

XML与功能块相结合的设备描述方案

马振芳,冯冬芹

(浙江大学 智能系统与控制研究所,杭州 310027)

(dqfeng@iipc.zju.edu.cn)

摘要:针对现有的设备描述方案的复杂性和不可通用性,研究了基于XML的设备描述语言和应用现场自动化的以太网标准(EPA)功能块,提出一种将设备描述语言和功能块相结合的设备描述新方法。将不同厂商生产的EPA设备的属性分为几大类,其中的功能属性按照功能块的结构划分,使模拟功能块的描述与现场设备功能块的描述相对应,并将这种方法应用到了EPAConfiguration组态软件中,实现了功能块和设备描述对现场设备的综合描述,有利于设备的管理和控制。

关键词:XML;设备描述语言;设备管理;功能块;DOM解析

中图分类号: TP311 **文献标志码:** A

Device description schema of XML combined with function block

MA Zhen-fang, FENG Dong-qin

(Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou Zhejiang 310027, China)

Abstract: The existing device description methods are not general but complex. Extensible Device Description Language (DDL) of XML-based was researched and Ethernet for Plant Automation (EPA) function blocks were applied in EPA device description language. According to the function block structure, the property of EPA equipments from different manufacturers was divided into several major categories, so the description of simulation function blocks could correspond with the description of equipment function blocks. This method was applied to the EPAConfiguration software. The comprehensive description of function block and device description was achieved, which can make the management and control of field devices easier.

Key words: XML; Device Description Language (DDL); device management; function block; DOM analysis

0 引言

工业生产现场的各类仪器设备越来越多,且越来越复杂,设备描述技术是实现不同设备之间互操作的主要手段。现在市场上存在的设备描述有几种,文献[1]中介绍的电子设备描述(Electronic Device Description, EDD)对于复杂设备和复杂参数算法的描述存在着局限性,其设备描述(Device Description, DD)文件的解析需要用户购买专门的解析软件;文献[2]中基于现场总线的现场设备工具(Field Device Tool, FDT)描述方法针对特定的标准,并且需要软件接口才能实现互操作。

为了使设备描述更加具有通用性和可读性,本文在研究应用于现场自动化的以太网标准(Ethernet for Plant Automation, EPA)的可扩展的设备描述语言(eXtensible Device Description Language, XDDL)和EPA的功能块^[3]结构的基础上,提出了将两者相结合对设备进行描述的方案,并将这种方案应用在EPAConfiguration2010软件中,证明了这种结合方案的有效性和实用性。

1 方案提出的背景

1.1 XDDL设备描述

XML是互联网协会(W3C)开发的标准通用标记语言(Standard Generalized Markup Language, SGML)的一个子集,是一种与平台无关的编程语言。其主要特性^[4-5]如下:

1)可以实现不同操作系统下的跨平台的集成,无需移植;

2)可以增强设备描述的可读性;

3)解决了设备描述语言的兼容性以及上位机软件和设备描述文件之间接口的统一问题^[6];

4)既可以将描述信息直接嵌入现场设备,也可以放在软盘或光盘中的描述文件内,还可以直接放在Internet上;

5)用户无须专门的解释程序,只需用标准浏览器,定义相应的样式表文件,即可解读设备描述,方便用户使用。

XML允许用户定义自己的元素,基于XML的EPA可扩展的设备描述语言XDDL中定义了自己的基本描述元素,包括:

1)块(blocks):描述了功能块的外部特征。

2)简单变量(variables):描述了通过主机应用显示给用户的简单变量数据。

3)结构(struct):描述了通过主机应用显示给用户的结构数据。

4)数组(arrays):描述了通过主机应用显示给用户的数组数据。

5)响应码(response codes):应用程序所规定的变量、结构、数组以及域的响应代码。

1.2 功能块结构

EPA功能块^[7-8]是将EPA标准应用于控制系统的用户层功能模块,如图1所示,它是变量及其处理算法的封装,一个功能块包含了一个或多个算法。一个功能块的描述是算法的列表,它与相关的数据输入、数据输出和参数一起被封装在功能块内。它既能实现现场总线式控制,又易于操作使用,且易于实现、推广。

