文章编号：1005-8451（2011）06-0022-04

铁路信息系统安全风险评估研究

沈 路
（武汉铁路局 信息技术处，武汉 430071）

摘 要：简述了信息系统安全风险评估的内容，探讨铁路信息系统安全风险评估的实施方法，对如何加强铁路信息系统安全风险评估工作提出了建议。

关键词：信息系统；安全；风险评估
中图分类号：U29-39 文献标识码：A

Discussion on security risk assessment of Railway Information System

SHEN Lu
(Information Technology Department of Wuhan Railway Administration, Wuhan 430071, China)

Abstract: This paper introduced the content of security risk assessment for Information System, discussed the implementation about the security risk assessment for Railway Information System, porposed the suggestion to enhance the work of security risk assessment for Railway Information System.

Key words: Railway Information System; security; risk assessment

随着我国经济社会的迅速发展，信息化建设取得令人瞩目的成绩，信息系统在各行各业的生产、经营工作中发挥着越来越重要的作用。铁路信息化是铁路现代化的重要标志，也是覆盖铁路现代化全局的战略举措。随着铁路各专业对铁路信息系统依赖程度的日益增加，信息系统安全问题受到普遍关注。

信息系统安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息系统安全风险，将风险控制在可接受的水平，最大限度地保障信息系统安全提供科学依据。

1 信息系统安全风险评估

信息系统安全风险评估工作主要是评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对各单位造成的影响。评估中的要素包括资产、风险、威胁、脆弱性和安全措施等内容，见图1所示。

收稿日期：2011-05-02
作者简介：沈 路，高级工程师。

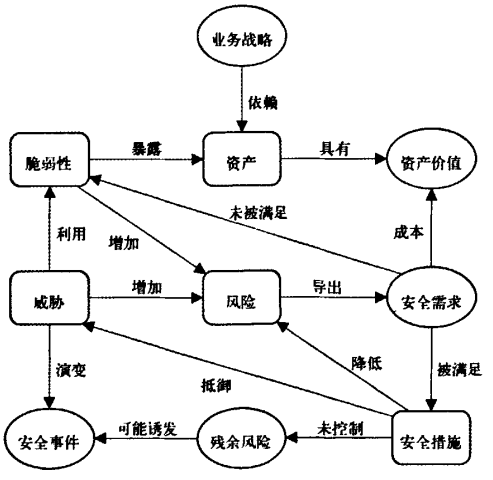

图1 风险评估要素关系

信息系统安全风险评估围绕着基本要素展开，在对基本要素的评估过程中，要充分考虑业务战略、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。

通过信息系统安全风险评估，各单位能进一步提高对信息系统资产价值的认识，识别出资产中存在的威胁和威胁发生时资产的脆弱性，根据威胁和威胁利用脆弱性的难易程度判断安全事件发生的可能性，并由此计算安全事件可能给单位造成的损失，从而鉴别信息系统是否存在不可接

受的风险，并因此确定是否要对当前的安全措施进行修正和完善，以不断提高单位对信息系统安全管理的能力和水平。

2 铁路信息系统安全风险评估的实施步骤

铁路信息系统安全风险评估过程就是在评估标准的指导下，综合利用相关评估技术、评估方法，针对铁路信息系统展开评估工作的完整历程。铁路信息系统安全风险评估可以分为3个阶段：评估准备阶段、要素识别阶段、风险分析阶段。铁路信息系统安全风险评估的具体过程可以参考图2。

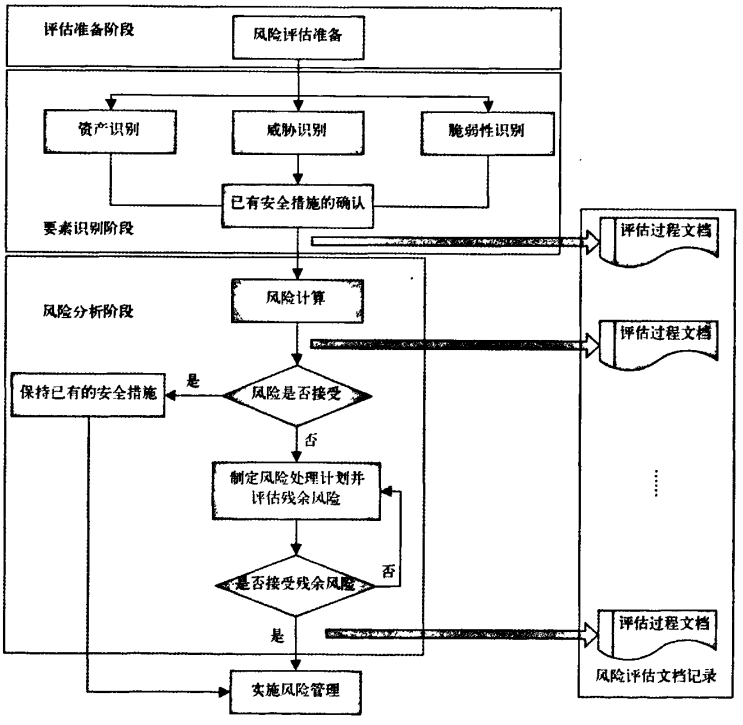

图2　铁路信息系统安全风险评估的实施步骤

2.1 评估准备阶段

评估准备阶段主要是要明确评估目标、确定评估范围、组建评估小组，对主要业务、组织结构、规章制度和信息系统进行初步调研，并进一步研究确定风险分析方法和评估项目的实施方案，以指导后续工作的开展。评估准备阶段是进行铁路信息系统风险评估的启动环节，只有通过充分的调研、准确的分析和精密计划，才能保证整个评估共组的顺利开展。

