

信号系统安全性、可靠性和可用性评估方法

李云 何世星 南京地下铁道有限责任公司 210000

摘要

文章介绍了城市轨道交通信号系统安全性、可靠性和可用性的定义及评估方法。

关键词

安全性;可靠性;可用性

前言

城市轨道交通信号系统安全性、可靠性及可用性三项指标不但涉及产品设计、工艺和生产,还涉及系统构成冗余度、故障检测水平、维修水平、系统设备运用环境等多种因素,而且安全性、可靠性及可用性三项指标又相互关联。因此,安全性、可靠性及可用性三项指标,必须通过综合分析的方法才能正确评价。

1. 安全性的评估方法

1.1 安全性定义

安全性是保证行车和人身安全的性能。对于信号系统,其特殊性在于:信号系统(设备、电路、机件、软件等)发生故障时,使设备对行车表现出更大的限制,避免由于误动和错误显示引起行车事故的性能,即故障导向安全性能。

1.2 安全性评估指标

信号系统是地铁各系统中安全水平等级最高、运用要求最重要的一个系统。地铁信号系统安全等级以国际标准定义为 4 级,最高安全等级,其故障—安全失效效率或故障—安全失效间隔时间为: $10^{-6} \sim 10^{-8} \text{h}$ 。

1.3 安全评估

安全评估也称危险度评价或风险评价,是以保证安全为目的,对系统中固有的或潜在的危险及其严重程度进行预先安全分析与评估,并以既定的指数、等级或概率作出定量表示,为系统安全设计、制定基本防护措施和管理决策提供依据。

安全评估涉及评估组织机构、安全系统生命周期各因素解析、硬件与软件的安全性评估、EMC 对于安全性的影响和对策、系统的安全性审查和文档处理等内容,最终期望能够确认系统的安全等级符合既定要求或得到修正。

1.3.1 安全性评估的基本程序

安全性评估主要是调查研究、分析和测试认证,可以采用由企业内部自行评估、企业与有关部门合作评估、邀请外部专家或委托专业安全评估机构承担等几种方式。无论何种方式,均须遵循以下基本程序:

- 评价准备
- 危险的确定与分析
- 危险的定量化
- 确定消除危险的对策
- 综合评价

1.3.2 安全性评价的基本方法

安全评价的方法很多,但目前广泛采用的主要是评价法、检查表法、概率法和综合法四种。

评分法:

1) 加法评分法:将被评价项目的得分依次相加,其和即评价价值,其公式如下:

$$S = \sum_{i=1}^n S_i$$

其中 $i=1 \sim n$, S —总评分数, S_i —项目得分, n —评价项目数。

2) 加乘法评价法:以项目分组求和再求积的方法,其公式如下:

$$S = \prod_{i=1}^m \sum_{j=1}^n S_{ij}$$

其中 $i=1 \sim n$, S —总评分数, S_i —项目得分, $j=1 \sim m$ 为评价组数, $i \sim n$ 为评价组内项目数。

检查表法:

本法根据经验及系统分析的结果,集中评价项目及环境的潜在危险,并列出检查项目清单逐项检查评定。

概率法:

本法将事故后果的分析与运行事故所发生概率分析相结合,并根据系统各组成要素的故障率和失效率,确定系统的安全度指标。概率法主要通过对事故树分析或事件树分析并建立数学模型,确定目标函数并求解。

综合评价法:

本法不是单一方法,是多种评价方法的归纳综合,包括危险度等级评定的多级综合、总分定级评价法,多级综合模糊评价法。

以上简单说明了目前常用的几种安全评价方法,通过上述方法可以求解安全度,但较为繁杂。鉴于可靠性是安全性的基础,因此可以将安全性分成二部分,其一为系统或设备的可靠性,其二为系统或设备的故障—安全失效间隔时间,并求其积即可得到相应的安全性评估值。

2.可靠性的评估方法

2.1可靠性定义

产品在规定的条件下和规定的时间内完成规定功能的能力。

2.2可靠性的研究对象

可靠性的研究对象包括系统、子系统、设备、装置、组合件、元器件等，定义中的产品，包含上位产品（系统）至下位产品（元件），也包含机械产品、机电产品和电子产品。对于信号系统而言，其研究的重点是设备和系统、电子产品和机电产品。