收稿日期:2011-05-10;修回日期:2011-07-04。 基金项目:国家自然科学基金资助项目(61074028)。

作者简介:马振芳(1987-),女,山东济南人,硕士研究生,主要研究方向:工业以太网技术;冯冬芹(1968-),男,江苏泰兴人,教授,博士生导师,主要研究方向:工业以太网技术、EPA标准、网络安全、功能安全。

根据功能块在控制流程中所起的作用,将功能块分为以下几类功能块:

输入型功能块 从技术块获得测量值,把测量值发布到下游功能块。

输出型功能块 从运算功能块或其他上游功能块获得运算结果,把控制数据传递到输出型技术块。

运算型功能块 是进行控制量运算的软件单元。

技术块 用于对过程量进行检测,并对检测信号进行处理转换,最终将过程量以数值形式输入到系统中;或将数值形式的控制量进行转换,以其他形式输出到执行机构。

根据设备的功能需求及性能,一个设备内可以仅具备一个类型的功能块,也可以同时具备两个或三个类型的功能块。每类功能块可存在一个或多个功能块实例。

所有同类型的功能块在设备中使用同样的算法和相同结构的参数表。但每一个功能块的实例的参数都相互独立不相干,参数表指定了功能块所有需要可访问的数据输入、数据输出和参数。

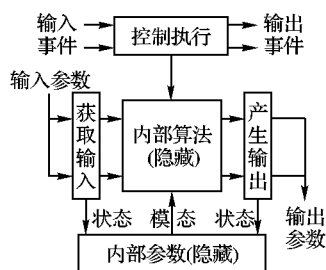


图1 功能块模型

2 XDDL 与功能块的结合描述方案设计

生产厂商开发了基于 EPA 的设备以后,就需要应用 XDDL 来描述设备,才能使得不同厂家生产的设备具有互操作性,设备商在描述 EPA 设备时要严格按照 XDDL 规范定义的格式来描述,XDDL 中只定义了描述基本元素的规范格式,但是在设备中各种参数的联系和组织关系未能体现出来,在此,提出一种 XML 和功能块结合描述的方法,将设备的所有参数按其功能和作用的不同分成不同的组,这样就可以有组织地描述各个参数,同时这种层次化的描述方法使得 DD 文件也更加易读。

2.1 结合描述的格式设计

DD 文件是用 XML 的语法规则来编写的,完全符合 XML 的格式和读写,而功能块最突出的特点是功能块的分类和功能块的结构以及各模块之间的通信,依据 XML 的语法规则和功能块的结构,基于 XML 和功能块的描述格式设计如下:

```
<?xml version="1.0" encoding="gb2312"?>
<XDDLDeviceDesc>
  <XDDLDocumentInfo> //XDDL 文件信息描述
    <XDDLDocCreateDate>2009-02-24
    </XDDLDocCreateDate>
    <XDDLDocRevision>10 </XDDLDocRevision>
  </XDDLDocumentInfo>
  <DeviceDescription> //设备描述
    <DeviceIdentify>
      <ManufactureID>CSCEPA </ManufactureID>
      <DeviceType>AI211 </DeviceType>
    </DeviceIdentify>
  </DeviceDescription>
  <BlockDescription> //功能块描述
    - <BLOCK TypeID="0510" BlockType="FB_Type">
    - <BLOCK_INFO>
```

```
<Name>DA_Transducer</Name> //DA 转换器
<BlockTag />
...
<ExecuteTimeUnit />
<NumOfParameters>6 </NumOfParameters>
<FirstAppID>1011 </FirstAppID>
<NumOfInstance>1 </NumOfInstance>
</BLOCK_INFO>
- <BLOCKPARAM> //功能块参数
- <VARIABLE ParaType="STRUCT_VARIABLE">
  <Name>BlockInfo </Name>
  <Label />
  <Help />
  <Class>contained </Class>
  <NumOfMembers>3 </NumOfMembers>
```

