轨道交通信号系统安全评估与认证体系研究

作者：唐涛　燕飞　郜春海

【摘　要】：轨道交通信号系统是保证列车运行安全，提高运输效率的安全相关系统，为了使该系统规范化、标准化、国际化，迫切需要建立一套轨道交通信号系统的安全评估与认证体系。本文首先介绍了轨道交通信号系统的功能和对其进行安全评估的迫切性，然后对相关的安全国际标准和国外安全认证体系进行了介绍和分析，最后结合我国轨道交通行业的实际情况探讨了在我国进行安全评估和认证的可行方法。

【关键词】：轨道交通　信号系统　安全认证　安全相关系统

1. 概述

随着社会进步、城市规模不断扩大、人口密度迅速增加，交通拥堵日趋严重已成为制约城市经济发展的一大障碍。由于城市轨道交通具有运量大、安全正点、快捷舒适及污染小等特点，建立以城市轨道交通为主的城市交通系统是解决城市交通拥堵问题的重要途径。人们对于城市轨道交通的要求越来越高，如何实现列车安全、快速、高效的运行是目前轨道交通领域亟待解决的根本性问题，作为保证行车安全、提高运营效率的轨道交通信号系统在提高运输效率、保证行车安全及旅客舒适度等方面具有决定性作用。

轨道交通信号系统是运用技术手段保证行车安全。它包括车站信号控制系统（车站联锁系统）和区间信号系统以及机车信号系统几个部分。信号系统的主要功能是保证行车安全、提高运营效率。信号系统虽然在工程投资中并不占很高的比重，但是由于信号系统担任着指挥列车安全运行的任务，关系到成千上万乘客的生命和财产安全，为此，需要专门考虑在系统出现故障，或操作人员不慎进行错误操作的情况下，系统仍能最大限度地维护乘客安全。目前无论是国产轨道交通信号系统还是国外设备国产化的推广应用所遇到的共同问题就是：国内开发的轨道交通信号系统缺乏权威的安全认证机构进行认证。而国际通行的方法都要求有安全认证这一步，这样国内开发的信号系统就难以参加相关项目的招投标。通过安全评估可以系统地从计划、设计、制造、运行等全过程中考虑信号系统的安全技术和安全管理问题，发现系统开发过程中固有的或潜在的危险因素，搞清引起系统灾害的工程技术现状，论证由设计、工艺、材料和设备更新等方面的技术措施的合理性学习。研究国际安全标准和相关的安全评估和认证体系，并结合中国轨道交通发展的实际情况建立轨道交通信号系统的安全评估和认证体系势在必行！

2. 相关的国际标准

世界发达国家的城市轨道交通系统已经有了百余年的发展历史，他们不断总结经验教训，完善管理，已经形成了一整套科学的安全评估、认证、管理体系，制定了一系列切实可行的安全评估的技术标准。

IEC61508 是国际电子电工委员会（IEC）制定的《电气/电子/可编程电子安全相关系统的功能安全》国际标准，是进行轨道交通安全评估和论证重要的参考标准。

在铁路运输领域里，人们对安全相关系统的研究主要集中于铁路信号控制系统中，首先

于 1963-1965 年在日本由信号保安协会开展起来，所进行的研究是以“电子技术信号设备的研究”为主体展开的，提出了相应的报告。

国际铁路联盟研究实验所（ORE）A118 课题在 1969 年至 1977 年期间共出版了 13 个报告和 2 个技术文件，系统地考证了“电子技术在铁路信号系统中的应用”， A155 课题在 1982 年至 1988 年期间发表了“在铁路信号设备中电子元器件的应用”报告，在 A155 课题的基础上，1990 年 1 月，国际铁路联盟（UIC）发布了 738R 规程，给出了安全信息的处理和传输的一系列建议。

欧洲国家在宣传和介绍 IEC61508 国际标准的同时，以 IEC61508 国际标准为基础，吸收该标准的精髓，制订行业标准。欧洲电气化标准委员会（CENELEC）下属 SC9XA 委员会，制定了以计算机控制的信号系统作为对象的铁道信号标准，它包括以下 4 个部分。