2.3可靠性的度量与评估方法

由可靠性定义可知，可靠性是产品完成正常工作的能力。从时间分析，产品在使用过程中会发生失效，即产生故障。而失效的发生具有概率性质，作为研究对象的产品，在相同工作环境或使用条件下，同一种类的多数产品经过长时间的工作后，其失效往往具有统计的规律性，即可靠性可以通过可靠度进行度量。可靠度是给定产品在规定的条件下和预定的时间内持续完成规定功能的概率，然而，由于可靠度是时间的函数，不同的运行时间可靠度值会有所不同，由于产品运行成功的概率取决于其运行条件和运行时间，因此可靠度的实际运用效果并不理想。对于用户而言，更为有用的是产品发生故障的平均间隔时间，即平均故障间隔时间 MTBF。MTBF 以小时表示，产品的 MTBF 是其故障率的倒数，换言之，产品的可靠性的评估，可以通过对运行产品的 MTBF 进行实际统计或通过对产品各个组成部件的故障率进行计算等方法得到。但实际 MTBF 的统计要依据具体的系统进行计算，对于用户而言，过程繁琐漫长不利于系统的比选。因此，必须寻求其它方法，尤其是工程方法，必须以简捷的方式评估可靠性。

2.3.1指数法可靠性评价

评价可靠性优劣程度的方法之一，是采用可靠性评价指数，见表 1。

2.3.2可靠性预测评估法

产品的工作可靠性由固有可靠性和使用可靠性组成，包括多种因素。其相关因素可见表 2。

从表 2 可知，所谓固有可靠性是指经设计、制造、试验等过程所确定的产品

可靠性，是保证工作可靠性的重要因素，产品交付用户时，应确定产品的设计、制造的可靠性。定量而言是设计时给定的可靠性计算值或是分析结果所得出的数值，而这一数值，伴随产品的复杂程度、环境的苛刻程度等不同条件而有很大区别。

而使用可靠性是有损工作可靠性的重要因素，将影响产品的使用。因此，在系统评价过程中，以上两个指标用户均非常关心，但作为初期选择产品可靠性时，其固有可靠性显得较为突出，而且是评估可靠性的重要内容。考虑到信号系统设备是可修复产品，能够实现状态修，因此，系统的工作可靠性应大于其固有可靠性。

2.3.3可靠性评估指标

可靠性一般以 MTBF（平均无故障间隔时间或平均无故障工作时间）作为指标，MTBF 以小时表示，产品的 MTBF 是其故障率的倒数。信号系统分为非安全系统和安全系统两大类，其中 ATP 子系统和联锁子系统为安全系统。

3.可用性的评估方法

3.1可用性定义

是指可修复产品在某一特定瞬间维持其功能的概率或在某一期间内维持其功能

的时间比率。可用性是产品可靠性、可维修性和维修保证性的综合指标。

通常产品的可用性可用下式表达：

可用性 = 能工作时间 ÷ (能工作时间 + 不能工作时间)

上式中能工作时间是指产品功能能够正常运行的时间，不能工作时间是指产品故障造成失去全部功能或部分功能至修复产品恢复失去功能从新投入运行的间隔时间。

3.2可用性的评估

该项指标的评估非常繁杂，而且往往不具备可操作性或确切性，其主要原因是作为计算主要因素的 MTBF 的不确切性以及影响可用性因素的多重性。信号系统在评估可用性时必须剔除由环境原因造成的干扰、轨道交通控制方面以外原因造成的干扰、由行车调度指挥中心操作人员错误操作或不慎行为造成的故障、由司机错误操作或不慎行为造成的故障、由于损毁、事故、供电系统故障引起的干扰、由于其它系统故障引起的干扰，以及不可抗力的影响等。

以往在评估信号系统的可用性时，一般采用如下公式：

下转第 89 页 ▶▶

表 1 可靠性评估指数表

项目	可靠性评估指数	内 容	备 注
1	运行成功率	成功次数 ÷ 总次数	目的达到率
2	损 失 率	失败次数 ÷ 总次数	目的未达到率
3	运行时间率	运行时间 ÷ 总时间	运行率
4	失效时间率	失效时间 ÷ 总时间	
5	重要度系数	因产品失效而妨碍运用成功率的次数 ÷ 产品总失效次数	
6	维 修 率	为保证产品运行，单位时间内所必需的维修时数	维护，状态修

表 2 可靠性预测评估表

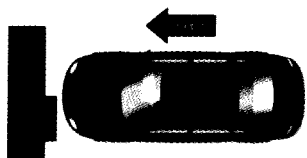
固有可靠性	使用可靠性
电路的选择及适应性、设计方式的选择	操作、维修人员的水平
零部件的适应性	操作、维修的实施方法
元器件工作的选择方法	操作条件的优劣、操作的难易
结构	可维修性
制造技术	辅助及备用设备
操作规则	工作环境
	保管、贮藏、库存的劣化程度
	运输及使用的影响

