文章编号：1005-8451（2015）02-0038-04

# 铁路信息安全等级保护实施工作建议

王亚民
（中国铁路总公司 运输局信息化部，北京 100038）

**摘 要：**信息安全等级保护制度是国家信息安全工作的基本制度，铁路行业在信息安全等级保护方面做了大量工作，对整个行业的信息安全工作起到了促进作用。本文从行业标准、系统定级备案、安全现状评估、等级保护测评、建设整改、安全措施落实等角度对如何将该等级保护工作落到实处进行了阐述。

**关键词：**信息安全；等级保护；安全实施
**中图分类号：**U29-39 **文献标志码：**A

## Implementation of railway information security level protection

WANG Yamin
( Informatization Department of Transport Administration, China Railway, Beijing 100038, China )

**Abstract:** Information security level protection system was the basic system of national information security work. A lot of work for the information security level protection was been down in railway industry to promote the industry of information security. This article was from the perspective of industry standards, system classification, security situation assessment, level protection evaluation, construction rectification and safety measures to elaborate on how to implement level protection work.

**Key words:** information security; level protection; security implementation

为适应国家铁路运输高速发展的需要，中国铁路总公司充分利用信息化手段，积极推进生产、经营、管理、决策等业务处理的全过程信息化，初步达到了行业运输生产自动化、客货管理现代化、高层决策科学化的总体目标，为铁路行业人、财、物集约化管理和数字化铁路建设提供了强有力的支撑。

中国铁路总公司（以下简称：总公司）从维护国家安全、社会稳定与公民权益出发，按照国家信息安全等级保护制度要求，将信息安全纳入铁路运输生产安全体系，自 2007 年铁路全面开展信息安全等级保护工作以来，对已投产运行的 49 个信息系统进行了定级，其中二级系统 24 个、三级系统 21 个、四级系统 4 个。但总公司信息安全等级保护工作相对国家有关标准规范和总公司信息安全实际需求还有一定距离，需要从以下几个方面加强。

## 1 行业标准制定

在信息安全方面，国家有一套完善的安全标准，涉及安全技术、等级保护、安全管理、安全设备等各个层面。但是国家标准是从宏观层面制定的策略，缺乏行业的针对性，需要在国家标准的基础上，针对行业的特殊要求，制定相应的行业标准。根据铁路现有信息化建设的总体情况，迫切需要制定以下几个方面的行业标准：

（1）与设计相关的标准：《铁路行业信息系统安全定级指南》，《铁路行业信息系统等级保护基本要求》，《铁路行业信息系统安全体系总体设计方案》，《铁路行业信息机房设计及建设规范》。

（2）与建设相关的标准：《铁路行业信息系统安全加固实施指南》，《铁路行业信息安全等级保护建设实施指南》。

（3）与运维管理相关的标准：《铁路行业信息系统上下线管理规范》，《铁路行业信息机房管理规范》。

## 2 系统定级备案

遵照公安部《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安 [2007]861 号）和《关于进一步做好铁路信息安全等级保护工作的通知》（铁公安 [2012]94 号）的文件精神，铁路总公司组织对目前用的部分信息系统进行了定级，但仍有

收稿日期：2014-10-08
作者简介：王亚民，高级工程师。

部分信息系统的安全方案还没有按GB/T 22239-2008《信息安全技术—信息系统安全等级保护基本要求》和GB/T 25070-2010《信息系统等级保护安全设计技术要求》对系统进行定级和安全设计。主要原因是国家标准只规定了定级的原则，对定级方法缺少可操作的指导意见，造成相关人员对定级标准和有关规定掌握不准，系统定为几级安全等级不好界定，因此需要针对铁路行业信息系统的业务特点，提出可操作的定级模型和定级方法，指导行业内人员对新建或已建信息系统开展系统安全定级工作。

## 3 安全现状评估

铁路投产运行的信息系统很多，有的系统按照等级保护要求确定了安全等级并建立了安全系统；有的系统在设计中考虑了安全等级，但在建设过程中并未按设计要求实施安全方案；还有的系统没有考虑安全措施。针对铁路信息系统投产运行后的实际情况，铁路总公司有必要组织内外部测评队伍，根据国家和总公司对信息安全的建设要求，对信息系统开展技术和管理两方面的现状评估，检查信息系统在物理安全、网络安全、主机安全、应用安全、数据安全以及安全管理上与相应安全等级标准的差距，进行差距分析，提出建设整改意见。

## 4 安全等级测评

在信息系统等级保护安全建设完成和投产之前，首先组织内部测评队伍对安全建设情况进行效果测评，发现不符合性提出整改建议。内部测评结束及整改验收后，再聘请有第三方测评资质的测评机构进行等级测评，验证与国家及行业等级保护标准的符合性。通过总公司内部和专业测评机构的两级测评，可有效地推进国家及行业信息安全标准在全路的落实完善。

按照GB/T 22239-2008《信息安全技术—信息系统安全等级保护基本要求》中的等级测评要求，信息系统在运行过程中，等级保护测评工作要定期开展，其中三级系统每年要测评一次，四级系统每半年要测评一次。根据该要求，结合每年铁路安全大检查工作的需要，制定每年的安全大检查计划，组织内外部专业测评队伍，对三级及以上的信息系统开展安全等级测评工作。

## 5 安全建设整改

### 5.1 机房物理环境整改

按照《铁路行业信息机房设计及建设规范》、《铁路行业信息机房管理规范》的要求，完善机房环境、设备管理、电源管理、安全管理和资料管理，并从防雷、防火、防水、防静电、防盗窃、防破坏、电力供应、机房电源及环境监控等方面对机房环境进行改造。

