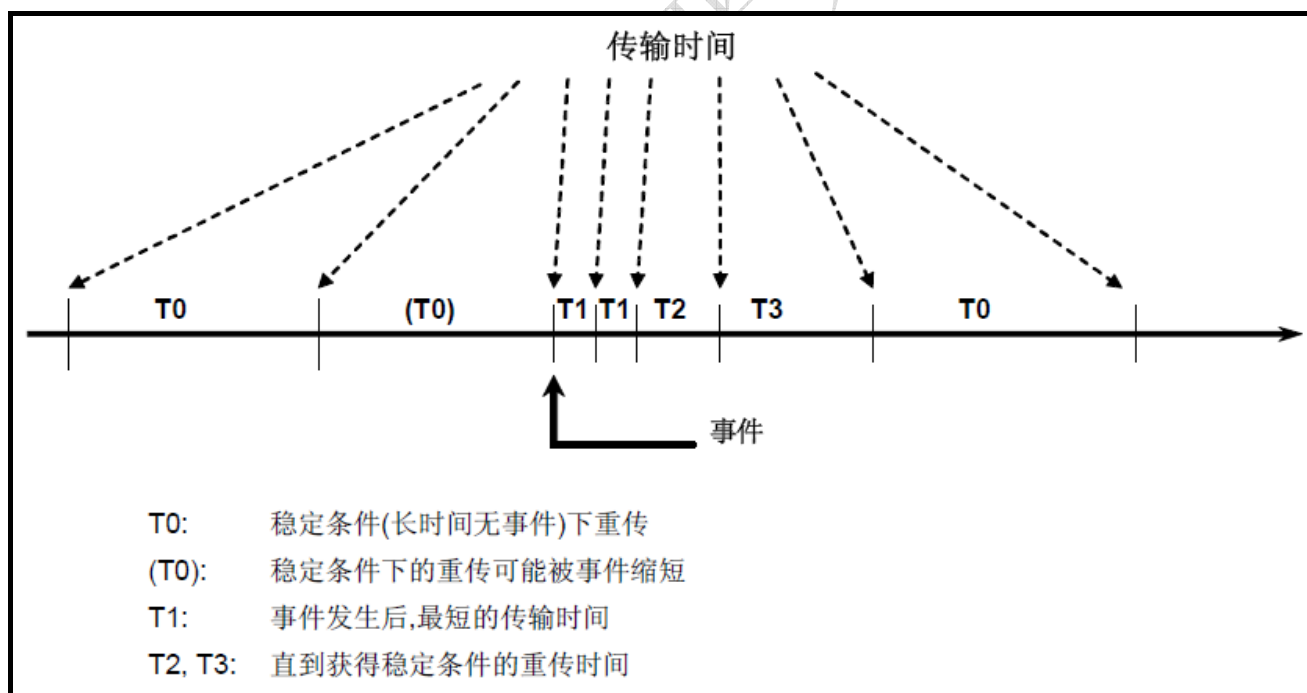
GOOSE 服务器将立即发送事件变化报文，此时T0时间间隔将被缩短；在变化事件发送完成一次后，GOOSE服务器将以最短时间间隔T1，快速重传两次变化报文；在三次快速传输完成后，GOOSE服务器将以T2、T3时间间隔各传输一次变位报文；最后GOOSE服务器又将进入稳态传输过程，以T0时间间隔循环发送GOOSE报文。

在 GOOSE 传输机制中，有两个重要参数 StateNumber 和 SequenceNumber，StateNumber (0~4294967295) 反映出GOOSE报文中数据值与上一帧报文数据值是否有变化，SequenceNumber (0~4294967295) 反映出在无变化事件情况下，GOOSE报文发送的次数。

当GOOSE服务器产生一次变化事件时，StateNumber值将自动加1（到最大值后，将归0重新开始计数），同时SequenceNumber归0；当GOOSE服务器无变化事件时，StateNumber值将保持不变，在每发送一次GOOSE报文后，SequenceNumber值将加1（到最大值后，将归0重新开始计数）

