北京航空航天大学学报 2011.09

基于 XML 的 EtherCAT 工业以太网协议解析技术

刘喆　　郇极　　刘艳强

（北京航空航天大学 机械工程及自动化学院，北京 100191）

摘　　要：重点研究了基于可扩展标记语言（XML）的 EtherCAT 工业以太网协议解析器技术和实现方法。介绍了 EtherCAT 协议报文格式和特点，分析了以太网数据侦听器和协议解析器的结构，针对通用以太网解析器在工业以太网领域应用的局限性，提出使用 XML 语言描述协议报文的方法，在此基础上开发出一种开放式、可重构的 EtherCAT 协议解析器。实验结果表明基于 XML 的协议报文描述方法及和解析器能够有效地描述和解析 EtherCAT 协议报文，使用者可以根据解析对象格式使用 XML 语言自定义、修改和扩展协议解析规则，获得清晰、直观的解析结果。

关　键　词：XML；工业以太网；EtherCAT；协议解析器

中图分类号：TN915.04

文献标识码：A

Parser of industrial Ethernet EtherCAT based on XML

Liu Zhe　Huan Ji　Liu Yanqiang

(School of Mechanical Engineering and Automation, Beihang University, Beijing 100191, China)

Abstract: The technology and realization method of industrial Ethernet EtherCAT parser based on eXtensible Markup Language（XML） were studied. The format of EtherCAT datagram was introduced. The structure of Ethernet probe and parser was analyzed. Common Ethernet parsers are limitative in the applications of industrial Ethernet. A method of protocol datagram description based on XML was proposed to deal with the problem of the EtherCAT protocol reconfiguration. According to this method, an open and reconfigurable industrial Ethernet parser was designed. At last, performance test of the method of protocol datagram description and open parser were carried out. The implementation shows that the method of protocol datagram description based on XML can describe EtherCAT datagram clearly, and the open industrial Ethernet parser can parser EtherCAT data. Users can define, modify and extend parsing rules according to the protocol object format, and obtain clear display of the protocol telegram.

Key words：XML，industrial Ethernet，EtherCAT，parser

工业以太网技术是以太网技术在自动控制领域延伸和发展，使用标准以太网器件和串行转发技术实现的工业以太网是其中的一个主要发展方向。此类工业以太网具有结构简单，数据传输效率高，实时性强等特点[1]。典型协议有 EtherCAT、Profinet 和 SERCOS III 等，本论文主要研究 EtherCAT 工业以太网技术。

以太网数据侦听器和解析器是工业以太网控制装置开发和维护的主要工具。本论文针对基于串行转发技术的 EtherCAT 工业以太网，研究协议解析技术，提出一种基于可扩展标记语言（XML, eXtensible Markup Language）的 EtherCAT 工业以太网协议报文描述方法，设计、实现了使用 XML 文档作为解析规则的开放式工业以太网协议解析器，解析器用户能够自定义、修改或扩充解析规则，完成数据对象的解析。最后通过实验验证了该协议

收稿日期：

作者简介：刘 喆（1985-），男，河南郑州人，博士，liuzhe12105@163.com

描述方法的可行性和解析器的功能。

1 EtherCAT 协议

EtherCAT是由德国BECKHOFF自动化公司于2003 年提出的实时工业以太网技术，使用标准以太网器件和串行转发技术实现，已经成为工业以太网的主流技术之一，获得广泛应用。目前 EtherCAT 已经成为国际标准 IEC 61158、IEC 61784-2、ISO 15745-4[2]。

EtherCAT 采用主从式控制结构，主站配置标准的 100Base-TX 以太网卡，从站采用专用芯片。图 1 为 EtherCAT 基本运行原理，主站发出下行报文遍历所有从站设备，每个从站在报文经过时从中读取主站发给本站的数据，再将本站返回给主站的数据写入指定的报文，然后传递报文给下一个从站。最后一个从站把经过完全处理的报文做为上行报文返回发送给主站。主站收到上行报文后，处理返回数据，一次通信结束[3]。

