ICS 45.060
CCS S 04

中华人民共和国国家标准

GB/T 28808—2021
代替 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

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

（IEC 62279:2015, MOD）

2021-12-31 发布　　2022-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替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》，与GB/T 28808—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了下列术语和定义：3.3可用性、3.5设计机构、3.7元素、3.11避错、3.16产品、3.18可靠性、3.19需求可追溯性目标（见2012年版的第3章）；

b) 增加了下列术语和定义：3.1.4组件、3.1.5配置管理员、3.1.6客户、3.1.8实体、3.1.16集成、3.1.17集成人员、3.1.18既有软件、3.1.19开源软件、3.1.21项目管理、3.1.22项目经理、3.1.23可靠性、3.1.24鲁棒性、3.1.25需求经理、3.1.26需求管理、3.1.30安全功能、3.1.33软件基线、3.1.34软件部署、3.1.41测试人员、3.1.42测试、3.1.43 T1类工具、3.1.44 T2类工具、3.1.45 T3类工具（见3.1）；

c) 更改了软件管理和组织的独立性要求（见第5章，2012年版的第5章、第6章、第7章）；

d) 增加了软件部署和软件维护方面的要求（见5.1）；

e) 增加了参与软件开发的角色的定义和个人能力的要求（见5.2）；

f) 增加了有关工具的新条款（见6.7）；

g) 增加了整体软件测试及相应要求（见7.7）；

h) 更改了对软件开发输出成果物的要求（见附录A，2012年版的附录A）；

i) 增加了附录C，进一步明确软件角色的关键能力及其职责（见附录C）。

本文件使用重新起草法修改采用IEC 62279:2015《轨道交通　通信、信号和处理系统 控制和防护系统软件》。

本文件与IEC 62279:2015相比做了下述结构调整：

——3.1.9对应IEC 62279:2015的3.1.10；

——3.1.10对应IEC 62279:2015的3.1.11；

——3.1.11对应IEC 62279:2015的3.1.9；

——附录B对应IEC 62279:2015的附录D，并增加了每一个目标和描述的章条编号；

——附录C对应IEC 62279:2015的附录B；

——附录D对应IEC 62279:2015的附录C。

本文件与IEC 62279:2015的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用等同采用国际标准的GB/T 19000代替了ISO 9000:2015（见6.5.4.2）；
- 用等同采用国际标准的GB/T 19001代替了ISO 9001:2008（见5.1.2.1、5.2.2.3、6.4.1.2、表A.9和表C.11）；
- 用修改采用国际标准的GB/T 25000.10代替了ISO/IEC 25010（见9.2.4.4、表C.11）。

本文件做了下列编辑性改动：

——删除了第2章规范性引用文件清单中的IEC 62278:2002；

——增加了描述以指明附录D（见5.3.2.14）；

——增加了缩略语“API”“CFG”“DSL”和“LCF”；

——更改了参考文献；

——更改了 IEC 62279:2015 中的错误：

- 6.6.3 中“(见 9.2.4.11)”改为“(见 9.2.4.10)”；
- 表 A.1 中，“见注 2”符号原标注在第 29、30、31 号文档，改为标注在第 30、31、32 号文档；
- 表 A.8 中“软件分析技术(6.3)”改为“软件分析技术(6.2)”；
- 表 A.9 中，参考条目中的“7.1”改为“6.5”；
- 表 A.12 中，第 2 个序号 9 和序号 10，改为序号 10 和序号 11。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由国家铁路局提出。

本文件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。

本文件起草单位：中车株洲电力机车研究所有限公司、同济大学、中国铁道科学研究院集团有限公司标准计量研究所、北京全路通信信号研究设计院集团有限公司、中国铁道科学研究院集团有限公司通信信号研究所、北京和利时系统工程有限公司。

本文件主要起草人：周志飞、刘布麒、徐中伟、赵天时、邱兆阳、张萍、汪小亮、李文波。

本文件及其所代替文件的历次版本发布情况为：

——2012 年首次发布为 GB/T 28808—2012；

——本次为第一次修订。

引　言

本文件与 GB/T 21562 和 GB/T 28809 配套使用。

GB/T 21562—2008 适用于大范围的轨道交通系统，而 GB/T 28809 适用于整个轨道交通控制和防护系统中可能存在的单个系统的批准过程。本文件关注于为提供满足安全完整性要求的软件而采用的方法，该安全完整性是通过更全面的考虑后赋予软件的。

本文件提供一系列有关开发、部署和维护方面的要求，任何用于轨道交通控制和防护应用的安全相关软件都应遵守这些要求。本文件规定了有关组织结构、组织之间的关系以及开发、部署和维护活动中涉及的职责分工等方面的要求，同时本文件也提供了人员资质和专业知识的准则。

