第36卷 第12期
2008年6月16日

电力系统保护与控制
Power System Protection and Control

Vol.36 No.12
June 16, 2008

IEC 61850标准中MMS映射分析及其编码/解码模块的设计

丁 力，王晓茹，王 林

（西南交通大学电气工程学院，四川 成都 610031）

摘要： 分析了IEC 61850标准和制造报文规范（MMS）之间模型和服务的映射关系。在分析ASN.1的BER编码规则的基础上，提出了MMS编码/解码模块的设计方案，实现MMS协议数据单元（PDU）的ASN.1抽象语法和传送语法之间的转换。基于该模块，编写一个简单的程序，实现了IEC 61850应用层报文编码/解码，分析了具体MMS报文的编码/解码过程。

关键词： IEC 61850； 特定通信服务映射（SCSM）； 制造报文规范（MMS）； ASN.1； 编码/解码

MMS mapping analysis and encoding/decoding module design in IEC 61850

DING Li, WANG Xiao-ru, WANG Lin

(School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: This paper analyzes mapping relationships between IEC 61850 standard and Manufacturing Message Specification (MMS) on model and service. On the basis of analysis on ASN.1's basic encoding rules (BER), a design scheme for MMS encoding/decoding module is brought forward, which is used for conversion between ASN.1 abstract syntax and transfer syntax of MMS Protocol Data Units (PDU). A simple encoding/decoding program is finished based on this module, and application message encoding/decoding is implemented. At last, the encoding/decoding of an MMS data flow is analyzed.

Key words: IEC 61850; specific communication service mapping (SCSM); manufacturing message specification (MMS); ASN.1; encoding/decoding

中图分类号： TM76 文献标识码： B 文章编号： 1674-3415(2008)12-0069-05

0 引言

电力系统自动化各种装置运行着不同的操作系统和通信协议，是一个典型的异构系统，存在信息孤岛问题[1,2]。制造报文规范（MMS）是应用层的一个协议标准，主要用于生产设备间控制信息的传送。MMS 规范了多厂商设备间的通信，为制造设备入网提供方便。IEC 61850 标准把 MMS 引入电力系统自动化，将 ACSI 核心服务映射到 MMS，可以有效地实现异构系统通信，解决信息孤岛问题。

ACSI核心服务到MMS映射的关键技术是MMS协议数据单元（PDU）抽象语法和传送语法之间的转换，即MMS编码/解码[3,4]。目前国内电力自动化厂家开发生产IEC 61850产品都需要购买SISCO公司的编码/解码模块，研究MMS编码/解码对实现IEC 61850产品关键技术国产化有重要意义。

MMS 规范（国际标准 ISO/IEC9506，国家标准 GB/T16720）由（1）服务规范、（2）协议规范、（3）机器人伴同规范、（4）数字控制器伴同规范、（5）可编程逻辑控制器伴同规范、（6）过程控制系统伴同规范六部分组成，其中（1）服务规范和（2）协议规范是基础规范，（3）~（6）则是用于不同领域的配套规范。IEC 61850 只使用了基础规范，IEC 61850映射的MMS对象和服务是MMS标准的一部分，即 MMS 的一个协议子集。

1 IEC 61850到MMS的映射

1.1 ACSI核心服务的OSI模型

IEC 61850把OSI参考模型分成应用协议集（A-PROFILES）和传输协议集（T-PROFILES）两部分，如图1所示[5]：

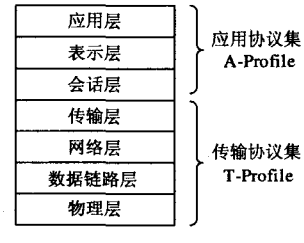

图1 OSI参考模型和协议集

Fig. 1 OSI reference model and profiles

应用协议集是OSI参考模型上3层（应用层、表示层和会话层）规范和协议的集合。传输协议集是OSI参考模型下4层（传输层、网络层、数据链路层和物理层）规范和协议的集合。

IEC 61850-8-1规定了四种通信协议集：客户/服务器服务，GSE和管理GOOSE服务，GSSE服务，时间同步。客户/服务器服务通信协议集是ACSI核心服务（包含大部分ACSI服务）的映射方式，故本文重点讨论这种通信协议集。

在客户/服务器服务协议集中，规定了两种传输协议集，TCP/IP方式和OSI方式。由于TCP/IP在LAN/WAN上广泛的使用，使得TCP/IP成了事实上的标准，而且各种软件平台和开发环境对TCP/IP通信也有良好的支持，所以TCP/IP方式是一种便于开发的选择。所以目前基本上所有的研究开发应用都建立在 MMS+TCP/IP+RFC1006 架构的基础上，如图2所示。

