文章编号：1005-8451（2016）10-0016-05

基于全生命周期且以风险为导向的信号系统独立安全评估

刘正东[1, 2]，杨　劲[1, 2, 3]，王成国[1]，于增明[4]
（1.重庆英华轨道交通安全评估服务有限公司，重庆　401123；
2.重庆市科学技术研究院，重庆　401123；3.重庆工商大学，重庆　400067；
4.信息产业部　电子第六研究所，北京　100083）

摘　要：主要对城市轨道交通信号系统的独立安全评估方法的应用进行研究，对基于全生命周期且以风险为导向的独立安全评估方法进行详细介绍，并与传统的以技术为导向方法进行比较。文章提出的方法更注重信号系统运营中的危害，对其潜在的风险进行控制及管理。独立安全评估可以帮助信号系统集成商将风险等级尽可能降低，为城市轨道交通信号系统的运营安全提供保障。该方法可以应用于城市轨道交通信号系统的设计和实现过程，以满足轨道交通主管部门提出的安全完整性等级要求。

关键词：信号系统；危害和风险；独立安全评估；生命周期；安全完整性等级
中图分类号：U284：TP39　**文献标识码：**A

Based on Whole Lifecycle and Risk-oriented Method of ISA of Railway Signal System

LIU Zhengdong[1,2], YANG Jin[1,2,3], WANG Chengguo[1], YU Zengming[4]
(1. Chongqing Railway Safety Management and Certification Centre Co. Ltd., Chongqing　401123, China;
2. Chongqing Academy of Science & Technology, Chongqing　401123, China;
3. Chongqing Technology and Business University, Chongqing　400067, China;
4. The 6th Research Institute of China Electronics Corporation, Beijing　100083, China)

Abstract: This paper researched on the application of the method of independent safety assessment of Signal System for Urban Transit, introduced a method based on the whole lifecycle and risk-oriented of independent safety assessment in detail, compared it with traditional technology oriented method. The proposed method focused on the hazard existing in the operation of Signal System, could control and manage the potential risks. Independent safety assessment (ISA) could help the signal system integrators reduce the risk level as lower as possible, and ensure safety for the operation of Urban Transit Signaling System. This method can be applied to the design and implementation of the Signal System, meet the requirements of safety integrity level proposed by the competent department.

Key words: Signal System; hazards and risk; independent safety assessment(ISA); life cycle; safety integrity level(SIL)

信号系统为列车控制系统的核心系统，指挥列车安全运行，关系着乘客的生命和财产安全。因此，为了保证安全运营，对信号系统/设备的安全性提出了最高的要求（SIL4）。随着计算机技术在铁路信号系统中的应用，原有的基于技术的安全质量保证方法已不能满足铁路信号系统越来越高的安全要求，基于全生命周期且以风险为导向的方法在铁路信号系统中的研究和应用已成为必然。

收稿日期：2015-11-04
作者简介：刘正东，工程师；杨　劲，高级工程师。

1　信号系统独立安全评估概述

信号系统作为保证列车安全、正点、快捷、舒适、高密度不间断运行的重要技术装备，在轨道交通系统中有着举足轻重的地位。为保证轨道交通的安全运营，应当在信号系统投入使用前，对其安全性进行独立安全评估。

1.1　独立安全评估定义

独立安全评估（ISA，Independent Safety Assessment）是根据铁路应用标准，例如：EN5012X 或

IEC61508，对铁路安全关键系统进行安全方面的审查和现场审核，并且给出系统在安全方面的评估报告。

独立安全评估的特点：独立性（与供应商、运营商独立）、专业性（专注系统安全和风险）、伴随系统全生命周期平行进行（从概念、需求、设计等到最后的验收、运营）。

1.2 独立安全评估发展历程

独立安全评估首次于 2008 年引入国内，国产化首套信号系统通过产品 ISA 认证，并在北京亦庄线信号系统中使用；2009 年至 2013 年信号系统的独立安全评估在国内开始逐步推广，国务院、住建部和质监总局等先后颁发了 ISA 相关的标准和指导意见。

国内从 2008 年至 2012 年，先后对欧洲颁发的轨道交通信号系统独立安全评估所参考的标准进行翻译并形成对应的国家标准。目前国内指导独立安全评估活动的标准主要包括，EN50126/EN50128/EN50129 /EN50159 及对应国家标准 GB/T28808/GB/T21562/GB/T28809 /GB/T24339 等。

