基于编译器的通信规约自动解析研究

张艳林[1]，李慧勇[1]，李绍滋[2]

(1.北京德威特电力系统自动化有限公司软件部，北京 101300;
2.厦门大学智能多媒体技术实验室，福建 厦门 361005)

摘要：目前国内变电站综合自动化系统中规约种类繁多，IEC 逐步提出的一系列通信规约技术标准制定周期又较长，导致国内变电站综合自动化系统中不同厂家或同一厂家在不同时期内对同一种通信规约的实现有所不同，这给现场维护带来极大不便。针对上述情况，提出了基于编译器的标准规约自动解析思想，并以部颁 CDT 通信规约为例进行了该思想的设计，在自主设计的变电站综合自动化软件系统中得以实现，有很高的实用价值。

关键词：规约； 解析； CDT； 编译器

Research on protocols' automatic analysis based on compiler

ZHANG Yan-lin[1], LI Hui-yong[1], LI Shao-zi[2]
(1. Software Dept，Beijing DEVOT Electric Power System Automation Co.Ltd,Beijing 101300，China；
2.Xiamen University, Intelligent Multimedia Technology Lab，Xiamen 361005，China)

Abstract: At present, in the field of domestic transformer substation synthesis automated system, different factories or same factories in different periods carry out the same standard protocol differently, which lead to revise the procedure for transformer substation protection system even it has been input products with same standard protocol. It brings enormous inconvenience for on-site maintenance. In view of above situation, this paper proposes standard protocol automatically parse method based on the template and compiler, and has carried on two kinds of thoughts, respectively by IEC60870-5-103 and CDT issued by the ministry communication protocol for the example. Moreover, combining IEC60870-5- 103 protocol applying for transformer substation synthesis automated software system, it has implemented this idea. After the test, it has a very good utility.

Key words: protocol；analysis；CDT；compiler

中图分类号： TM76 文献标识码：A 文章编号： 1674-3415(2010)02-0101-05

0 引言

通信规约对变电站综合自动化系统安全与可靠的运行起着极其重要的作用。但由于规约种类繁多，致使众多的厂商的产品不能很好地兼容，给通信的双方造成极大困难。为改变这种局势，IEC 逐步提出了一系列通信规约技术标准。但由于这些系列标准的制定周期较长，如 IEC60870 系列标准的制定超过 10 年[1]，各方面对该系列标准的理解与应用情况很不平衡，还有许多厂家为满足自己产品的测量或控制需要而对标准规约有所扩充，而导致同一厂家不同时期或者不同厂家对这些标准规约的理解和应用情况各不相同。普遍存在的问题有[2]：①对规约解释不一致。②规约实现选项不一致。例如 103 规约遥测的上传，南自用通用分类服务来实现，可是有的厂家用 ASDU3、9、10 或 50 实现。③规约参数选集不一致。例如许继 103 中的信息序号除基本全部采用专用标准范围外，还有一些是自己扩展的，比如继电保护功能的控制操作命令的信息序号 INF77 的语义是过负荷投退；而南瑞虽然大部分是按照标准完成，可也有部分是自己扩展的，比如 RCS 系列的保护设备信息序号 INF42 的语义是监视方向闭锁。④通信过程不一致。由于对规约不同的理解，导致了不同的通信过程，例如在 103 规约 SEND/CONFIRM 服务中，有的厂家不遵守链路层过程，而直接进行应用层的确认，致使许多使用 SEND/CONFIRM 服务的命令功能无法实现。⑤采用的数据结构不一致。这些情况导致国内变电站综合自动化系统中不同厂家或同一厂家在不同时期内对同一种通信规约的实现有所不同，从而使变电站

基金项目：福建省科技重点项目(2006H0037)