2.2 要素识别阶段

要素识别阶段的工作内容是对铁路信息系统安全风险的资产、威胁和脆弱性等几个要素进行识别，并验证已有的安全措施的有效性，同时要根据风险评估方法对各相关要素进行分类量化赋值，为风险分析阶段提供必要的基础数据。

2.2.1 资产识别

铁路信息系统的资产包括文档数据、软硬件产品、外部服务、关键人员等内容。资产识别主要是评价其保密性、完整性和可用性，3个安全属性的达成程度或者是这3个安全属性未达成时造成的影响程度。一般通过对资产的保密性、完整性和可用性进行量化赋值，并进行加权计算得到资产价值最终量化赋值结果。

2.2.2 威胁识别

铁路信息系统的威胁主要包括自然灾害、环境影响、系统故障、网络故障、设备故障、操作错误、管理失职、越权访问、网络攻击、恶意代码攻击、篡改信息、物理破坏、信息泄露等内容，可按威胁出现的频率分类量化赋值。

2.2.3 脆弱性识别

脆弱性识别是风险评估中最重要的一个环节，要以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估。铁路信息系统的脆弱性包括物理环境、网络结构、系统软件、应用系统、保护策略、组织管理等方面的内容，可以根据脆弱性对资产的暴露程度、技术实现的难易程度对已识别的脆弱性的严重程度进行量化赋值。

2.2.4 已有安全措施的确认

安全措施的确认应该是评估安全措施的有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。对有效的安全措施应当继续保持，对确认不恰

当的安全措施应当取消或进行修正完善。

2.3 风险分析阶段

风险分析阶段的主要内容是根据前面两个阶段的数据，采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性，并对风险评估的结果进行等级化处理。对发现的不可接受的风险根据导致该风险的脆弱性制定风险处理计划，选择合适的安全措施以降低风险的影响，并进行再次评估以确定残余风险是否已经降低到可接受的水平。风险分析结束时，风险评估小组要提供风险分析报告和风险控制建议。

2.3.1 风险计算

风险计算的常用函数为：

$$R=f(L(t,v),F(a,v)) \quad (1)$$

其中，R 表示风险值，a 表示资产价值，t 表示威胁发生的频率，v 表示脆弱性严重程度，L 表示威胁利用资产的脆弱性导致安全事件的可能性，F 表示安全事件发生后造成的损失。常用的风险计算方法有矩阵法和相乘法两种，相对而言相乘法比较简单而且应用较广。常用的相乘法的计算方法为：

$$z=f(x,y)=\sqrt{x\cdot y} \quad (2)$$

其中 x 和 y 代表要素所赋的数值。

风险计算的步骤为：

（1）对要素威胁和脆弱性使用相乘法计算威胁利用资产的脆弱性导致安全事件的可能性；（2）其次对要素资产和脆弱性使用相乘法计算安全事件发生后造成的损失；（3）对安全事件发生的可能性和安全事件发生后造成的损失使用相乘法计算风险值。

对于信息系统的任何一个资产而言，可能面对不同的威胁和不同的脆弱性，而同一个脆弱性又可能被不同的威胁利用，因此对于信息系统的每一项资产所面对的每一项威胁及其对应的每一项脆弱性都要进行计算。

2.3.2 风险结果判定

为了实现对风险的控制与管理，应当对风险评估的结果进行等级化处理。一般可以将风险划分为5个等级，等级越高，风险越大。评估小组要根据风险值的计算结果设定不同等级的风险值范围，并对每一个风险计算结果都进行等级化处理。等级化处理后，如果资产的风险是可以接受的，应保持现有的安全措施不变；如果资产的风险不可接受，必须调整安全措施以降低安全风险。

3 对铁路信息系统安全风险评估工作的建议

当前铁路信息系统安全风险评估工作的重要性已经得到广大信息技术工作人员的认可，但是由于铁路信息系统安全风险评估工作起步较晚，对铁路信息系统安全风险评估的研究还不深入。另外，由于铁路信息系统的不断发展，以及其所在环境的不断变化，任何安全措施都不能保证在铁路信息系统长时间运行过程中的万无一失。因此，应当对铁路信息系统进行定期安全风险评估，以保证铁路信息系统的安全运行。因此，对于铁路信息系统安全风险评估工作建议如下：

