ICS 91 140 90
Q78

中华人民共和国国家标准

GB/T 35850.2—201×

电梯、自动扶梯和自动人行道安全相关的可编程电子系统的应用 第2部分：自动扶梯和自动人行道（PESSRAE）

Programmable electronic systems in safety-related applications for lifts (elevators), escalators and moving walks Part 2: Escalators and moving walks (PESSRAE)

（ISO 22201-2:2013, MOD）

（征求意见稿）

（本稿完成日期：2018年3月9日）

请注意：
在提交反馈意见时，请将所知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××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 35850《电梯、自动扶梯和自动人行道安全相关的可编程电子系统的应用》拟由下列几部分组成：

——第 1 部分：电梯；

——第 2 部分：自动扶梯和自动人行道；

——第 3 部分：PESSRAL和PESSRAE相关的可编程电子系统的生命周期指南（技术报告）。

本部分为GB/T 35850 的第 2 部分。

本部分按照GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法修改采用ISO 22201-2:2013《电梯、自动扶梯和自动人行道安全相关的可编程电子系统的应用 第 2 部分：自动扶梯和自动人行道（PESSRAE）》（英文版）。

本部分与ISO 22201-2:2013 的技术性差异及其原因如下：

—— 关于规范性引用文件，本部分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 20438.1代替了IEC 61508-1；
- 用等同采用国际标准的GB/T 20438.2代替了IEC 61508-2；
- 用等同采用国际标准的GB/T 20438.3代替了IEC 61508-3；
- 用等同采用国际标准的GB/T 20438.4代替了IEC 61508-4；
- 用等同采用国际标准的GB/T 20438.5代替了IEC 61508-5；
- 用等同采用国际标准的GB/T 24808代替了ISO 22200；
- 用等同采用国际标准的GB 28526代替了IEC 62061。

—— 基于GB 16899—2011中的表6，并参考EN 115-1:2017，本部分做了以下修改：

- 在表1中，删除了第16项、第17项、第19项、第20项、第21项、第23项、第24项，以便与GB 16899—2011一致；
- 在表2中，删除了第16项、第17项、第19项、第20项、第21项、第23项、第24项，以便与GB 16899—2011一致；
- 在表2中，自动扶梯和自动人行道安全功能（装置）栏中的“检查附加制动器的动作”所对应的安全状态要求栏中的“切断主机和工作制动器电源”由非SIL相关改为SIL相关，以便与GB 16899—2011一致；
- 在表2的安全状态要求栏中，删除了SIL相关的“切断附加制动器电源”、“阻止其他的检修控制设备”、“防止正常启动”，删除了非SIL相关的“切断主机和工作制动器电源”、“声音报警”，以便与GB 16899—2011一致；
- 在表2中，修改了R注释的内容，以便与GB 16899—2011一致。

