普通高等教育铁道部规划教材

铁路信息安全技术

彭代渊 主编　韩 臻 主审

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

普通高等教育铁道部规划教材

铁路信息安全技术

彭代渊 主 编
韩 臻 主 审

中国铁道出版社
2010年·北 京

内 容 简 介

本书是普通高等教育铁道部规划教材。全书共七章，主要包括铁路信息系统概论、铁路信息系统密码技术、铁路信息系统数据完整性技术、铁路信息系统认证技术、铁路通信网络安全技术、信息安全技术在GSM-R中的应用和铁路信息系统的安全设计等内容。

本书为高等学校铁路相关专业的本科生与研究生教学用书，也可以作为铁路相关专业高等职业院校的教材，并可供相关企事业单位业务与管理人员的学习和参考。

图书在版编目(CIP)数据

铁路信息安全技术/彭代渊主编. —北京：中国铁道出版社，2010.5
普通高等教育铁道部规划教材
ISBN 978-7-113-11252-3

Ⅰ.①铁… Ⅱ.①彭… Ⅲ.①铁路运输—信息系统—安全技术—高等学校—教材 Ⅳ.①U29-39

中国版本图书馆CIP数据核字(2010)第066562号

书　　名：铁路信息安全技术
作　　者：彭代渊　主编

责任编辑：薛丽娜　**电话**：010-51873134　**电子信箱**：tdxuelina@163.com　**教材网址**：www.tdjiaocai.com
封面设计：崔丽芳
责任校对：孙　玫
责任印制：陆　宁

出版发行：中国铁道出版社(100054，北京市宣武区右安门西街8号)
网　　址：http://www.tdpress.com
印　　刷：河北省遵化市胶印厂
版　　次：2010年5月第1版　2010年5月第1次印刷
开　　本：787 mm×960 mm　1/16　**印张**：15.75　**字数**：338千
印　　数：1～3 000册
书　　号：ISBN 978-7-113-11252-3
定　　价：32.00元

前　言

本书是普通高等教育铁道部规划教材，是由铁道部教材开发领导小组组织编写，并经铁道部相关业务部门审定，适用于高等院校铁路特色专业教学以及铁路专业技术人员使用。本书为铁路信息技术系列教材之一。

随着铁路信息化建设的不断深入，铁路各项业务工作与信息技术日益融合，对铁路网络和信息系统的依赖程度越来越高。铁路信息网承载运行大量的业务信息系统，记录了铁路各专业的基础数据，网络系统与信息安全问题尤其突出。如果网络和信息系统受到攻击，将会影响信息系统正常运行，造成重大损失，甚至危及铁路运输安全。

为适应信息技术发展的需要，我国政府和科技界已将信息安全技术列为今后一段时期的重点发展领域。许多大专院校都设立了信息安全专业，开设了信息安全课程，迫切需要合适的教材。

本书围绕铁路特色，系统阐述了信息安全技术及在铁路上的应用。全书共有七章。第一章铁路信息系统概论，介绍了我国铁路信息系统发展现状、面临的安全威胁及安全模型。第二章铁路信息系统密码技术，介绍了密码学基本概念、流密码原理与设计、高级加密标准 AES、RSA 公钥密码体制、ElGamal 公钥密码体制、密钥的分配与管理。第三章铁路信息系统数据完整性技术，介绍了数据完整性意义、安全 Hash 算法 SHA-1、消息认证与认证码、RSA 数字签名体制、ElGamal 数字签名体制、数字签名标准 DSS。第四章铁路信息系统认证技术，介绍了认证系统模型、基本认证协议、身份认证、指纹识别、USB Key。第五章铁路通信网络安全技术，介绍了防火墙技术、入侵检测技术、访问控制和审计跟踪、公共密钥基础设施、SSL 和 TLS 协议、虚拟专用网(VPN)、黑客攻击与防范、计算机病毒及其预防。第六章信息安全技术在 GSM-R 中的应用，介绍了 GSM-R 系统结构、基于 GSM-R/GPRS 的铁路综合信息无线接入系统、GSM/GPRS 系统的安全保密技术、GSM-R/GPRS 系统中的安全保密技术、GSM-R/GPRS 中核心密码算法、铁路业务应用层安全保密技术。第七章铁路信息系统的安全设计，介绍了铁路信息网

