OPC UA技术简介

Introduction of OPC UA Technology

方晓时 王麟琨
（机械工业仪器仪表综合技术经济研究所，
北京 100055）

摘 要: OPC UA技术的发展状况，阐述OPC UA技术的总体架构、信息建模、服务及安全等关键技术要素，并给出应用展望。

关键词: OPC UA COM/DCOM 地址空间 信息建模 服务

Abstract: In this paper, current status of OPC UA technology is introduced, moreover some key technical elements of OPC UA including architecture, information model, services and security of OPC UA are described and analyzed.

Key words: OPC UA COM/DCOM Address space Information model Services

项目编号：国家科技支撑计划课题（2012BAB18B02）

1 概述

目前工业控制系统使用技术的多样性，为企业多层次的数据集成带来很大问题。如：现场总线和工业以太网总计有超过20种解决方案。因此需要一种能够有效进行数据访问和管理的开放标准，能够在工业控制计算环境中的各个数据源之间灵活进行通信。

OPC（Object Linking and Embedding（OLE）for Process Control）是微软公司的对象链接和嵌入技术在过程控制方面的应用，被称为控制系统“中间件技术”，是专为在现场设备、自控应用、企业管理应用软件之间实现系统无缝集成而设计的接口规范。OPC自发布以来已广泛应用在工业控制系统的信息集成，但由于对微软COM/DCOM技术的依赖性，导致其在OPC的安全性、跨平台性以及连通性方面都存在很多问题。如：很难通过Internet/Intranet，尤其是企业防火墙；难运行在非微软系统，也难以在嵌入式系统中实现；很多上层应用没有OPC-COM接口，难以进行远程调用等。

鉴于此，OPC基金会发布了最新的数据通信统一方法—OPC统一架构（OPC UA）。OPC UA有效地将现有的OPC规范（DA、A&E、HDA、命令、复杂数据和对象类型）集成进来，并进行扩展。OPC UA提供一致、完整的地址空间和服务模型，解决过去同一系统的信息不能以统一方式被访问的问题。OPC UA规范可以通过任何单一端口进行通信。这

让穿越防火墙不再是OPC通信的路障，并且为提高传输性能，OPC UA消息的编码格式可以是XML文本格式或二进制格式，也可使用多种传输协议（如TCP）进行传输。OPC UA 访问规范明确提出标准安全模型，用于OPC UA应用程序之间传递消息的底层通信技术提供加密功能和标记技术，保证消息的完整性和安全性。OPC UA软件从过去只局限于Windows平台拓展到Linux、Unix、Mac等各种其它平台。OPC UA支持基于Internet的WebService服务架构（SOA）和非常灵活的数据交换系统。OPC UA新的技术特点将使其获得更广泛的应用。

2 OPC UA技术架构

2.1 OPC UA技术规范

OPC技术规范目前已成为IEC 62541系列标准。IEC 62541系列共分为13个标准，可将该系列标准分为3个部分：核心规范、访问类型规范和应用规范。核心规范规定了实现OPC UA的基础技术内容，包括标准中的1~7个部分。访问类型规范规定了如何通过OPC UA进行不同类型数据访问（DA、A&E、HAD等），包括标准中的8~11个部分。应用规范规定了OPC UA在实际应用中如何解决一些具体技术问题。

2.2 OPC UA应用结构

OPC UA并不限定为一种层次结构，可按不同的可剪裁的层次结构表示数据，客户端能按喜欢的方式浏览数据。这种灵活性结合对类型定义的支持，使得OPC UA适用于更广泛的应用领域。如图1所示，OPC UA的设计目标不仅应用于底层数据的SCADA、PLC和DCS接口，还可作为在更高层次功能之间提供重要互操作性的方法，如企业级上层管理与生产过程管理的数据集成与共享等见图1。

OPC UA允许其他技术组织或开发团体在其定义的信息模型基础上构造自己的模型，如IEC开始制定FDI（现场设备集成）标准。FDI合并了EDDL和FDT，并兼容OPC UA规范。

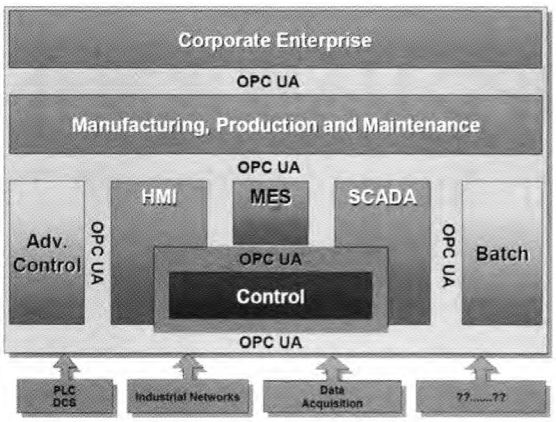

图1 OPC UA应用结构

3 OPC UA地址空间模型

OPC UA服务器中对于客户端可见的信息集合称为地址空间。信息集合包含对象集和相关信息。OPC UA对象模型定义了对象包含的变量和方法，对变量进行读/写操作，对方法进行调用。变量用来表示值。对象模型中的方法与面向对象编程中基于类的方法相类似，方法被客户端调用，在服务器上完成，然后返回结果到客户端。对象模型的定义通过到其他对象的引用表达与其它对象的关系。

