



# 中华人民共和国国家标准

GB/T 28809—2012/IEC 62425:2007

---

## 轨道交通 通信、信号和处理系统 信号用安全相关电子系统

Railway applications—Communication, signaling and processing systems—  
Safety related electronic systems for signaling

(IEC 62425:2007, IDT)

2012-11-05 发布

2013-02-01 实施

---

中华人民共和国国家质量监督检验检疫总局 发布  
中国国家标准化管理委员会

中 华 人 民 共 和 国  
国 家 标 准  
轨道交通 通信、信号和处理系统  
信号用安全相关电子系统  
GB/T 28809—2012/IEC 62425:2007

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100013)  
北京市西城区三里河北街16号(100045)

网址: [www.gb168.cn](http://www.gb168.cn)

服务热线: 010-68522006

2013年3月第一版

\*

书号: 155066·1-45972

版权专有 侵权必究

## 目 次

前言 .....	III
引言 .....	V
1 范围 .....	1
2 规范性引用文件 .....	2
3 术语和缩略语 .....	2
3.1 术语 .....	2
3.2 缩略语 .....	7
4 整体框架 .....	8
5 安全验收和审批条件 .....	9
5.1 安全论据 .....	9
5.2 质量管理证据 .....	10
5.3 安全管理证据 .....	11
5.4 功能安全和技术安全证据 .....	15
5.5 安全验收和审批 .....	17
附录 A (规范性附录) 安全完整性等级 .....	20
A.1 概要 .....	20
A.2 安全需求 .....	20
A.3 安全完整性 .....	21
A.4 安全完整性需求的分配 .....	21
A.5 安全完整性等级 SIL .....	28
附录 B (规范性附录) 技术需求 .....	31
B.1 概要 .....	31
B.2 功能正确运行的保障(技术安全报告第 2 章) .....	31
B.3 故障的影响(技术安全报告第 3 章) .....	33
B.4 外界影响下的运行(技术安全报告第 4 章) .....	37
B.5 安全相关应用条件(技术安全报告第 5 章) .....	39
B.6 安全合格测试(技术安全报告第 6 章) .....	41
附录 C (规范性附录) 硬件元器件失效模式的识别 .....	43
C.1 概要 .....	43
C.2 一般规程 .....	43
C.3 针对集成电路的规程(包括微处理器) .....	43
C.4 带内在物理特性元器件的规程 .....	43
C.5 元器件失效模式的通用说明 .....	44
C.6 带有内在物理特性元器件的附加通用说明 .....	44
C.7 带有内在物理特性元器件的特别说明 .....	45
附录 D (资料性附录) 补充资料 .....	59

D.1 概要 .....	59
D.2 内部物理独立性的获得 .....	59
D.3 外部物理独立性的获得 .....	60
D.4 单一故障分析方法示例 .....	61
D.5 多重故障分析方法示例 .....	61
附录 E (资料性附录) 安全相关电子信号系统避免系统性故障以及控制随机故障和系统性故障 的技术和措施 .....	66
参考文献 .....	72

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准采用翻译法等同采用 IEC 62425:2007《轨道交通 通信、信号和处理系统 信号传输用和安全性相关的电子系统》。