络的体系结构和关键技术、铁路内网与外网的安全构建、安全设计、管理与实施、网络安全管理的实施。

本书内容全面，讲述深入浅出、概念清楚、易读好懂，适合于课堂教学和自学。可作为高等院校铁路信息技术、信息安全、计算机、通信、电子工程、交通控制、管理等专业本科生和研究生的教材，也可作为铁路信息管理人才的培训教材。

本书由西南交通大学彭代渊主编，北京交通大学韩臻主审。编写分工如下：西南交通大学黄文培编写第一章和第七章；兰州交通大学伍忠东编写第二章和第六章；兰州交通大学兰丽和周冬梅编写第三章；西南交通大学李晓航编写第四章；西南交通大学张文芳编写第五章。全书由彭代渊统稿。

本书在编写过程中得到了铁道部相关部门的大力支持。西南交通大学的硕士研究生陈帅进行了资料收集与整理、并仔细阅读了部分初稿，提出了不少宝贵的修改意见。在此对所有参加编写与修改工作的老师和同学表示衷心感谢。本教材参考了大量的文献，在书末列出了主要参考文献，对这些文献的作者表示感谢。

限于作者知识与水平所限，书中不妥与错误之处在所难免，殷切希望读者指正。

编　者

2009 年 11 月

目　录

第一章

铁路信息系统概论

铁路运输是国民经济的大动脉，除了完成日常的客货运输任务以外，还担负着落实国家宏观经济调控政策、保障社会稳定和国家安全的重要职责。随着国民经济的高速发展，传统的铁路运输、管理、调度模式已无法满足经济发展的需求。采用先进的计算机、网络通信技术，提高调度管理水平，推进铁路运输、管理和调度现代化是实现铁路快速发展的重要措施，也是保证铁路运输安全畅通，充分挖掘现有运输潜力，实现铁路现代化建设的重要内容。在信息技术快速发展的今天，没有铁路信息化就没有铁路现代化，没有铁路现代化就没有铁路的快速发展。

第一节　铁路信息系统发展现状

铁路运输信息化是国家运输信息化的重要内容，是铁路运输管理、市场营销和体制改革的有效保障手段，是推进铁路运输现代化的主要内容。经过30多年的建设，铁路信息化取得了令人瞩目的成就。铁路信息系统从无到有、从小到大，从单机版本到多层次的网络应用，全路信息技术人员总数已达5 500多人，拥有大、中、小型计算机1 600余台，微型计算机近10万台，建立了覆盖铁道部、铁路局和主要站段的计算机网络及传输网、交换网、数据通信网三大通信基础网。铁路通信光缆长度已达到74 000多公里，接入网23 000多公里。铁路71条干线，基础通信网达到了光缆化、数字化，主要的车站均具备多个两兆高速接入端口。

为了提高铁路运输生产和管理决策的自动化程度和水平，30多年来，铁路相继完成了列车调度指挥系统、铁路运输管理信息系统、客票发售与预订系统、办公自动化系统等的建设，面向公众的铁路政府网站和中国铁路电子商务网站已经正式开通运营。随着铁路信息化建设的不断深入，信息技术已经越来越广泛地渗透到了铁路的运输生产、客户营销、经营管理等各个领域，并成为铁路运输和铁路发展的重要保障。

一、铁路运输管理信息系统

铁路运输管理信息系统（Transportation Management Information System，简称TMIS）是一个规模庞大、结构复杂、功能众多、实时性强的计算机网络应用系统。从1994年开始实施

到2004年底TMIS各子系统全面建成，历经10年。通过构建全路计算机网络，TMIS将全路部、局、主要站段的计算机设备连成一个整体，从而实现了对全路近50万辆货车、1万多台机车、2万多列列车、几十万个集装箱及所运货物的实时追踪管理。

TMIS建成之前，铁路运输犹如一个“黑洞”，车辆、集装箱和所运货物，一经发出就很难知道在何处，直到到达目的地后才从“黑洞”中冒出来，这种服务质量远不能满足市场经济的需要。TMIS建成后，系统可以随时提供任何一辆货车、一台机车、一列列车、一个集装箱及所运货物的地点及设备的技术状态，并预见它们3天内的动态变化，随时提供车流的动态变化情况，特别是预见编组站、分界口、限制口的车流变化，从而为铁路系统运输指挥人员提供及时、准确、完整的动态信息和决策方案，同时也为货主提供实时追踪服务。