地址空间中模型的元素被称作节点，对象及其组件在地址空间中表示为节点集合，为每个节点分配节点类并且每个节点类代表对象模型的不同元素。节点由属性描述并由引用互连。地址空间的节点根据其用途和含义进行分类，节点类为OPC UA定义了元数据。基本节点类定义所有节点通用的属性，允许标识、分类和命名。每个节点类继承这些属性并可能定义自己的属性。

节点类的定义包含属性和引用，当在地址空间里定义节点时，节点类应实例化（给定值）。属性是节点类的基本组件，描述节点的数据元素。客户端可以通过读、写、询问和订阅/监视项服务访问属性值。引用表示了相关节点间的关系，与属性一样，这些引用被定义为节点的基本组件。

为提高客户端和服务器的互操作性，OPC UA地址空间按层次进行了划分，其顶层对于所有服务

器都是相同的。尽管在地址空间的节点可通过层次结构进行访问，节点间可以互相引用，以允许地址空间表示节点的互连网络。OPC UA服务器可将地址空间划分为子集-视图，以简化客户端访问。

4 OPC UA服务

OPC UA服务是抽象服务，可看做是抽象远程过程调用的集合。OPC UA服务由服务器实现，被客户端调用。OPC UA客户端和服务器之间的所有交互都通过服务实现，如安全机制等。OPC UA共定义了10种服务集。

5 OPC UA安全架构

工业控制系统是国家生产设施和基础设施的关键组成部分，随着信息技术在工业领域应用的不断深入，以及近年来针对工业系统的攻击行为大幅增长，工业系统的信息安全面临严峻挑战。鉴于此OPC UA建立了完整的安全机制。OPC UA安全架构在传输层之上的应用层和通信层上构建，如图2所示。

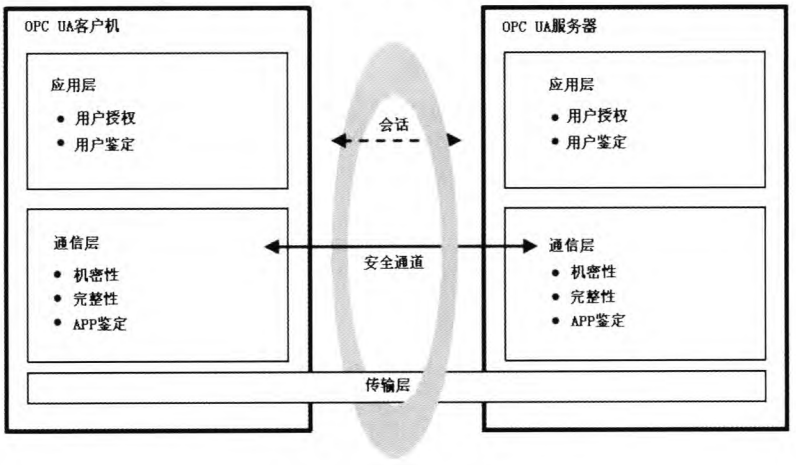

图2 OPC UA安全架构

客户端应用和服务器传输工厂信息、设置和命令这些日常工作由应用层的会话完成。应用层通过用户鉴别和用户授权管理安全目标。应用层的会话在安全通道上通信并依靠安全通道实现安全通信，安全通道由该通信层产生。所有的会话数据传递给通信层做进一步处理。

通信层提供安全机制以实现作为安全目标的机密性、完整性和应用鉴别。满足上述安全目标的关键机制是建立安全通道，安全通道用于保障客户端和服务器之间通信的安全。安全通道提供加密以维护机密性，提供消息签名以维护完整性，提供数字证书为来自应用层的数据提供应用鉴别，并向传输层传递“安全”的数据。由通信层管理的安全机制由OPC UA规定的安全通道服务提供。由安全通道服务提供的安全机制由实现选择的协议栈提供。

传输层处理发送、接送和传输通信层提供的数据。为恢复已断开的传输层连接（例如：TCP连接），通信层实现负责重新建立传输层连接，而不中断逻辑安全通道。

6 应用展望

最新发布的OPC UA相比传统的OPC技术具备更强的通用信息建模能力、更好的通信传输性能以及跨平台等特点，让数据采集、信息模型化以及底层与企业层面之间的通信更加安全、可靠。这使得OPC UA在多个技术领域获得应用和关注，如在IEC、美国和DKE等国家或标准化组织发布的智能电网标准化Roadmap，都将OPC UA技术作为重要的支撑标准列出。德国提出的新一代工业制造技术-工业4.0中也将OPC UA作为支撑技术之一。鉴于传统的OPC技术已经在智能楼宇控制中获得了广泛应用，OPC UA在楼宇控制中应用是可以预期的。综上所述，OPC UA技术作为重要的信息集成标准，将在不同领域和企业不同层级即横纵向2个层次获得广泛应用。

参考文献

1 IEC/TR 62541-1, OPC Unified Architecture – Part 1~Part 13.

作者简介：方晓时，一直致力于标准修订及电工电子产品的检测。