（1） EN－50126 铁路应用：可靠性、可用性、可维护性和安全性（RAMS）规范和说明。

（2） EN－50129 铁路应用：安全相关电子系统。

（3） EN－50128 铁路应用：铁路控制和防护系统的软件。

（4） EN－50159.1 铁路应用：通信、信号和处理系统。

它们的相互关系和涉及到的具体信号领域见图 2-1。

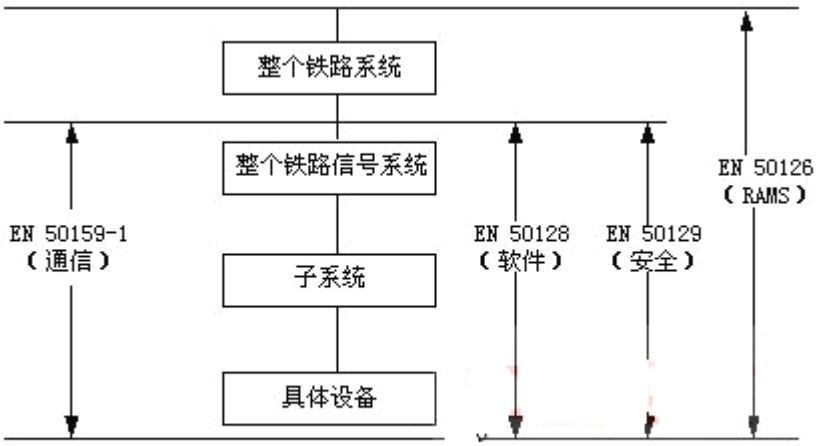

图 2-1 EN50126、EN50128、EN50129 和 EN50159-1 标准相互关系

2.1 IEC61508 标准

IEC61508 国际标准规范了电气/电子/可编程电子安全相关系统软硬件生存周期的各个阶段的任务和目标，提供一个制定安全需求规范的方法。它由 7 个部分组成：

第 1 部分 总的要求

第 2 部分 电气/电子/可编程电子系统的需求

第 3 部分 软件需求

第 4 部分 定义和缩略语

第 5 部分 决定安全完整性级别的方法实例

第 6 部分 应用 IEC61508－2 和 IEC61508－3 指南

第 7 部分 技术和方法总论

其主要目标：

1) 对所有的包括软、硬件在内的安全相关系统的元器件生命周期范围提供一个安全监督的系统方法。

2) 提供一个确定安全相关系统安全功能要求的方法。

3) 建立一个基础标准，使其可直接应用于所有工业领域，同时，亦可指导其他领域的标准，使这些标准的起草具有一致性（如基本概念、技术术语、对规定安全功能的要求等）。

4) 让使用者和维护者放心使用以计算机为基础的技术。

5) 建立一个概念统一、协调一致的标准。

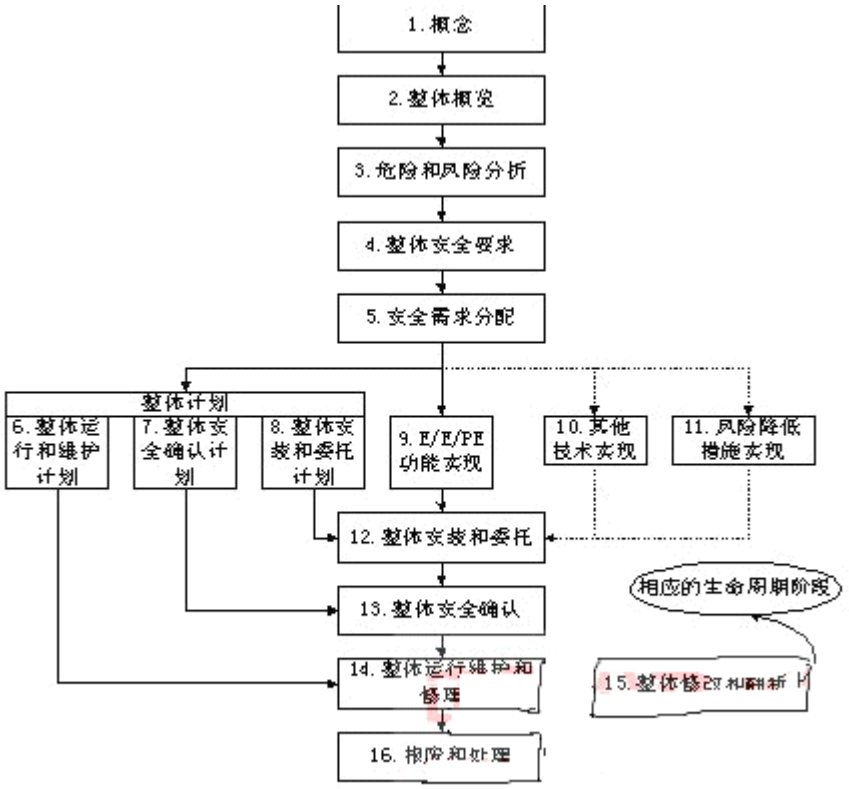

图 2-2　系统安全生命周期流程图

