

专

稿

轨道交通相关系统 安全完整性的探讨

王 奇

(株洲南车时代电气股份有限公司, 湖南 株洲 412001)



作者简介: 王 奇(1964-), 男, 高级工程师(教授级), 长期从事轨道交通信号技术与安全技术研究。

摘 要: 简要介绍了轨道交通相关标准的发展以及在我国的应用情况, 对如何理解“安全相关”等概念进行了分析, 阐述了安全完整性等级确定与分配的过程和方法、可靠性与安全性的关系以及安全完整性等级的使用, 特别针对安全完整性等级的理解与使用方面可能存在的模糊或误解进行重点说明, 并提出了作者对这些问题的认识与思考。

关键词: 轨道交通; 安全相关; 安全完整性等级; 危害; 风险

中图分类号: U298; U229 **文献标识码:** A **文章编号:** 1000-128X(2015)02-0001-03

doi: 10.13890/j.issn.1000-128x.2015.02.001

Discussion on Safety Integrity of Safety-related System for Railway Application

WANG Qi

(Zhuzhou CSR Times Electric Co., Ltd., Zhuzhou, Hunan 412001, China)

Abstract: Development of safety-related standard for railway traffic and application of the standard in China was introduced. The way to understand the concept such as safety-related was analyzed. The process and method for assigning and allocating the safety integrity level, the relationship between reliability and safety were described, as well as the application of safety integrity level. Illegibility or misunderstand on applying safety integrity level was explained in detail, and writer's understanding and consideration were proposed.

Keywords: railway traffic; safety-related; safety integrity level; hazard; risk

0 引言

轨道交通作为大众运输工具具有运载量大、运输成本低以及环境污染小等特点, 如何提高系统及其设备的安全性一直是各国轨道交通领域研究的重要课题。在经历了许多惨痛的事故教训以后, 欧洲一些轨道交通相对发达的国家在上世纪 90 年代开始对安全相关系统安全性问题进行系统、深入的研究, 并且在安全理论与实践方法等方面取得积极的成果, 形成了轨道交通相关的一系列标准并在欧洲得到贯彻与实施。这些安全思想与理念、安全相关标准也正在逐步推广至包括中国在内的世界一些国家。

近年来, 我国轨道交通发展速度已远超欧洲以及其他国家, 且轨道交通主管部门、系统集成商以及设备供应商对于轨道交通安全性问题的日益重视, 特别是在“7·23 事故”发生后, 轨道交通各利益相关方无

论在安全意识的提高, 还是在安全标准以及安全相关技术的采用等方面都较以往发生了重大变化。但由于这些安全理论与方法源自欧洲国家并在我国实施时间较短, 我国轨道交通领域对于安全的认识与理解仍然存在一定程度的模糊与差异, 甚至在一些系统上出现过度追求安全性的趋向。本文旨在从不同的角度对轨道交通安全相关系统安全性的相关问题进行初步探讨, 并期待为相关实体在认识、理解以及实施安全相关系统安全性方面提供可能的参考。

1 关于“安全相关”概念的基本认识

1.1 “安全相关”概念

在讨论安全相关系统的安全完整性之前, 应该首先明确“安全相关”的含义。根据国标 GB/T 28809 (等同 IEC 62425 或 EN 50129) 的定义: “安全相关”是指对安全性负有责任。如果继续对相关概念进行追溯, 可以得到如下几个定义: 安全性是指避免不可接受的风险; 风险是危害 (也称隐患) 发生的频度与其后果

的组合；危害是可能导致事故的一种状况（例如失效）；事故是导致人员伤亡、商业损失或者环境破坏的事件。由此，通过逻辑推导的方法，可以认为一个系统是否“安全相关”的判定依据就是其失效后果是否与死亡/伤害、商业损失或者环境破坏相关，如图 1 所示。

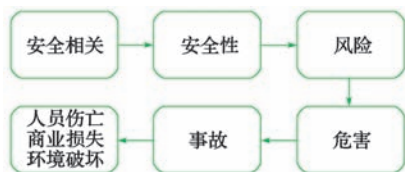


图 1 安全相关概念关联关系

1.2 安全相关与失效后果的关系

如果一个系统或设备的失效（包括系统性失效与随机失效）可能导致人员的死亡或伤害，这样的系统毫无疑问是安全相关系统，例如轨道交通信号系统中的 ATP 子系统就是典型的安全相关系统。问题在于如果一个系统或设备的失效可能导致商业损失或者环境破坏，这样的系统是否可以定义为安全相关系统？如果定义为安全相关系统，则几乎所有的系统都可以认为是安全相关系统，因为所有的系统在失效时都会导致商业损失，例如通常情况下，系统的失效往往会导致轨道交通不同程度的运营丧失、服务终止以及信誉损失等等。事实上，导致商业损失的系统失效应该是属于可靠性、可用性以及可维护性（RAM）研究的范围，而不宜定义为安全相关，否则会产生安全性与可靠性混淆的问题（关于安全性与可靠性的关系在本文第 5 节阐述）。