本部分与ISO 22201-2:2013相比还做了下列编辑性修改：

—— 删除了引言中与本部分无关的内容，因为其存在与否对本部分的理解和使用没有任何影响；

—— 删除了第2章，因为其内容已包含在第5章中，并且与GB/T 35850.1—2018的结构保持一致。另外，调整了后续的章节条款号；

—— 在术语和定义中，删除了4.1和4.2，因在本部分中未被使用，并调整了后续的条款号；

—— 在符号与缩略语中，增加了EUC和MTTR；

—— 在符号与缩略语中，删除了PCB，因为其未在本部分中使用；

—— 表1中，将第26项的内容改为了注释，因为其不是安全功能；

—— 调整了表1和表2中的自动扶梯和自动人行道安全功能（装置）的序号，以及表2中的R注释的序号，以便于应用；

—— 删除了附录B（资料性附录）的表B.1中ASME A17.1-2004和日本建筑法规相关的条款及内容，因

为与我国的实际应用不符；

—— 在表B.1中，增加了自动扶梯和自动人行道安全功能（装置）对应GB 16899—2011和EN 115-1:2017的条款号，以便于应用；

—— 在参考文献中，用国家标准代替了对应的国际文件，以便于应用。

本部分由全国电梯标准化技术委员会（SAC/TC 196）提出和归口。

本部分起草单位：（暂空）

本部分主要起草人：（暂空）

引　　言

近年来包含电气、电子部件的系统在很多领域被用于执行安全功能。以计算机为基础的系统，一般被划归为可编程电子系统（PE system），在很多领域越来越多的被应用于执行安全功能。安全有效地利用计算机系统技术，关键在于决策者在做安全方面的决策时需要有充分的指导。大多数情况下，安全性由依靠多领域技术（如机械、液压、气动、电气、电子、可编程电子等）的多个保护系统共同完成。因此任何安全策略不仅必须考虑独立系统（如传感器、控制设备和执行器件）内的所有元器件，而且必须考虑所有用来构成完整安全相关系统的安全相关部件。

本部分阐述了对用于执行自动扶梯和自动人行道安全功能的由可编程电子部件和可编程电子系统（PE system）组成的系统的具体要求。本部分的目的在于对自动扶梯和自动人行道安全相关的可编程电子系统（PESSRAE）的技术一致性、性能要求和合理性作出具体规定。

风险分析、术语名词和技术解决方案主要参考了GB/T 20438系列标准。对表1中每项安全功能的风险分析确定了PESSRAE的电气安全功能的等级划分。表1和表2对每个电气安全功能分别给出了安全完整性等级和功能性要求。

电梯、自动扶梯和自动人行道安全相关的可编程电子系统的应用

第2部分：自动扶梯和自动人行道（PESSRAE）

1　范围

1.1 本部分适用于自动扶梯和自动人行道，当可编程电子系统被用于执行自动扶梯和自动人行道电气安全功能时，应采用本部分。当自动扶梯和自动人行道规范、标准中所定义的自动扶梯和自动人行道安全功能应用PESSRAE时，应引用本部分。

1.2 本部分也可应用于新的或与本部分描述有差异的PESSRAE。

1.3 如果电气安全装置符合本部分和其他相关标准的所有要求，则不必考虑其失效的可能性。

1.4 本部分：

a）使用了安全完整性等级（SIL）来规定用PESSRAE实现安全功能的目标失效量；

b）规定了达到某一功能的安全完整性的要求，但没有规定实施和保持该要求的责任主体（如：设计者、制造商、供应商或业主等）；

c）应用于自动扶梯和自动人行道的可编程电子系统（PE system），符合自动扶梯和自动人行道相关标准（如：GB 16899等）的最低要求；

d）明确了与GB/T 20438以及GB/T 24808之间的关系；

f）适用于软件和硬件设计的阶段和活动，但不包括设计之后的阶段和活动，如：采购与制造等；

g）要求PESSRAE制造商提供说明书，向实施该自动扶梯和自动人行道组装、连接、调试、维护的组织详细说明如何保持PESSRAE的完整性；

h）规定了与软硬件安全确认相关的要求；

i）为具体的自动扶梯和自动人行道安全功能规定了安全完整性等级；

j）规定了达到特定的安全完整性等级所需要的技术和措施；

k）提供了应用PESSRAE的风险降低的决策表；

l）规定了要求的PESSRAE最高安全完整性等级为SIL3，最低安全完整性等级为SIL1。

1.5 本部分不包含：

a）PE system装置自身产生的危险，如电击等；

b）失效安全的概念。在失效模式定义良好且复杂度相对较低的情况下失效安全可能是有价值的，因为本部分范围内的PESSRAE复杂度很高，所以失效安全概念在此是不合适的；

c）对自动扶梯和自动人行道安全功能中的PESSRAE的完整运用所必需的其他相关要求，如：系统集成规范，温度和湿度，机械结构，开关、执行器件、传感器的安装和标识等。这些要求应符合相关自动扶梯和自动人行道标准；

d）由恶意或未授权行为引起的，涉及安全威胁的可预见的误操作。需要考虑某一安全威胁分析时，如果重新评估了特定的SIL，可以使用本部分。

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 20438.1　电气/电子/可编程电子安全相关系统的功能安全 第1部分：一般要求（GB/T 20438.1—2006，IEC 61508-1:1998，IDT）