保护系统即使接入使用同一通信规约的电力设备也要修改程序，对变电站设备间的互操作性和设备与变电站控制系统间的无缝通信带来极大的不便。

本文针对规约实现选项和参数选集不一致的问题，笔者提出了基于编译器的标准规约自动解析实现方法。基于这种方法维护通信规约时，用户不需要修改变电站综合自动化系统规约程序主站端的源代码，方便了不同厂家使用此标准规约的设备接入综合自动化系统，大大减少了规约维护的工作量。更重要的是省掉了去现场修改程序而浪费的大量人力物力和财力。

1 总体设计思想介绍

我们可以用数据模型、信息模型、服务模型来描述变电站综合自动化系统中智能电子设备 IED 通过规约来实现通信的过程：IED 收到数据后，对其进行分析，从中提取出对方传达的信息，接着提供对方相应的服务。如果所有设备的三种模型都统一或兼容，那么设备之间就能实现互操作了，通信模型如图 1 所示。

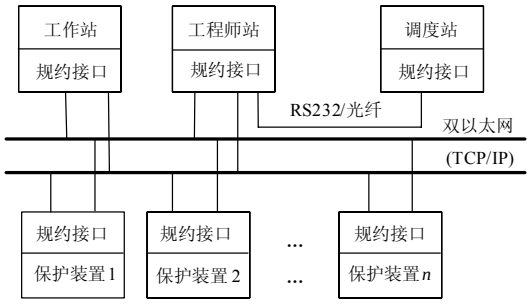

图 1 综合自动化系统简单通信模型

Fig.1Simple communication model

可是目前同一厂家不同时期或不同厂家设备产品的数据模型就不完全一致，所以目前要想实现无缝通信，必须采用某种方法先使通信的双方能识别对方发来的全部数据帧。

笔者在对各类不同版本的标准规约认真分析与总结后，提出了规约编译器的设计思想。

为了弥补数据模型的缺陷，首先要根据某类标准规约的一般技术要求和不同厂家实现情况的差异，编译器解决文法的生成以及每个产生式的所有候选式。

不同厂家在实现时为配合自己产品的测量或控制需要，有所变动的往往是传输控制部分，例如部颁 CDT 规约的功能码，有的厂家实现时会有所扩展。我们可以称传输控制部分为数据选集或参数选集，不管哪类标准规约具体实现时都是传输控制部分的全部对象或其子集对象的一个具体排列。

由于上下文无关文法具有很强的表述能力，现存的国内外流行规约几乎都可以通过上下文无关文法来表述，进而解决同一类型标准规约的实现选项或参数选集不一致的问题。

根据以上思想，并结合部颁 CDT 标准规约的技术要求，下面叙述基于编译器的 CDT 规约自动解析的设计及实现。

2 编译器在 CDT 上的设计和实现

2.1 理论基础

2.1.1 编译原理[3]

编译器是将一种语言翻译成另一种语言的计算机程序。编译器的工作从输入源程序开始到输出目标程序为止。这一过程如图 2 所示。

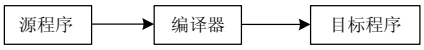

图 2 编译过程

Fig.2 Compile process

编译程序步骤如图 3 所示。

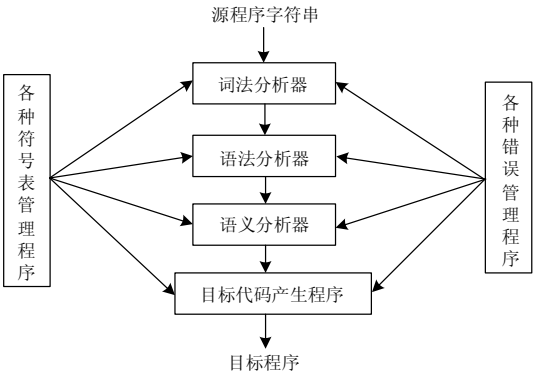

图 3 编译流程

Fig. 3 Compile process

2.1.2 CDT 规约[4]

CDT 循环远动规约采用可变帧长度、多种帧类别的传送方法，将远动帧分为若干类型，分别以“帧格式”编码来加以区别，每帧长度按实际需要而定，数据以帧格式循环发送。帧格式如表 1 所示。