GOOSE服务器通过重发相同数据来获得额外的可靠性，比如通过增加SeqNum 和不同传输时间。

如下图所示：对GOOSE传输这个过程进行了示意。



2. GOOSE 信号传输

GOOSE 服务器传输 GOOSE 报文，都是以数据集形式发送，一帧报文对应一个数据集，一次发送，将整个数据集中所有数据值同时发送。

GOOSE 跳闸、遥控、遥信采集、遥测采集报文传输过程完全一致，在此仅以 GOOSE 跳闸为例进行说明。

如下图所示：某个 GOOSE 服务器发出的 GOOSE 跳闸报文

一帧 GOOSE 报文由 AppID、PDU 长度、保留字 1、保留字 2、PDU 组成，其中 PDU 为可变长度，由数据集中 FCDA 的个数决定，每个 FCDA 在报文中占 3 个字节。

AppID: GOOSE 报文的 AppID 范围为 0x0000~0x3fff，其值来源于 GOOSE 配置文本中目的地址中的 Appid。

PDU 长度：从 AppID 开始计数到 PDU 结束的全部字节长度。

保留字：两个保留字值默认为 0x0000。

PDU：协议数据单元，其中包含报告控制块信息及数据信息。

PDU 控制块信息如下：

控制块引用名：来源于 GOOSE 文本中控制块的 GoCBRef。

允许生存时间：该报文在网络上允许生存的时间，超时后收到的报文将被丢弃，主要受交换机报文交换延时影响。

数据集引用名：控制块对应的数据集引用名，来源于 GOOSE 文本中控制块的 DataSet。

GOOSEID: GOOSE 控制块 ID，来源于 GOOSE 文本中控制块的 AppID。

事件时标：该帧报文产生的时间。

状态号：范围 0~4294967295，从 0 开始，每产生一次变化数据，该值加 1。

序号：范围 0~4294967295，从 0 开始，每发送一次 GOOSE 报文，该值加 1。

TEST：检修标识，表示 GOOSE 服务器的检修状态。

配置版本：来源于 GOOSE 文本中控制块的 ConfRev，可在 GOOSEID 文本中配置，默认为 1。

Needs Commissioning：暂时未使用到。

数据集条目数：控制对应的数据集中的条目数。

数据：数据集中每个数据的实时值。

```
IEC 61850 GOOSE
AppID*: 282
PDU Length*: 150
Reserved1*: 0x0000
Reserved2*: 0x0000
PDU
  IEC GOOSE
  {
    Control Block Reference*: PB5031BGOLD/LLN0$GO$gocb0
    Time Allowed to Live (msec): 10000
    DataSetReference*: PB5031BGOLD/LLN0$dsGOOSE0
    GOOSEID*: PB5031BGOLD/LLN0$GO$gocb0
    Event Timestamp: 2008-12-27 13:38.46.222997 Timequality: 0a
    StateNumber*: 2
    Sequence Number: 0
    Test*: TRUE
    Config Revision*: 1
    Needs Commissioning*: FALSE
    Number Dataset Entries: 8
    Data
    {
      BOOLEAN: TRUE
      BOOLEAN: FALSE
      BOOLEAN: FALSE
    }
  }
```

3. 常见问题

①测控收不到智能终端传输来的遥信或保护已跳闸，智能终端未跳闸

分析：通过网络抓包工具，在线抓取 GOOSEID 报文，查看是否有变位报文传送，同时检查报文中的检修标识值与接收装置的检修状态是否一致，GOOSEID 传输中，要求发送侧与接收侧，只有在检修状态一致的情况下，才认为数据有效。