在 IEC61508 中有个重要的概念：安全生命周期。安全生命周期是指从方案的确定阶段开始到所有的电气/电子/可编程电子安全相关系统、其它技术的安全相关系统、外部风险降低设备不再可用时为止，这个时间周期内发生为实现安全相关系统所必需的活动。图 2-2 是 IEC61508 描述的系统安全生命周期流程图。

2.2 EN 标准

2.2.1 EN50126

该标准定义了系统的 RAMS（reliability、availability、maintainability 和 safety），即可靠性、可用性、可维护性和安全性，并且规定了安全生命周期内各个阶段对 RAMS 的管理和要求。但是在该标准中，未定义 RAMS 的具体的定量目标。此处的生命周期和 IEC61508 中安全生命周期是一个概念。

RAMS 作为系统服务质量衡量的一个重要特征，是在整个系统安全生命周期内的各个阶

段通过设计理念、技术方法而得到的。为了达到规定的RAMS，必须针对前面的RAMS影响因素，在整个系统的生命周期内有效控制RAMS的影响因素，即系统的随机故障和系统故障。EN50126要求在整个安全生命周期进行RAMS管理，针对每个阶段给出应需要完成的RAMS任务，同时给出相关的具体文档和要求。

2.2.2 EN50128

由于在信号系统中采用计算机（包括微机、单片机）越来越广泛，由软件来承担安全性需求的比重越来越大，因此软件安全性问题变得更加突出。为此EN50128针对软件的安全保证提出了相关的规范和设计标准。在该标准中，对铁路控制和防护系统的软件进行了安全完善度等级的划分，针对不同的安全要求制订了相应的标准，按不同等级对整个软件开发、检查、评估、检测过程包括对软件需求规格书、测试规格书、软件结构、软件设计开发、软件检验和测试、软硬件集成、软件确认评估、质量保证、生命周期、文档等提出相应的程序与规范的要求。

