文章编号：1005-8451（2013）01-0071-04

动车组管理信息系统信息安全体系研究

张莉艳，崔丽新，张惟皎
（中国铁道科学研究院 电子计算技术研究所，北京 100081）

摘 要：为了更好地保护动车组管理信息系统中的信息安全，设定信息安全目标，研究建立信息安全体系，对动车组管理信息系统面临的风险进行分析，建立信息安全模型。在此基础上，对信息保护相关的安全技术进行研究分析，为动车组管理信息系统信息安全提供保障。

关键词：动车组；安全模型；安全技术；安全体系
中图分类号：U266.2：TP39 **文献标识码：**A

Research on security system for EMUs-MIS

ZHANG Liyan, CUI Lixin, ZHANG Weijiao
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: In order to protect information better in the EMU Management Information System(EMUs-MIS), set information security goal and establish Information Security System, the paper analyzed the risk to EMUs-MIS and established the information security model. Based on that, it was researched and analyzed the security technologies about information protection to provide information security protection for EMUs-MIS.

Key words: Electric Multiple Units(EMUs); security model; security technologies; security system

铁路动车组管理信息系统（以下简称系统）主要在铁道部、铁路局、动车段和运用所4级部署，各级之间需要不断交互多种信息。随着系统的深入开发和广泛应用，积累了大量有价值的业务信息，需要从物理层、网络层、系统层、应用层及用户层等多个层面考虑系统面临的风险。综合采用相关安全技术，建立完整的信息安全体系，以保证动车组管理信息系统的安全[1]。

1 动车组管理信息系统安全体系研究

1.1 动车组管理信息系统安全目标

为了信息系统的安全，在系统建设初期就需要制定信息安全目标，信息系统安全体系就是要为实现安全目标而服务的，并且随着信息化的发展和信息安全技术的发展持续改进[2]。动车组管理信息系统的安全目标是建立有效的灾备策略，能够在现场数据出现问题时快速恢复，保证系统的正常运行；保证数据存储安全，避免数据非法访问和越权使用；保证数据传输安全，避免数据在传输过程中泄露，数据传输不完整等[3]。

收稿日期：2012-11-12
作者简介：张莉艳，助理研究员；崔丽新，助理工程师。

1.2 动车组管理信息系统的安全体系

动车组管理信息系统安全体系需要从安全策略、灾备、访问控制、系统安全整体考虑，其安全体系框图如图1所示。

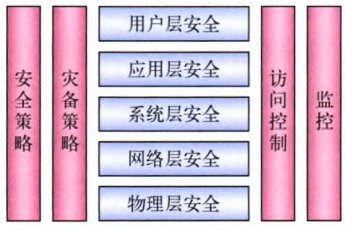

图1 动车组管理信息系统安全体系框图

（1）安全策略：安全策略包括安装防病毒软件、入侵检测及分层分级防护，针对物理层、网络层、系统层、应用层、用户层分别制定防护策略，在不同层内，根据安全防护的重要程度，采用分级防护措施，分为机密、秘密、一般、非密不同级别防护。

（2）灾备策略：对于重要数据及关键服务器制定合理的灾备策略，关键节点工作站、服务器采用双机热备方式，非关键节点多机互备，节省资源。存储的数据信息在指定设备定期备份。

（3）访问控制：对接入系统的用户实行身份认证、权限管理的方式，并按照用户权限配置策略，

开放系统资源，屏蔽用户使用权限以外的资源情况。

（4）监控：对系统各层运行情况综合监控分析，包括物理设备运行状态、网络连通情况、系统运行状态及用户接入情况。

（5）物理层安全：对系统部署在各级各地的服务器进行统一管理，采用IP地址与MAC地址匹配策略，准确标识系统设备。

（6）网络层安全：系统采用专网连接，在需要与外网交互时通过安全保障平台进行安全防护。

（7）系统层安全：保证业务运行的系统环境安全，定期检查系统漏洞、系统升级维护、补丁安装等。

（8）应用层安全：安装防病毒软件及防火墙，定期维护管理业务应用软件、补丁升级等。保护数据应用和业务应用安全。

（9）用户层安全：采用权限管理和身份认证方式，保护用户在权限许可范围内完成业务应用。

2 信息安全模型

2.1 系统数据安全风险概述

在动车组管理信息系统中，核心安全问题是数据安全，信息安全模型主要由风险分析、安全策略、安全监控、安全技术组成。风险分析是安全策略制定、安全监控范围选择和安全技术采用的基础。数据安全的风险主要包括以下几个方面：