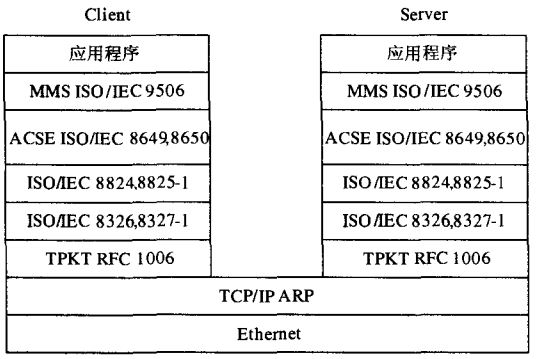

图 2 MMS+TCP/IP+RFC1006 架构

Fig. 2 MMS+TCP/IP+RFC1006 frame

1.2 IEC 61850到MMS的映射

MMS 广泛应用于工业生产领域，是非常庞大的一个协议集，定义了各种模型和服务。IEC 61850只应用了 MMS 基础规范的其中一部分。模型主要包括环境（Content）、虚拟制造设备（VMD）、域（Domain）、有名变量（Named Variable）、有名变量列表（Named Variable List）、日志（Journal）和文件管理（File Management）模型[5]。IEC 61850模型到 MMS 模型的映射关系见表 1。

环境服务主要用于建立和中止 MMS 用户之间的联接，包括服务有：以正常方式结束与另一用户的通信，以中断方式停止与用另一用户的通信；取消服务请求，拒绝服务。只有建立了联接，才可应用引用其它的服务。VMD 服务允许用户获取 VMD 的状态，用户可以通过这类服务查询 VMD 的各种特征，包括 VMD 服务的内容、级别和可以申请的资源等。域是 MMS 中的一个重要概念，表示了某种特定应用的 VMD 的资源子集。域可以是动态的，也可以是静态的。动态的域由 MMS 服务或者局部动作进行创建和删除。有名变量和有名变量列表提供的服务包括数据值的访问和修改，获取数据定义和属性。日志管理服务向 MMS 客户提供对日志进行操作的能力，允许客户记录和检索按时间顺序发生的有关事件及有关的变量，从而可以使得 MMS 客户了解事件之间的关系。文件服务提供对文件的打开、关闭、读、写、获得、重新命名、删除等操作。

表 1 IEC 61850 到 MMS 的对象映射

Tab. 1 Object mapping from IEC 61850 to MMS

IEC 61850 模型/控制块	MMS 模型
关联（Association）	上下文（Content）
服务器（Server）	虚拟制造设备（VMD）
逻辑设备类（LogicalDevice Class）	域模型（Domain）
逻辑结点类（LogicalNode Class）	有名变量（NamedVariable）
数据类（DATA Class）	
报告控制块（RCB）	
日志控制块（LCB）	
设置组控制块（SGCB）	
控制（CONTROL）	
数据集（DataSet）	有名变量列表（NamedVariableList）
记录（Log）	日志（Journal）
文件（File）	文件（File）

在 MMS 的数据模型中，虚拟制造设备 VMD 中包含域对象、变量对象、变量列表对象等。变量对象和变量列表对象可以具有域特定范围属性或者 VMD 特定范围属性。在 MMS 的数据模型中最多只能表示对象的 3 层的隶属关系。在 IEC 61850 模型中，服务器中包含逻辑设备，逻辑设备中包含逻辑节点，逻辑节点中包含数据，数据中包含数据属性，数据属性也可能包含其他数据属性，对象的隶属层次很多。由于隶属层次的差别，MMS 模型和 IEC 61850 模型之间无法直接建立映射关系。IEC 61850 通过在变量或者变量列表的名称中分出层次关系来解决了这一问题，逻辑设备和逻辑节点之间加入了“/”符号，不同层次的变量名称之间加入了“$”符号，这样通过对象的名称，就可以区分数据模型中对象的层次关系。

