轨道交通系统安全工程

GUIDAO JIAOTONG XITONG ANQUAN GONGCHENG

董锡明 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

轨道交通系统安全工程

董锡明　编著

中国铁道出版社

2014年·北京

内 容 简 介

本书全面介绍轨道交通系统安全工程。内容包括：系统安全工程概念，事故及其预防，系统安全分析及其技术，安全风险管理，系统安全验证与评价，系统安全管理及功能安全等。

本书可供从事轨道交通的管理人员、科研设计人员及相关专业人员在工作中学习参考。

图书在版编目(CIP)数据

轨道交通系统安全工程/董锡明编著. —北京：
中国铁道出版社，2014.5
ISBN 978-7-113-18236-6

Ⅰ.①轨… Ⅱ.①董… Ⅲ.①轨道交通—交通运输安全 Ⅳ.①U298

中国版本图书馆 CIP 数据核字(2014)第 057326 号

书　　名：轨道交通系统安全工程
作　　者：董锡明　编著

责任编辑：聂清立　田　甜　　**电话**：010-51873116
封面设计：郑春鹏
责任校对：马　丽
责任印制：陆　宁　高春晓

出版发行：中国铁道出版社(100054，北京市西城区右安门西街 8 号)
网　　址：http://www.tdpress.com
印　　刷：三河市宏盛印务有限公司
版　　次：2014 年 6 月第 1 版　2014 年 6 月第 1 次印刷
开　　本：700 mm×1 000 mm　1/16　**印张**：24.75　**字数**：474 千
书　　号：ISBN 978-7-113-18236-6
定　　价：75.00 元

前　言

安全是轨道交通运输的生命线，是运输生产的永恒主题。轨道交通运输安全不仅关系到企业的生产效率和经济效益，还会对国民经济、社会生活和社会安定造成重大影响。随着我国铁路高速化、重载化的进程，城市轨道交通网的建设与发展，轨道交通安全越来越受到人们的重视。现代轨道交通安全观念与过去相比有很大的变化与发展，如果我们将传统的安全观念称为“技术安全”，现代的安全观念则称为“系统安全”，当前各行各业的安全管理都在由传统的“技术安全”向现代化的“系统安全”转换与发展。现代的系统安全与传统的技术安全相比，虽然它们的目的都是为了实现系统的安全，但其工作范围和实施方法却有很大区别，主要区别在于：

(1)安全观念不同。传统的“技术安全”是指一般的技术安全工作。它是针对生产过程中发生的事故进行分析，汲取经验教训而进行的预防工作。传统的技术安全工作总是跟在事故的后面跑，很难做到防患于未然，特别是跟不上技术装备日益复杂、事故频增的发展趋势。而“系统安全”则是在传统技术安全工作的基础上，按照系统工程的观点，应用系统分析的方法来研究系统不发生事故的能力。它是从根本上提高技术装备安全水平的有效方法。

(2)安全工作范围不同。传统的“技术安全”工作范围主要是在生产和使用现场，保证操作人员和设备不受到伤害和损坏。它基本上不直接涉及设备的设计，最多只是向设计反馈不安全因素。而“系统安全”则是研究装备的全寿命过程，包括方案论证、设计、试验、制造和使用维修等各阶段的安全工作，并且重点在设计研制阶段。

(3)安全问题处理方法不同。传统的“技术安全”工作大多凭经验和直觉来处理安全问题，因而难以彻底改善安全状况。而“系统安全”则是利用系统工程方法，从系统、人为因素和环境影响及其相互关系

来研究安全问题，从而能较深入和全面地找到潜在危险和不安全问题，预防事故的发生。

(4)局部和全面解决问题的不同。传统的“技术安全”工作是局部的解决安全问题，是处于被动的状态解决问题，因而不能从根本上提高安全水平。而“系统安全”则是从装备论证设计就开始进行系统的安全分析，它考虑了全系统中所有可能的危险，并随着研制工作的进展，逐步细化安全分析的内容，使安全工作主动而全面地发挥作用。