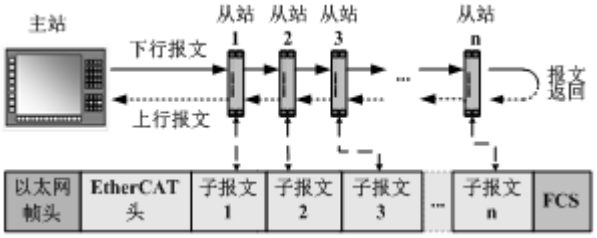

图 1 EtherCAT 运行原理

EtherCAT 帧结构如图 2 所示，EtherCAT 数据帧使用以太网 V2 格式的 MAC 帧，以太网类型为 0x88A4[4]。EtherCAT 数据帧包含 EtherCAT 子报文，各子报文的结构相同，因此本文将 EtherCAT 子报文称为重复报文，重复报文中包含一个重复终止标志，即 EtherCAT 的“M”字段。表 1 所示为“子报文”字段以下所有各子叶字段的长度和含义。

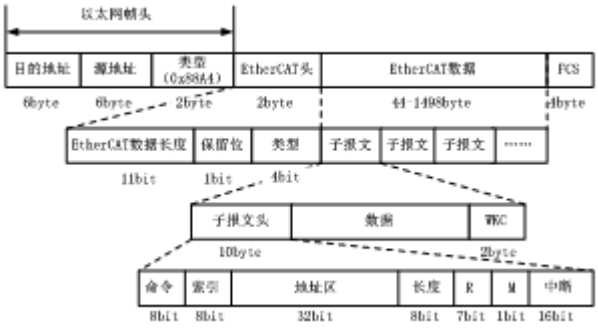

图 2 EtherCAT 帧结构

表 1 “子报文”字段的各子字段含义

字段名称	长度	含义
命令	8bit	寻址方式及读写方式
索引	8bit	帧编码
地址区	32bit	从站地址
长度	8bit	“数据”字段长度
R	7bit	保留，未使用
M	1bit	是否为最后一个子报文，重复终止标志
中断	16bit	中断到来标志
数据	由“长度”字段指示	工业以太网数据
WKC	2byte	工作计数器

2 数据侦听器和协议解析器结构

以太网数据侦听器和协议解析器用于以太网故障诊断和协议分析，是工业以太网设备开发和维护的重要工具，它们组成的系统结构如图 3 所示。

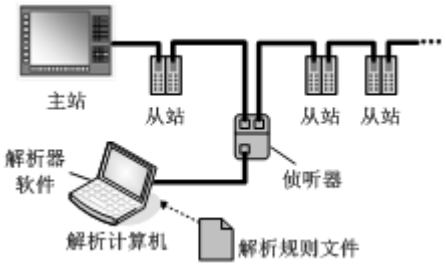

图 3 侦听器和解析器构成

数据侦听器是硬件单元，可以串联在以太网通讯链路中，并通过标准以太网接口与解析计算机连接。侦听器的功能是捕捉全双工链路上的以太网数据，为每个数据帧加上时间标记，打包后传输给解析计算机。侦听器捕捉和转发数据帧的过程不影响被侦听链路的正常通讯工作。

协议解析器是安装在解析计算机上的软件系统，其功能是分析被侦听器截获并传输至解析计算机的以太网数据，并将这些数据按照解析规则进行解析、统计和显示。解析器的解析规则由解析规则文件定义。功能完善的协议解析器解析深度可以达到应用层协议。

本论文研究的重点是协议报文解析规则描述方法和解析器设计部分。

3 工业以太网协议解析技术

目前并没有专用的 EtherCAT 工业以太网协议解析器，如果需要分析 EtherCAT 工业以太网数据，只能使用通用以太网协议解析器，如 WireShark、Sniffer、OmniPeek 等[5-6]。这些解析器功能丰富，但是大部分缺少向用户开放的协议解析规则。WireShark 和 OmniPeek 提供动态链接库（DLL ,Dynamic Link Library）格式的解析规则文件，用户如果想新建或修改某协议的解析规则，必须根据相应解析器的开发文档，熟练掌握指定编程语言编译生成 DLL 文件。因此，通用以太网协议解析器在解析规则开放性方面有局限性，解析规则开发难度大，调试工作量大，开发周期长。

工业以太网技术的快速发展促使新工业以太网协议不断被提出，旧版本的工业以太网协议不断升级。因此上述通用以太网协议解析器在分析 EtherCAT 等工业以太网数据时将面临协议扩展难

