Software Engineering and Applications 软件工程与应用, 2013, 2, 31-34
http://dx.doi.org/10.12677/sea.2013.21006 Published Online February 2013 (http://www.hanspub.org/journal/sea.html)

Design on Security Structure of Operation Dispatching System Information Sharing Platform of High Speed Railway

Lin Yang

Signal & Communication Research Institute, China Academy of Railway Sciences, Beijing
Email: capotyl@sina.com

Received: Jan. 14th, 2013; revised: Jan. 26th, 2013; accepted: Feb. 10th, 2013

Abstract: This article introduce to applying SOA to build security platform of operation dispatching system information sharing platform of high speed railway. the security platform provide the authentication, access control, data security, journal audit, firewall, anti-virus and so on, through the security system, external system can access the information sharing platform of high speed railway in safety.

Keywords: SOA; Information System; Security Structure; Information Sharing Platform

高速铁路运调系统信息共享平台安全架构设计

杨　林

中国铁道科学研究院通信信号研究所，北京
Email: capotyl@sina.com

收稿日期：2013 年 1 月 14 日；修回日期：2013 年 1 月 26 日；录用日期：2013 年 2 月 10 日

摘　要：本文介绍了采用 SOA 架构来搭建高速铁路运调信息共享安全平台，通过安全平台提供的身份认证、访问控制、数据安全、日志审计等功能，以及通过配置防火墙、防病毒等软件，实现外部接入系统对高速铁路运调系统信息共享平台的安全访问和稳定、可靠的信息共享。

关键词：SOA；信息系统；安全架构；共享平台

1. 引言

高速铁路是继航空航天业之后最庞大复杂的现代化系统工程，它是由稳定可靠的铁路基础设施、性能优越的高速列车、先进可靠的列车控制系统、高效的运输组织与管理体系等综合集成。运营调度系统作为高速铁路运输组织指挥的中枢，利用先进的计算机技术实现对列车运行、牵引供电控制、以及运输计划、设备维修等的综合管理。信息共享平台作为运调系统的接口平台，为运调系统[1]提供来自防灾系统、综合维修、基本计划、旅客服务、客票等多个系统的信息，是运营调度系统中重要组成部分。由于信息共享平台面对多个外部接口系统，是运调系统和外部系统信息交互的门户，因此信息共享平台的安全建设非常重要，一旦共享平台出现问题，将对整个运调系统和外围生产系统产生非常大的影响，进而影响铁路日常运输作业，甚至造成人员、财产伤亡。本文阐述了采用 SOA 架构，设计高速铁路运调信息共享安全平台，为各接入子系统提供安全、可靠的信息共享。

2. SOA 架构

SOA(Service Oriented Architecture)[2]——面向服务的架构是一种将信息系统模块化为服务的架构风格。拥有服务之后，可以通过编配服务给业务流程带来生命力。在成功的 SOA 中，可以迅速地将服务按不同

方式重新组合，从而实现新的或更好的业务流程。通过 SOA，软件可以灵活的为服务提供者和消费者选择实现技术和部署位置，通过稳定的服务接口，隔离服务消费者和服务提供者之间的耦合，大大缩小接口双方由于业务或者技术的改变而对另外一方造成的影响。由于运调系统共享平台面对多个外部系统，外部系统的业务、技术升级是不可避免的，采用 SOA 架构来设计共享平台的安全体系，可以使得共享平台应对灵活多变的外部系统，搭建可高、稳定的安全平台。

3. 高速铁路运调系统信息共享平台的业务环境

信息共享平台是实现高速铁路运营调度系统及其相关支撑系统中各类信息相互交换和综合应用的基础设施，既要满足运营调度指挥过程中诸如调度命令、停送电申请、施工维修计划申请、防灾安全报警信息、各种作业计划下达等调度指挥业务流程必须的信息交换，又要满足直接关系到高速铁路运输组织管理的共享数据例如各种基本计划、实施计划、基础数据、列车正晚点信息、统计分析报表、规章制度等信息的共享发布，其面对的业务环境如图 1 所示。

从图可以看出，信息共享平台需要接入运调等多个系统，它是各个系统信息交互的总线，鉴于各个外部系统接入共享平台的接口方式、通信协议不完全相同，安全架构设计要统一考虑，安全架构体系要满足多个层次的安全需求。