上述描述文件的实例中描述了一个 DA 转换器的功能模块,包括其各类参数和变量的描述,基本语法是基于 XML 的,而结构设计是基于功能块的,也就是将功能块中的元素移植到 XML 中作为自定义的元素,专门用于描述 EPA 的设备。

2.2 结合描述模型设计

在这种结合应用中,设备描述 DD 文件描述的内容要和设备的功能块划分保持一致,上位机解析 DD 文件后能够生成与现场设备相对应的模拟功能块,以数据结构的形式存储在内存中,用户对软件上模拟功能块的操作会通过 EPA 读写服务传给现场设备,同时现场设备参数的变化也会通过检测功能块检测出来,通过读写服务传回上位机,从而达到现场设备和软件上的模拟设备一致的控制和管理。设备描述与功能块结合应用的模型如图 2。

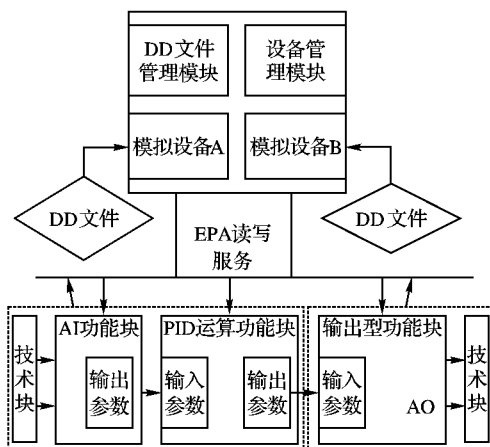


图2 设备描述与功能块的结合模型

对于更复杂、更多功能的应用,可在模型的基础上对功能块进行拓展^[9],可添加自定义参数、自定义控制或运算功能的实现。

3 应用实例功能设计

EPAConfiguration2010 是一款用于组态 EPA 设备的软件,它可以用于对 EPA-RT 设备、EPA-FRT 设备、EPA 无线设备、PLC 设备的组态、监控和管理。通过对工业现场的 EPA 设备进行上线识别,全局组态,从而对现场设备进行管理、变量监控以及对现场的数据进行收集和管理,可以获取现场设备的拓扑结构,使上位机的操作人员更好地对现场设备的实施状况进行监视和控制。

在 EPAConfiguration2010 中主要有以下三个模块用到了结合方案的设备描述及 DD 文件的解析功能。

DD 文件管理模块 是设备描述文件与软件交互的主要模块,DD 文件在文件管理模块中显示出来。

系统数据存储模块 此模块的内存中存储了与功能块参数相关的数据结构。一个数据结构描述了一类对象的特征,包括对象的元素、每个元素的读写权限和数据类型。

设备管理模块^[10] 是 EPAConfiguration 软件的重要模块,此模块从系统数据存储模块读取设备节点的信息,并将其以树形的形式显示给主界面上,用于用户和软件的交互。

此三个模块之间的关系可以从图 3 中看出。

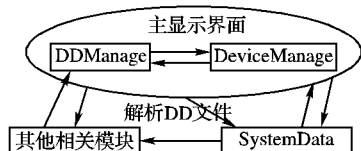


图 3 模块间的关系

3.1 DD 文件管理模块功能设计

DD 文件管理模块主要负责将标准路径下的各个厂商提供的 DD 文件扫描出来显示在界面上,并对其进行检查是否符合 DD 文件规范;用户也可以在设备管理模块上对设备进行 DD 文件加载,但需要将欲加载的 DD 文件交由该模块进行规范性检查,如果被加载的 DD 文件是非标准路径下的,DD 文件管理模块需复制一份到标准路径下,并将新的文件地址传递给设备管理模块。另外,用户也可以将本地其他路径下的 DD 文件添加到标准路径下,并对其进行规范性检查;加载非标准路径下的 DD 文件到设备时,也会对 DD 文件进行预检查。