（1）非可预见性风险。这些风险是不可预见、不可控制的，包括因硬件设备突然损坏或硬件设备故障造成的数据丢失、传输网络问题造成的数据丢失等。这种风险造成的数据损失较大。

（2）误操作风险。因误操作造成数据丢失、数据不完整等。这种风险造成的数据损失严重程度有大有小，有的可以通过回退操作或修正操作进行恢复或还原，但有的误操作造成的损失是无法弥补的。

（3）人为蓄意破坏风险。人为窃取数据或通过病毒软件破坏数据，造成数据丢失、数据损毁、数据失真等情况。这种风险造成的损失往往难以评估。

2.2 系统安全策略

综合考虑安全风险，制定安全策略包括以下几个方面：

（1）关键设备冗余设置。关键服务器等设备采用双机热备，部分服务器之间互相备份。

（2）数据备份。定期备份数据，采用逻辑备份和物理备份相结合的方式。

（3）制定数据更改规范。不能直接修改现场业务数据。现场数据更改需要导出，修改经测试后由专人导入现场数据库。

（4）数据库授权访问。现场数据库采用权限认证的方式，其他人没有权限登录现场数据库。

（5）制定安全操作规范，定期组织安全培训。

2.3 系统安全监控

良好的安全监控措施可以起到防患于未然的作用，在动车组管理信息系统中安全监控从以下几个方面入手：

（1）设备状态监控。数据存储服务器状态监控，定时发送和收取心跳信息，以此判断服务器运行状态。

（2）数据库操作监控。数据库操作日志记录，对数据库的每一次操作都记录日志。

（3）用户访问监控。对尝试连接系统或进入数据库的用户进行记录。

2.4 系统信息安全模型

系统信息安全模型如图2所示。

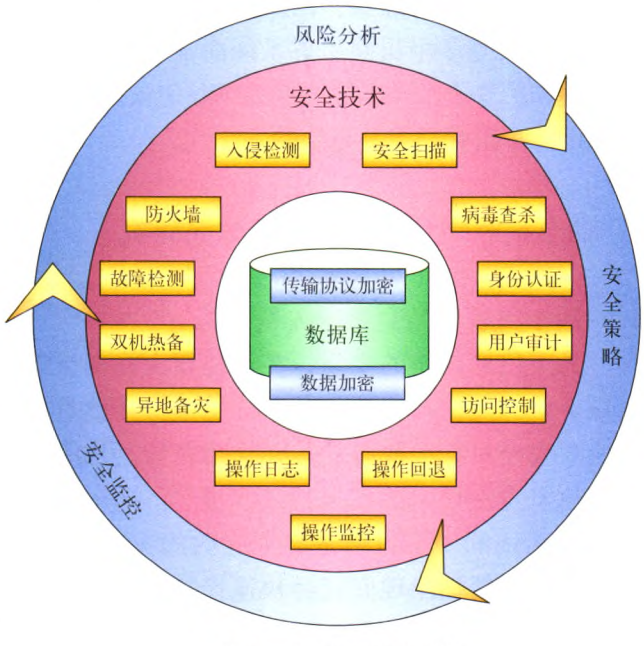

图2 系统信息安全模型

3 动车组管理信息系统关键安全技术

为确保动车组管理信息系统安全，采用的安

全技术如表1，包括硬件安全技术、网络安全技术、数据安全技术、用户安全技术等[4]。

表1　系统采用的安全技术

安全防护级别	安全技术
物理层	故障检测技术
	主机主动防御技术
网络层	安全协议
	传输加密
	防火墙技术
系统层	应用安全扫描技术
	抗DDOS技术
	虚拟化安全技术
	数据加密技术
	安全传输协议技术
应用层	全同态加密技术
	可信计算技术
	隔离技术
	用户审计技术
	访问控制技术
用户层	权限管理技术
	身份认证技术
	安全审计技术