本文件的关键概念是软件安全完整性等级(SIL)。本文件标识了五个软件安全完整性等级：SIL0～SIL4，其中 SIL0 为最低等级，SIL4 为最高等级。软件失效带来的风险越高，软件安全完整性等级就越高。

本文件明确了五个软件安全完整性等级的技术和措施，SIL0～SIL4 所需的技术和措施在附录 A 的规范性表格中列出。本文件中 SIL1 和 SIL2 所需的技术要求相同，SIL3 和 SIL4 所需的技术要求相同。对于某个给定的风险，本文件并没有给出哪种软件安全完整性等级是合适的指导意见。因为该决策取决于多个因素，包括应用的性质、其他系统承担的安全功能的范围，以及社会及经济因素。

将安全功能分配到软件的过程由 GB/T 21562 和 GB/T 28809 定义。

本文件规定了满足这些要求的必要措施。

GB/T 21562 和 GB/T 28809 要求采用系统性的方法以：

a) 识别危害、评估风险并基于风险准则作出决策；

b) 确定必要的风险降低措施以满足风险接受准则；

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

d) 选择一个合适的系统架构；

e) 规划、监督和控制所必需的技术和管理活动，这些技术和管理活动把安全需求规格说明转化成安全完整性得到确认的安全相关系统。

在将规格说明分解到由安全相关的系统和组件组成的设计当中时，需要对安全完整性等级作进一步分配，并最终形成所需要的软件安全完整性等级。

以目前的技术发展水平，无论是质量保证措施(所谓的故障规避措施和故障检测措施)的应用还是软件故障容忍方法的应用，都无法保证软件的绝对安全。尚无途径证明一个相对复杂的安全相关软件中不存在缺陷，特别是规格说明的缺失和设计的缺陷。

应用于开发高完整性软件的原则，包括但不限于：

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) 经过验证的组件和组件库；

e) 清晰的文档与可追踪性；

f) 可审核的文档；

g) 确认；

h) 评估；

i) 配置管理和变更控制；

j) 组织和个人能力方面的相应考虑。

系统安全需求规格说明识别了分配给软件的所有安全功能，同时确定了这些安全功能的安全完整性等级。图 1 给出了应用本文件时的一系列实用的步骤并说明如下：

a) 定义软件需求规格说明，同时考虑软件架构；软件架构是为软件和软件安全完整性等级制定安全策略的地方，见 7.2 和 7.3；

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，设计、开发和测试软件，见 7.4 和 7.5；

c) 在目标硬件上进行软件集成和软硬件集成，以及功能验证，见 7.6；

d) 接受和部署软件，见 7.7 和 9.1；

e) 在软件生命周期的运行阶段，如果软件需要维护，如适用，重启本文件进行处理，见 9.2。

许多活动与软件开发交叉进行，这些活动包括：测试(见 6.1)、验证(见 6.2)、确认(见 6.3)、评估(见 6.4)、质量保证(见 6.5)，以及修改和变更控制(见 6.6)。

本文件对支持工具(见 6.7)和由应用数据或算法配置的系统(见第 8 章)也作出了要求。

本文件对软件开发过程中涉及的角色的独立性和个人能力(见 5.1、5.2 和附录 C)也作出了要求。

本文件不强制要求使用特定的软件开发生命周期，在 5.3、图 3、图 4 和 7.1 给出了示范的生命周期和文档集。

格式化表格针对软件安全完整性等级列出了各种技术/措施符合附录 A 的要求。与该表格交叉引用的是附录 B 给出的技术词汇，它对每项技术/措施的目标和内容作了简要描述。

