

基于IEC 61970标准的CIS接口服务 安全控制方法与实现

对基于IEC 61970 CIS标准的接口服务在被客户端访问时存在的各种安全性问题进行了分析,并在此基础上提出了一种服务连接层、方法调用层和数据对象层相结合的CIS接口安全性控制方法。通过服务连接层安全控制解决了CIS接口服务被非法客户端访问的问题;通过方法调用层的安全控制解决了因客户端非法调用关键接口方法而使公共数据遭到破坏的问题;通过数据对象层的安全控制解决了敏感数据被客户端越权访问的问题。对实现技术方法和实际应用情况进行了介绍,对存在的问题和后续需要研究的方向进行了探讨。

马 强¹ 张永庆² 田大伟¹/1.国网山东省电力公司 2.积成电子股份有限公司



马 强/高级工程师

关键词/Keywords

IEC 61970 ·
CIS接口 ·
访问安全控制 ·

为了解决各种电力信息与控制系统间的标准化信息集成与数据共享问题,国际电工委员会第五十七技术委员会(IEC TC57)提出了IEC 61970系列标准,其核心内容是公共信息模型(CIM)和组件接口规范(CIS)^[1]。CIM是一种抽象模型,采用面向对象技术和统一建模语言,提出了一种用对象类、属性和它们之间的关联关系表示电力系统资源的标准方法,使应用或系统能够不依赖于信息内部访问公共数据、交换信息^[2];CIS定义了应用或组件间进行信息交换的标准化接口以及这些接口所使用的事件类型和消息内容,并建立了接口与特定技术间的映射,其目的在于为独立开发的应用或系统间的集成提供标准化的接口,在中间件的选择上尽可能灵活,在保证互操作性的前提下,减少企业应用集成所需的工作^[3]。

IEC 61970 CIM/CIS系列标准提出

之后,被国内外的电力企业广泛接受并采纳。大量的研究人员对基于IEC 61970 CIM/CIS的系统设计与实现技术开展了深入研究,也成功开展了多次互操作试验^[4]。近几年来,IEC 61970 CIM/CIS系列标准在国内的电力企业中得到了广泛的推广应用,其应用领域和范围也得到了很大的扩展^[5]。目前主流的电网调度自动化系统、配电自动化系统都能够支持CIM/CIS标准。CIM/CIS标准也为电力企业不同部门、不同系统间的信息集成与交换提供了重要基础。如基于IEC 61970 CIM/CIS系列标准建设的电网调度综合数据平台,通过CIS接口在全省范围内实现了电网调度全景数据信息交换与共享^[6]。

在CIS接口技术推广应用的过程中,安全性问题是遇到的问题之一。CIS组件接口规范主要考虑的是接口的标准化和开放性,基本没有考虑信息安全问题。CIS接口服务是开放的,接口是标准的,任何能够连接到服务的客户端都能够访问接口的所有数据。这在完全可信、相对封闭的网络环境下没有太大问题,但是当推广到更大的范围和相对开放的环境下应用时,信息安全就是一个不得不面对的问题。

本文对基于CIS接口的信息交换过程中安全性问题进行了分析,在此基础上提出了一种安全性控制策略,对基于这种安全控制策略的CIS服务实现方案以及实际应用效果进行了详细描述,并结合工程实际对CIS接口安全性相关的技术与应用进行了展望。

基于CIS接口的信息交换安全问题

符合IEC 61970 CIS接口规范的数据服务主要包括通用数据访问接口（GDA）服务、高速数据访问接口（HSDA）服务、时间序列数据访问接口（TSDA）服务和通用事件订阅接口（GES）服务。其中，GDA服务用来提供模型数据的访问接口^[7]；HSDA服务用来提供实时数据的访问接口^[8]；TSDA服务用来提供历史数据的访问接口^[9]；GES服务用来提供事件的发布与订阅。这些接口中，GDA、HSDA和TSDA接口应用广泛，实用化程度高；而GES接口应用较少，实用化程度较低。

本文以基于IEC 61970 CIM/CIS标准的电网调度综合数据平台为例，讨论基于CIS接口的信息交换过程中安全性问题，主要涉及GDA、HSDA和TSDA接口。

电网调度综合数据平台利用标准CIM/CIS向电力调度控制中心内外的各种应用系统提供电网调度全景信息模型、实时数据和历史数据的访问服务。在通过CIS接口提供数据访问服务的过程中，所担心的安全性问题主要包括以下几个方面：

- 1) CIS接口服务被未允许的客户端非法访问。
- 2) 系统的公共数据被客户端非法调用写入接口而受到破坏。
- 3) 敏感数据被客户端越权访问。
- 4) 无法对客户端的访问行为进行监视与控制。