二、列车调度指挥系统

为了改变多年来铁路运输调度指挥一张图、一支笔、一把尺、一块橡皮来推算车流的落后工作方式，提高铁路的运输能力、服务质量和管理水平，铁道部组织开发和建设了调度管理信息系统(Dispatching Management Information System，简称DMIS)。2005年，根据铁路信息化总体规划要求，该系统被规范为列车调度指挥系统(Train operation Dispatching Command System，简称TDCS)。TDCS系统是我国铁路调度指挥现代化进程中的一个重要环节。利用现代信息技术，TDCS建立了以通信、信号、计算机网络、数据传输、多媒体等融为一体，覆盖全路的三级四层(即铁道部、铁路局、原铁路分局三级再加上基层信息采集层)分散控制、集中管理的运输调度指挥系统。

作为全路各级调度指挥管理人员实施列车调度指挥的手段和平台，TDCS能够对全路局的行车进行实时、集中和透明的指挥。铁路调度员通过简单地点击鼠标即可实现运行线的自动铺画、调整，下达阶段计划和调度命令等操作。由于系统实现了自动报点和车次号自动跟踪、列车实际运行图自动绘制、自动过表、车站行车日志自动生成，改变了过去车站值班员用电话向调度员人工报点、调度员用电话向车站下达计划和命令，车站手抄再复诵的落后方式。系统建成后，极大地优化了运输调度指挥管理的手段，提高了铁路调度管理水平和运输效率。经过10多年的建设，哈尔滨、呼和浩特、南宁、成都、兰州、乌鲁木齐等铁路局已全面完成了TDCS系统的建设，郑州、济南、上海、武汉、昆明等铁路局主要干线均实现了计算机自动绘制列车运行图。

三、调度集中系统

调度集中系统(Centralized Traffic Control System，简称CTC)利用遥信和远动技术实现行车调度的远程控制，是铁路运输生产指挥现代化的重要手段。通过调度集中，铁路调度中心可以对某一区段内的铁路信号设备进行集中控制，对列车运行实施直接地指挥和管理。CTC的基本功能包括列车运行实时显示及区段透明、车次号追踪及早晚点显示、列车作业和调车作

业分散自律控制、信号设备集中自动控制、列车进路按计划自动排路等。

鉴于调度集中具有显著提高铁路运输生产效率、减员增效的作用，在发达国家得到了广泛应用。日本调度集中营业里程达 2.6 万 km，占总营业里程的近 90%；美国铁路的编组站往往是多个铁路公司交叉接入的枢纽地区。因编组站的作业较复杂，又是各铁路公司多方车流的集结地，一个铁路公司无法对编组站进行集中控制。但是，在各铁路公司管辖范围内，CTC 系统的建设仍坚持使用统一的软硬件平台。法国高速铁路、加拿大和北美的重载运输，已经全部实现了综合指挥调度。2003 年，我国在青藏铁路建设了世界先进的分散自律调度集中系统。青藏铁路 CTC 建成后，青藏线西哈段共有 17 个车站，10 个车站实现行车指挥无人化，无人化率达到 58.8%，车务部门运转人员减少 119 人，仅此一项每年可节约人工成本支出 122 万元。如果算上管理费以及各种补贴等费用，年节约运输成本支出超过 200 万元，效果十分显著。

四、客票发售与预订系统

铁路客票发售与预订系统(Ticketing and Reservation System，简称 TRS)建设始于 1996 年，属“九五”国家科技重大攻关项目。TRS 由铁道部客票中心、地区客票中心和车站客票系统三级构成。其中，车站售票系统主要负责售票的实时交易服务，地区客票中心主要负责以座席为核心的调度控制和客运业务管理，铁道部客票中心主要负责全路客运的协调管理、营销分析，并保障全路的联网售票。10 多年来，TRS 先后经历了四次大的改版。1.0 版实现了全国统一车站售票，2.0 版实现了地区内联网售票，3.0 版完成了全路联网异地售票，4.0 版适应了客运体制改革和收入清算需求。近年来，为了适应铁路发展的要求，体现“以人为本”的服务理念，构筑以市场需求为导向的客票销售体系，满足旅客多层次需求，实现客票销售渠道网络化、服务手段现代化、运营管理信息化的战略目标，TRS 已升级到 5.0 版。