通过该模块,用户还可以新建 DD 文件、删除 DD 文件以及打开 DD 文件等操作。该模块包含了界面、数据以及逻辑处理等部分。

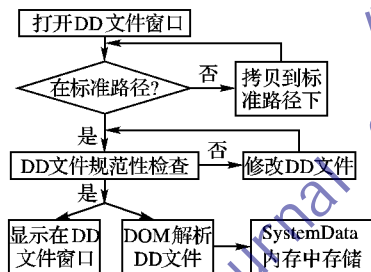


图 4 DD 文件管理模块流程

3.2 系统数据模块设计

作为 EPA 组态软件的重要组成模块,系统结构数据管理模块负责组织、存储、查找、修改整个组态工程的系统结构数据,包括工程节点、网段节点、设备节点、功能块节点等。DD 文件中的信息经解析后会以一定的数据结构存储在此模块中,这些节点按照相互之间的关系组织成一个系统结构树,软件的其他模块通过提供的接口就能够方便地访问每一个节点。同时其他模块对信息的改动也会返回给此模块,相应的信息会发生变化。

W3C 定义了解析 XML 文档的文档对象模型规范 (Document Object Mode, DOM)。DOM 是一种独立于语言和平台的定义,定义了构成 DOM 的不同对象,但没有提供特定的实现,可以用任何编程语言来实现。此实例中应用 VS2005 平台, C++ 编程语言来实现,利用 DOM 中的对象,可以对设备描述文件进行读写操作。首先解析 XML 文档,将 XML 文档分解为独立的元素、属性和注释等作为文档节点,并在内存中以节点树的形式创建文档的标识,通过节点树浏览文档的内容,并且可以对文档的内容进行读写操作,从而实现软件读

取设备描述文件的统一接口。

当需要设置某个设备的描述文件时,首先判断输入节点是否为设备节点,然后清除该设备下所有子节点,再解析设备描述文件,并根据解析的结果依次传到添加功能块类型节点子流程,整个流程如图 5 所示。

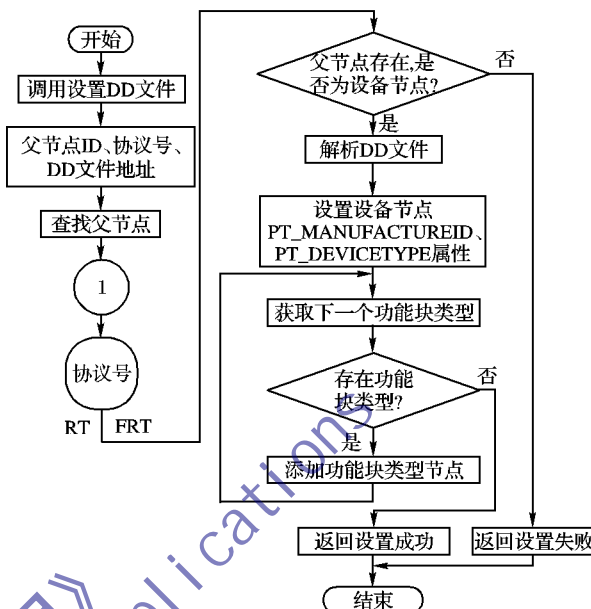


图 5 设置设备描述文件流程

当需要添加功能块类型的节点时,创建功能块类型的节点,并根据设备描述文件的解析结果添加 PT_NAME、PT_XDDLID、PT_MANUFACTUREID、PT_DEVICE TYPE 等属性,然后将解析结果依次传到添加功能块类型参数节点子流程。

设备管理模块用于显示设备列表,并可以对设备及功能块进行基本操作,其功能主要有:

- 1) 依据设备所属网段以树形列表形式显示出当前工程的所有设备;
- 2) 提供设备的基本信息查询及修改;
- 3) 提供设备的添加与删除;
- 4) 提供设备组态操作。

4 软件测试

EPAConfiguration2010 软件已经设计编写完成,并在实际的系统中运行使用,对于本文所涉及的设备描述与功能块部分,相关的模块运行良好,达到了预期的效果。

建立工程后,在设备管理窗口可以添加设备,在添加设备窗口可以选择符合标准规范的描述文件,选中描述文件后,系统数据库模块对 DD 文件中的数据进行解析存储,设备管理文件通过读取系统数据模块中的数据生成可视化的设备列表。