2 信号系统风险管理技术研究

2.1 风险管理及控制流程

城市轨道交通信号系统应保障列车的安全运营、人员的生命及财产安全，将信号系统存在的风险降低到合理的、可接受的水平。

信号系统的风险管理及控制流程包括：危害识别、风险分析、风险控制和风险监控，如图 1 所示。后续小节将对风险管理及控制关键流程的要求和方法进行介绍。

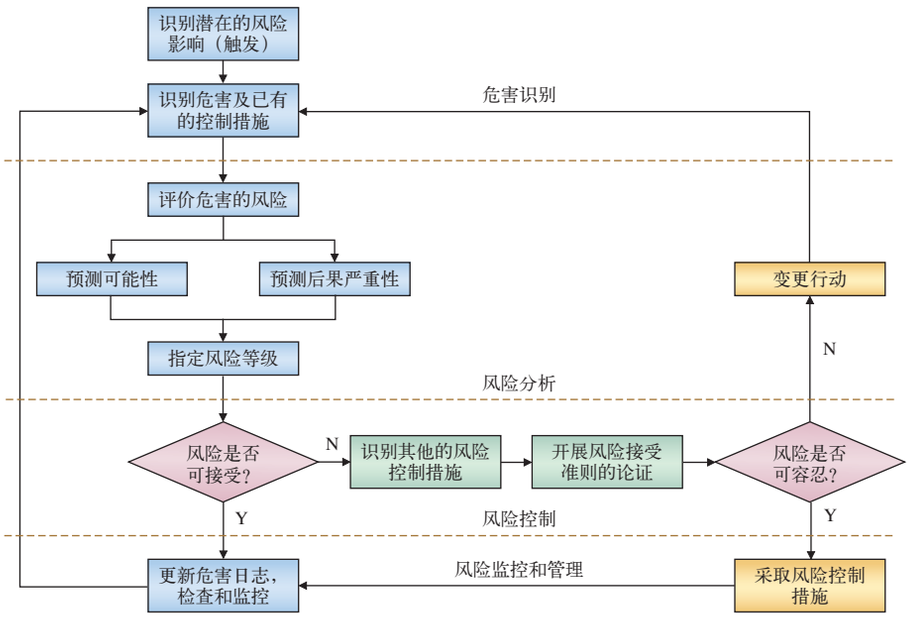

图1　风险管理及控制流程图

2.2 危害识别

信号系统的风险管理应界定风险管理对象与目标，确定风险评估的系统或设备，制定信号系统的安全完整性等级（SIL）标准要求。轨道交通主管部门应定义系统（与技术实现无关）、识别与系统相关的危害。

危害识别包括对产品、流程、系统或任务进行系统的分析，以确定在整个生命周期中可能发生的造成人员伤害或环境破坏的不利条件。危害依赖于系统定义，特别是系统边界，系统和子系统的危害可以分层构建。这也意味着危害识别和原因分析应在系统和子系统层次间重复进行。

如图 2 所示，在系统层面一个危害产生的原因可认为是子系统级的一个危害（针对子系统边界），这是一种结构化和层次化危害分析和危害跟踪的方法。即子系统危害是系统产生危害的原因，系统级的危害最终导致事故。

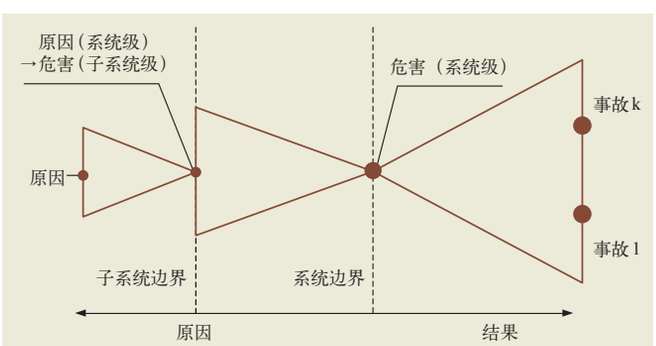

图2　危害分析和危害跟踪方法

所识别的危害宜按风险等级排序，并且所有已识别的危害和其他相关信息应记录在危害日志中。危害日志主要记录危害描述、危害的风险分类和风险

控制等信息的表格，包括但不限于以下内容：危害编号、危害描述、可能成因、影响 / 后果、原本风险（频率、严重性、风险等级）、剩余风险（频率、严重性、风险等级）、减轻措施、状态等。