度高，应用范围局限的难题。针对这些问题，本文要实现的目标为：

（1）研究一种直观的协议报文描述方法，能够描述 EtherCAT 协议报文；

（2）建立一个开放式协议解析器，能够支持上述工业以太网协议报文描述方法，具有完善的协议接口，能够实现 EtherCAT 工业以太网数据的解析；

（3）解析器用户能够通过编写文本格式的 XML 文档自定义、修改和扩充解析规则，满足各种 EtherCAT 协议设备开发和系统维护需要。

4 基于 XML 的协议报文描述方法

针对 EtherCAT 工业以太网报文特点，本文提出一种基于 XML 的协议报文描述方法，使用此方法可以编写 XML 文档作为协议解析器的解析规则文件。

4.1 报文映射原理

层次模型是用树形结构表示实体之间联系的模型，只能表示“1：M”关系。如图 4 所示，层次模型的结构特点是：

（1）有且仅有一个无双亲的根结点；

（2）根结点以外的其它结点有且仅有一个父结点。

层次模型的结点中相同父结点的称为兄结点，没有子结点的称为叶结点[7]。

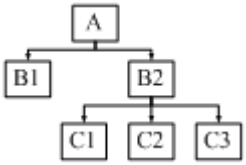

图 4 层次模型

按照层次模型的定义，EtherCAT 协议报文和 XML 文档都可以表示成为树状结构，因此二者均可以用层次模型表示。报文中具有相同父字段的称为兄字段，没有子字段的称为叶字段，同理可得 XML 文档中兄元素和叶元素的定义。

图 5 是一个协议报文与 XML 文档的映射示例。左边是一个报文片段，共有 A、B、A1、A2 和 A3 五个字段，各字段长度如图所示；右边是对应的 XML 文档片段，其中包括五个名称为“node”的元素，分别表示报文的五个字段，元素的属性表示元素对应字段的性质。基于这种映射关系，可以用 XML 文档描述 EtherCAT 协议报文。

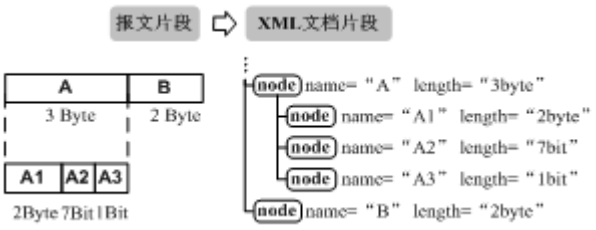

图 5 报文与 XML 文档的映射关系

4.2 报文定义

XML 元素和属性是 XML 文档语法的核心部分，通过增添 XML 元素和设置元素属性，可以描述 EtherCAT 报文格式。

首先建立 XML 根元素。XML 根元素名称为“root”，不表示报文任何字段，而表示报文整体。XML 根元素的属性表示报文的性质，各属性的含义分别为：

(1)“name”属性表示报文的名称；

(2)“abbreviation”属性表示报文的缩写名称；

(3)“ethertype”属性表示报文的以太网类型，属性值为四位十六进制数。

然后添加 XML 非根元素。XML 非根元素名称均为“node”，表示对应的报文字段，XML 非根元素的属性表示对应字段的性质。

(1)“name”属性表示对应字段的名称；

(2)“length”属性表示对应字段的长度。该属性的值分为三种情况：①字段的长度是以字节（Byte）或位（Bit）为单位的确定值，此时“length”属性值为具体长度值和单位，如“10byte”；②字段的长度是变量，由另一个字段的数值指示得到，如 EtherCAT 协议报文中“数据”字段的长度是由“长度”字段指示。此时需要使用 XML 的 XPath 信息寻址查找机制，通过 XPath 表达式可以方便的寻址找到 XML 结构文档树中的任何一个结点。“length”属性值为一个 XPath 表达式，通过该 XPath 表达式可以寻址到长度指示字段对应的 XML 元素，为后续解析过程建立有关字段长度的指示联系；③字段的长度是变量，由所有子字段长度的和决定，如 EtherCAT 协议报文中的“子报文”字段。此时可以不添加“length”属性或者“length”属性值设为空；

(3) “displaytype”属性表示对应字段数据的显示格式，“displaytype”属性值的类型及对应的数据显示格式如表 2 所示。其中枚举显示类型的含义是：使用者将数据值和用户自定义文字的对应关系作为枚举项，在 XML 文档中声明。当解析到枚举显示类型的字段数据时，解析器匹配枚举项，将用户自定义的文字代替字段数据显示。在 XML 文档的声明方法是：给"node"元素添加一个名称为"enum"的子元素，"enum"元素属性个数与枚举项个数相同，每个属性表示一个枚举项，如 0x0a="LRD 读数据";

