ICS 45.060
S 04

中华人民共和国国家标准

GB/T 28808—2012/IEC 62279:2002

轨道交通　通信、信号和处理系统 控制和防护系统软件

Railway applications—Communication, signaling and processing systems—Software for railway control and protection systems

(IEC 62279:2002,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
中国国家标准化管理委员会　发布

目　　次

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 62279:2002《轨道交通　通信、信号和处理系统　控制和防护系统软件》。

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见附录 NA。

本标准做了下列编辑性修改：

——将第 3 章中引用的 IEC 60050-191、ISO/IEC 2382、ISO/IEC 9126、IEEE 610.12 文件补充到第 2 章规范性引用文件中；

——修改了 IEC 62279:2002 中第 2 章的脚注 1，因为 IEC 62278 已发布；脚注 1 改为对 ISO 9000、ISO 9000-3、ISO 9001 提醒存在新版文件；

——采用等同采用 IEC 62425:2007 的 GB/T 28809—2012 代替 ENV 50129；

——修订正文中引用的 ISO 9000、ISO 9000-3、ISO 9001 的版本号，与第 2 章声明的版本号一致；

——IEC 62279:2002 的一级子列项编号采用的是 i)、ii)、…或 1)、2)、…，本标准中统一修改为字母编号形式：a)、b)、…；

——附录 B 中，对每章内的单列一行的黑体字符“目标”、“描述”和“参考文献”进行编号，以符合中文习惯。

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、赵天时、王奇。

本标准参加起草人：范祚成、孙超、严云升、陈邦兴、黄银霞、呼爱蝉、牛道恒。

引　言

本标准与 GB/T 21562(IEC 62278)和 GB/T 28809—2012(IEC 62425:2007,IDT)配套使用。GB/T 21562 (IEC 62278)适用于大范围的系统问题,而 GB/T 28809—2012(IEC 62425:2007,IDT)适用于整个轨道交通控制和防护系统中某单个系统的批准过程。为提供满足安全完整性要求的软件,本标准关注于通过更全面考虑后提出软件安全完整性要求所要采用的方法。

本标准从 IEC/TC 65 第九工作组(WG9)早期工作中得到很多指导。

同时,对铁路信号工程师协会(IRSE)的工作也加以了考虑,特别是关注相同主题的 1 号技术报告。

本标准的关键思想是其对软件安全完整性等级的考虑。软件失效的后果越严重,软件安全完整性等级也就越高。

本标准确定了从最低 0 级到最高 4 级的 5 个软件安全完整性等级的技术和措施。其中 1 级～4 级指的是安全相关软件,0 级指的是非安全相关软件。将 0 级包括进本标准是为了让非安全相关系统软件开发向安全相关系统软件开发实现顺利过渡。附表给出了各个软件安全完整性等级和非安全相关等级要求的技术和措施。在本版本中,1 级和 2 级的技术要求相同,3 级和 4 级的要求相同。本标准没有给出某一风险应适用于哪个软件安全完整性等级的具体指导意见。这一结论需要考虑诸多因素,包括应用的特性、其他系统承担的安全功能范围以及社会和经济因素。

软件安全功能的分配由 GB/T 21562(IEC 62278)和 GB/T 28809—2012(IEC 62425:2007,IDT)规定。

本标准规定了满足这些需求的必要措施。该过程见图 1。

GB/T 21562(IEC 62278)和 GB/T 28809—2012(IEC 62425:2007,IDT)需采用系统性的方法,以:

a) 确定危害、风险和风险准则;

b) 为满足风险准则,确定必要的风险降低(措施);

c) 为实现所需的风险降低,为必要的安全防护措施定义一个全面的系统安全需求规范;

d) 选择一个合适的系统结构;

e) 规划、监督和控制那些把系统安全需求规范变成安全性能(或安全完整性)已确认的安全相关系统。

在将该规范分解到由安全相关系统和组件组成的设计当中时,对安全完整性等级的进一步分配就完成了,并最终形成所需的软件安全完整性等级。

目前,无论是质量保证法(即避错措施)还是软件容错法的应用,都无法保证系统的绝对安全。尚未发现可证明一个较复杂的安全相关软件中不存在错误的方法,特别是规范和设计的错误。