CIS接口安全控制方法与实践

1. CIS接口访问安全控制策略

通过对CIS接口服务面临的安全性问题以及接口服务的实际应用特点进行分析，提出了一种层次化安全控制策略，具体内容如下：

1) 对CIS接口服务采取连接层、方法层和数据对象层相结合的复合安全控制策略。

2) 采取连接层安全控制，即CIS服务在客户端连接时，识别客户端是否为被授权的客户端，对于未授权的客户端，拒绝连接。

3) 采取方法层安全控制时，即根据CIS接口规范的定义，CIS接口服务提供一系列的方法以便

客户端调用。在CIS接口服务的方法入口检查调用客户端是否具备该方法的调用权限，对于未授权的客户端调用，拒绝访问，直接返回错误信息。按照此控制策略，非法客户端不被授予调用写接口的权限，可有效解决公共数据被非法客户端写入而破坏的问题。

4) 采取数据对象层安全控制时，即为每个被授权访问CIS接口服务的客户端指定一个数据对象视图，该视图定义了一组数据对象过滤条件。该客户端在调用CIS接口的方法读取数据时，CIS接口服务端对传入的数据对象进行验证，只有当传入的数据对象在授权的数据对象视图内时，才返回该数据对象的相应数据。利用这种策略，可有效解决敏感数据被客户端越权访问的问题。

2. 总体实现技术架构

系统管理员通过专门的客户端注册与授权管理功能注册客户端基本信息，并为客户端分配访问权限，所录入的客户端与授权信息保存在配置库中。CIS接口服务加载客户端注册与授权信息，并在客户端访问CIS接口服务时根据客户端授权信息控制该客户端的访问行为，同时对客户端的访问行为进行跟踪记录。在客户端具备访问权限的条件下，根据访问操作要求返回或更新电网调度数据中心的电网模型、实时数据以及历史数据。系统管理员可以通过客户端访问监视与审计功能对客户端的访问行为进行监视与分析。

系统的总体技术架构如图1所示。

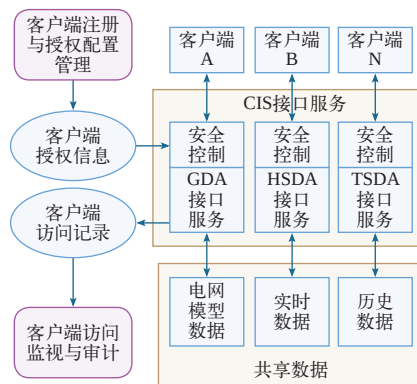


图1 总体技术架构

3. 主要功能与技术实现

CIS接口服务访问安全控制涉及的主要功能包括客户端信息注册与权限设置、CIS接口服务访问安全控制与跟踪记录以及客户端访问监视与审计等部分。下面分别作详细说明。

(1) 客户端信息注册

本系统以客户端的IP地址作为标识，需要注册的客户端信息包括客户端系统的名称、简介、负责部门、负责人与联系方式、所属安全区域、IP地址、访问的数据类型、接口、内容范围以及频度等信息。

(2) 客户端访问权限设置

根据上述安全策略，本系统提供的客户端授权管理功能主要包括如下内容：

- 1) 配置客户端可访问的接口服务器节点。
- 2) 配置客户端可访问的接口服务以及具体的接口方法。

3) 配置客户端可访问的数据对象集合或数据视图。为了简化数据视图的配置操作、提高服务端权限验证性能，根据电力调度信息的数据类型、敏感性以及电力调控中心内外的客户端访问需求，定义了一组典型的数据对象视图。每个数据对象视图定义了一组数据对象过滤条件（包括所属区域、厂站电压等级、设备类型和量测类型等）。

(3) CIS接口服务端访问权限控制

对CIS接口服务（GDA/HSDA/TSDA）进行改造，增加访问权限认证与控制功能，主要包括：

- 1) 加载客户端注册信息与授权信息，基于客户端的IP地址等特征有效识别访问客户端。
- 2) CIS接口服务在被访问时，检查该客户端授权访问的接口服务器节点是否与本服务器节点相符。如相符，则允许访问；否则拒绝访问。
- 3) CIS接口服务的方法在被调用时，在方法函数入口检查该客户端是否具有访问权限。若有访问权限，则执行所调用的方法；否则拒绝访问。
- 4) 在HSDA和TSDA接口服务的量测数据读取方法被访问时，对每个量测验证数据视图条件。只有符合条件时才返回量测数据。

CIS接口服务端权限验证控制过程如图2所示。

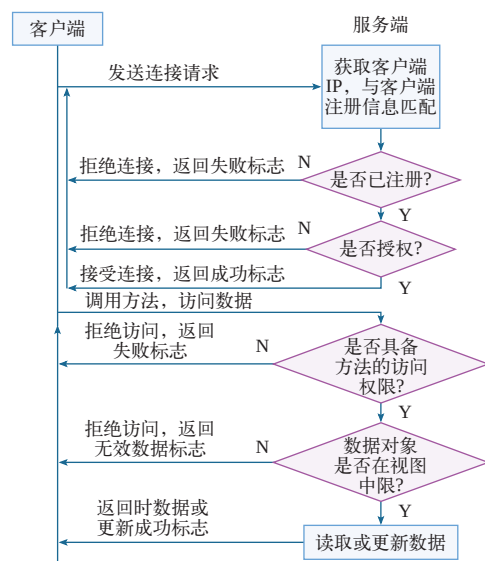


图2 权限验证与控制过程

(4) CIS接口服务访问监视与审计

在CIS接口服务被访问时，将客户端访问的时间、调用的方法、会话建立与撤销以及访问的数据对象数等信息记录下来。系统提供CIS接口服务访问监视与审计管理界面，供系统管理员对客户端的访问行为进行监视与审计。