### 5.2 安全域划分

按照《铁路行业信息系统安全体系总体设计方案》，根据信息系统的安全等级，采用交换机划分VLAN、设置访问控制策略、部署防火墙等技术措施对信息系统进行安全域划分[1]。

### 5.3 边界网络防护

明确总公司信息网络、业务专网和互联网的网络边界，对网络边界部署内、外部网络访问控制策略、入侵检测等多项防护措施，并加强网络边界的监测。

### 5.4 主机安全加固

遵照《铁路行业信息系统安全加固实施指南》，通过配置安全策略、安装安全补丁、修补系统漏洞、强化身份鉴别等方法对各类主机设备的操作系统、数据库、中间件等及时进行策略配置和加固。

### 5.5 应用及数据安全防护

依照国家和行业标准，从用户身份认证、访问控制、数据加密、容错能力、日志审计等方面进行应用系统安全改造和建设。在数据安全防护方面，采用有效的数据备份策略对重要数据进行定期和增量备份，采用安全移动存储介质进行必要的数据交换。

### 5.6 强化信息安全队伍建设

从安全管理、运行、监督、技术支持等方面加强行业内信息安全队伍建设，确保安全责任落实。做好总公司、铁路局两级和一线服务、二线运维、三线技术支持安全运维服务队伍，负责各系统日常安全运行维护工作。

### 5.7 完善信息安全管理工作

为切实做好信息安全管理工作，总公司需要结合信息安全管理体系建设项目，以等级保护为抓手，

将等级保护与信息安全日常管理紧密结合，将信息安全管理全面纳入铁路运输安全生产管理体系，按照“谁主管谁负责、谁运行谁负责”和属地化管理原则，逐级落实信息安全责任，建立与总公司信息化发展相适应的信息安全监督机制、应急机制、故障通报与处理机制、事件责任追究机制和风险管理机制[2]。

总公司在加强信息系统建设管理方面，需制定一系列的规章制度，包括《铁路行业信息系统上下线管理规范》和《铁路行业计算机应用软件通用安全要求》等，明确系统定级备案、方案设计、产品采购使用、密码使用、软件开发、验收交付、等级测评、安全服务等管理内容。

## 6 安全措施落实

### 6.1 建立铁路信息系统安全技术体系

研究建立“一个中心（安全管理中心），三重防护（计算环境、区域边界、信息网络）”的铁路信息系统安全纵深防护和主动防御的技术体系，按总公司、铁路局、站段三级管理模式和信息系统运输生产专网、内部服务网、外部服务网三网的特点，实现运输组织及客货营销类信息系统“分级分区、专网专用、横向隔离、纵向认证”的安全策略，经营管理类信息系统“三级独立成域、主动防御、内外兼防”的安全策略。

### 6.2 建设铁路信息安全综合管理平台

铁路信息安全综合管理平台是为总公司及下属单位开展与信息安全管理相关工作的综合工作平台，功能将覆盖总公司及其下属单位的信息安全管理工作的主要内容，并支持公安部等级保护管理工作。平台主要提供以下 3 类功能：（1）以信息系统定级、备案、整改、测评和检查等规定步骤为主线，实现等级保护工作任务的下发、执行、进度监控和督办；（2）风险管理、应急管理、安全检查和事故通报等专项管理功能；（3）日常办公的综合管理、培训教育、标准管理等。

### 6.3 建设铁路信息安全一体化运行监控平台

铁路信息安全一体化运行监控平台是集综合网管、应用防护、IT 运维、机房监控为一体的信息系统安全运行监控管理平台，实现网络监控、主机监控、机房监控、边界防御、桌面终端安全的全方位监控功能。监控平台如图 1 所示。

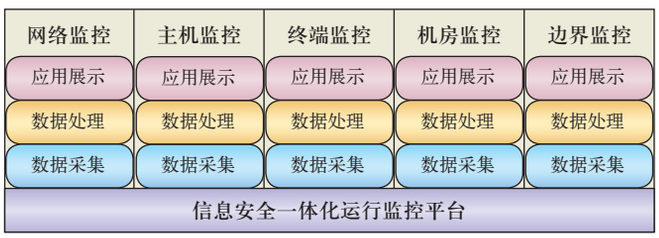


图1 信息安全一体化运行监控平台

### 6.4 开展国产化和自主可控技术研究

在信息安全越来越重视国产化的大技术背景下，开展铁路行业的信息安全国产化和自主可控技术的研究尤为重要。在国产化方面，紧紧围绕铁路网络安全自主可控战略目标，根据国产产品成熟情况，结合铁路业务发展、业务需求，按照“统筹规划、分步实施，应用牵引、平台重构，项目推动、政策保障”的工作思路，采取“直接采用、对等替换、平台替换”技术策略，进行信息系统国产化改造和构建铁路信息安全等级保护技术体系的积极探索。

在自主可控方面，通过统一标准、自主研发、自主实施、产权管理、风险评估、安全测评、安全管控、安全巡检等手段实现信息系统全生命周期各阶段的安全可控。

### 6.5 开展基于云计算的安全技术探索

云计算已成为信息技术的重要发展方向，建立铁路云应用平台将对铁路信息化应用技术产生深远影响。云计算环境下的信息安全问题是信息安全技术领域面临的一个新课题，在开展铁路云应用平台研究的同时，同步开展云安全应用技术的研究和探索，使基于云计算的铁路应用平台在设计、建设、投产 3 个环节将信息安全同步纳入。

### 6.6 建立铁路信息安全评测体系与技术督查体系

采用安全检查、风险评估、内外评测、安全运维等管理和技术手段，建立有效的安全测评与技术督查体系。通过在重要时间节点（如春运、暑运等）开展安全检查和自查工作，使路局、站段管理人员保持安全意识；按照等级保护标准要求定期开展风

（下转 P54）