在开发高度完整性软件时采取但不仅限于以下原则:

a) 自顶向下的设计方法;

b) 模块化;

c) 开发生命周期每个阶段的验证;

d) 经验证的模块和模块库;

e) 清晰的文档;

f) 可审核的文档;

g) 确认测试。

这些原则以及相关的其他原则应正确应用。本标准规定了在每个软件安全完整性等级下证明其(保证能处于该安全完整性等级)所需的保证等级。

在得到或形成了系统安全需求规范后，分配给软件的安全功能和系统安全完整性等级就确定了，图2给出了应用本标准的功能步骤，并如下所示：

a) 定义软件需求规范，同时考虑软件结构。软件结构是为软件和软件安全完整性等级开发基本安全策略的架构（第5章、第8章和第9章）。

b) 根据软件质量保证计划、软件安全完整性等级和软件生命周期来设计、开发和测试软件（第10章）。

c) 在目标硬件上集成软件（第12章）。

d) 确认软件（第13章）。

e) 如果在运行过程中需要软件维护，那么可再适当运用本标准进行处理（第16章）。

许多活动都是在软件开发过程中交叉进行的，这其中包括验证（第11章）、评估（第14章）和质量保证（第15章）。

给出了由应用数据所配置的系统的需求（第17章）。

给出了从事软件开发人员能力的需求（第6章）。

本标准没有强制要求使用特定的软件开发生命周期，但是给出了推荐的生命周期和文档集（第7章，图3和图4）。

针对5个软件安全完整性等级明确制定了各种技术和措施表格。表格见附录A。对表格交叉引用的是对每个技术或措施做了简要描述的、同时附带更多信息源做参考的文献目录。附录B列出了文献目录。

轨道交通　通信、信号和处理系统 控制和防护系统软件

1　范围

1.1　本标准规定了轨道交通控制和防护设备应用中可编程电子系统开发所需的规程和技术要求，适用于任何有隐含安全性的领域。这些应用系统的范围涵盖了从安全苛求系统（如安全信号系统）到非安全苛求系统（如管理信息系统）。这些系统可能通过采用专用微处理器，可编程逻辑控制器，分布式多处理器系统，大规模集中处理器系统或者其他结构来实现。

1.2　本标准只适用于软件以及软件和系统之间的交互作用。

1.3　0级以上的软件安全完整性等级用于失效可导致人员死亡后果的系统。然而，从经济或环境因素方面考虑也能采用高级别的安全完整性等级。

1.4　本标准适用于轨道交通控制和防护系统开发和实现中的所有软件，包括：

——应用程序设计；

——操作系统；

——支持工具；

——固件。

应用程序设计包括高级程序设计，低级程序设计和专用程序设计（如可编程逻辑控制器梯形逻辑）。

1.5　本标准还涉及了标准、商用软件和工具的使用。

1.6　本标准还对由应用数据配置的系统提出了要求。

1.7　本标准并不涉及商务问题，这些问题宜作为合同的基本部分提出。但本标准中的所有条款在任何商务活动中都需被仔细考虑。

1.8　本标准不是追溯性的，主要应用于新的开发；对于既有系统，仅当进行大的修改时才进行全面应用，对于小的修改，仅第16章适用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 28809—2012　轨道交通　通信、信号和处理系统　信号用安全相关电子系统（IEC 62425：2007，IDT）

IEC 60050-191　国际电工词汇　第191章：可靠性和服务质量[International electrotechnical vocabulary (IEV)—Chapter 191: Dependability and quality of service]

IEC 62278　轨道交通　可靠性、可用性、可维修性和安全性（RAMS）规范及示例[Railway applications—Specification and demonstration of reliability, availability, maintainability and safety (RAMS)]

IEC 62280-1　铁路设施　通信、信号和处理系统　第1部分：在封闭的传输系统中有关通信安全（Railway applications—Communication, signalling and processing systems—Part 1: Safety-related communication in closed transmission systems）

IEC 62280-2　铁路设施　通信、信号和处理系统　第2部分：在开放的传输系统中有关通信安全（Railway applications—Communication, signalling and processing systems—Part 2: Safety-related