TRS 的建设彻底改变了我国铁路客票近百年的手工作业方式，使硬版票成为历史。它缓解了长期存在的买票难问题，提高了铁路客运经营水平和服务质量，受到了广大旅客的欢迎，改善了铁路的企业形象，取得了良好的社会和经济效益。

五、5T 系统

5T 系统(THDS、TFDS、TADS、TPDS 及 TCDS，简称 5T)是利用红外线轴温探测系统(THDS)、货车运行故障动态图像检测系统(TFDS)、货车滚动轴承早期故障轨边声学诊断系统(TADS)、货车运行状态地面安全检测系统(TPDS)、客车运行安全监控系统(TCDS)等先进的检测手段和信息化技术，对运行中的客货车辆进行动态检测、集中监控的综合系统。

1. 红外线轴温探测系统

该系统利用轨边红外线探头，对通过车辆的每个轴承的温度进行实时检测，并将检测结果实时上传到铁路局车辆运行安全检测中心，进行实时报警。通过配套故障智能跟踪装置，实现车次、车号跟踪，热轴货车车号的精确预报。本系统重点探测车辆两轴承温度，对热轴车辆进

行跟踪报警，防范热切轴事故。目前，THDS已实现了联网运行，每个探测站都能直观显示车辆轴温探测信息，实现跟踪报警。

2. 货车运行故障动态图像检测系统

该系统利用轨边高速摄像头，对运行货车隐蔽故障和常见故障进行动态检测，及时发现货车运行故障，重点检测货车走行部、制动梁、悬吊件、枕簧、大部件、钩缓等安全关键部位，重点防范制动梁脱落事故，防范摇枕、侧架、钩缓大部件裂损、折断，防范枕簧丢失和窜出等危及行车安全的隐患。

3. 货车滚动轴承早期故障轨边声学诊断系统

该系统是利用轨边噪声采集阵列，实时采集运行货车滚动轴承噪声，通过数据分析，及早发现轴承早期故障。重点检测货车滚动轴承内外圈滚道、滚子等故障，防范切轴事故。

4. 货车运行状态地面安全监测系统

该系统利用设在铁路正线直线段上的轨道测试系统，动态监测轮轨间的动力学参数，实现对货车运行状态的分级评判。TPDS同时兼有车轮擦伤及超偏载监测功能，重点防范货车脱轨事故，车轮踏面的擦伤和剥离，监视货物超载、偏载等行车安全隐患。另外，TPDS可以对运行品质不良的货车实施联网跟踪报警，向前方列检预报车轮踏面擦伤，预警货物超载。

5. 客车运行安全监控系统

该系统通过车载装置对客车运行安全关键部位进行实时监测和诊断，通过无线、有线网络，将监测信息向地面传输、汇总，形成实时的客车安全监控运行图，使各级车辆管理部门及时掌握客车运行安全状况。系统重点监测160 km/h及以上客车轴温、制动系统、转向架安全指标、火灾报警、客车供电、电器及空调系统运行安全状况。全线实现160 km/h及以上客车运行安全实时监控。重点防范客车热轴事故，防范火灾事故，防范走行部、制动部、供电、电器及空调故障。

铁路5T系统的建设实现了运输安全监控体系的三个转变——由传统向现代、由人控向机控、由粗放管理向集约管理的转变。通过该系统，各级车辆管理、决策部门能够全面掌握全路车辆运行质量状况，及时调整车辆运用、管理、维修维护政策和计划，实现车辆检修由定时修转向状态修，实现系统动态检测、数据集中、联网运行、远程监控、信息共享，构筑监控、管理、维修、决策为一体的监管体系。

除了上述信息系统外，铁路信息系统还包括铁路办公信息系统（Office Management Information System，简称OMIS）、铁路门户网站建设、基于SOA的智能化铁路信息系统构建等。

实现铁路运输现代化，需要行车装备、运输指挥和经营管理现代化，其基础就是实现信息现代化。只有实现了信息化，才能准确掌握运输生产情况，科学地进行组织指挥，才能跟踪市场动态，了解竞争对手情况，提高竞争能力，才能合理配置资源，提高经济效益。铁路信息系统及其安全保障技术在运输市场营销、运输组织指挥、运输经营管理、运输安全保障等方面将发