2.2.3 EN50129

这个标准定义了为了保证安全相关的铁路信号电子系统/子系统/设备安全所必须满足的条件。这些条件包括：

1) 质量管理措施
2) 安全管理措施
3) 功能和技术安全措施
4) 安全接受和论证

作为一个安全相关系统要作到系统的安全能够得到接受和论证，必须经过前三个步骤。EN 50129就是针对一个安全事例来指导系统研究开发人员在整个系统

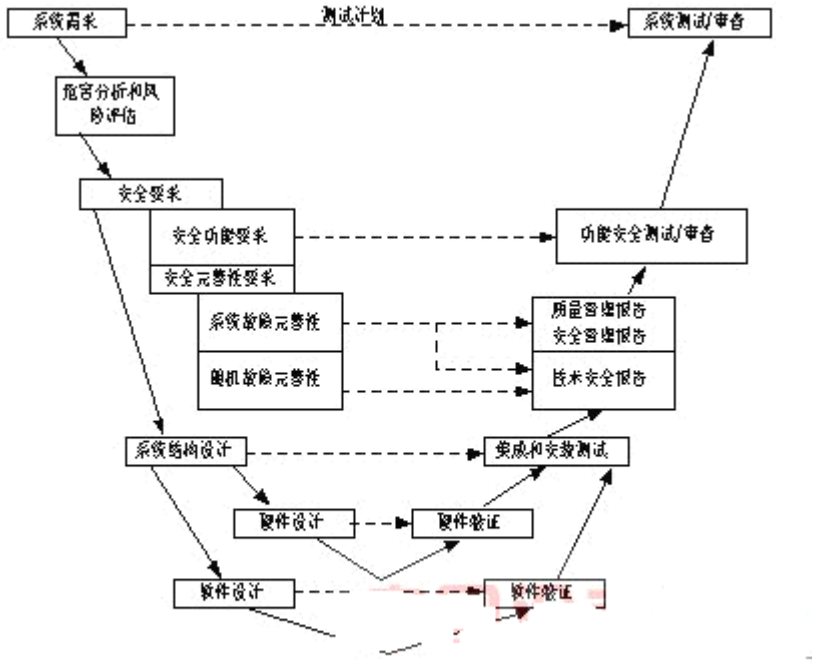

图 2-3 “V”安全设计周期

研制开发生命周期内所要完成的质量管理、安全管理和相关的技术安全措施的实施。对于安全管理，引入 IEC61508 提出的安全生命周期概念，就是说对于安全相关系统的安全部分，在设计时按照该步骤进行设计，并且需要进行全程的安全评估和验证，目的是进一步减少和安全相关的人为失误，进而减少系统故障风险。图 2-3 将系统各个层次的开发和评估论证对应起来，描述的是“V”字型系统安全生命周期。

2.2.4 EN50159.1EN－50159.1

铁路应用：通信、信号和过程控制系统在铁路中应用第一部分：封闭传输系统中安全相关通信。这个标准适用于采用封闭传输系统实现通信目的的安全相关系统。对安全相关设备和传输系统的通信接口信息传输提出安全要求。

3. 国外的安全评估体系

欧美国家开展轨道交通信号系统的安全研究比较早，目前已经形成了比较完善的安全评估体系，如英国 CASS 安全评估框架，德国 TUV 评估体系等，它们主要以 EN 铁路标准为基准，依托第三方评估机构，对已有线路和在建项目的信号系统进行安全性论证。下面以英国 CASS 安全评估框架为例进行详细说明。

3.1 英国 CASS 安全评估框架

CASS 是英国工商部（Department of Trade & Industry）和健康安全部门（Health & Safety Executive）制定的一个安全评估认证框架项目，为此还成立了 CASS 策划公司，它的任务和目标是为基于 IEC61508 标准的安全相关系统开发一个标准的认证框架。

在 CASS 框架中，评估员由权威部门考核和认证，并要求独立于运营商和系统制造商。评估员对认证机构负责，认证机构对客户负责。政府相关监督部门由具有安全认证经验的专家组成，CASS 也有自己的技术委员会，确保满足技术发展的需要，CASS 相关的标准和规范会根据 IEC61508 的修订进行修改。在英国 UKAS 是唯一授权安全论证