3.1 数据库备份技术

数据库备份技术，是为了避免数据意外丢失、数据损坏而采取的防护措施。根据备份方式不同可以分为逻辑备份和物理备份。逻辑备份是一种面向对象的备份方案，直接备份数据库对象，包括数据表、用户、存储过程等，可直接导入到数据库进行恢复。此种方式操作简单，但备份和恢复时间较长。物理备份不直接备份数据对象，而是备份控制文件、归档日志文件等，利用控制文件、归档日志文件恢复数据库。此种方式备份恢复速度快，但恢复的环境要求与备份环境一样，否则不能恢复成功。

动车组管理信息系统综合2种备份方式的优点，采用逻辑备份和物理备份相结合的方式。支持实时业务应用的小数据量备份，采用逻辑备份方式，为减少数据备份时对业务的影响，在后台通过备份软件采用异步方式导出要备份的数据表。这种方式有利于小数据量的快速恢复。对于整个业务系统数据，由于数据量大，采用物理备份方式，提高备份和恢复速度。由于业务系统要求7 d × 24 h运行，因此物理备份采用联机备份方式，通过LAN备份到磁带库上。

3.2 数据库授权访问技术

数据库授权访问技术，对访问数据库的用户进行控制，避免非法访问和越权使用数据情况发生。数据库通过建立不同的角色，为角色授予权限的方式，控制用户的访问和操作。数据库权限包括数据库连接权限、数据库系统权限和数据库对象权限。数据库连接权限是防止非法访问数据库的第1层屏障。系统级权限是拥有对数据库系统进行操作的权限，包括用户分组、组策略制定等，是数据库防护的第2层屏障。数据库对象权限是具体对数据库对象进行操作的权限，包括数据表查询、更新等，是数据库防护的第3层屏障。

在动车组管理信息系统中，对数据的访问通过设置数据库连接权限、数据库系统权限和数据库对象权限，分3个层次对数据库访问进行防护。在基本防护的基础上，制定视图策略，通过建立数据视图，屏蔽数据库中受保护的基础数据。

3.3 数据库加密技术

对于存储在数据库中部分机密信息，采用加密技术对数据进行加密，这部分数据以密文形式保存。一旦发生数据泄露，没有密钥，也不会有数据泄密情况的发生。

在动车组管理信息系统中，对数据进行分级防护，机密数据以加密方式保存，在数据表中以密文形式存储，密钥保存在专用的安全数据库中。同时为了增加数据安全性采用双层密钥的方式，即密钥本身也处于加密状态，而密钥的密钥则保存在另外数据库中，2个密钥分别由安全管理员和数据库管理员掌握。

3.4 数据传输过程中数据加密

为了有效防止在传输过程中的数据泄露带来的安全隐患，对传输数据加密，传输数据加密可以分为2种：（1）对称密钥加密，指加密和解密都采用相同的密钥，密钥需要保密，较难破解，也称为保密密钥加密技术。（2）非对称密钥加密，是指一对用于加密和解密的密钥不相同，加密密钥可以公开发布，但解密密钥必须保密。

在动车组管理信息系统中，在铁道部、动车段及运用所之间经常需要互相传递数据，主要通过MQ进行数据传输。为了更有效地保护数据传输安全，采用对称密钥加密技术。数据在传输前进行加密，到目的地后再用密钥解密还原，采用