部、胸部、大腿部和小腿部,每个部位最高得分分别为5分、2分、5分、2分和2分。

评分以驾驶员侧假人的伤害指数为基础,只有当乘员侧假人相应部位的得分低于驾驶员侧假人相应部位的得分时,才采用乘员侧相应部位得分来代替。对于每个假人,基本的评分原则是:设定高性能指标限值和低性能指标限值,分别对应每个部位的最高得分和0分;若同一部位存在多个评价指标,则采用其中的最低得分来代表该部位的得分;所有单项得分保留到小数点后两位。

(2) 正面40%重叠可变形壁障碰撞试验

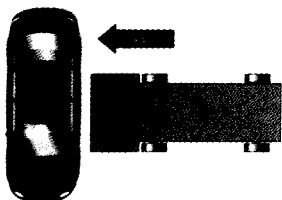
试验车辆40%重叠正面冲击固定可变形吸能壁障。碰撞速度为 56_{-1}^{+1} km/h。在后排驾驶员和乘员位置分别放置一个Hybrid III型第50百分位男性假人,用以测量前排人员受伤害情况。在第二排座椅最左侧座位上放置一个Hybrid III型第5百分位女性假人,用以考核安全带性能。



在这项试验中,可以得到的最高分数为16分,评分部位为假人的头颈部、胸部、大腿部和小腿部,每个部位最高得分都为4分,评分方法与原则同正面100%重叠刚性壁障碰撞试验。

(3) 可变形移动壁障侧面碰撞试验

移动台车前端加装可变形吸能壁障,垂直冲击试验车辆驾驶员侧,碰撞速度为 50_{-1}^{+1} km/h。在驾驶员位置放置一个EuroSID II型假人,用以测量驾驶员位置受伤害情况。



在这项试验中,可以得到的最高分数为16分,评分部位为假人的头部、胸部、腹部和骨盆,每个部位最高得分都为4分,评分方法与原则同正面100%重

叠刚性壁障碰撞试验。

4. C-NCAP 星级评定方法

C-NCAP 中最高得分为51分。其中,以上三项试验每项试验满分为16分,三项试验总得分满分为48分。对安全带提醒装置及侧气囊(及侧气帘)分别有2分和1分的加分。将以上三项试验的得分及加分项得分之和记为总分,并按以下条件确定评价星级。

根据总分,按照以下星级评分标准对试验车辆进行星级评价:

总分	星级
≥ 50 分	5+ (★★★★★☆☆)
≥ 45 且 < 50 分	5 (★★★★★)
≥ 40 且 < 45 分	4 (★★★★)
≥ 30 且 < 40 分	3 (★★★)
≥ 15 且 < 30 分	2 (★★)
< 15 分	1 (★)

除总分外,5星级车和4星级车,还必须满足其他条件。对于5星级车,在三项试验中,假人的特定部位不能为0分,否则该车将被降为4星级车。在正面100%重叠刚性壁障碰撞试验和正面40%重叠可变形壁障碰撞试验中,特定部位为头部、颈部和胸部;在可变形移动壁障侧面碰撞试验中,特定部位为头部、胸部、腹部和骨盆。对于4星级车,在三项试验中,每项试验的得分不能低于10分,否则该车将被降为3星级车。

上接第87页

$$A=B/(C-D)$$

式中:A:系统可用性,是描述系统不影响正常功能或使用的一种能力,在试验结束时所获得的值;

B:在试验期间内实际运营的总小时数;

C:根据测试期间的时刻表所规定的运营总小时数;

D:系统干扰即指系统除信号系统之外其它因素完全中断列车运行的总小时数。

影响系统可用性的很多原因属于信号系统之外,如下所列:

由环境原因造成的干扰;

非轨道交通控制方面原因造成的干扰;

由行车调度指挥中心操作人员错误操作或不慎行为造成的故障;

由司机错误操作或不慎行为造成的故障;

由于损毁、事故、供电系统故障引起的干扰;

由于其它系统故障引起的干扰。

总结

安全性、可靠性及可用性是任一系统或设备设计、制造、应用的重要指标。信号系统是涉及行车指挥和列车控制、提高行车效率、保证列车运行安全的复杂系统;因此,安全性、可靠性及可用性是信号系统必须时刻关注的重要指标。

参考文献

[1]南京地铁二号线初步设计文件.2005年

[2]尼尔森(美).可用性工程.机械工业出版社.2004年

作者简介

李云,男,1981年2月生,毕业于兰州交通大学自动化专业,工学学士,南京地下铁道有限责任公司建设处工程师,助理工程师,主要从事地铁信号系统、旅客资讯系统、站台安全门项目建设工作。

何世星,男,1981年2月生,毕业于西南交通大学电子信息专业,工学学士,南京地下铁道有限责任公司运营分公司工程师,助理工程师,主要从事地铁信号系统、旅客资讯系统设备维护工作。