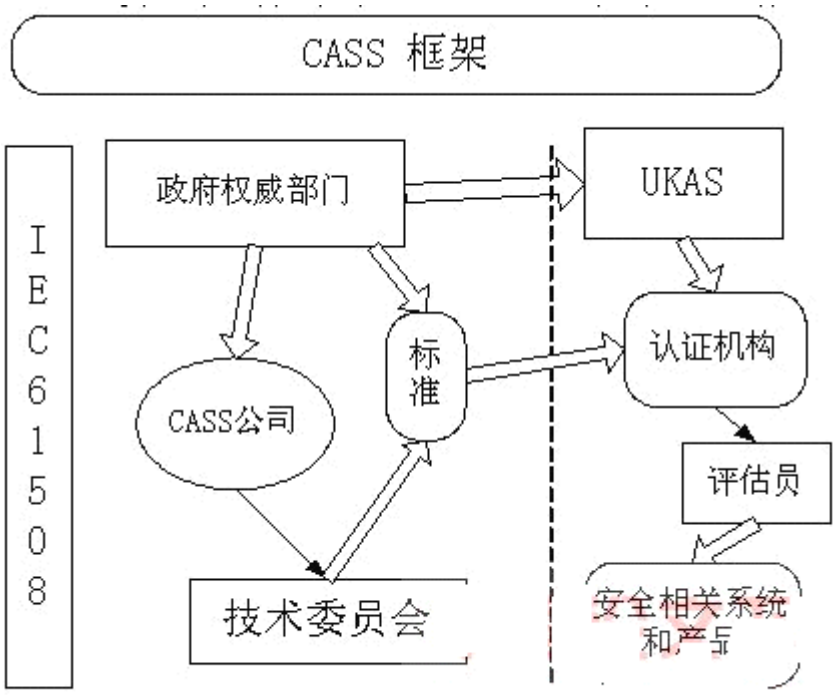

图 3-1　CASS 运作模型

的机构，进行 CASS 框架认证的机构都要向 UKAS 申请授权。系统制造商再向这些 UKAS 承认认证机构申请评估。CASS 公司会对评估员进行考核，监督评估过程[12]。

3.2 英国铁路工程安全评估原则和方法

目前英国在铁路安全管理中普遍应用 ALARP 原则（As Low As Reasonable Practicable）[13]，它是将安全相关系统的风险分成以下三类：

1) 足够大的风险，我们不能接收；

2) 足够小的风险，我们可以忽略；

3) 介于以上两种风险之间的风险，我们必须采取适当的、可行的、合理成本下的方法将其降到可以接收的最低程度。

对于第三种风险，我们采用 ALARP（As Low As Reasonably Practicable）原则进行风险的减低，该原则的含义是采用尽可能低的成本、合理的、可行的方法进行风险降低。我们将以上三种风险在图 3－2 中进行描述。

在图 3－2 的最上层，即高于不可接收风险等级，该部分的风险被认为是不可接收的风险，在任何情况下都不能，必须拒绝；

在不可接收风险等级以下，我们采用 ALARP 原则进行风险的减低，在该阶段，必须对风险减低而花费的代价进行评估，在风险和代价

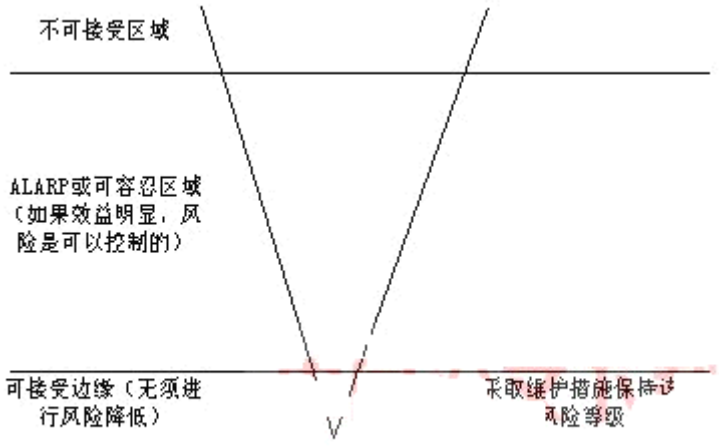

图 3-2　三种风险的关系

之间进行平衡。在可接收区域边缘以下，该区域的风险有些微不足道，可以忽略。我们不需要采用任何方式或方法去减低它，当然我们必须将该区域的风险始终保持在该等级水平上。

在 Railtrack 铁路咨询公司出版的工程安全管理黄页[13]中把安全评估过程分为两部分：安全审核和安全认证。

安全审核是要检查工程的安全管理是否完善，能否和安全计划保持一致。评估员应该检查一下安全计划里说明的标准和步骤是不是被正确的执行了，看一下工程行为和安全计划是不是具有继承性。安全审核最后要有一个安全审核报告，这个报告应该包括：对项目和安全计划一致性的评价、认为安全计划可行的评价和计划相符或是有所改进的建议。

安全认证是一个判断和系统相关的风险扩大或者减小到一定等级的过程。系统的安全要求是安全认证的核心。评估员应该根据产品制造商提供的安全事例（Safety Case）回顾一下安全需求规范以评价它对控制系统风险是不是已经足够，以及系统能不能满足安全需求规范。进行安全认证的目的就是收集足够的信息来证明系统的风险是可以接受的。