挥越来越重要的作用。

第二节　铁路信息系统建设总体目标与规划

2005 年铁道部在全路信息化工作会议上明确提出大力实施《铁路信息化总体规划》(以下简称《规划》),开创铁路信息化建设新局面。《规划》提出铁路信息系统建设要以运输组织、客货营销、经营管理为信息化建设重点,加强基础建设,整合既有资源,经过 5～10 年的努力,在东部地区和六大干线基本建成中国特色的铁路运输信息系统,至 2020 年在全路建成技术先进、结构合理、功能完善、管理科学、经济适用、安全可靠、具有中国特色的铁路智能运输信息系统,其总体水平跃居世界先进行列。实现调度指挥智能化、客货营销社会化、经营管理现代化,在提高运输效率、扩大运输能力、优化资源配置、保障运输安全、提高服务质量、提升管理水平、增加经济效益等方面发挥明显作用,为铁路跨越式发展提供技术支撑与保障。为了实现这一总体建设目标,《规划》将铁路信息化的体系结构概括为 3 大信息化应用领域、5 个基础平台、10 个建设方面、38 个具体应用系统,如图 1-1 所示。建设内容涵盖了铁路行业各主要业务环节。

一、铁路信息化重要应用领域

运输组织、客货营销、经营管理是铁路信息化的三大应用领域。运输组织领域的信息系统,主要服务于铁路运输的调度指挥、生产作业部门和人员,以提高运输生产效率和保障运输安全为目标,涵盖运输生产的各个主要环节。客货营销领域的信息系统,主要服务于铁路市场营销人员和旅客、货主,以提高铁路运输市场竞争能力、增运增收为目标,向旅客和货主提供优质服务。经营管理领域的信息系统,主要服务于运力资源、经营资源管理与运营决策支持的部门和人员,以保障铁路运输的运力资源的优化配置和降低运输成本为目标,提高铁路运输效益。

二、铁路信息化基础平台

铁路信息化的公共基础平台主要是为业务应用层的各应用系统提供公用的基础环境。公共基础平台包括通信网络基础平台、计算机网络与信息安全、信息共享平台、公用基础信息平台和铁路门户五类平台。

三、铁路信息化的主要建设方面和重要应用系统

在铁路信息化 3 个重点建设领域划分的基础上,铁路信息化可以分为 10 个主要建设方面和 38 个重要应用系统。运输组织领域包括运输调度指挥、运输生产组织、列车运行控制和行车安全监控 4 个方面 14 个应用系统。客货营销领域包括客运营销和货运营销 2 个方面 6 个应用系统。经营管理领域包括运力资源,经营资源、办公信息管理和决策支持 4 个方面 18 个