讨论

山东电力调度控制中心基于IEC 61970 CIM/CIS技术建设了电网调度综合数据平台，系统基于CIS接口规范实现了电网调度数据的交换与共享，为电力调度控制中心内外的大量业务应用提供了电网公共模型、实时和历史数据。在CIS接口应用的过程中，遇到了前面所述的各种安全性问题。利用本文所述的CIS接口服务安全控制方法和实现技术，使上述安全性问题得到了有效解决，系统对CIS接口服务的访问实现了有效管控。

系统针对电力调控中心内外的访问需求，部署了两套CIS接口服务器，对于电力调控中心外部的应用系统配置只能访问外CIS的接口服务器，在连接层实现了内外安全隔离。对于GDA服务，主要通过限制客户端对更新服务写入方法的访问权

限，解决公共模型被客户端非法写入的问题。对于HSDA和TSDA服务，一方面通过限制客户端对写接口的调用，避免了公共数据被客户端非法修改的问题；另一方面利用数据视图的方法，限制了每个客户端访问数据的范围，避免了敏感数据被越权访问的风险。

在实际应用过程中,发现增加安全控制措施后,对CIS接口服务的性能会产生一定程度的影响。如果性能问题解决不好,将直接影响服务的正常访问,从而影响安全控制功能的实用化。因此,性能优化是影响CIS接口安全控制功能实用化的重要因素。为了将对性能的影响降至最低,采取了多种技术措施。如对系统内部的接口访问进行特殊处理,避免系统内部访问对性能的影响;简化数据对象视图的设置与验证方法,通过按对象层次设定过滤条件、配置一组典型数据对象视图以及预加载数据视图配置信息并生成内存映射等措施,有效降低了数据对象权限认证引起的性能损耗。测试结果表明,在没有应用CIS接口安全控制的情况下,访问HSDA接口服务每次读取2 500个量测,并读取100次,耗时4 250 ms,平均读取58 823.53 个/s。在应用CIS接口安全控制的情况下,访问HSDA接口服务每次读取2 500个量测,读取100次,耗时4 558 ms,平均读取54 848.61 个/s,约为不应用安全控制情况下的93.24%,因此能够满足实用要求。

结束语

实践结果表明,利用本文所述的CIS接口服务安全控制方法和实现技术,可以有效解决基于IEC 61970 标准的CIS接口服务访问安全性问题。但是对于CIS接口服务安全控制方法和实现技术研究才刚刚开始,还有大量的技术细节需要进一步研究与实践。如在保证数据访问安全的条件下,如何保证CIS接口服务的运行性能;如何实现对不同客

户端提供差异化的服务水平控制，避免不友好的客户端访问造成的CIS服务性能恶化，这些都是今后在实际应用过程中需要研究并解决的问题。

参考文献

- [1] 张慎明, 刘国定. IEC 61970标准系列简介 [J]. 电力系统自动化, 2002, 26 (14): 1-6.
- [2] DL/T 890.301—2004 能量管理系统应用程序接口 (EMS-API) 第401部分: 公共信息模型 (CIM) 基础 [S]. 北京: 中国电力出版社, 2005.
- [3] DL/Z 890.401—2006 能量管理系统应用程序接口 (EMS-API) 第401部分: 组件接口规范 (CIS) 框架 [S]. 北京: 中国电力出版社, 2007.
- [4] 叶峰, 叶清华. 顾全关于组件接口规范的应用研究及实现 [J]. 电力自动化设备, 2006, 26 (7): 47-51.
- [5] 曹阳, 姚建国, 杨胜春, 等. 智能电网核心规范 IEC 61970最新进展 [J]. 电力系统自动化, 2011, 35 (17): 1-4.
- [6] 马强, 荆铭, 延峰, 等. 电网调度综合数据平台的标准化设计与实现 [J]. 电力自动化设备, 2011, 31 (11): 125-129.
- [7] International Electrotechnical Commission (IEC). IEC 61970 TC57 energy management system application program interface (EMS-API) part-403: generic data access [S]. USA: IEC, 2003.
- [8] International Electrotechnical Commission (IEC). IEC 61970 TC57 energy management system application program interface (EMS-API) part-404: high speed data access [S]. USA: IEC, 2006.
- [9] International Electrotechnical Commission (IEC). IEC 61970 TC57 energy management system application program interface (EMS-API) part-407: time series data access [S]. USA: IEC, 2006.

(收稿日期: 2015-02-10) EA

欢迎订阅 欢迎投稿 欢迎刊登广告