与本标准中规范性引用文件有一致性对应关系的我国文件如下：

- GB/T 16935.1—2008 低压系统内设备的绝缘配合 第 1 部分：原理、要求和试验 (IEC 60664-1:2007, IDT)；
- GB/T 16935.3—2005 低压系统内设备的绝缘配合 第 3 部分：利用涂层、罐封和模压进行防污保护 (IEC 60664-3:2003, IDT)；
- GB/T 16935.5—2008 低压系统内设备的绝缘配合 第 5 部分：不超过 2 mm 的电气间隙和爬电距离的确定方法 (IEC 60664-5:2007, IDT)；
- GB/T 20438.1—2006 电气/电子/可编程电子安全相关系统的功能安全 第 1 部分：一般要求 (IEC 61508-1:1998, IDT)；
- GB/T 21562—2008 轨道交通 可靠性、可用性、可维修性和安全性规范及示例 (IEC 62278:2002, IDT)；
- GB/T 24338.1—2009 轨道交通 电磁兼容 第 1 部分：总则 (IEC 62236-1:2003, IDT)；
- GB/T 24338.3—2009 轨道交通 电磁兼容 第 3-1 部分：机车车辆 列车和整车 (IEC 62236-3-1:2003, IDT)；
- GB/T 24338.4—2009 轨道交通 电磁兼容 第 3-2 部分：机车车辆 设备 (IEC 62236-3-2:2003, MOD)；
- GB/T 24338.5—2009 轨道交通 电磁兼容 第 4 部分：信号和通信设备的发射与抗扰度 (IEC 62236-4:2003, IDT)；
- GB/T 24338.6—2009 轨道交通 电磁兼容 第 5 部分：地面供电装置和设备的发射与抗扰度 (IEC 62236-5:2003, IDT)；
- GB/T 24339.1—2009 轨道交通 通信、信号和处理系统 第 1 部分：封闭式传输系统中的安全相关通信 (IEC 62280-1:2002, IDT)；
- GB/T 24339.2—2009 轨道交通 通信、信号和处理系统 第 2 部分：开放式传输系统中的安全相关通信 (IEC 62280-2:2002, IDT)；
- GB/T 25119—2010 轨道交通 机车车辆电子装置 (IEC 60571:2006, MOD)；
- GB/T 28808—2012 轨道交通 通信、信号和处理系统 控制和防护系统软件 (IEC 62279:2002, IDT)。

本标准做了下列编辑性修改：

- 第 2 章规范性引用文件删除了 IEC 62236-4，因为之前已有 IEC 62236（所有部分）列项，包含了 IEC 62236-4；
- 第 2 章规范性引用文件中，EN 50124、EN 50125、EN 50155 已按 IEC TC9 和 CENELEC TC9X 合作战略转化为 IEC 60571，全文用 IEC 60571 替换 EN 50155、IEC 62497-1 代替 EN 50124-1、IEC 62498-1 代替 EN 50125-1、IEC 62498-3 代替 EN 50125-3；
- 5.1 下增加下一级编号，以符合中文编排习惯；
- 附录 E 中引用表 E.1～表 E.10 语句删除了表编号后的表标题，简化阅读。

本标准由中华人民共和国铁道部提出。

本标准由全国牵引电气设备与系统标准化技术委员会(SAC/TC 278)归口。

本标准主要起草单位:同济大学、铁道部标准计量研究所。

本标准参加起草单位:株洲南车时代电气股份有限公司、北京全路通信信号研究设计院。

本标准主要起草人:徐中伟、孙超、王奇。

本标准参加起草人:范祚成、严云升、赵天时、陈邦兴、黄银霞、呼爱蝉、师进。

## 引 言

安全相关电子信号系统包括硬件和软件两方面。为安装完整的安全相关系统,在系统整个生命周期中,这两个方面都应加以考虑。在本标准中定义了安全相关硬件和整个系统的需求,其他需求在相关的 IEC 标准中定义。

相互认可是面向通用的而不是面向特定应用的审批。

由于本标准涉及安全相关系统验收的相关证据,这些证据包括:在验收阶段之前所应完成的生命周期活动;在验收阶段之后还需要执行的附加的有计划的活动。因此需要证明在整个生命周期中安全性是得到满足的。