表 1 帧格式

Tab.1 Frame format

同步字	控制字	信息字1	…	信息字*n*	同步字	…

其中同步字、控制字、信息字的格式如表 2、表 3 和表 4 所示。

表 2 同步字

Tab.2 Synchronized bytes

D7H\ EBH	B0字节
09H\ 90H	B1
D7H\ EBH	B2
09H\ 90H	B3
D7H\ EBH	B4
09H\ 90H	B5

表 3 控制字

Tab.3 Control bytes

控制字节
帧类别
信息字数*n*
源站址
目的站址
校验码

表 4 信息字

Tab.4 Information bytes

功能码	B*n*字节
b7…b0	B*n*+1
b7…b0	B*n*+2
b7…b0	B*n*+3
b7…b0	B*n*+4
校验码	B*n*+5

2.2 编译器的设计和实现

根据上一小节介绍的相关知识，CDT 规约的自动解析分为四个部分来实现：词法分析、语法分析、语义分析和出错处理，其中前三个是最重要的。解析流程如图 4 所示。

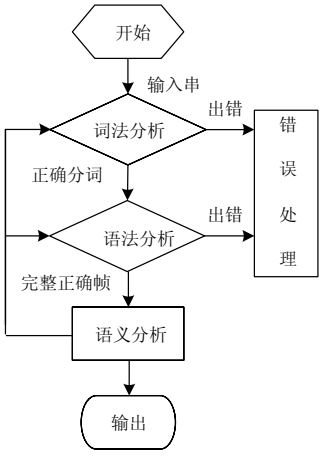

图 4 编译器流程

Fig.4 Compiler flow

2.2.1 词法分析

开始输入一个完整的帧。词法分析部分分析和识别出词法单位和它们的属性。由于 CDT 规约的帧格式比较整齐划一，我们可以用长度来进行分词，包括同步字、控制字、信息字。

2.2.2 语法分析

语法分析部分用于判断输入的帧(语法单位)是否完整并正确。采用自底向上的 LR 分析法，因其使用范围广，尤其是效率高，这对电力系统提高实时性是很重要的。分析表的构造用 SLR(1)方法，它构造简单且容易实现。

CDT 规约一个完整的帧可以用一棵树来描述，如图 5 所示。树根可看成是编译器的语法单位，树叶可看成是编译器的词法单位。

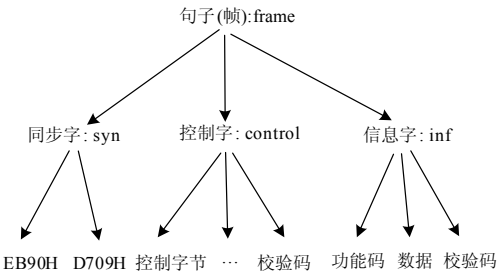

图 5 帧的树结构

Fig.5 Frame's tree structure

根据图 5，一个完整帧的文法可如下描述[5]：

G[E]：E→SC I

S→ eb90 eb90 eb90 | d709 d709 d709

C→ cb ft in sd dd cc

I → I fc db^4 cc I | fc db^4 cc

其中同步字 S(syn 的首字母，下同)、控制字 C（control）、信息字 I(inf) 、控制字节 cb(Control Byte)、帧类别 ft(Frame Type)、信息字数 in(Inf Num)、源站址 sa(Source Addr)、目的站址 da(Destination Addr)、功能码 fc(Function Code) 、校验码 cc(Check Code)，数据字节 db(Data Byte)。

为表示直观，以 a 代替同步字 eb90 eb90 eb90、b 代替同步字 d709 d709 d709、c 代替控制字 cb ft in sd dd cc、d 代替信息字 fc db^4 cc，则原文法的拓广文法可如下描述：