表 2 “displaytype”属性值对应数据显示格式示例

属性值	类型	原始数据	显示数据
address	地址格式	45 d8 9a 75 01 d2	45:d8:9a:75:01:d2
numberhex	十六进制数	4f 5c	0x4f5c
numberdec	十进制数	10 28	1028
nool	布尔型变量	1/0	True/False
origin	原始数据	45 d8 9a 75 01 d2	45 d8 9a 75 01 d2

enum	枚举	0a	LRD 读数据
nondisplay	不显示	45 d8 9a 75 01 d2	-

(4)“repeat”属性表示对应字段数据是重复报文，“repeat”属性值为一个 XPath 表达式，通过该 XPath 表达式可以寻址到表示重复终止标志的 XML 元素。如 EtherCAT 协议的“子报文”字段数据是重复报文，“M”字段是重复终止标志，因此“子报文”字段对应的 XML 元素的“repeat”属性值是“M”字段对应的 XML 元素的 XPath 表达式。

4.3 报文描述示例

利用 4.2 节 EtherCAT 报文的 XML 描述方法，可以建立协议解析器需要的描述报文解析规则的 XML 文档。以下是对应图 2 示例和表 1 内容的部分 XML 文档代码，代码包含 XML 文档根元素以及“子报文”字段的各子字段对应的 XML 元素。代码中省略了部分枚举项和 XPath 表达式，XPath 表达式使用带方框的文字表示。

```
<root name="EtherCAT" abbreviation="ECAT" ethertype="0x88a4">
…（略）
    <node name="子报文" repeat="“M”元素的 XPath 表达式" displaytype="nondisplay">
        <node name="子报文头" length="10byte" displaytype="nondisplay">
            <node name="命令" length="8bit" displaytype="enum">
                <enum …（略）
                    0x0a="LRD 读数据"
                    …（略）/>
            </node>
            <node name="索引" length="8bit" displaytype="numberhex"/>
            <node name="地址区" length="32bit" displaytype="address"/>
            <node name="长度" length="11bit" displaytype="numberdec"/>
            <node name="R" length="4bit" displaytype="nondisplay"/>
            <node name="M" length="1bit" displaytype="bool"/>
            <node name="中断" length="16bit" displaytype="origin"/>
        </node>
        <node name="数据" length="“长度”元素的 XPath 表达式" displaytype="origin"/>
        <node name="WKC" length="2byte" displaytype="numberdec"/>
    </node>
…（略）
</root>
```

5 协议解析器设计

针对 EtherCAT 工业以太网协议解析器的要求，本文提出一种基于上述 XML 描述协议报文方法的开放式协议解析器。该解析器安装在解析计算机上，使用 XML 文档作为解析规则文件，使用者能够方便实现自定义、修改和扩展解析规则，能够实现数据对象的解析。解析器具有充分的开放性。

协议解析器组成架构如图 6 所示，侦听器串联在 EtherCAT 网络中，并通过标准 Ethernet 接口与解析计算机连接。解析器在启动时加载 XML 文档，将文档描述的协议报文解析规则存储在解析规则库中，并设置捕捉数据帧的数量或捕捉数据帧的时间。在数据捕捉过程中，侦听器将截获到的数据帧转发给解析计算机，解析器读入数据帧，并保存在数据帧存储单元。在数据捕捉过程结束后，解析器从数据帧存储单元中读取报文，按照给定的解析规则，完成后续解析、显示工作。

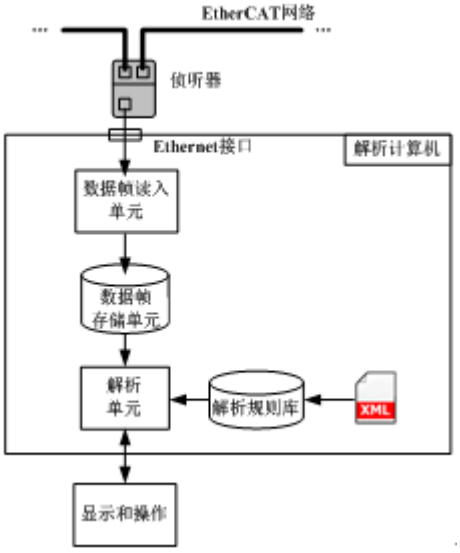

图 6 协议解析器结构

6 实验验证系统

实验验证系统的结构图如图 7 所示，硬件部分包括：1 个运行在 PC 上的 EtherCAT 控制主站、5 个 EtherCAT-IO 从站、1 个侦听器和 1 个协议解析计算机，设备间使用以太网线连接。侦听器采用 Beckhoff 公司的 ET2000 多通道侦听器，它是一种用于 10Mbit/s 和 100Mbit/s 工业以太网，可对 4 个独立的通道进行同步记录的通用数据帧捕捉设备。