（下转P77）

自身发掘调试条件。实时对调试计划加以控制，避免出现最后所有工期压力都集中在信息系统。

（2）重视协调工作，紧密衔接各接口单位

由于信息系统实施范围涵盖动车段、动车运用所各建筑，接口众多。开展调试前及调试过程中需要花费大量精力进行沟通、协调工作，从技术接口到管理职能衔接，从主管单位、业主建设部门、业主运营部门到设计、监理、总包单位和各供应商全部囊括。信息系统调试接口干系人架构如图4所示。

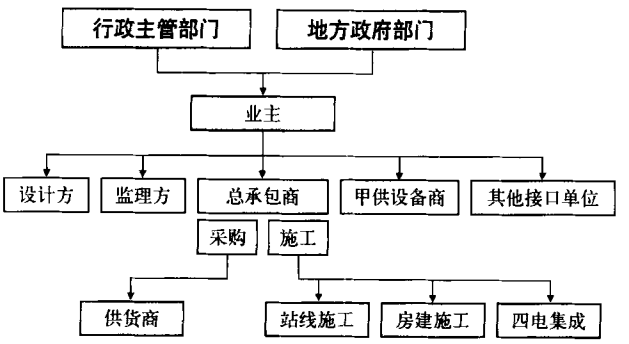

图4　信息系统调试接口干系人架构图

（3）不同地域的系统建设，要进行有针对性的设备调试

根据铁路发展长期规划，动车段和动车运用所遍布全国各地。在不同地域开展系统调试时，要注重本地环境特点。东南部地区，如：福州、广州动车所，应加强防雷、防雨、防潮的测试；东北地区，如：哈尔滨、沈阳动车所，应加强防寒测试；沿海地区，如：三亚动车所，应加强防腐蚀测试。

4　结束语

动车组管理信息系统已经在全路7个动车段、20多个动车运用所实施，多年来不断总结完善建设经验。系统硬件平台调试技术也根据实际工作的需要不断丰富和改进，并形成了一套相对完整的知识体系。在这套知识体系的指导下，新建动车段、动车运用所大幅缩短了系统调试工期、进一步确保了系统运行质量，为整个信息系统顺利投产和平稳运营提供了有效的基础支撑。

参考文献：

[1] 铁道部运输局．动车组管理信息系统总体方案[R]．北京：铁道部运输局，2009.

[2] 崔德山，张　彦，刘育欣．高速铁路客运服务系统联调联试技术研究[J]．铁路计算机应用，2012，20(1)：1-4.

[3] 陈　韬．光纤测试原理及测量仪表使用[M]．北京：邮电出版社，2002.

责任编辑　方　圆

（上接P73）

此种加密技术既不影响数据传输速度，又能有效地保护数据的安全[5~7]。

4　结束语

信息安全目标的设定和信息安全体系的建立，能有效地保护信息的安全。但随着信息化技术的发展，动车组管理信息系统还会面临更多的安全挑战，需要不断研究相关安全技术[8]，持续改进，增强安全防护技术水平和提高安全防护意识，才能有效地保护信息安全，为业务系统的安全运行保驾护航。

参考文献：

[1] 周元德，董凤翔，胡　波．基于等级保护的信息安全风险评估方法[J]．铁道工程学报，2006，99（9）：89-92.

[2] 左　锋．信息安全体系模型研究[J]．信息安全与通信保密，2010（1）：70-72.

[3] 张新豪，郭喜建，宋　朝．网络信息安全及信息安全性等级研究[J]．软件导刊，2011，10（12）：145-147.

[4] 王斌君，吉增瑞．信息安全技术体系研究[J]．计算机应用，2009，29（6）：59-62.

[5] 周　霞．数据库安全技术及趋势研究[J]．学周刊，2012，153（7）：6.

[6] 徐江峰，庄海燕，杨　有．Oracle数据库加密技术分析[J]．计算机科学，2006，33（1）：134-136.

[7] 魏道洪．浅谈ORACLE数据库安全技术及其应用[J]．计算机光盘软件与应用，2012（10）：158.

[8] 周　可，李春花，牛中盈．大规模数据中心的存储安全访问控制[J]．中国计算机学会通讯，2012，8（10）：32-37.

责任编辑　方　圆