4.我国轨道交通信号系统安全评估与认证体系框架设想

我们设想中的轨道交通安全评估与认证体系参照的是 CASS 框架，由轨道交通主管部门牵头，组织专家组制定安全认证标准和方法，相关单位可以据此申请成为第三方认证机构，聘请评估员对于安全相关系统进行安全认证，包括安全认证机构、安全标准、安全认证方法以及相关各方（政府、设备生产企业、运营单位、认证机构）之间的制约关系、权利和义务等等。如图 4－1 所示。

可以概括为以下四个层次：

第一层次：在体系建立初期，政府主管单位集中安全、质量、科技、生产等管理部门成立轨道交通信号系统安全评估体系领导小组；

第二层次：安全评估体系领导小组组织权威专家和相关技术人员成立权威机构，进行安全评估相应标准和规范的制订工作；

第三层次：进行安全评估者的资格论证，考核独立的个人或机构进行安全评估的资格，这些个人或机构应独立与轨道交通信号系统的研制开发、生产、销售等业务；可以批准多个评估机构，但每年论证机构必须对这些评估机构或个人进行资格审查或评估；

第四层次：对参与信号系统设计、生产、维护、测试的主要人员进行安全设计、安全管理、

安全测试和安全生产方面的培训和评估，保证在整个体系中，安全意识得到整体体现。

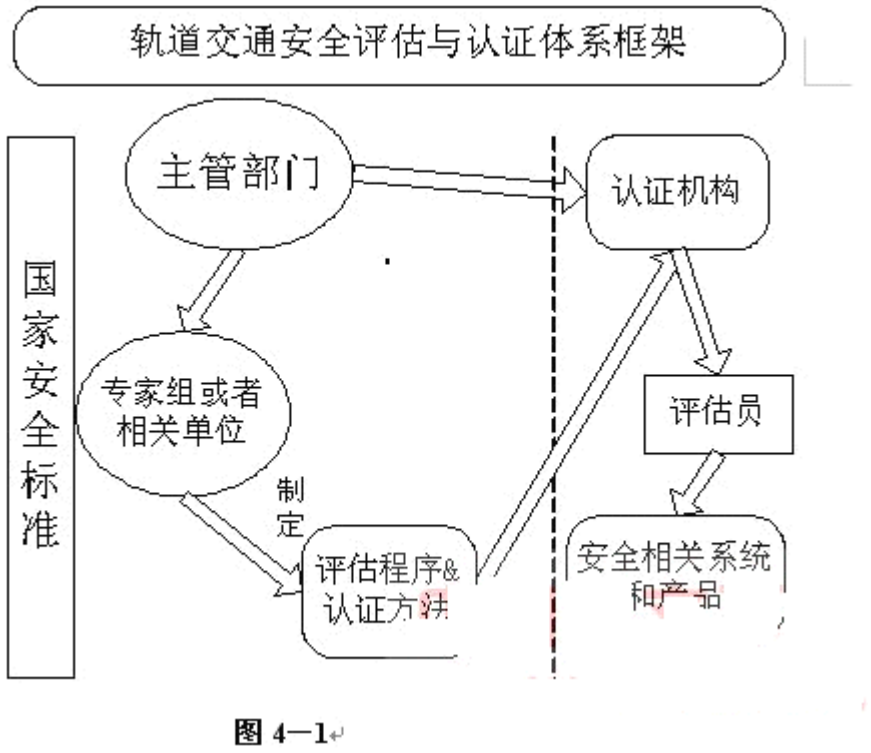

图 4—1

图 4-1　我国轨道交通安全评估与认证体系设想

5.结论

借鉴国外先进方法建立我国轨道交通信号系统安全评估与认证体系具有重大意义，可以迅速缩小和国际先进水平的差距，同时轨道交通信号系统的研制开发和应用也可以逐步走向规范化、系统化，切实保障轨道交通的运行安全。

参 考 文 献

【1】. CENELEC prEN50129，Railway Applications：Safety related electronic system for signaling，1999

【2】. CENELEC prEN50159-1，Railway Applications：,Signaling and processing systems, Part 1：Safety related Communication in closed transmission systems，2001

【3】. Stuart R. Nunns, Conformity assessment of safety related systems to IEC 61508－the CASS initiative, Computing & Control Engineering Journal, Feb.2000: 33～39.

【4】. Engineering Safety Management Issue 3 Yellow book 3, Railtrack on behalf of the UK rail industry.