设备列表按物理网络层次显示出所有的设备及其参数。同时实现界面文本内容的检索与定位功能。图 6 是设备列表界面图。

模拟功能块是对现场设备的功能块的一个映射,反映现场设备的运行状况,同时,对于模拟功能块的操作也会通过 EPA 读写服务传给现场设备,对其进行操作和控制。组态模块根据系统中的数据和结构会在软件中生成相应的模拟功能块,用户对模拟功能块的控制会反馈到实际的现场设备中,从而实现了现场设备的检测和控制,图 7 显示了 DD 文件映射到软件上的模拟功能块的组态过程。

(下转第 2953 页)

文询问 O_{Dec} 后分析加密方案 E_k 并正确判断挑战密文 $e_{MH} = E_{k_{MH}}(m_b)$ 和 $TID_{MN} = r_{MH}Q_{MN}$ 是来自 m_0 或 m_1 , 设 D 成功破解 E_k 的优势为 $Adv_{E_k,D}(k)$; 2) D 利用 TID_{MN} 计算 $H_2(\hat{e}(S_{MN}, r_{MH}Q_{HA}))$, 从而判断挑战密文 e_{MH} 和 TID_{MN} 来自 m_0 或者 m_1 , 设 D 解决 BDH 假设的优势为 $Adv_{BDH,D}(k)$; 3) D 完全通过猜测判断挑战密文 e_{MH} 和 TID_{MN} 来自 m_0 或者 m_1 , 设猜测正确的概率为 $1/2$ 。则有:

$$\begin{aligned} Adv_{E_k,D}(k) + Adv_{BDH,D}(k) &\geq \Pr[D \text{ guess } b' = b] - 1/2 = \\ &= (1/2 + Adv_{IDMA,U})1/k + 1/2(1 - 1/k) - 1/2 = \\ &= (Adv_{IDMA,U} - 1/2)/k \end{aligned}$$

若 U 获胜的优势 $Adv_{IDMA,U}(k)$ 是不可忽略的, 也就意味着 D 已不可忽略的优势攻破选择明文攻击安全的 E_k 或解决 BDH 问题, 故假设不成立。证毕。

由定义 1 和定理 1 在 BDH 和对称加密方案能够抵抗选择明文攻击假设下, 且 HA 是全可信的且未被攻陷情况下, 本方案满足匿名性和不可跟踪性。

3 结语

本文在传统的基于代理的无线认证方案基础上, 提出了可信计算环境下的无线网络接入认证方案。该方案以无需可信第三方的基于属性的平台身份证明代替现有的基于证书的平台身份证明, 更好地体现了分布式的特点。在用户身份接入认证中, 如果只是建立起移动节点和代理节点间的对称密钥, 则改进后的方案没有现有的方案效率高, 但本文提出的方案可以满足通过建立对称密钥实现节点间的直接认证, 而现有的协议不具备这个功能。此外, 通过 ROM 分析, 本文的方案满足无线平台移动接入网络时的匿名性需求。

参考文献:

- [1] CAIMU T, OLIVER W. Mobile privacy in wireless networks revisited [J]. IEEE Transactions on Wireless Communications, 2008, 7(3): 1035 - 1042.
- [2] TIN Y S T, VASANTA H, BOYD C, et al. Protocols with security proofs for mobile applications[C]// ACISP 2004: The 9th Australasian Conference on Information Security and Privacy, LNCS 3108. Berlin: Springer-Verlag, 2004: 358 - 369.
- [3] 杨力, 马建峰, 朱建明. 可信的匿名无线认证协议[J]. 通信学报, 2009, 30(9): 29 - 35.
- [4] 杨力, 马建峰, 裴庆祺, 等. 直接匿名的无线网络可信接入认证方案[J]. 通信学报, 2010, 31(8): 98 - 104.
- [5] Trusted Computing Group. TCG specification architecture overview [EB/OL]. [2011 - 04 - 12]. <http://www.trustedcomputing-group.org>, 2007.
- [6] 吴振强, 周彦伟, 乔子芮. 移动互联网下可信移动平台接入机制[J]. 通信学报, 2010, 31(10): 158 - 169.
- [7] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271 - 1281.
- [8] 姜奇, 马建峰, 李光松, 等. 基于身份的异构无线网络匿名漫游协议[J]. 通信学报, 2010, 31(10): 138 - 145.
- [9] CHEN L Q, LOHR H, MANULIS M, et al. Property-based attestation without a trusted third party [C]// Proceedings of the 11th International Conference on Information Security. Berlin: Springer-Verlag, 2008: 31 - 46.
- [10] BELLARE M, ROGAWAY P. Random oracles are practical: A paradigm for designing efficient protocols[C]// CCS'93: Proceedings of the 1st ACM Conference on Computer and Communications Security. New York: ACM, 1993: 62 - 73.