4. 信息共享平台的安全架构体系

共享信息平台的安全设计要充分考虑各个层面的安全风险，构建完整的安全防护体系，为共享信息平台、接入系统间的数据交换提供信息安全的标准服务，充分保证信息共享平台和接入系统的安全性。信息共享平台安全架构体系总体上来说包括防火墙系统、防病毒系统、应用安全管理系统、安全审计系统。其构成如图 2 所示。

4.1. 信息共享平台的防火墙系统

在信息共享平台交换机处统一部署防火墙系统，保证接入系统和信息共享平台之间的逻辑隔离，屏蔽外部系统非法入侵。

4.2. 信息共享平台防病毒系统

鉴于网络病毒的特点和有效的多层保护措施的必要性，结合系统的网络结构、安全性和实时性的要求，按照“统一管理、集中监控、多重防护”的原则，将整体反病毒系统部署在信息共享平台网络结构中各个层面(包括各服务器和工作站)，覆盖范围包括共享平台的通信服务器、应用服务器、数据库服务器和维护终端。

4.3. 信息共享平台应用安全管理系统

用户的安全性，通过信息共享平台中用户认证模块的接口连接，来保证用户的身份安全和访问安全。

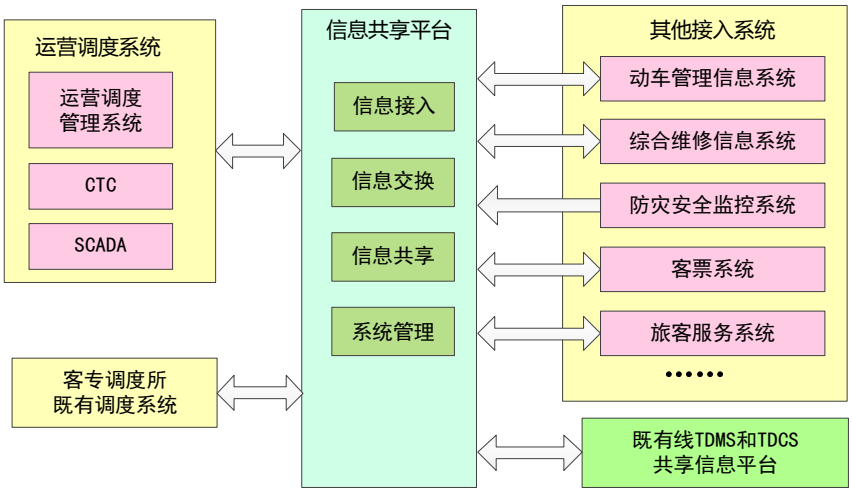

Figure 1. The business environment of operation dispatching system information sharing platform of high speed railway
图 1. 高速铁路运营调度系统信息共享平台业务环境

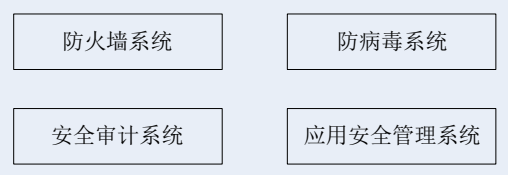

Figure 2. The security structure of information sharing platform
图 2. 信息共享平台安全架构

数据自身的安全性，通过对数据库自身内容的安全备份和恢复功能，保证数据的准确性、可恢复性。应用程序的安全性，通过信息共享平台用户认证模块、访问授权模块、共享信息资源目录对共享数据库中的数据以及平台中的服务访问进行安全保护。信息共享平台应用安全管理系统整体逻辑架构如下图 3 所示。

信息共享平台安全体系中，外部系统通过用户接入模块接入信息共享平台中。用户接入模块对外提供三种形式的接口：数据库接口、WebService[3]服务接口、MQ 消息接口。针对这三种接口，共享平台采取不同的策略来实现外部系统的安全接入：

1) 数据库接口

针对外部系统通过 ODBC/JDBC 数据库接口接入共享平台，其安全实现流程是：共享平台检测到有外部系统数据库接口接入时，调用平台中的身份认证模块，身份认证模块从 LDAP 资源库中校验用户合法身份后，将用户身份返回到访问授权模块，访问授权模块从 LDAP 中取得用户的访问权限信息，调用资源目录服务，获取此用户所能操作的资源(例如用户所能操作的数据库 IP 地址、数据库名、表、字段等信息)，最后对相应的数据库表进行操作，将返回结果通过用户接入模块发送给用户。在此过程中的任何一步操作，都会和日志模块交互，将相关信息记录到日志模块中。同时，如果在此过程中任何一步验证失败，都不能进行下一步操作，会将相关失败信息记录到日志中，同时将错误结果返回给用户。