关于“安全相关”的概念，目前欧洲比较普遍的认识也是不将“商业损失或者环境破坏”纳入安全性研究范围（除非导致重大财产损失或环境破坏），因为一方面不直接与人员伤亡相关，此外也基于存在难以量化的问题。我国轨道交通领域各相关实体（包括主管部门、系统集成商以及设备供应商等）在考虑安全性问题时也宜根据合理、可行的原则明确“安全相关”的概念以及“安全相关”系统，例如是否与人员的死亡或伤害相关；如果将非人员伤亡类的损失定义为安全相关，则应明确定义损失的程度。从安全性的角度考虑，在无法准确定义“安全相关”系统的条件下，不宜进行安全完整性等级的定义并开展相关任务的实施。

2 安全完整性等级的确定

2.1 容许危害率与安全完整性等级

为便于表述与沟通，人们常常采用安全完整性等级作为指标来要求或衡量安全相关系统的安全性能。事实上，由于系统的失效包括系统性失效（人为错误导致）与随机失效（硬件故障导致），安全相关系统的安全完整性也包括系统性失效完整性与随机失效完

整性。随机失效完整性采用可量化的容许危害率（THR）来定义，而由于系统性失效的不可量化特征，其完整性则采用定性的安全完整性等级（SIL）来衡量。二者不仅在含义上完全不同，所要求采取的管理措施与技术方法也存在差异。因此，满足量化的 THR 要求并不意味着已达到 SIL 要求，同样满足定性的 SIL 要求也并不等于可以达到 THR 要求。之所以采用不同的指标来定义安全完整性并且明确 2 种指标之间的关系，是需要在系统性失效完整性与随机失效完整性之间取得合理的平衡，单独提高或降低 SIL 要求而不考虑 THR 要求是没有意义的。THR 与 SIL 两者之间的对应关系在 GB/T 28809 等安全标准已有明确定义。

2.2 安全完整性等级确定过程

一个非常重要但又容易被忽略的基本原则是，在确定 SIL 前应首先确定 THR。THR 的确定存在一个从顶层开始并且不断分解与细化的过程。THR 的确定主体与确定方法依据其研究对象的不同而不同，研究对象通常包括系统、子系统以及设备等（根据系统的大小，中间的子系统也可分为多层）；确定主体主要包括轨道交通主管部门、安全主管部门、系统集成商以及设备供应商，在许多时候，设备供应商也可以被认为是其设备的系统集成商。

对于轨道交通系统而言，通常由轨道交通主管部门或与安全主管部门一同确定轨道交通系统的顶层 THR，同时也确定主要子系统的 THR。理论上，顶层 THR 应通过系统级的风险分析（包括隐患识别）并且结合相关安全法律、条例以及社会经济水平（也就是风险接受准则）来确定。

如图 2 所示，在对危害进行识别并确定其后果的严重程度后，就可以依据风险接受准则得到 THR。该过程看似简单，但如何确定风险接受准则却是许多国家正在研究的课题。尽管一些欧洲国家已经形成各自的风险接受准则（例如英国的 ALARP、法国的 GAMAB 以及德国的 MEM），但包括中国在内的大部分国家仍然缺乏相应的研究以及可以依赖或参考的体系。

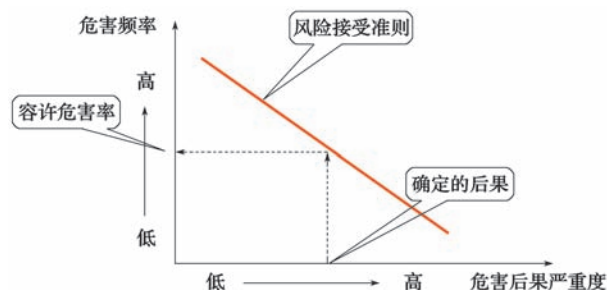


图 2 风险分析过程

2.3 风险接受准则的建立

目前在我国轨道交通领域安全分析过程中，存在一个普遍的现象就是声称风险分析采用 ALARP 原则，