2 ASN.1 抽象语法表示和 BER 编码规则

2.1 ASN.1

ASN.1是一种对分布计算机系统之间交换的数

据进行抽象描述的规范化语言，是位于表示层的语言，通过抽象语法以及编码/解码规则的定义，从而实现不同系统之间的通信，独立于机器以及通讯媒介。它可分为两个部分，即语法规则和编码规则。语法规则[6~8]：从数据类型、内容顺序或结构等方面来描述消息的内容；编码规则：如何表示实际消息中的数据。经ASN.1描述的信息独立于任何应用环境，不会因为应用环境的不同而引起二义性的解释，从而为不同环境中的应用实体之间的通信奠定了基础。ASN.1提供了多种编码规则：BER（Basic Encoding Rules），DER（Distinguished Encoding Rules），CER（Canonical Encoding Rules），PER（Packet Encoding Rules）等。IEC 61850在MMS编码/解码中使用的是BER基本编码规则。

作为一种高级抽象描述语言，ASN.1具有以下特点：

（1）与平台和编程语言无关。它以一种高度抽象的形式表示数据结构信息。当需要在计算机网络里传输数据结构信息时，ASN.1提供相应的编解码规则，通过相应的位模式来传递数据结构信息。

（2）ASN.1使不同组织制定的标准协议都采用相同的规范表示形式，确保了互操作性。

（3）ASN.1提供了丰富的数据结构和灵活的扩展机制，因此可以描述非常复杂的协议内容。

（4）利用ASN.1开发的某个产品的最新版本可以很好地兼容早期版本。

2.2 BER基本编码规则

ASN.1 的基本编码规则 BER 的编码结构由 3 部分构成：（1）标签八位位组，（2）长度八位位组，（3）内容八位位组，一般称为 ASN. 1 编码的 TLV 结构[8]。标签用来区分类型和负责内容的解释。长度用来说明内容的长度。内容是数据单元的实体，包括了数据单元中准备传送的主要信息。

标签八位位组：由类型（Class）、格式（Form）、标签编号（Tag Code）组成，如图 3 所示。

bit7	bit6	bit5	bit4	bit3	Bit2	bit1	bit0
类型		格式	标签编号				

图 3 标签八位位组格式

Fig. 3 Tag octet format

标签的类型可以分为通用类、应用类、上下文特定类和专有类四种类别，对应的bit7，bit6编码分别为00，01，10，11。标签的格式bit5指明数据单元是基本类型(bit5=0) 还是构成类型(bit5=1) 。标签的编号可分为单字节格式和扩充格式。在单字节格式中，标签的bit0到bit4就是标签编号，提供的标签码值的范围从00000～11110（十进制的0～30）。若标签码的值大于30，需采用多字节的扩充格式。扩充的方法是把bit0到bit4编码为11111，接下来的八位位组的bit7比特作为扩充指示比特。如果bit7置1，表示下一个八位位组也用来作为标签码的扩充，如果bit7为0，表示该八位位组是最后一个扩充标签码。合成的标签码由每个扩充八位位组的bit0到bit6组成，第一个扩充八位位组的bit6是最高位，最后扩充的八位位组的bit0是最低位。

长度八位位组指明内容八位位组的数目，它不包括标签和长度八位位组。长度八位位组有短、长和不定三种格式。如果长度小于等于127，采用短格式。它只占一个字节，最高位bit7置0，bit0到bit6为长度的二进制编码值。如果内容长度大于127 个八位位组，长度字段采用长格式。第一个八位位组的bit7编码为1，bit0到bit6表示后继长度八位位组的个数。后继八位位组构成的二进制编码值表示实际的内容长度。当信息单元是一个构成式时,可以用不定格式来代替短格式或长格式。在不定格式中,长度字段占1 个八位位组,其编码固定为10000000 ,它并不表示信息内容的长度,只是标志采用不定格式。用一个特定的内容结束字节组来标志信息单元的终止。

内容八位位组表示包含的具体信息，允许TLV格式嵌套。在简单类型的编码中，该字段表示实际的内容；在结构类型当中，该字段是一个或多个数据的嵌套形式。

3 MMS 编码/解码模块设计

3.1 编码/解码过程分析

MMS 协议使用 ASN.1 语法描述 MMS 抽象语法，即 MMS PDU 格式，并规定任何遵循 MMS 协议标准的实系统都必须采用 ASN.1 基本编码规则形成的传送语法来支持 MMS 抽象语法。ASN.1 编码/解码用于实现 MMS 语法和传送语法的转换。

ASN.1 编码过程可分为两个步骤进行，首先通过对 MMS PDU 的 ASN.1 定义和对应的数据结构的分析取出一对对标签和值，然后调用相应编码函数进行具体的编码；解码时，首先从接收的八位位组中依次取出 MMS PDU 的标签，据此产生一个对应的空结构用来存放解码产生的值，然后根据整个 MMS PDU 的长度依次取出标签和长度，进行具体的解码，获得的信息填入前面产生的结构中，返回给用户。解码和编码实际上是相反的过程。