2) 服务接口

服务接口其安全接入过程和数据库接口类似，也是通过身份认证模块验证、访问授权模块授权，从资源目录服务中获取用户所访问的服务资源信息(如服务所在主机的 IP 地址、服务接口名、接口函数名等)，将服务资源信息传递给信息共享平台的企业服务总线，由企业服务总线调用相关服务，将最终结果返回给用户。

3) MQ 接口

信息共享平台中的 MQ 接口安全访问是通过在共享平台中设立 MQ 安全接口服务器来实现的。在 MQ 接口服务器中，通过对 MQ 服务器与外部系统连接的发送方、接受方通道进行加密，采用 RSA[4]加密算法、设定 MQ 访问特定用户、应用或者 IP，实现外部系统对 MQ 接口的安全访问控制功能，防止未授权的用户访问接口队列管理器以及对接口队列管理器中消息进行加密功能。

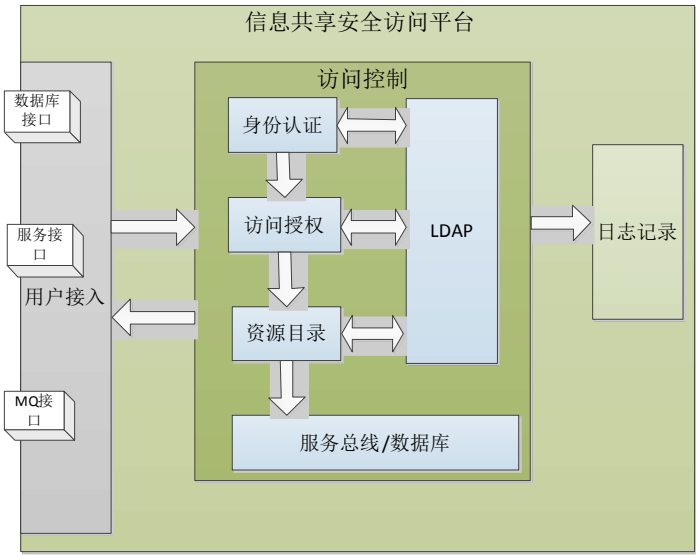

Figure 3. The logical structure of information sharing platform of application security
图 3. 信息共享平台应用安全管理逻辑架构

4.4. 信息共享平台安全审计系统

安全审计系统通过监测及采集信息共享平台中的安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统整体安全状况的全面审计。具体来说，安全审计类服务提供 3 大类审计信息：用户管理审计服务、用户接入审计服务、用户操作审计类服务。运营人员通过安全审计系统收集、分析、评估系统安全信息，及时掌握系统安全状态、制定安全策略，确保整个系统安全体系的完备性、合理性和适用性。

5. 结束语

高速铁路运调系统信息共享平台是运调系统与相关信息系统信息交换的枢纽，外部接入系统与信息共享平台进行信息交换时，采用网络安全和数据安全隔离措施，既保证实现信息共享又互不影响。采用 SOA 架构设计共享平台的安全体系，搭建信息共享平台的安全平台，使其成为共享平台的重要组成部分。信息共享安全平台作为高速铁路运调系统信息共享平台的 SOA 架构中的一个子平台，为共享平台提供身份认证、访问授权、数据安全、用户管理、安全审计等功能，实现接入系统间信息的安全共享。

参考文献 (References)

[1] 客运专线总体技术组. 铁路客运专线运营调度系统总体技术方案[Z]. 铁集成【2008】49 号文, 2008, 9: 26-28.

[2] P. C. Brown. Implementing SOA—Total architecture in practice [M]. 北京: 机械工业出版社, 2009, 3: 151-158.

[3] T. Erl 等. Web service contract design and versioning for SOA [M]. 北京: 人民邮电出版社, 2010, 1: 86-88.

[4] C. Steel 等. Core security patterns [M]. 北京: 北京机械工业出版社, 2006, 8: 78-82.