ICS 45.060
S 30

中华人民共和国国家标准

GB/T 24339.2—2009/IEC 62280-2:2002

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

**Railway application—
Communication, signalling and processing systems—
Part 2: Safety-related communication in open transmission systems**

(IEC 62280-2:2002, 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

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2部分。

本部分等同采用IEC 62280-2:2002《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》(英文版)。

本部分与IEC 62280-2:2002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、附录B、附录C、附录D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、范祚成。

引　言

开放式传输系统由特性未知或部分未知的系统组成，本部分专用于开放式传输系统下安全相关信息传输应考虑的要求。

如果安全相关电子系统涉及到不同位置间的信息传输，那么通信系统就成为安全相关系统的一个组成部分，而且应根据 EN 50129 说明端对端传输是安全的。

数据通讯系统的安全要求取决于其可知或未知的特性。为简化证明系统安全性方法的复杂性，考虑了两种类型的传输系统。第一种是封闭式传输系统，它的组成可由安全系统设计者在一定程度上控制，其安全性要求在 GB/T 24339.1 中规定。第二种是开放式传输系统，GB/T 24339 的本部分规定了开放式传输系统的安全要求。

本部分考虑的传输系统，总体上没有特定的先决条件需要满足。从安全角度看，该系统是非置信的或非完全置信的，被视为“黑箱”。

对于用于常规认证而不是用于特殊应用的交叉验收(cross acceptance)，其要求应与 EN 50129 的要求相同。

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

1　范围

GB/T 24339的本部分规定了连接在开放式传输系统上的安全相关设备之间的安全相关通信的基本要求。适用于采用开放式传输系统达到通信目的的安全相关电子系统及其安全需求规范,以便实现指定的安全完整性等级(SIL)。

安全需求规范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EN 50129:2003中规定。本部分的主题是通信相关的功能性和技术性安全论据的要求。开放式传输系统的性质和行为,只用于定义特性,而不用于安全性,因而从安全观点看,开放式传输系统可以潜含任何特性,例如各种传输方式、报文存储、非法访问等,安全进程只能依赖于各种特性,这些须在安全论据中说明。

本部分不适用于在本部分颁布之前已被采用的既有系统。

本部分没有规定:

——开放式传输系统;

——开放式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。

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)

EN 50129:2003　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

访问保护　access protection

为防止非法读取或更改信息,在用户安全相关系统内或在传输系统内设计的进程。

3.1.1

黑客　hacker

蓄意绕开访问保护的人。

3.2

真实性　authenticity

信息有效且已知该信息来自指定信息源的状态。