四、 如何看 SMV 报文

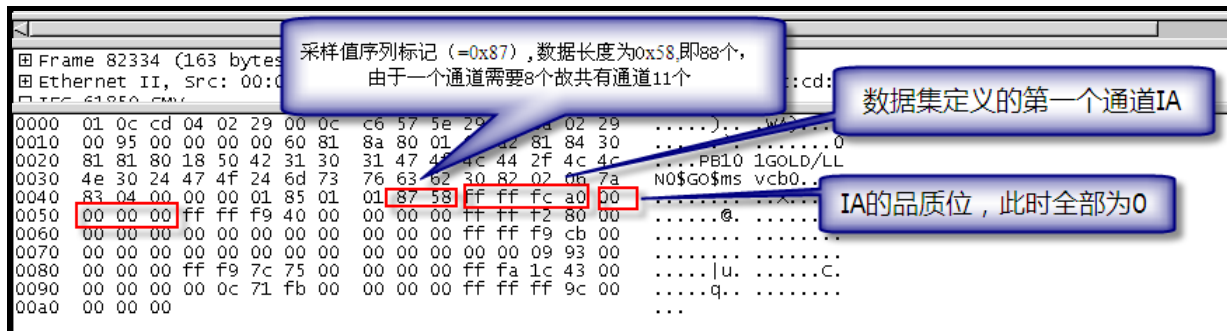
目前采样值传输有三种标准（60044-8，9-1，9-2），其中 60044-8 标准最简单，点对点通讯，报文传输采用固定通道模式，报文传输延时确定，技术成熟可靠，但需要铺设大量点对点光纤；9-1 标准，技术先进，通道数可配置，报文传输延时确定，需外部时钟进行同步，但仍为点对点通讯，且软硬件实现较复杂，属于中间过度标准；9-2 标准，技术先进，通道数可灵活配置，组网通讯，需外部时钟进行同步，但报文传输延时不确定，对交换机的依赖度很高，且软硬件实现较复杂，技术尚未普及。

三种标准中，9-2 是未来的方向，现仅以 9-2 传输报文为例。

1. 9-2 报文

工程实施过程中，9-2 抓包可使用 MMS-ethreal、EPT61850 来抓取，但两个工具均不支持对采样值数据内容的解析，所以我们需要直接通过原始数据帧来分析，一般来讲，我们需要从采样值序

列标记 (0x87) 看起, 0x87 之后为数据长度, 例如对于 12 通道的为 0x60, 对于 11 通道为 0x58, 这里一个通道为 8 个字节, 前 4 个字节为数值, 后 4 个字节为品质, 我们可以通过个办法依次找到每个通道的具体值。



品质位共 4 字节, 如下图示

7	6	5	4	3	2	1	0
默认 0x00							
默认 0x00							
			OpB	检修	源	细化品质	
细化品质						有效性	

品质位仅使用 Validity、Test 属性, 其他属性暂不考虑。即 00000001 为无效, 这个无效位由 MU 置无效, 目前 MU 做法不一, 有些 MU 在失步时即置无效, 有些 MU 如电子互感器合并单元在没有接上电子互感器及硬件故障会置无效; 00000800 即为检修, 当检修压板投入时, 置检修位, 大比例变的 MU 检修逻辑是当 MU 和保护的检修位一致时, 保护动作。

源地址（目前在config中可配）

目的地址即组播地址

应用标识

SVID

计数器，目前程序中都是1秒中MU中送出4000帧，Samplecount循环记录从0到3999，在整4000处清零

同步标志，由MU置同步标志，大母变采用1588定时，当MU没有收到同步报文时则进入守时模式，当偏差超过 $\pm 4\mu s$ 时，则退出守时模式，置失步标志即此处显示False

No.	Time	Source	Destination	Protocol	Info
1	2009-10-24 18:33:32.607007	00:0c:c6:57:5e:29	01:0c:cd:04:02:29	IECSMV	SMV 9-2 Publish
7	2009-10-24 18:33:32.607256	00:0c:c6:57:5e:29	01:0c:cd:04:02:29	IECSMV	SMV 9-2 Publish
13	2009-10-24 18:33:32.607506	00:0c:c6:57:5e:29	01:0c:cd:04:02:29	IECSMV	SMV 9-2 Publish
19	2009-10-24 18:33:32.607758	00:0c:c6:57:5e:29	01:0c:cd:04:02:29	IECSMV	SMV 9-2 Publish

```

AppID*: 0x0229
PDU Length*: 149
Reserved1*: 0x0000
Reserved2*: 0x0000
SMV 9-2
{
  Number of ASDU: 1
  Start of ASDU
  {
    ASDU
    {
      ID*: PB10GOLD/LLNO$GO$msvcb0
      Sample Count: 3594
      Config Rev*: 1
      Sample Synched*: TRUE
      Samples {
      }
    }
  }
}
0000 01 0c cd 04 02 29 00 0c c6 57 5e 29 88 1b a2 81 84 30 .....(..WA)...)
0010 00 95 00 00 00 00 60 81 8a 80 01 01 a2 81 84 30 .....0
0020 81 81 80 18 50 42 31 30 31 47 4f 4c 44 2f 4c 4c ....PB10 1GOLD/LL
0030 4e 30 24 47 4f 24 6d 73 76 63 62 30 82 02 06 7a NO$GO$ms vcb0...Z
0040 83 04 00 00 00 01 85 01 01 87 58 ff ff fc a0 00 .....X.....
0050 00 00 00 ff ff f9 40 00 00 00 00 ff ff f2 80 00 .....@.....
0060 00 00 00 00 00 00 00 00 00 00 00 ff ff f9 cb 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 09 93 00 .....
0080 00 00 00 ff f9 7c 75 00 00 00 00 ff fa 1c 43 00 .....|u.....C.
0090 00 00 00 00 0c 71 fb 00 00 00 00 ff ff ff 9c 00 .....q.....
00a0 00 00 00
  