软件部分包括：控制主站上的 EtherCAT 通讯程序和解析计算机上运行的协议解析器。

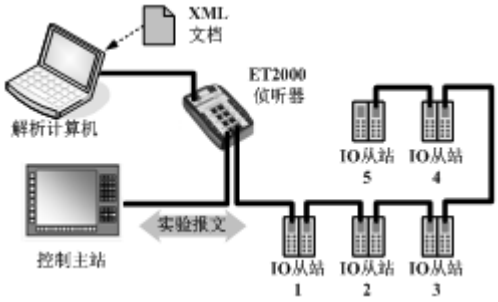

图 7 实验验证系统

实验数据包括：①描述 EtherCAT 协议解析规则的 XML 文档；②EtherCAT 实验报文，该报文由主站产生，包含 5 个子报文，每个子报文的内容对应 IO 从站的读写操作命令。

实验过程如下：①启动协议解析器，加载 XML 文档格式的解析规则文件，设置解析器捕捉 16000 个数据帧；②启动数据侦听器截获报文并转发给解析计算机，解析计算机将数据保存在数据帧存储单元；③捕捉 16000 个数据帧后停止捕捉过程，解析器处理保存在数据帧存储单元的数据帧。图 8 是一个 EtherCAT 数据帧的解析显示结果，可以看出解析器按照 4.3 节定义的 EtherCAT 解析规则，将数据帧完整、清晰的解析并显示。

图 8 截获报文的解析结果

7 结束语

本文提出一种基于 XML 的 EtherCAT 协议报文描述方法，并设计一种开放式工业以太网协议解析器。研究和实验结果表明，基于 XML 的协议报文描述方法及和解析器能够有效地描述和解析 EtherCAT 协议报文，能够方便地实现解析对象的扩展和重构，提高了解析器的通用性。此方法也可以扩展到应用层协议解析。

参考文献(References)

[1] Zhiyuan Gong, Bin Liu, Shunkun Yang, Xiaoyu Gui. Analysis of industrial ethernet's reliability and realtime performance[C]// The Proceedings of 2009 8th International Conference on Reliability, Maintainability and Safety.Chengdu, Institute of Electrical and Electronics Engineers Inc.,2009:1133–1136

[2] EtherCAT Technology Group (ETG). EtherCAT: The Ethernet Fieldbus[J]. PC Control, 2005,7:14-19

[3] 邹极，肖文磊，刘艳强.工业以太网 EtherCAT 冗余和热插拔技术[J].北京航空航天大学学报，2009,2:158-161。
Huan Ji, Xiao Wenlei, Liu Yanqiang. Redundancy and hot swap technology in industry Ethernet EtherCAT[J]. Journal of Beijing University of Aeronautics and Astronautics, 2009, 2:158-161

[4] 邹极，刘艳强. 工业以太网现场总线 EtherCAT 驱动程序设计及应用[M].北京：北京航空航天大学出版社,2010:5-10
Huan Ji, Liu Yanqiang. Driver Design and Application of Industrial Ethernet fieldbus EtherCAT [M]. Beijing: Buaa Press, 2005:5-10(in Chinese)

[5] Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R.. Network Traffic Analysis and Intrusion Detection Using Packet Sniffer[C]// ICCSN '10. Second International Conference on Communication Software and Networks, 2010. Singapore, IEEE Computer Society, 2009:313-317

[6] Chafer I., Felser M. .Precision of ethernet measurements based on software tools[C]//The Proceedings of 12th IEEE Conference on Emerging Technologies and Factory Automation, 2007 ETFA Programe. Patras, IEEE, 2007:510-515

[7] Bansiya J., Davis C.G.. A hierarchical model for object-oriented design quality assessment [J]. IEEE Transactions on Software Engineering, 2002, 28(1), 4-17