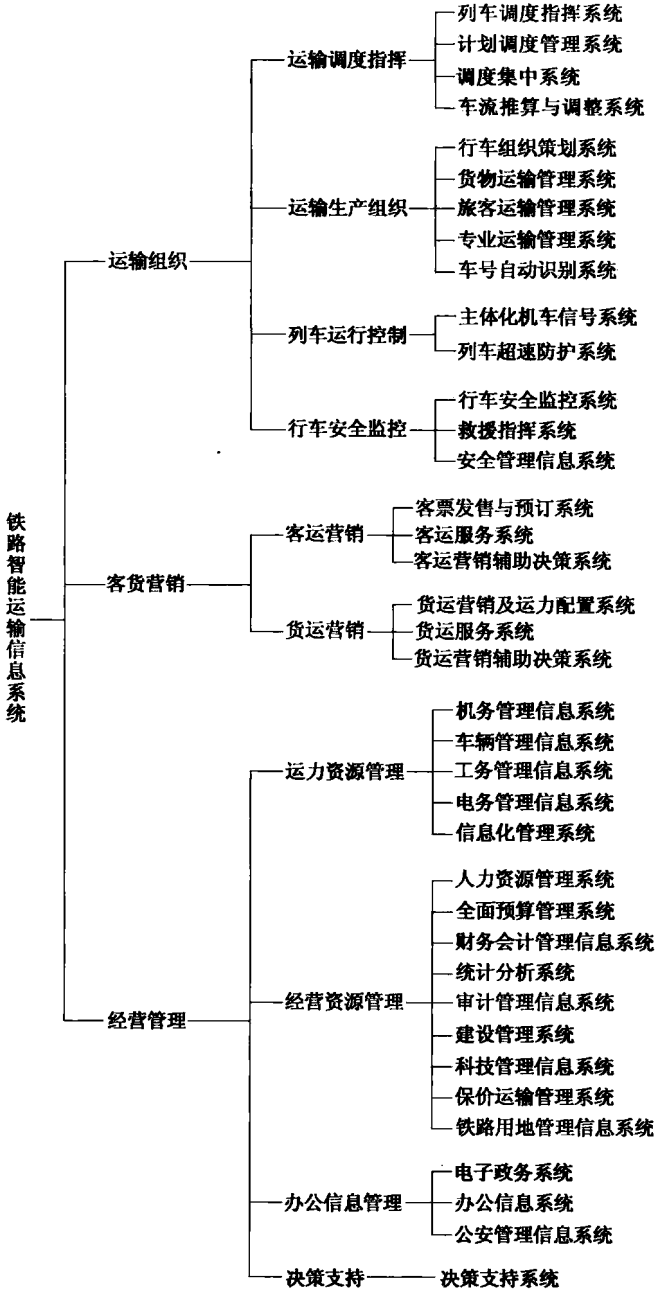

图 1-1　铁路信息化的体系结构

应用系统。

第三节　铁路信息系统的安全威胁

当前铁路信息系统与社会网络已经建立了千丝万缕的联系。每个城市都有客票代售点、货运代办点、内部信息收集接入点，大部分系统采用电话接入，致使铁路信息系统面临诸多安全威胁。过去，铁路信息系统开发过程中对安全的考虑和投入较少，许多应用系统的数据库是开放的，注册信息长期不变。近年来，随着 TMIS、TDCS、CTC、TRS、5T 等系统的建设，铁路信息系统在运输生产、指挥调度、资源配置、服务保障等领域发挥着越来越重要的作用。鉴于铁路信息系统具有规模大、结构复杂、网络接入点众多等特点，铁路信息系统的安全管理和维护面临着严峻的挑战。当前铁路信息系统的安全威胁主要包括以下几个方面。

一、外部或内部的非法入侵和攻击

铁路信息系统的网络可以划分为内部生产网、办公网和外部服务网三个部分。目前，许多应用系统、网络都可以通过 ADSL 拨号、无线网访问。随着接入点的不断增多，系统极易遭受来自外部或内部的非法入侵和攻击。以客票发售与预订系统为例，当黑客入侵一台客票代售点的终端后，采用转向入侵很可能实施大范围的网络攻击。另外，随着铁路信息系统网络规模的不断增大，内网设备的安全监控和管理日益复杂。安全管理制度漏洞、安全审计与设备监控手段不完善也会给内部人员实施攻击提供可能。

二、计算机病毒、蠕虫及恶意代码攻击

通过 E-mail、文件下载、网页浏览等方式，计算机病毒可能从外网、无线网入侵铁路信息系统。目前，多数铁路信息系统已经具备主机防病毒功能，然而，近年来由于蠕虫、木马等新的攻击手段的出现，计算机病毒仍有在全路快速蔓延的可能。

三、内部人员的误操作和违规操作

防止铁路信息系统业务人员、管理人员、系统操作员的误操作、违规操作，避免非法操作造成的经济损失和系统故障一直是铁路信息系统安全管理的一个重点。网络安全管理实践表明，业务和管理人员的误操作、违规操作可能导致信息系统数据库服务器数据的丢失、损坏和非法篡改，严重时会导致系统瘫痪。目前，由于一些信息系统尚未建立严密的操作监控与审计平台，在发生非法操作时，应用系统尚不能提供法律意义上的抗抵赖凭据。

四、网络和系统的安全漏洞隐患

铁路信息系统是一个典型的跨地域分布式异构复杂网络。网络拓扑结构上，多数系统以

铁道部为中心，通过 DDN 专线，2 M、10 M 以太网，100 M、1 000 M 光纤骨干网等构成一个覆盖全国的星形广域网。系统硬件方面，铁道部、铁路局及车站主机分别采用了 HP、Compaq、IBM、SUN 及 Siemens 等多个厂家、不同型号的产品。软件运行环境方面，服务器端操作系统有 HP UNIX、AIX、Solaris、DEC UNIX 及 SCO UNIX 等多个版本。网络的复杂性和应用系统的多样性不仅给系统管理、维护带来不便，而且容易导致网络安全漏洞的产生。