2.3 风险分析

风险分析即时对识别出的危害进行进一步分析，分析内容主要包含以下几个方面：

（1）后果分析：危害导致的事故；

（2）原因分析：导致危害发生的原因；

（3）定量分析：危害发生的频率；

（4）定性分析：危害导致事故的严重程度。

其中，轨道交通主管部门应负责风险事故损失分析、定义风险接受准则（比较常用的风险接受准则有 ALARP/MGS/GAMAB/MEM/NMAU 等）、导出可容许危害率（THR）。其中，对于 THR 需求，供应商会将 THR 连同系统方案提供给轨道交通主管部门，或者轨道交通主管部门和供应商户一起来确定这些需求。

风险分析的方法应根据信号系统的特点、评估要求和风险类型进行选取，风险分析方法主要包括以下 3 类：

（1）定性分析方法，包括检查表法、专家调查法（包括德尔菲法）、“如果……怎么办”法、失效模式和影响分析法（FMEA）；

（2）定量分析方法，包括可靠度分析法、等风险图法、神经网络方法、数值模拟法等；

（3）综合分析方法，包括专家信心指数法、事故树法、事件树法、影响图方法、风险矩阵法等。

通过对风险的分析和评估，可以输出各种危害的发生频率、严重程度及风险等级等数据。

2.4 风险控制

风险控制包括对所必需的 THR 和相关安全功能的实施管理。风险控制主要是信号系统集成商以及各分包商的责任。风险控制管理是指对危害采取相关的控制措施、使风险降低到轨道交通主管部门可接受水平的具体实现的管理。

对于信号系统集成商：（1）需要根据轨道交通主管部门提供的风险接受准则，并结合风险分析的结果，判断各危害存在的风险是否达到了轨道交通主管部门可接受的水平；（2）需要对不可接受的风险制定降低风险措施，使其风险达到轨道交通主管部门可接受的水平。

风险控制措施的制定需要考虑以下几个方面：

（1）系统的功能；

（2）系统的应用环境要求；

（3）设计特点，建造特点；

（4）运营维护限制。

结合以上几个方面按照以下优先等级来选择风险控制措施：

（1）消除危害；

（2）降低危害发生频率；

（3）降低事故发生频率；

（4）降低事故发生后的损失。

2.5 风险监控和管理

对于危害识别、风险分析及风险控制的结果需要录入到危害日志，并进行动态管理。当发现新的危害或者危害的信息发生变化时需要及时更新危害日志，然后再进入流程循环，对新的危害进行风险分析并制定相应的控制措施，从而实现对风险的监控和管理。

3 基于全生命周期且以风险为导向的信号系统独立安全评估

传统的基于技术规范的安全质量保证方法是根据信号系统的技术标准及规范对系统进行设计和评估，此方法缺乏针对性，已不能满足越来越高的安全要求。基于全生命周期且以风险导向的方法，是将安全技术和理念贯穿于信号系统全生命周期，如设计、开发、生产、安装、运营和维护过程中。