(5)安全分析方法不同。传统的“技术安全”分析工作只是对生产和使用现场的事故进行具体的定性分析和预测，没有将分析工作上升到系统理论的高度，未能利用现代系统工程的新成果。而“系统安全”工作则在安全分析中与系统工程、RAMS 工程、优化理论等相结合，充分利用各种概率统计方法、安全检查和危险分析、FMEA、FTA、ETA 以及风险评估等先进技术，将安全分析上升为系统的理论，形成了一门新学科。

几十年来，我国铁路运输的安全观念基本上都是处于“技术安全”的状态，即在发生事故后查找原因、汲取教训、采取预防措施，防止事故再次发生。技术安全措施通常有：在生产和使用部门设立专职机构(例如技术安全科室等)，颁发安全生产法规，设置安全防护设备和工具，监督安全生产和使用，进行安全宣传和教育等。这种传统的“技术安全”工作虽然在防止事故中起到了重要的作用，并且至今仍是安全工作的重要基石，但也应看到，它不能满足现代轨道交通向复杂化、自动化、智能化发展而对安全方面提出的要求。

我国铁路于 2011 年 7 月 23 日发生甬温线列车追尾特别重大事故以后，原铁道部党组做出了在全路推行安全风险管理的决策部署，并于 2012 年 3 月 14 日发布“关于推行铁路安全风险管理的指导意见”(铁安监[2012]46 号文件)，要求铁路各单位“全面引入风险管理的理念和方法，构建铁路安全风险控制体系，把风险管理与既有安全管理有机融合，切实强化安全生产过程控制和超前防范，严格落实‘作业标准化、管理规范化’，最大限度地降低安全风险，使铁路安全工作

更具超前性、针对性和主动性，促进铁路安全管理的规范化、系统化和科学化。”由于安全风险管理是系统安全管理的主要内容之一，引入和推行铁路安全风险管理，实质上是吹响了我国铁路安全管理由“技术安全”走向“系统安全”的号角，使我国铁路安全管理从此进入了系统安全管理的新时代。

面对我国铁路引入和推行安全风险管理，步入系统安全管理的新阶段，急需一本全面介绍轨道交通安全系统工程的书籍，因此作者撰写了本书。本书命名为“轨道交通系统安全工程”有两方面的意思：一方面是介绍现代轨道交通系统的安全工程，即从安全的角度对现代轨道交通系统进行研究，以查明事故发生的原因，找出灾害的本质和规律，寻求消除或减少事故及其损失，保障轨道交通运输安全的措施和方法；另一方面是介绍现代轨道交通的系统安全工程，此处的系统安全工程或称为安全系统工程，即以系统论、信息论、控制论为理论基础，以系统工程、可靠性工程的原理和方法为手段，以安全管理、安全技术、职业健康为载体，对研究对象中的风险进行辨识、分析、评价与控制，以实现系统及其全过程的安全目标。

本书分为八章。第一章介绍了系统安全的基本概念，系统安全与其他专业的关系，系统安全工程的发展，系统安全的相关标准；第二章介绍了事故及其预防，包括事故相关的基本概念、事故致因及影响因素、事故的预防；第三章介绍了系统安全分析，包括系统安全分析的基本概念、初步危险分析、分系统危险分析、系统危险分析、使用和维修危险分析和职业健康危险分析；第四章介绍了系统安全分析技术，包括系统安全分析技术概况、安全检查表、危险分析表、危险和可操作性研究、FMECA、FTA、ETA 和人为差错分析等；第五章介绍了安全风险管理，包括安全风险基本概念、安全风险评估和安全风险控制；第六章介绍了安全验证与评价，包括安全性验证、安全性评价和符合安全法规的评价；第七章介绍了系统安全管理，包括系统安全管理的基本概念、系统安全大纲和寿命周期各阶段的系统安全工作；第八章介绍了功能安全，包括功能安全的基本概念、功能安全的风险评估和功能安全管理。

在编写本书时参考了国内外媒体发表的许多文章、资料和书籍，在此表示诚挚的谢意。

感谢中国铁道科学研究院机车车辆研究所的同事们，特别要感谢维修理论研究室同仁的鼓励和支持，感谢王华胜同志的支持和帮助。最后，还要感谢我的老伴黄厄文女士的辛勤付出，使我衣食无忧地专心写作；她还帮助我进行了大量的图表文整工作，使本书得以顺利完成。