GB/T 20438.2　电气/电子/可编程电子安全相关系统的功能安全 第2部分：电气/电子/可编程电子安全相关系统的要求（GB/T 20438.2—2006，IEC 61508-2:2000，IDT）

GB/T 20438.3　电气/电子/可编程电子安全相关系统的功能安全 第3部分：软件要求（GB/T 20438.3—2006，IEC 61508-3:1998，IDT）

GB/T 20438.4　电气/电子/可编程电子安全相关系统的功能安全 第4部分：定义和缩略语（GB/T 20438.4—2006，IEC 61508-4:1998，IDT）

GB/T 20438.5　电气/电子/可编程电子安全相关系统的功能安全 第5部分：确定安全完整性等级的方法示例（GB/T 20438.5—2006，IEC 61508-5:1998，IDT）

GB/T 24808　电磁兼容性 电梯、自动扶梯和自动人行道的产品系列标准 抗扰度（GB/T 24808—2009，ISO 22200:2009，IDT）

GB 28526 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全（GB 28526—2012，IEC 62061:2005，IDT）

3　术语和定义

在GB/T 20438.4中给出的术语和定义适用于本部分，但是本部分作出的定义应优先于通用标准GB/T 20438。

3.1

非SIL相关安全状态要求　non-SIL-relevant safe-state requirement

对某个SIL相关安全功能的动作作出响应，而执行该响应的功能无SIL要求。

注：参见图4和表2。

3.2

可编程电子 programmable electronic

PE

以计算机技术为基础，可以由硬件、软件及其输入和（或）输出单元构成。

注：本术语包括以一个或多个中央处理器（CPU）及相关的存储器等为基础的微电子装置。

举例：下列均是可编程电子装置：

—微处理器；

—微控制器；

—可编程控制器；

—现场可编程门阵列（FPGA）；

—专用集成电路（ASIC）；

—可编程逻辑控制器（PLC）；

—其他以计算机为基础的装置（智能传感器、变送器、执行器等）。

3.3

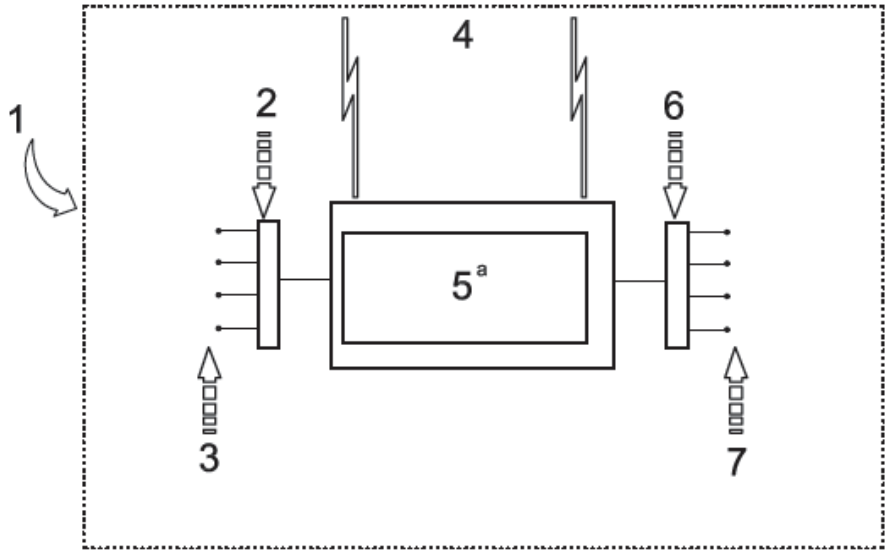
可编程电子系统 programmable electronic system

PE system

基于一个或多个可编程电子装置的控制、保护或监视的系统，包括系统中所有部件，如电源、传感器和其他输入装置、数据总线和其他通信路径、执行装置和其他输出装置。

注1：参见图1。

注2：PE system可执行满足SIL要求或非SIL要求的功能。功能的SIL分级只需考虑PE system中执行SIL相关功能要求的部分。