(上接第 2949 页)

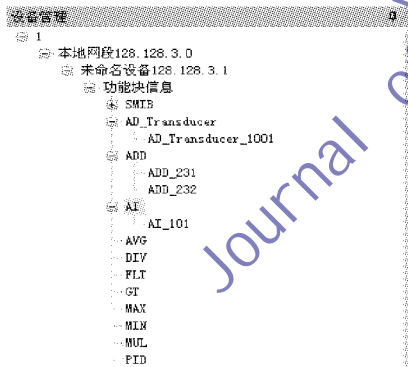


图 6 设备列表显示界面

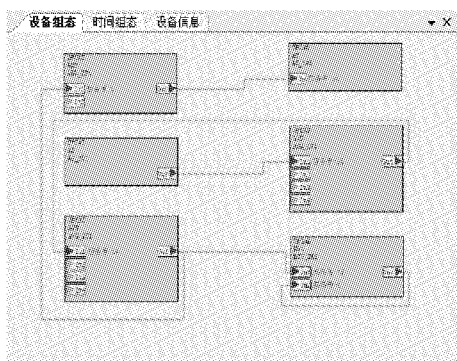


图 7 模拟功能块组态图

5 结语

本文主要研究了 EPA 标准中的 XDDL 设备描述语言和

EPA 功能块的结构及其在 EPA 设备中的作用, 将 XDDL 与功能块相结合, 用层次化的描述语言来描述现场设备, 并可以在上位机软件中映射成相应的模拟模块, 使用户更加容易掌握设备的信息。设备描述在 EPAConfiguration2010 软件中的应用证明, 功能块与设备描述相结合的方案有利于 EPA 设备的描述, 对于统一管理不同厂商的设备和 EPA 在各类设备中的应用推广有实用性。

参考文献:

- [1] 黄仁杰, 刘枫. 一种基于 XML 扩展的电子设备描述方法[J]. 西南师范大学学报, 2005, 30(6): 1026 - 1029.
- [2] 刘娟, 冯冬芹, 赖晓健, 等. 基于 XML 的基金会现场总线设备描述技术[J]. 工业控制计算机, 2003, 16(11): 32 - 34.
- [3] GB/T 26796.4—2011, 用于工业测量与控制系统的 EPA 规范, 第 4 部分: 功能块的技术规范[S], 2011.
- [4] 尹家凡, 王孙安, 盛万兴. XML 语言在变电站设备描述中的应用[J]. 计算机工程与应用, 2003, 39(21): 209 - 210.
- [5] 王忠锋, 王宏. 基于 XML 的现场总线设备描述[J]. 计算机工程, 2004, 30(8): 183 - 185.
- [6] 包伟华, 陈华. Profibus 产品的设备描述技术[J]. 自动化仪表, 2005, 26(11): 12 - 14.
- [7] 周侗, 徐皑冬, 王宏. EPA 功能块及用户层技术研究[J]. 自动化仪表, 2006, 27(9): 16 - 18.
- [8] 付迎利, 王平. 基于 EPA 标准功能块的设计与实现[J]. 重庆邮电学院学报, 2006, 18(2): 243 - 246.
- [9] 余淑军, 王平, 付迎利, 等. EPA 功能块的研究与实现[J]. 计算机应用与软件, 2008, 25(1): 38 - 40.
- [10] 阙宝栋, 付敬奇. EPA 组态软件设备管理模块设计与实现[J]. 仪表技术, 2010(1): 21 - 23.