由于 ASN.1 的清晰性和中立性，可以用 ASN.1 编译器把 ASN.1 描述的 MMS 协议转换成 C/C++语言的结构和相关的编解码函数，实现计算机自动编

码/解码，如图 4 所示。

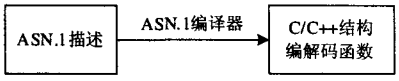

图 4 ASN.1 编译器原理

Fig. 4 Principle of ASN.1 compiler

经ASN.1编译器编译后，ASN.1描述转换成C/C++的结构。与ASN.1描述的MMS结构类似，编译产生的C/C++的结构也是树型嵌套结构，层层嵌套，一直到ASN.1的基本数据类型对应的C/C++结构。每个C/C++的结构有对应的编码/解码函数，这些函数按照数据结构的嵌套关系逐层调用，完成编码/解码功能。

C/C++的结构中的成员除了与MMS结构的信息一一对应的映射数据，还需要一种数据用于指明上下文环境，当前数据在上层结构中的位置以及当前编码/解码步骤的信息。例如，RejectPDU（ASN.1描述可以在ISO 9506-2查找）编译后对应的结构如下：

```
typedef struct RejectPDU
{
    long  *originalInvokeID;
    struct RejectPDU__rejectReason
    {
        RejectPDU__rejectReason_PR present;
        union RejectPDU__rejectReason_u
        {
            long   confirmed_requestPDU;
            long   confirmed_responsePDU;
            long   confirmed_errorPDU;
            …//省略
            long   conclude_errorPDU;
        } choice;
        asn_struct_ctx_t _asn_ctx;
    } rejectReason;
    asn_struct_ctx_t _asn_ctx;
} RejectPDU_t;
```

在该结构的不同层次中两次出现了asn_struct_ctx_t 类型的 _asn_ctx数据成员，这就是上下文结构参数。

各类数据至少包括两个成员函数，编码函数和解码函数。MMSPDU 类的编码函数为 int MmsPduEncode(const MmsPdu *pdu, char *pBuf)，作用是把 MMS PDU 变成二进制字节流，第一个参数 pdu 是待编码信息 MMS PDU 的指针，第二个参数 pBuf 是编码后报文输出的首地址，返回值是报文长度。MMS PDU 类的解码函数为 void MmsPduDecode (char *pBuf, int nLen, MmsPdu *MmsPduRet)，作用是解读报文，把信息存储在 MMS PDU 结构体中，第一个参数 pBuf 是输入，待解码报文的首地址，第二个参数 nLen 是报文长度，第三个参数 MmsPduRet 是解码得到 MMS PDU 的存储地址。

应用协议数据单元的 ASN.1 描述是独立于任何应用环境的一种抽象描述，在具体实现时用编程语言有关的数据结构来表示。因此，对于每一类数据，都存在一个 ASN.1 抽象定义和一个相应的数据结构。编解码过程如图 5 所示。

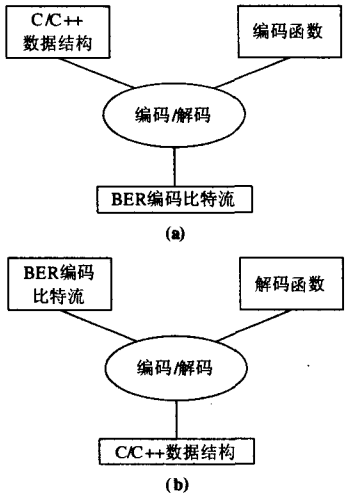

图 5 编码/解码过程

Fig. 5 Encoding and decoding process

3.2 MMS编码/解码模块的应用

以前面设计的MMS编码/解码模块为基础，本文编写了一个MMS报文编码/解码程序，可以组装和解读MMS PDU报文。输入MMS PDU报文A0 0E 02 01 02 A1 09 A0 03 80 01 02 A1 02 80 00，通过解码可以知道是一条GetNameList请求报文。MMS PDU报文通过以下途径获取：从nettedautomation网站下载Tamarac Client/Server程序，通过抓包软件（例如Wireshark Network Analyzer）可以截获Tamarac Client/Server的通信报文。