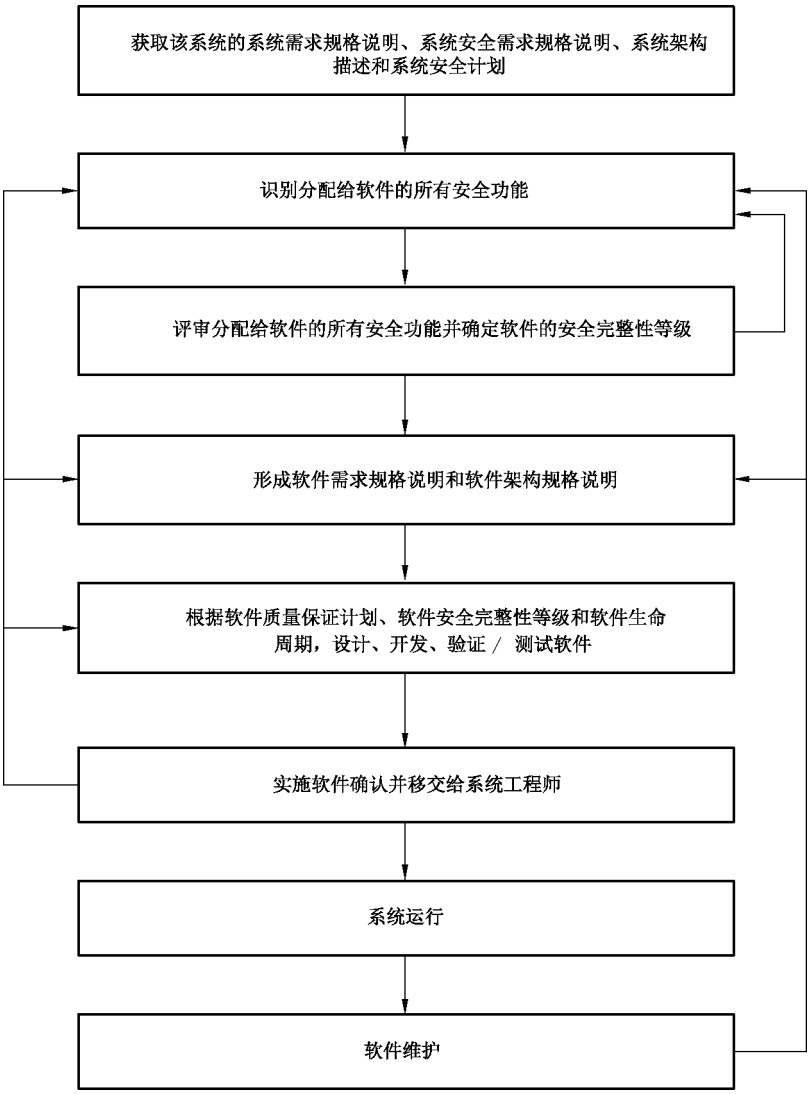
获取该系统的系统需求规格说明、系统安全需求规格说明、系统架构描述和系统安全计划
识别分配给软件的所有安全功能
评审分配给软件的所有安全功能并确定软件的安全完整性等级
形成软件需求规格说明和软件架构规格说明
根据软件质量保证计划、软件安全完整性等级和软件生命周期，设计、开发、验证 / 测试软件
实施软件确认并移交给系统工程师
系统运行
软件维护

图 1　软件路线图示例

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　本文件规定了轨道交通控制和防护应用中使用的可编程电子系统软件开发所需的过程和技术要求。它适用于任何有隐含安全性的领域。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架构来实现。

1.2　本文件只适用于软件以及软件与软件所在系统之间的交互。

1.3　本文件与被认定为对安全没有任何影响的软件无关，即软件失效不会影响任何已识别的安全功能。由于在风险评估甚至危害识别时存在不确定性，因此引入了 SIL0 的概念。对于安全性影响低于 SIL1 功能的软件部分，至少要满足本文件 SIL0 的要求。

1.4　本文件适用于轨道交通控制和防护系统中使用的所有安全相关软件，包括：

a)　应用程序设计；

b)　操作系统；

c)　支持工具；

d)　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：可编程逻辑控制器的梯形逻辑）。

1.5　本文件也涉及了既有软件和工具的使用。如果要使用该类软件，则要满足 7.3.4.7 和 6.5.4.16 中对既有软件的特定要求，以及 6.7 中对工具的要求。

1.6　根据本文件的任何版本开发的软件，都被视为符合本文件规定，不受针对既有软件的要求约束。

1.7　本文件考虑了目前流行的以适用多种应用场合的通用软件为基础进行应用设计的情况，这些通用软件通过数据、算法或二者同时配置后，为应用生成可执行的软件。第 1 章～第 6 章和第 9 章既适用于通用软件也适用于应用数据或算法。第 7 章仅适用于通用软件，第 8 章仅适用于应用数据或算法。

1.8　本文件不涉及商务问题，商务问题宜作为合同的基本部分提出。但在任何商务活动中都需仔细考虑本文件的所有条款。

1.9　本文件不是追溯性的，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，对于小的变更，仅需要应用 9.2。评估人员需要分析软件文档中提供的证据，以便确认对软件变更范围和性质的认定是否充分。当对既有软件进行升级或维护时，宜应用本文件。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 19000　质量管理体系　基础和术语（GB/T 19000—2016，ISO 9000：2015，IDT）

GB/T 19001　质量管理体系　要求（GB/T 19001—2016，ISO 9001：2015，IDT）

GB/T 25000.10　系统与软件工程　系统与软件质量要求和评价（SQuaRE）　第 10 部分：系统与软件质量模型（GB/T 25000.10—2016，ISO/IEC 25010：2011，MOD）