ICS 45.060
CCS S 35

中华人民共和国国家标准

GB/T 24339—2023
代替 GB/T 24339.1—2009 和 GB/T 24339.2—2009

轨道交通　通信、信号和处理系统 传输系统中的安全相关通信

Railway applications—Communication, signalling and processing systems—Safety related communication in transmission systems

（IEC 62280:2014，MOD）

2023-11-27 发布　　2024-03-01 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 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》和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》，与GB/T 24339.1—2009和GB/T 24339.2—2009相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了范围(见第1章)；
b) 更改了危害分析的定义(见3.1.23，GB/T 24339.2—2009的3.11.1)；
c) 增加了术语隐含数据及其定义(见3.1.24)；
d) 更改了术语非加密安全编码及其定义(见3.1.36，GB/T 24339.1—2009的3.9)；
e) 增加了术语公共网络及其定义(见3.1.38)；
f) 增加了术语可信及其定义(见3.1.61)；
g) 增加了安全相关通信的主要危害(见第5章)；
h) 更改了防护措施根据GB/T 28809执行时的要求[见7.2.5，GB/T 24339.2—2009的6.2 d)]；
i) 增加了安全论据的安全完整性和安全相关功能特性相适应的要求(见7.3.8.1)；
j) 增加了安全编码性能的概率分析应与安全目标兼容的要求，提供故障模式的模型，并对所有计算假设进行验证和确认的要求(见7.3.8.2.4)；
k) 更改了加密技术的技术选择(见7.3.9.2，GB/T 24339.2—2009的6.3.8.2)；
l) 增加了加密架构的技术选择(见7.3.9.2)；
m) 更改了安全编码和加密技术在非安全相关传输系统中的选择和应用(见B.2，GB/T 24339.2—2009的A.2)；
n) 更改了安全编码长度的描述(见B.4，GB/T 24339.1—2009的附录A)；
o) 增加了安全相关和非安全相关应用之间的通信说明(见B.5)；
p) 更改了通信授权方和攻击者之间的关联关系(见C.3.1，GB/T 24339.2—2009的D.3)；
q) 增加了传输系统的分类(见D.1)；
r) 增加了传输系统的分类和威胁的关系(见D.2)。

本文件修改采用IEC 62280：2014《轨道交通　通信、信号和处理系统　传输系统中的安全相关通信》。

本文件与IEC 62280：2014相比做了下述结构调整：

——3.1.4～3.1.65对应IEC 62280：2014的3.1.5～3.1.66；
——附录A对应IEC 62280：2014的附录E；
——附录B对应IEC 62280：2014的附录C；
——附录C对应IEC 62280：2014的附录A；
——附录D对应IEC 62280：2014的附录B；
——附录E对应IEC 62280：2014的附录D。

本文件与IEC 62280：2014的技术性差异及其原因如下：

——用规范性引用的GB/T 28809替换了IEC 62425：2007(见第1章、第4章、第5章、7.2.5、7.2.8)，以适应我国的技术条件，提高可操作性。

本文件做了下列编辑性改动：

——将 IEC 62280:2014 中脚注 1 更改为第 5 章的注；

——将 IEC 62280:2014 中脚注 6 更改为 3.2 的注；

——用资料性引用的 GB/T 21562 替换了 IEC 62278(见 C.4.2.2.1、E.1.3)，并列入参考文献；

——更改了参考文献。

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。

本文件由全国轨道交通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：北京交通大学、中车株洲电力机车研究所有限公司、北京鉴衡认证中心有限公司、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标准计量研究所、上海申通地铁集团有限公司。

本文件主要起草人：唐涛、步兵、方光华、王业流、赵骏逸、耿宏亮、薄云览、刘贵、王一民、高莺、王大庆。

本文件及其所代替文件的历次版本发布情况为：

——2009 年首次发布为 GB/T 24339.1—2009 和 GB/T 24339.2—2009；

——本次为第一次修订。

引　言

如果安全相关电子系统涉及不同位置间的信息传输，则传输系统成为安全相关系统的一个组成部分，而且根据 GB/T 28809 说明端对端传输安全。

本文件所考虑的传输系统，用于不同位置之间的信息传输，总体上没有特定的先决条件需要满足。从安全角度看，该系统是非可信的或非完全可信的。

本文件专用于此类传输系统下安全相关信息传输考虑的要求。

本文件未考虑 RAM 相关内容，但其是全局安全的主要方面。

安全要求取决于传输系统的特性。为简化证明系统安全性方法的复杂性，考虑了 3 种类型的传输系统：

——第 1 类是包含由安全系统设计者控制并在其生命周期内保持固定的系统；

——第 2 类是包含部分未知或不固定的部分，但排除未经授权访问的系统；

——第 3 类是不在设计者控制下，且考虑未经授权访问的系统。

之前第 1 类系统的要求在 GB/T 24339.1—2009 中规定，其他系统的要求在 GB/T 24339.2—2009 中规定。

当根据上述标准认证的安全相关通信系统需要维护或扩展时，使用附录 A 对本文件的条款和先前系列标准的条款进行追溯。

轨道交通　通信、信号和处理系统 传输系统中的安全相关通信

1　范围

本文件规定了在与传输系统相连的安全相关设备之间实现安全相关通信所需的基本要求。

本文件适用于数字通信的安全相关传输系统，该系统不一定是为安全相关系统设计的，而是：

——在设计人员控制下并在生命周期内固定；

——部分未知或不固定，但可以排除未经授权的访问；

——不在设计人员的控制下，并且考虑未经授权的访问。

安全相关和非安全相关设备均可连接至传输系统。

安全要求通常在根据 GB/T 28809 设计的安全相关设备中实施。在某些情况下，只要有安全措施满足所分配的安全要求，这些要求可以在传输系统的其他相关设备中实施。

安全需求规格书是安全相关电子系统的安全论据的先决条件，关于安全论据所需的证据（包括质量管理和安全管理等）在 GB/T 28809 中规定。

本文件不适用于在本文件发布之前的既有系统。

本文件未定义下列术语：

——传输系统；

——传输系统所连接的设备；

——解决方案（如：互操作性）；

——安全相关数据的界定。

通过开放式传输系统连接的安全相关设备可能受到多种不同的 IT 安全威胁，针对这些威胁制定整体方案，包括管理、技术和操作方面。

本文件中的信息安全，仅考虑通过消息对安全相关应用程序的故意攻击。

本文件不包括一般的信息安全问题，特别是不包括下列有关信息安全方面的问题：

——确保安全相关信息的机密性；

——防止传输系统过载。

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 28809　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，IDT）

3　术语和定义、缩略语

3.1　术语和定义

下列术语和定义适用于本文件。