3.1 进一步加强铁路信息系统安全风险评估的制度建设

（1）建立铁路信息系统安全风险评估标准，保证风险评估工作开展有据可依、方法正确。（2）建立铁路信息系统安全风险评估机制，明确相关部门在信息系统安全风险评估工作中的职责，确定信息系统安全风险评估周期及结果运用办法。（3）细化铁路信息系统安全风险评估办法，使信息系统安全风险评估在信息系统的规划、研发、建设、运维、升级及退出的整个生命周期都能有效地开展。（4）解决好信息系统安全风险评估与铁路信息系统等级保护工作之间的衔接问题，让信息系统安全风险评估为铁路信息系统安全保护工作提供科学的依据，为确立信息系统的安全保障能力提供判断标准。

3.2 进一步加强铁路信息系统安全风险评估人员培训与技能管理

（1）加大培训力度，制订全路信息系统安全风险评估工作的培训计划，编写培训教材，通过学习提高技术水平。（2）合理使用社会资源，通过聘请富有经验的专家、学者，或是邀请第3方评估机构在路内进行评估试点，并组织评估人员现场学习和交流，不断积累评估工作经验，提高实际评估技术能力。（3）对技术人员进行系统的认证培训，实行信息系统安全风险评估工作持证上岗。

3.3 进一步加强铁路信息系统安全风险评估的研发与创新

（1）加大研发力度，针对铁路信息系统现状研制出专业的风险评估工具。（2）创新工作思路，将信息系统安全风险评估工作与信息系统运维工作紧密结合，充分使用信息系统安全风险评估工具和计算机系统监控等自动化平台代替人工劳动，争取对信息系统进行实时风险分析，实现铁路信息系统的安全可控。

4 结束语

铁路信息系统安全风险评估工作对于铁路信息系统的安全运行至关重要，只有不断提高认识、完善机制、加强管理，才能真正推动铁路信息系统安全风险评估工作不断发展，保证铁路信息系统安全稳定运行，为铁路协调发展、和谐发展、可持续发展提供坚实的信息技术支撑。

参考文献：

[1] 宁家骏.关于推进我国信息安全风险评估的思考[J].专题研究，2010，9.

[2] 冯登国，张　阳，张玉清，等.信息安全风险评估综述[J]，通信学报，2004，7.

[3] 信息安全技术信息安全风险评估规范[S]. GB/T 20984—2007.

[4] 范　红，冯登国，吴亚非.信息安全风险评估方法与应用[M]，北京：清华大学出版社，2006，5.

责任编辑　徐侃春

（上接P21）

据中心系统框架的管理体系，在系统建设与运行的各环节进行规范和约束。

4.6 技术平台和规范

（1）体系架构规范。以面向服务架构（SOA）为支撑，各专业系统的不同功能单元通过二次开发，包装成服务（Webservice），在共享平台的企业服务总线注册，供各类应用系统调用。（2）应用接口规范。各专业系统把应用模块包装成符合服务（Webservice）规范的接口。（3）数据接口规范。数据交换原则上采用XML格式，借助于多种数据传输方式。（4）既有系统改造。既有系统功能模块，可按照应用接口规范进行改造，注册到共享平台的企业服务总线，对外提供服务调用。既有系统数据可通过中间件或服务调用方式集中到数据中心。（5）数据字典规范。数据字典定义采用国标、铁标数据字典定义及规范，根据业务发展需要进行必要延伸。（6）用户认证规范。新建系统必须采用共享平台提供的统一用户身份认证，用户权限采用共享平台统一认证与应用系统两级管理方式。

5 实施方案

基本思路是，整合现有应用系统和业务流程，搭建面向服务的技术架构（SOA），提供地理信息系统(GIS)和门户(Portal)展示平台。

（1）系统环境构建。包括网络、服务器环境构建和共享平台构建。该阶段主要困难在于协调各专业系统将现有的复杂的网络环境实现互联互通。

（2）业务数据集中。将各专业业务原始数据采集、处理、集中到数据中心。该阶段主要困难是协调各专业系统提供数据采集接口。

（3）应用中心构建。根据各专业系统的需求，整合各专业系统应用，开发各专业系统的服务组件，构建应用平台。该阶段主要困难是协调各专业系统明确业务需求，组织协调开发相关应用。

6 结束语

当前，上海铁路局正按照构建覆盖全局的安全生产指挥中心的统一部署，加快推进信息资源整合，强化信息共享平台建设，力争用较短的时间，为全局信息化可持续发展打下良好的基础，为铁路加强安全管理、推进社会化信息服务提供优良的技术保障。

参考文献：

[1] 铁路信息化总体规划[Z]，中华人民共和国铁道部，2005.

[2] 李学伟.铁路信息资源管理与规划[M].北京：中国铁道出版社，2009.

[3] 刘　云.铁路信息系统集成与应用[M].北京：中国铁道出版社，2009.

责任编辑　徐侃春