G[E']：(0) E'→E

(1) E→ SC I

(2) S→ a

(3) S→ b

(4) C→ c

(5) I → I d

(6) I → d

LR 分析器我们采用下推自动机这种数据模型[6]，它包括输入符号串、状态栈、符号栈和 LR 分析表。

由 G[E'] 很容易地能得出它识别规范句型活前缀的有穷自动机和它的 SLR(1)分析表分别如图 6、表 5 所示。

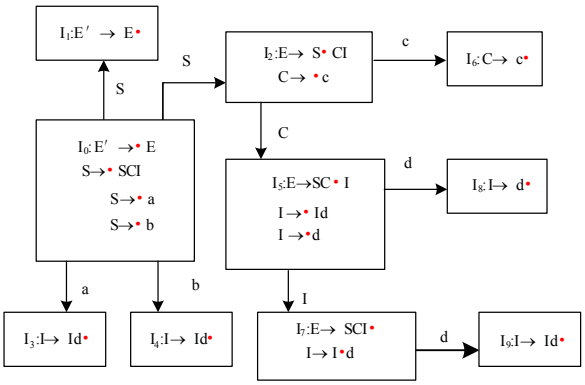

图 6 G[E']识别活前缀的有穷自动机

Fig. 6 G[E']'s DFA that distinguish living prefix

表 5G[E']的 SLR(1)分析表

Tab.5 G[E'] ' s Analysis table

	ACTION					GOTO			
	a	b	c	d	#	E	S	C	I
0	S3	S4				1	2		
1					acc				
2			S6					5	
3					r2				
4					r3				
5				S8					7
6					r4				
7				S9	r1				
8					r6				
9					r5				

下推自动机开始工作时，初始状态栈为 0，符号栈中只有语句括号#,输入缓冲区中有输入符号串 w#(w 为若干字节组成的字节数据流,即 CDT 报文);当状态栈上只有语句括号#和文法开始符号 E 时，输入缓冲区也只有语句括号#时停机。

用自然语言描述的 LR 算法如下：

LR 算法:

设置 ip 指向 w#的第一个符号
repeat forever begin
　令 s 是栈顶状态，a 是 ip 所指向的符号
　if action[s, a] = shift s' then begin
　　把 a 和 s'分别压入两个栈
　　使 ip 指向下一符号
　end
　else if action[s, a] = reduce A→β
　　then begin
　　从栈顶弹出 2*｜β｜个符号
　　令 s'表示当前栈顶状态
　　把 A 和 goto[s', A] 分别压入两个栈
　　输出产生式 A→β
　end
　else if action[s, a] = accept then
　　return
　ele
　　error()
　end

根据此算法对模拟输入符号串 acdd#(即由一个同步字、一个控制字和两个信息字组成的 CDT 报文)识别的过程，如表 6 所示。

表 6 符号串 acdd#的分析过程

Tab. 6 String acdd# parsing process

Step	Syms	Status	Input	Action	Goto
1	#	0	acdd#	S2	
2	#a	03	cdd#	r2	2
3	#S	02	cdd#	S6	
4	#Sc	026	dd#	r4	5
5	#SC	025	dd#	S8	
6	#SCd	0258	d#	r6	7
7	#SCI	0257	d#	S9	
8	#SCId	02579	#	r5	7
9	#SCI	0257	#	r1	1
10	#E	01	#	acc	

2.2.3 语义分析

因词法和语法分析的需要，语义分析穿插在它们中间进行，例如用长度信息对信息字分词时必须要知道它的个数，这就要先对控制字的第三个节字进行语义分析了。不过语义分析主要还是在语法分析中完成的，例如发现了遥测帧的信息字这样一个可归约串，就要立即对其语义分析以取出遥测值。

3 结论

基于编译器的 CDT 规约解析程序能对子站端 CDT 设备不同参数选集的上行帧进行自动识别和解析，如一个上行帧的同步字是 d709H，则可用第二条产生式的第二个候选式去匹配。

本文只是提供了一种比较便捷通用的开发模式，除 CDT 规约外，其它类的标准规约也可用此思想来实现自动解析，所不同的只是根据其它类具体标准规约的技术要求来生成相应的文法并构造出分