五、操作系统、通信协议及数据库系统的脆弱性

目前，铁路信息系统使用的操作系统大多数属于 TCSEC 的 C2 级。作为一般商业用途，C2 级操作系统的安全性是足够的。但是作为覆盖全国、关系国计民生的关键应用，铁路信息系统需要更高安全级别操作系统的支持。另外，TCP/IP 通信协议及商用数据库自身的脆弱性也会直接威胁铁路信息系统的安全运行。

六、计算机系统、网络设备及通信介质等硬件的损坏和敏感信息泄漏

由于铁路信息系统的网络规模大、范围广，入侵者很容易找到破坏点。利用搭线窃听、截取辐射等手段，入侵者可以捕获电缆、显卡、打印机等设备泄漏的信息。另外，网络通信基础设施的损坏也将直接影响系统安全。

七、安全管理策略不完善、员工安全意识薄弱

信息系统安全不完全是一个技术问题，行业里常讲“三分技术，七分管理”，因为许多安全事故源于人们缺乏必要的安全意识。例如，空口令、基于亲友生日的口令等。另一方面，信息系统的安全管理策略需要在实践中不断地完善和修改，许多安全漏洞是在系统运行过程中被不断发现的。当系统出现新的安全漏洞，管理策略未能及时弥补时，系统也将面临安全威胁。

第四节　铁路信息系统安全保障体系

目前，铁路信息系统的建设已初具规模，铁路计算机应用系统在行车指挥与调度、客货运输管理和经营管理等关键领域发挥着越来越重要的作用。覆盖全路的铁路计算机网络已经成为铁路信息化的重要战略基础设施。在多年的建设过程中，信息系统的安全始终被视为重要的建设目标，铁道部及相关部门采取了许多安全保障技术和管理措施。如在网络中部署防火墙、入侵监测系统、查杀病毒软件。在管理方面进行过安全评估，同时制定了一系列的安全管理条例，如《铁路计算机信息系统安全保护办法》等。这些措施对于保障网络和信息系统安全起到了重要的作用。随着铁路信息化应用安全需求的不断提高，铁路信息系统急需加强整体的安全保障体系建设，以满足铁路运输生产日益发展的需求。

一、基于 P2DR 的铁路信息系统动态安全模型

1985 年，美国国防部国家计算机安全中心（NCSC）发布了可信计算机安全评估准则（TCSEC）。这个准则的发布对操作系统、数据库等方面的安全保障起到了很大的推动作用，被称为信息安全的里程碑。但是，TCSEC 是基于主机/终端环境的静态安全模型建立起来的标准，是在当时的网络发展水平下被提出来的。随着网络技术的快速发展，该标准已经不能完全适应当前的技术需要，无法完全适应分布式、动态变化、发展迅速的 Internet 安全需求。

传统的信息安全技术主要集中在系统自身的加固和防护上，这是一种不断增加“铠甲”的防御手段。由于没有紧密结合信息系统安全的实际需求，一味地强调安全防护系统的建设，一方面造成了安全防护系统在功能上的浪费，另一方面很难完全防范各类攻击。针对网络上日益严重的信息系统安全问题和越来越突出的安全需求，“动态安全模型”应运而生（如图 1-2 所示）。在整体网络安全策略（Policy）的控制和指导下，P2DR 模型利用各种检测工具（如漏洞评估、入侵检测等系统）了解和评估信息系统的安全状态，同时综合运用防护（如防火墙、操作系统身份认证、加密等手段）和响应工具将系统调整到“高安全”和“低风险”的状态。

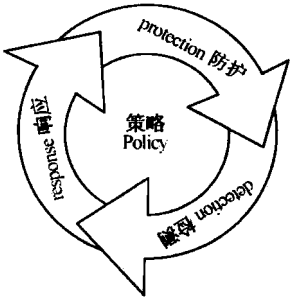

图 1-2　P2DR 安全模型

结合 P2DR 动态安全模型，铁路信息系统的安全目标应该是尽可能地增大保护时间，减少检测时间和响应时间。为此，一方面要加强防火墙、加密、认证等静态安全技术在铁路信息系统的运用和部署；另一方面，需要部署和建设全路统一的检测和监控网络，及时发现系统自身的脆弱性及外部威胁，为响应和防护提供可靠依据。