```

对于数值，由于 9-2 里面 20ms 内采样有 80 个点，且都是一次值的瞬时值，所以看起来不太好看，我们一般先找到峰值，然后算出其有效值，如下图示，0x000c71fb，换算成二进制为 815611，即 $815611 \times 10\text{mV}$ (8.15611kV)，再换算成有效值为 5.768kV。

注意：电压的精度为 10mV，电流的精度为 1mA。

0C71FB折十进制为815611，因为电压以10mV为精度，所以为8.15611kV，折成有效值为5.77kV

0000	01 0c cd 04 02 29 00 0c c6 57 5e 29 88 ba 02 29(..WA)....)
0010	00 95 00 00 00 00 60 81 8a 80 01 01 a2 81 84 300
0020	81 81 80 18 50 42 31 30 31 47 4f 4c 44 2f 4c 4cPB10 1GOLD/LL
0030	4e 30 24 47 4f 24 6d 73 76 63 62 30 82 02 06 7a	NO\$GO\$ms vcb0...Z
0040	83 04 00 00 00 01 85 01 01 87 58 ff ff fc a0 00X.....
0050	00 00 00 ff ff f9 40 00 00 00 00 ff ff f2 80 00@.....
0060	00 00 00 00 00 00 00 00 00 00 00 ff ff f9 cb 00
0070	00 00 00 00 00 00 00 00 00 00 00 00 09 93 00
0080	00 00 00 ff f9 7c 75 00 00 00 00 ff fa 1c 43 00 u.....C.
0090	00 00 00 00 0c 71 fb 00 00 00 00 ff ff ff 9c 00q.....
00a0	00 00 00	...

这里正数用原码表示，负数用补码表示，即对正数按位取反，如下图对 9611 这台 MU 而言，其一个周波的波谷为 0xFFFF38ECB，将其减 1，后取反得 0xc7135 即 815413，表示 -8.15413kV。

0000	01	0c	cd	04	02	29	00	0c	c6	57	5e	29	88	ba	02	29). .wA)...)
0010	00	95	00	00	00	00	60	81	8a	80	01	01	a2	81	84	300
0020	81	81	80	18	50	42	31	30	31	47	4f	4c	44	2f	4c	4cPB10 1GOLD/LL
0030	4e	30	24	47	4f	24	6d	73	76	63	62	30	82	02	06	a3	N0\$G0\$ms vcb0...
0040	83	04	00	00	00	01	85	01	01	87	58	ff	ff	f9	40	00X...@.
0050	00	00	00	00	00	06	bf	00	00	00	00	00	00	00	00	00
0060	00	00	00	ff	ff	f9	40	00	00	00	00	ff	ff	f6	4a	00@.J.
0070	00	00	00	ff	ff	ff	98	00	00	00	00	ff	ff	f9	86	00
0080	00	00	00	00	05	a8	c2	00	00	00	00	00	06	bb	04	00
0090	00	00	00	ff	f3	8e	cb	00	00	00	00	00	00	00	00	00
00a0	00	00	00														...

电压最低值

2. 常见问题

① r XXX

分析：