析表，不过可以采用同一个 LR 分析器去实现解析。即不同类的标准规约生成不同的文法，采用同一个 LR 分析器去解析。

基于编译器的规约自动解析设计方法方便了使用同一标准规约的不同设备接入变电站综合自动化系统，使现场的调试与维护更加容易，特别是基于编译器的程序代码易于修改和扩充。

以上介绍的两种规约实现方法，虽已有初步成果，但仍需继续深入研究和不断完善：基于编译器的思想更适用于标准 103 规约，而且 IEC61850 的应用和推广的大趋势不可逆转，要加快基于编译器的 103 标准规约的实现并向 IEC61850 靠拢，使将来 103 设备与 61850 的参数配置转换上更加方便。

参考文献

[1] 杨剑锋,贺春. 规约应用中存在的问题及解决方法的探讨 [J].继电器,2004,32(19):71-73.
YANG Jian-feng, HE Chun. Problems and Solutions in Protocol Implementation[J].Realy,2004,32(19):71-73.

[2] 张艳林,李绍滋. 基于模板的电力保护系统的通信规约研究[J].继电器,2007,35(22):23-26.
ZHANG Yan-lin，LI Shao-zi.Research on Communication Protocols Based on Template in Power Protection System [J]. Relay ,2007,35(22):23-26.

[3] 高级编译器设计与实现[M].赵克佳，译. 北京：机械工业出版社，2005.
Advanced Compiler Design Implementation[M]. ZHAO Ke-jia，Trans. Beijing: China Machine Press,2005.

[4] DL451-91，循环式远动规约[S].
DL451-91，Circulating Telecontrol Protocols[S].

[5] 傅钦翠, 陈剑云. 基于有限状态机的远动规约的设计和实现[J]. 电网技术, 2006，30（19）:214-217.
FU Qin-cui,CHEN Jian-yun. Design and Implementation of Communication Protocol Based on FSM[J].Power System Technology, 2006，30（19:214-217.

[6] 吉林大学软件教研室. 编译原理 [EB/OL].
http://softlab.jlu.edu.cn/2005/exc.html
SoftLab. of JLU. Compiler construction Principle and Implementation Techniques[EB/OL].
http://softlab.jlu.edu.cn/2005/exc.html.

收稿日期：2009-02-07；　修回日期：2009-03-18

作者简介：

张艳林(1980-)，男，硕士，主要研究方向为规约标准及变电站自动化系统；E-mail：linfeng0929@163.com

李慧勇(1977-)，男，硕士，主要研究方向为软件体系结构、变电站自动化系统、嵌入式系统、网络通讯体系结构等；

李绍滋(1963-)，男，教授，博士生导师，主要研究方向为人工智能与多媒体信息检索、网络多媒体及 CSCW 技术、软件体系结构与中间件技术、变电站自动化系统等。

（上接第 85 页　continued from page 85）

参考文献

[1] 北京超高压公司，房山 500kV 变电站现场运行规程[Z]. 北京：2006.

[2] GE Power Management. ALPS Advanced Line Protection System Instruction Manual[Z]. Canada：2001.

[3] 南瑞继保，LFP-921A 断路器失灵保护及自动重合闸装置[Z].南京南瑞继保电气有限公司技术说明书.2000.

[4] Mitsubishi Electric Corporation. Instruction Manual of MCD-H PCM Current Differential Relay Scheme for 500kV Transmission Line of NORTH CHINA INTERNATIONAL POWER ECONOMIC&TRADE CORP. （NCIP）[Z].Japan: 1985.

[5] GE Power Management.L90 Line Differential Relay UR Series Instruction Manual[Z].Canada:1985.

收稿日期：2009-02-13；　修回日期：2009-04-16

作者简介：

胡卫东（1977-），男，硕士研究生，从事继电保护维护、检修和技术管理等工作；E-mail：hwd77@sina. com

王凤岭（1973-），男，本科，工程师，长期从事继电保护维护、检修和技术管理工作；

柏　峰（1982-），男，在职研究生，长期从事继电保护维护、检修和技术管理工作。