二、铁路信息系统的七层安全服务保障体系

铁路是国家的重要基础设施，其运输涉及国家的经济和其他重要活动。铁路信息系统安全是一个系统工程，单一的信息安全技术、管理和服务机制极其简单组合不能保证信息系统安全、有序和有效地运行。因此系统的安全需要对整个网络中的各个环节进行统一的综合考虑和规划。如图 1-3 所示，铁路信息系统的安全可以归纳为如下七个层次。

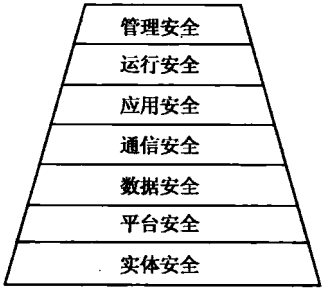

图 1-3　铁路七层安全服务保障体系

（一）实体安全

实体安全是铁路信息系统安全的基础，参照公安部实体安全标准，铁路信息系统实体安全包括机房安全、场地安全、机房环境（温度、湿度、电磁、噪声、防尘、静电、振动）、建筑防火、建筑防雷、建筑围墙、建筑门禁、设施安全、设备可靠性、通信线路安全性、辐射控制与防泄露、动力、

电源、空调、灾难预防与恢复。

（二）平台安全

平台安全泛指操作系统和通用基础服务安全，主要用于防范黑客攻击。目前，市场上大多数安全产品均限于解决平台安全。以通用信息安全评估准则 CC 为依据，铁路信息系统平台安全应该包括操作系统漏洞检测与修复、UNIX/Windows 系统及网络协议安全、网络基础设施漏洞检测与修复、路由器/交换机、通用基础应用程序漏洞检测与修复、数据库、Web/FTP/Mail/DNS/其他各种系统守护进程、信息安全产品部署。铁路平台安全的实施可以采用市场上常见的信息安全产品，如防火墙、入侵检测、脆弱性扫描和防病毒产品等。

（三）数据安全

数据安全的目标是防止数据的丢失、崩溃、非法篡改和被非法访问。根据用户的实际需求和数据安全的实际威胁，铁路信息系统数据安全的内容包括介质与载体安全保护、数据访问控制、系统数据访问控制检查、标识与鉴别、数据完整性、数据可用性、数据监控和审计、数据存储与备份安全。

（四）通信安全

为了保障铁路信息系统之间通信的安全，防止系统间通信的安全脆弱性威胁，铁路安全通信可以采取的措施包括通信线路和网络基础设施安全性测试与优化、安装网络加密设施、设置通信加密软件、设置身份鉴别机制、设置并测试安全通道、测试各项网络协议运行漏洞。

（五）应用安全

应用安全是保障铁路运输相关业务在铁路计算机网络系统上的安全运行。应用安全的脆弱性可能给铁路信息系统带来重大损失和致命威胁。结合铁路应用系统的特点及系统面临的实际威胁，铁路信息系统应用安全的评估内容包括业务软件的程序安全性测试（bug 分析）、业务交往的防抵赖测试、业务资源的访问控制验证测试、业务实体的身份鉴别检测、业务现场的备份与恢复机制检查、业务数据的唯一性/一致性/防冲突检测、业务数据的保密性测试、业务系统的可靠性测试、业务系统的可用性测试。测试实施后，测试部门需要有针对性地为铁路业务系统提供安全建议、修复方法、安全策略和安全管理规范。

（六）运行安全

运行安全是保障系统安全性的稳定，在较长时间内控制计算机网络系统的安全性在一定范围内。以网络安全系统工程方法论为依据，为运行安全提供的实施措施包括应急处置机制和配套服务、网络系统安全性监测、信息安全产品运行监测、定期检查和评估、系统升级和补丁提供、跟踪最新安全漏洞及通报、灾难恢复机制与预防、系统改造管理、信息安全专业技术咨询服务。运行安全是一项长期的服务，包含在信息安全系统工程的售后服务包内。

（七）管理安全

管理安全针对上述各个层次的安全性提供管理机制。铁路信息系统安全管理可以设置的机制包括人员管理、培训管理、应用系统管理、软件管理、设备管理、文档管理、数据管理、操作