由于水平所限，遗漏、谬误恐所难免，对所提出的批评指正，谨致谢意！

董锡明

2013.9 于北京

目　录
CONTENTS

第一章 绪 论

第一节 系统安全工程概念

系统安全工程是以效能、进度和费用为约束条件，在装备寿命周期内的各阶段上，利用专门知识和系统工程方法，识别、评价、消除或控制系统和设备中的危险，从而使系统具有最佳的安全程度的工程技术。它是从20世纪60年代以来，为了适应复杂技术装备安全的需要而发展起来的一门综合性的应用科学，也可称为安全系统工程。

一、术语与定义

（一）安全术语

与安全有关的术语和定义罗列如下（按汉语拼音字母顺序排列）：

1. 安全（safety）

将伤害（对人）或损坏的风险限制在可接受水平的状态。（ISO 8402—94、GB/T 6583—94）

2. 安全功能（safety function）

针对特定的危险事件，为达到或保持EUC的安全状态，由E/E/PE安全相关系统、其他技术安全相关系统或外部风险降低设施实现的功能。（IEC 61508—1998）

3. 安全计划（safety plan）

用于实现组织结构、责任、流程、活动、能力和资源的一套时间进度活动、资源和事件的文档，以确保产品满足与规定合同或项目相关的安全性要求。（IEC 62278—2002）

4. 安全寿命周期（safety lifecycle）

安全相关系统实现过程中所必需的寿命活动，这些活动发生在从一项工程的概念阶段开始，直至所有的E/E/PE安全相关系统、其他技术安全相关系统、以及外部风险降低设施停止使用为止的一段时间内。（IEC 61508—1998）

5. 安全相关系统（safety-related system）

（1）必需要能实现要求的安全功能，以达到或保持EUC的安全状态。

（2）自身或与其他E/E/PE安全相关系统、其他技术安全相关系统或外部风险降低设施一道，能够达到要求的安全功能所需的安全完整性。（IEC

61508—1998)

6. 安全计划(safety plan)

用于实现组织结构、责任、流程、活动、能力和资源的一套时间进度活动、资源和事件的文档,以确保产品满足与规定合同或项目相关的安全性要求。(IEC 62278—2002)

7. 安全完整性(safety integrity)

在规定的条件下和规定的时间内,安全相关系统成功实现所要求的安全功能的概率。(IEC 61508—1998)

8. 安全完整性等级(safety integrity level,SIL)

一种离散的等级(4 种可能等级之一),用于规定分配给 E/E/PE 安全相关系统的安全功能的安全完整性要求。在这里,安全完整性等级 4 是最高的,安全完整性等级 1 是最低的。(IEC 61508—1998)

9. 安全性(safety)

(1)不发生不可接受损害风险的可能性。(IEC 62278—2002)

(2)不导致人员伤亡、危害健康及环境、不给设备和财产造成破坏和损伤的能力。(GJB 1405—92)

10. 安全性论证报告(safety case)

产品符合规定安全性要求的论证说明。(IEC 62278—2002)

11. 安全主管部门(safety regulatory authority)

负责制定或同意轨道交通安全性要求,并保证轨道交通符合这些要求的国家政府机构。(IEC 62278—2002)

12. 必要的风险降低(necessary risk reduction)

为保证不超过允许风险,由 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施达到的风险降低。(IEC 61508—1998)

13. 保障性(supportability)

系统的设计特性和计划的保障资源能满足平时战备及战时使用要求的能力。(GJB 3872—99)

14. 保障资源(support resource)

使用与维修装备所需的全部物资与人员的统称。(GJB 3872—99)

15. 电气/电子/可编程电子(electrical/electronic/programmeable electronic,E/E/PE)

基于电气(E)和/或电子(E)和/或可编程电子(PE)的技术。(IEC 61508—1998)

16. 残余风险(residual risk)

采取防护措施以后仍存在的风险。(IEC 61508—1998)

17. 风险(risk)

发生引起损害危险的概率及其损害的严重程度。(IEC 62278—2002)

18. 风险评价(risk assessment)

对风险及其有关影响的综合评定。(GJB/Z 99—97)