以下是基于技术规范和基于全生命周期且以风险为导向的信号系统独立安全评估方法的分析比较。

3.1 基于风险的全生命周期

图 3 为一般系统的生命周期和具有安全需求的系统生命周期流程图，从生命周期各阶段要求来看，主要区别是在系统需求和设计阶段：

（1）以技术为导向的设计方法：起始阶段为系统规划阶段，根据系统的规划及行业技术规范编写系统需求，该系统需求主要是功能和性能方面的需

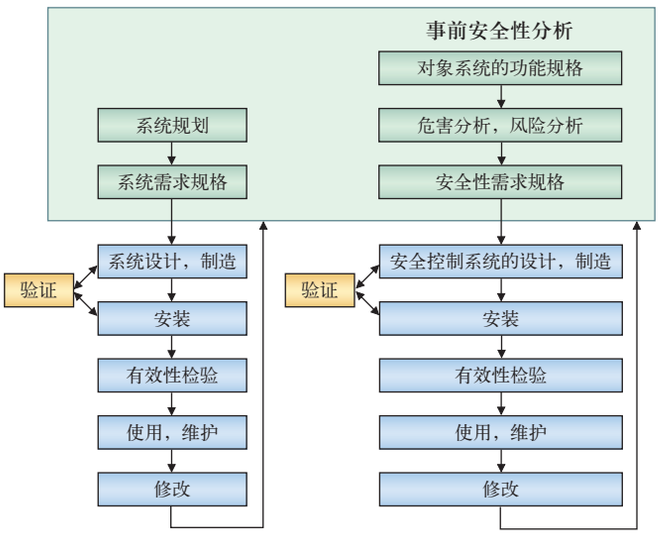

图3　系统生命周期流程图

求，不包括安全方面的需求；

（2）以风险为导向的设计方法：从事故发生前进行安全分析，从对象系统的功能规格入手，对其进行危害分析和风险分析，从而得出对象系统与安全相关的需求规格。

3.2　基于风险的安全系统设计特点

以技术为导向的方法：根据技术标准和规范等进行设计。从铁路信号系统层面来看，ATP/ATO、联锁、ATS 都是由相对独立的专家（或公司）进行设计、评审及控制，如图 4 所示。设计特点如下：

（1）各个子系统被认为是独立的系统，其设计依据为技术标准或用户要求；

（2）每个专家（或公司）关注在各自负责的子系统。

以风险导向的方法：是从影响运营安全的潜在危害入手，对整套信号系统进行分析。通过各种风险分析，根据风险分析结果可以将如控制进路、控制列车运行、监视等不同类型的功能分配到规划子系统中，如图 4 所示。

设计特点如下：

（1）各子系统的功能划分是根据危害的类别、风险分析的结论等来确定；

（2）各子系统的组成是根据功能接口和功能架构来决定；

（3）每个专家都需要相互合作，作为一个整体对安全进行管理。

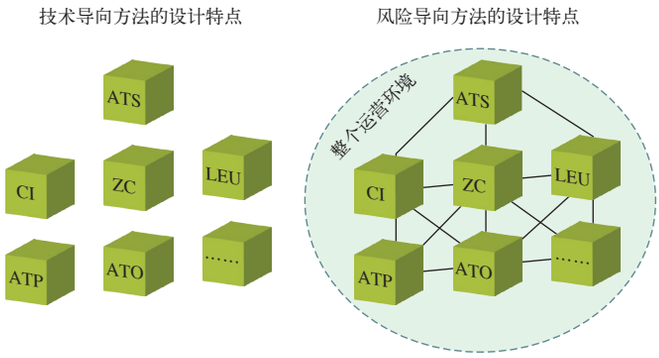

图4　技术导向方法和风险导向方法的设计特点

3.3　技术导向与风险导向的设计及实现方法对比

在设计和实现方面，技术为导向方法主要是根据铁路总公司颁发的相关技术标准进行设计，后期根据实际发现的问题进行更新；风险为导向方法是根据运营的要求，从安全角度考虑，对潜在的风险制定相应的改进措施，是基于安全需求的实现方法。技术导向和风险导向方法的差异比较如下。

技术导向的设计及实现方法：

（1）通过事故、经验、尝试和试验等来学习 / 改进；

（2）每个安全问题将被删除或附上补丁；

（3）设计规范和计划基于技术标准或内部规定；

（4）基于技术规范进行的的符合性评估。

风险导向的设计及实现方法：

（1）通过运营要求，满足安全需要，达到最低风险，可参考行业代表性的风险矩阵；

（2）系统地分配安全职责和需求；

（3）系统设计是基于安全需求；

（4）基于相关的安全过程文件进行符合性评估。

3.4　以风险为导向的独立安全评估特点

针对不同的信号系统设计方法，存在两种评估方法，即以技术为导向和以风险为导向的评估方法。以技术为导向的评估方法主要关注于系统设计的技术要求，系统的更新是在事故发生后进行修补升级；以风险为导向的评估方法主要关注于系统运营过程中面临的各种风险，对可能发生的危害是否进行规避、转移和控制等进行审核。表 1 对两种方法在独立安全评估活动中的区别及各自的关注点进行了对比说明。