本标准关注的是提交何种证据。除确认为适合之外,本标准不规定由谁来执行必要的工作,因为在不同的环境下情况不一样。

对于包含可编程电子设备的安全相关系统,软件的附加条件都定义在 IEC 62279 中。

对于安全相关数据通信的附加需求定义在 IEC 62280 中。

# 轨道交通 通信、信号和处理系统

## 信号用安全相关电子系统

### 1 范围

本标准适用于轨道交通信号应用中的安全相关电子系统(包括子系统和设备)。

本标准涉及的范围以及其他 IEC 国际标准的关系如图 1 所示。

本标准适用于所有安全相关轨道交通信号系统/子系统/设备。但在 IEC 62278 和本标准中定义的危害分析和风险评估过程对于所有的轨道交通信号系统/子系统/设备来说是必要的,以便确定安全需求。如果分析表明无安全需求存在(也就是非安全相关的情况),并且倘若此结论不受后续变化影响的话,那么可终止本安全标准的应用。

本标准既适用于整体信号系统的规范、设计、建造、安装、验收、运行、维护和修改/扩展阶段,也适用于整体信号系统中的单个子系统和设备。附录 C 包括与电子硬件元器件相关的规程。

本标准适用于通用的(包括与应用类型无关的和专门应用类别的)子系统和设备,也适用于特定应用中的系统/子系统/设备。

本标准不适用于既有系统/子系统/设备(即在本标准创建之前它们已被接受)。但只要合理并符合实际,对既有系统、子系统和设备的变更与扩展推荐采用本标准。

本标准主要适用于为轨道交通信号应用专门设计和制造的系统/子系统/设备。只要合理并符合实际,它也宜适用于那些作为安全相关信号系统部件的通用或工业设备(比如电源、调制解调器等)。至少,应提供证据证明:

- 不依靠此设备来实现安全;
- 可依靠此设备来实现安全相关功能。

本标准适用于轨道交通信号系统的功能安全,它不涉及职业健康和个人安全问题,这方面问题由其他标准讨论。

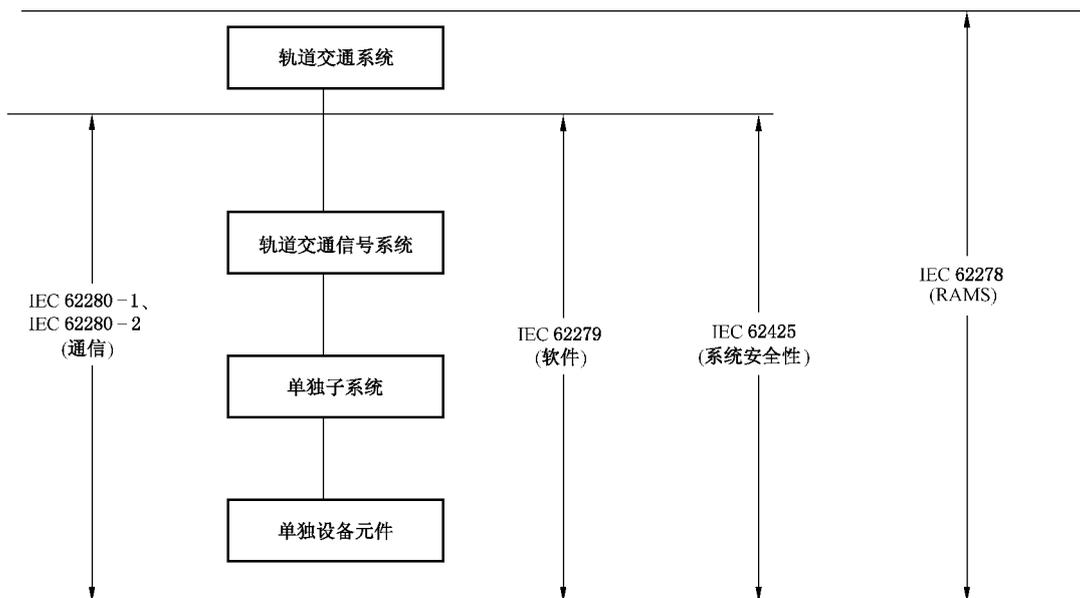


图 1 轨道交通主要标准的应用范围