ICS 45.060
S 30

中华人民共和国国家标准

GB/T 24339.1—2009/IEC 62280-1:2002

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

**Railway applications—
Communication, signalling and processing systems—
Part 1:Safety-related communication in closed transmission systems**

(IEC 62280-1:2002,IDT)

2009-09-30 发布　　2010-01-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　参考结构 …… 2
5　传输系统特征和安全规程之间的关系 …… 4
5.1　功能完整性要求 …… 4
5.2　安全完整性要求 …… 4
6　安全规程要求 …… 5
6.1　总则 …… 5
6.2　安全相关设备间的通信 …… 5
6.3　安全相关设备与非安全相关设备之间的通信 …… 5
6.4　非安全相关设备间的通信 …… 6
7　安全编码要求 …… 6
7.1　总则 …… 6
7.2　安全目标 …… 6
7.3　安全编码的长度 …… 6
附录A（资料性附录）　安全编码的长度 …… 7

前　言

GB/T 24339《轨道交通　通信、信号和处理系统》分为两部分：

——第1部分：封闭式传输系统中的安全相关通信；

——第2部分：开放式传输系统中的安全相关通信。

本部分为GB/T 24339的第1部分。

本部分等同采用IEC 62280-1:2002《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》(英文版)。

本部分与IEC 62280-1:2002相比，主要差异如下：

a) “本国际标准”一词改为“本部分”；

b) 用小数点“.”代替作为小数点的逗号“,”；

c) 删除国际标准的前言；

d) 引用文件ENV 50129:1998改为EN 50129:2003。

本部分的附录A为资料性附录。

本部分由铁道部提出。

本部分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。

本部分起草单位：北京交通大学、株洲南车时代电气股份有限公司。

本部分主要起草人：唐涛、张利芝、徐田华、严云升、牛儒、刘贵。

引　言

封闭式传输系统指可连接设备的最大数量和拓扑结构是已知的，传输系统的物理特征是固定的传输系统。

GB/T 24339 的本部分适用于封闭式传输系统的安全相关设备间的安全相关通信，GB/T 24339.2 适用于开放式传输系统。

安全相关和非安全相关设备都可以与传输系统连接。

在错误影响到安全相关通信时，需要：

——检查错误；

——启动一个安全反应。

本部分未对非置信的传输系统自身提出安全要求，但规定了非置信系统的特性和物理特征。

出于安全目的，只需考虑物理传输通道。通过在安全相关设备中应用安全规程和安全编码来保证安全，安全编码添加在传输系统非置信的通信协议上层。

尽管本部分不考虑可靠性，但应切记可靠性是整体安全性的主要因素。

本部分的适用范围也可从车辆总线扩展到所有的封闭式传输系统。

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

1　范围

GB/T 24339的本部分规定了连接在传输系统上的安全相关设备之间的安全相关通信所需要的基本要求。

本部分适用于采用封闭式传输系统进行通信的安全相关电子系统,适用于封闭式通信系统的安全需求规范和设计,以便获得指定的安全完整性等级(SIL)。

安全要求规范是安全相关电子系统的安全论据的先决条件。有关安全论据的详述(包括安全管理和质量管理等)见EN 50129。本部分只讨论其中的功能安全和技术安全论据。

本部分不适用于在本部分颁布之前的既有系统。然而,对于既有系统、子系统和设备的修改或扩展,要尽可能地使用本部分。

本部分用于满足以下前提条件的封闭式传输系统,并且需要提供相关证据说明系统满足这些条件:

——只允许授权的访问;

——可连接设备最大数量已知;

——传输介质已知且固定。

封闭式传输系统不局限于数据总线,也可以包括如应答器连接或两个安全相关的计算机之间简单的串行连接传输方式。

本部分没有给出以下内容的定义:

——传输系统;

——传输系统所连接的设备;

——详细的解决方案(如互操作性);

——安全相关数据的界定。

2　规范性引用文件

下列文件中的条款通过GB/T 24339的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 21562　轨道交通　可靠性、可用性、可维修性和安全性(RAMS)规范和示例(GB/T 21562—2008,IEC 62278:2002,IDT)

IEC 62279　轨道交通　通信、信号和处理系统　轨道控制和防护系统的软件

EN 50129　轨道交通　用于信号系统的安全相关电子系统

3　术语和定义

下列术语和定义适用于GB/T 24339的本部分。

3.1

真实性　authenticity

信息有效且已知该信息来自指定信息源的状态。