4　结束语

综合上述，以风险为导向且贯穿全生命周期的

表1　2种评估方法的比较

特点	以技术为导向的评估	以风险为导向的评估
评估焦点	控制流程、技术规范	面临的各种风险
评估回应	事后的、不连续的	实时的、连续的监控
评估测试	重点在技术	重点在风险
评估方法	强调技术的完整性	强调所涵盖的各种风险的重要性
评估报告	控制效果和实质性控制缺陷	流程风险和风险管理建议 规避化风险、转移风险、控制风险
评估目的	评估与监控技术功能实现	确保危险得到控制，确保风险被降低到可以接受的水平等

信号系统独立安全评估方法比传统的技术导向的设计和评估方法更具备前瞻性，更关注于信号系统的潜在风险及风险管理过程。在信号系统安全评估过程中以风险为导向的评估方法，可以帮助集成商更好地对信号系统的全生命周期过程中的所有风险进行有效控制，并降低其风险等级，确保城市轨道交通的运营安全。

参考文献：

[1] 孙华平，张艳兵．北京地铁亦庄线信号系统工程独立安全评估 [J]. 城市轨道交通研究，2013（1）．
[2] 郜春海，燕　飞，唐　涛．轨道交通信号系统安全评估方法研究 [J]. 中国安全科学学报，2005，15（10）．
[3] 马　章．欧洲铁路信号系统安全性标准的学习与引进 [J]. 铁道通信信号，2007，43（8）．
[4] 赵　阳，张　萍，王　鲲．我国铁路信号系统安全评估的研究 [J]. 铁道通信信号，2010，46（2）．
[5] 范　明，王　菲．高速铁路信号系统的安全评估研究 [J]. 中国铁路，2009（2）．
[6] 唐　涛，燕　飞，郜春海．轨道交通信号系统安全评估与认证体系研究 [J]. 都市快轨交通，2004，1（17）．

责任编辑　徐侃春

（上接 P12）

[2] 王志斌．哈大铁路客运专线雪深监测系统研究 [J]. 铁道标准设计，2012（5）：165-168.
[3] 常瑜静，常瑜青．雪深传感器的安装及维护 [J]. 科技与企业，2014（14）：443.
[4] 王跃红．新型自动气象站数据异常的判断与处理 [J]. 中国农业信息，2015（17）：113.
[5] 杨　兰，郑美仪．浅谈自动气象站记录数据的维护、审核和异常情况处理 [J]. 气象研究与应用，2013（4）：70-73.
[6] 王柏林，花卫东，阳艳红，等．基于相位法激光测距原理的雪深传感器研究与应用 [J]. 气象科技，2013（4）：597-602.
[7] 王　彤．高速铁路防灾安全监控系统研究与开发 [J]. 中国铁路，2009（8）：25-28.
[8] 史　宏，王　彤，沈敬伟．高速铁路防灾安全监控系统测试技术研究 [J]. 中国铁路，2012（7）：61-64.
[9] 王　瑞，喻麒睿，王　彤．高速铁路灾害监测系统优化升级 [J]. 中国铁路，2013（10）：17-20.

责任编辑　徐侃春

（上接 P15）

行相应多路径选路算法的应用。

参考文献：

[1] Microsoft Corporation. Microsoft Storage Technologies Multipath I/O [DB/OL]. http://www. microsoft.com/windowsserversysterm/storage/technologies/mpio/default.mspx, 2011-3-1.
[2] 刘　明．存储区域网络冗余路径 [D]. 北京：北京理工大学，2004.
[3] 谭毓安，曹元大．冗余 SCSI 路径驱动程序的设计与实现 [J]. 北京理工大学学报，2002，22（5）：604-607.
[4] Microsoft Corp. Windows Server High Availability with Microsoft MPIO [DB/OL]. http: //www.microsoft.com/MPIO, January 2009.
[5] Microsoft Corporation. Microsoft Multipath I/O Step-by-Step Guide [DB/OL].http://technet.microsoft.com/zh-cn/library/ee619778(WS.10). aspx, 2011-12-13.
[6] IS0/IEC 14776-454. Information technology SCSI Primary Command-4(SPC-4) [S]. 2009.

责任编辑　徐侃春