19. 符合(compliance)

证实产品的特点或特性满足规定要求。(IEC 62278—2002)

20. 功能安全(functional safety)

与 EUC 和 EUC 控制系统有关的整体安全的组成部分,它取决于 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施功能的正确行使。(IEC 61508—1998)

21. 共因失效/故障(comm cause failure)

由一个事件引起两个或两个以上部件同时失效/故障,从而导致系统不能实现规定功能的失效/故障。(IEC 62278—2002)

22. 轨道交通工业(railway support industry)

表示整个轨道交通系统、子系统和组成零部件供应商的通称。(IEC 62278—2002)

23. 轨道交通主管部门(railway authority)

对轨道交通系统运营的管理者负全部责任的机构。注意有时铁路主管部门对总系统或其部件和寿命周期活动的责任分摊给一个或多个团体或组织,例如:系统的一部分或多部分的拥有者或代理商;系统的操作人员;系统的一个或多个部件的维修者等等。这些责任的划分是基于法定文件或合同契约,因此应在系统安全寿命周期的早期阶段就予以明确。(IEC 62278—2002)

24. 故障—安全(fail-safe)

当某故障发生时能使产品保持安全或使产品恢复到不产生事故的状态的一种设计特性。(GJB/Z 99—97)

25. 故障模式(fault mode)

相对于给定的规定功能,故障产品的一种状态。(IEC 60050(191)、GB/T 3187—94)

26. 故障模式与影响分析(fault modes and effects analysis,FMEA)

研究产品的每个组成部分可能存在的故障模式,并确定各个故障模式对产品其他组成部分和产品要求功能的影响的一种定性的可靠性分析方法。(GB/T 3187—94)

27. 故障树分析(fault tree analysis,FTA)

以故障树的形式进行分析的方法。它用于确定哪些组成部分的故障模式或外界事件或它们的组合可能导致产品的一种已给定的故障模式。(GB/T 3187—94)

28. 后勤保障(logistic support)

在要求的寿命周期费用内,为运用和保持系统工作在规定的可用性水平上,

安排和组织的所有资源。(IEC 62278—2002)

29. 恢复(restoration)

产品发生故障后其恢复执行规定功能的事件。(ICE 60050(191))

30. 可靠性(reliability)

产品在规定条件下和规定时间内,完成规定功能的能力。(GB/T 3187—94)

31. 评估(assessment)

通过现场调查、客观事物的核实或事物性质的分析,判定是否符合标准要求的活动。(GJB 1405—92)

32. 确认(validation)

通过检验和客观证据来证实专门用途的特殊要求是否得到满足。(IEC 62278—2002)

33. 其他技术安全相关系统(other technology safety-related system)

基于电气/电子/可编程电子技术之外的安全相关系统,举例:排放系统、防火墙和堤都是外部风险降低设施。(IEC 61508—1998)

34. RAMS 和 RAM

RAMS 表示可靠性(Reliability)、可用性(Availability)、维修性(Maintainability)和安全性(Safety)组合在一起的缩写;RAM 为可靠性、可用性和维修性组合的缩写。(IEC 62278—2002)

35. 任务(mission)

系统完成基本工作的目标描述。(IEC 62278—2002)

36. 任务剖面(mission profile)

在寿命周期各运行阶段内,任务有关参数(例如时间、负载、速度、距离、停车和隧道等)的预期范围和变化的概要描述。(IEC 62278—2002)

37. 容许(允许)风险(tolerable risk)

轨道交通主管部门可以接受的产品最大等级的风险。(IEC 62278—2002)

38. 软件危险分析(software hazard analysis)

对软件程序进行的一种分析,以保证程序在其设计的运行环境中,不会引起或诱发对人员或设备的危害。(GJB/Z 99—97)

39. 审核(audit)

为决定一个产品按技术要求所采取的措施是否符合规定的方案,是否被有效执行,是否有利于获得规定的目标而进行的一系列系统而又独立的验证。(IEC 62278—2002)

40. 事故(mishap,accident)

造成人员伤亡、职业病、设备损坏、财产损失或环境损害的一个或一系列意外事件。(GJB/Z 99—97)