MMS PDU报文和MMS数据的对应关系如下文所示，左边是MMS的ASN.1描述，右边是对应报文字节的十六进制值。

```
MMSpdu ::= CHOICE
{
    confirmed-RequestPDU [0]              A0 0E
```

```
IMPLICIT Confirmed-RequestPDU,
    confirmed-ResponsePDU [1]
IMPLICIT Confirmed-ResponsePDU,
    ...
}
Confirmed-RequestPDU ::= SEQUENCE
{
    invokeID Unsigned32,                    02 01 02
    service ConfirmedServiceRequest
}
ConfirmedServiceRequest ::= CHOICE
{
    status [0] IMPLICIT NULL,
    getNameList [1]                         A1 09
IMPLICIT GetNameList-Request,
    identify [2] IMPLICIT Identify-Request,
...
}
GetNameList-Request ::= SEQUENCE
{
    objectClass [0] ObjectClass,            A0 03
    objectScope [1] CHOICE                  A1 02
    {
        vmdSpecific [0] IMPLICIT NULL,      80 00
        domainSpecific [1] IMPLICIT Identifier,
        aaSpecific [2] IMPLICIT NULL
    },
    continueAfter [2]
IMPLICIT Identifier OPTIONAL
}
ObjectClass ::= CHOICE
{
    basicObjectClass [0]                    80 01
IMPLICIT INTEGER
    {
        namedVariable (0),
        namedVariableList (2),              02
        namedType (3),
        ...
    } (0..13)
}
```

4　结论

制造报文规范MMS是IEC 61850的核心，也是实现IEC 61850变电站通信的关键技术。研究MMS的ASN.1编码/解码对实现IEC 61850通信具有重要意义。本文编写了MMS报文的编码/解码程序，实现了IEC 61850报文应用层的编码/解码。IEC 61850的应用层、表示层协议都采用ASN.1作为其编解码的规范，故本文提出的设计方案对表示层的实现具有借鉴意义。

参考文献

[1] 高湛军，潘贞存，卞鹏，等．基于IEC 61850标准的微机保护数据通信模型[J]．电力系统自动化，2003，27(18)：43-46.
GAO Zhan-jun, PAN Zhen-cun, BIAN Peng, et al. A Data Communication Model for Microprocessor Based Protection Based on IEC 61850 Standard[J]. Automation of Electric Power Systems,2003,27(18): 43-46.

[2] 茹锋，夏成军，许扬．IEC 61850标准在变电站自动化系统中的应用探讨[J]．江苏电机工程，2004，23(3)：8-12.
RU Feng, XIA Cheng-jun, XU Yang. Study on the IEC 61850 Standard Applied to Substation Automation System[J]. Jiangsu Electrical Engineering,2004,23(3): 8-12.

[3] 辛耀中．电力系统数据通信协议体系[J]．电力系统自动化，1999，23(1)：40-44.
XIN Yao-zhong. Data Communication Protocol Series for Power System[J]. Automation of Electric Power Systems, 1999, 23(1): 40-44.

[4] 李永亮，袁志雄，陈斌，等．对基于TCP/IP的IEC 61850特定通信服务映射MMS的分析与实现[J]．电网技术，2004，28(24)：33-38.
LI Yong-liang, YUAN Zhi-xiong, CHEN Bin, et al. Analysis and Implementation of TCP/IP Bbased Specific Communication Service Mapping MMS in IEC 61850[J]. Power System Technology, 2004, 28(24): 33-38.

[5] IEC 61850-8-1, Communication Networks and Systems in Substations, Part 8-1: Specific Communication Service Mapping (SCSM)-Mapping to MMS (ISO/IEC 9506 Part 1 and Part 2) and to ISO/IEC 8802-3[S].

[6] IEC 8824-1, Information Technology-Abstract Syntax Notation One (ASN.1) -Part 1: Specification of Basic Notation [S].

[7] IEC 8824-2, Information Technology-Abstract Syntax Notation One (ASN.1) -Part 2: Information Object Specification [S].

[8] IEC 8825-1, Information Technology-ASN.1 Encoding Rules[S].

收稿日期：2007-09-24

作者简介：

丁　力（1982-），男，硕士研究生，研究方向为电力系统通信、变电站综合自动化；E-mail: dl_082@163.com

王晓茹（1962-），女，教授，博士生导师，主要研究方向为电力系统保护和安全稳定控制、配电网和变电站自动化技术；

王　林（1983-），男，硕士研究生，研究方向为轨道交通电气化及其自动化、IEC 61850、电能质量监测。