图中：

1——PE system的范围；

2——输入接口（如A/D转换器）；

3——输入装置（如传感器）；

4——通讯；

5——可编程电子装置（PE）；

6——输出接口（如D/A转换器）；

7——输出装置/终端元件（如执行装置）；

[a] 图中所示的可编程电子装置在中心位置，但是它可以存在于PE system的多个位置。

图1 基本PE system结构

3.4

自动扶梯和自动人行道安全相关的可编程电子系统 programmable electronic systems in safety-related applications for escalators and moving walks

PESSRAE

基于软件的PE system在自动扶梯和自动人行道安全相关系统中的应用。

3.5

检验测试 proof test

周期性测试，用以检测安全相关系统中危险的隐性失效，在必要时通过维修，把系统复原到“新的”状态或实际上接近这种状态。

注1：在本部分中使用“检验测试”，但要注意到同义的术语“周期性测试”。

注2：检验测试的有效性取决于失效覆盖和维修的有效性。在实践中除了简单E/E/PE安全相关系统外，100%的隐性失效的检测很难达到，这是个目标。至少所有要执行的安全功能按E/E/PE安全相关系统安全要求规范进行检查。如果使用多个独立的通道，则对每个通道分别进行检验测试。对于复杂的部件，需进行分析，以证明在E/E/PE安全相关系统整体生命周期内，未被检验测试所检测出的隐性危险失效的概率可忽略不计。

注3：检验测试需要一定时间完成。在此时间内E/E/PE安全相关系统可能被部分或全部禁用。在测试过程中，仅当EUC已停机或E/E/PE安全相关系统被测试的部分仍能在要求动作时保持有效，检验测试持续时间可以忽略。

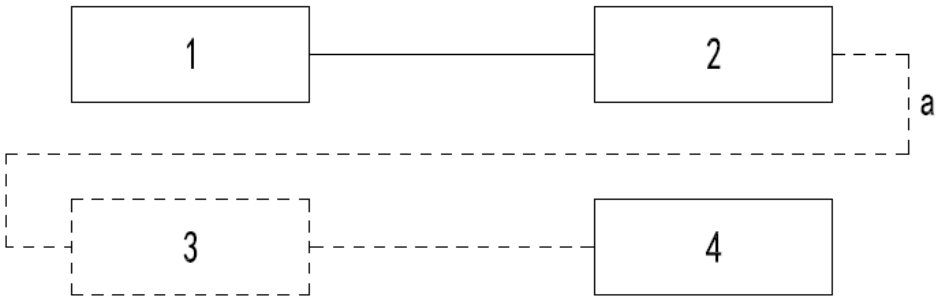
注4：在检验测试期间，E/E/PE安全相关系统可能部分或全部不能响应动作要求。仅在修复过程中EUC停机或使用其他等效的风险措施来代替时，用于SIL计算的MTTR可以忽略。

3.6

安全回路　safety circuit

所有安全装置的组合，完成自动扶梯和自动人行道的一组或所有安全功能。

注：参见图2。



图中：

1——安全装置1，功能1；

2——安全装置2，功能2；

3——安全装置n，功能n；

4——安全装置（n+1），功能（n+1）；

a——一组或全部必要的自动扶梯和自动人行道安全功能（见表1）。

图 2　安全回路

3.7

安全装置 safety device

安全相关系统的组成部分，包括必要的控制电路，用于独立地实现自动扶梯和自动人行道安全功能，可由PE system部件和非PE system部件组成。

注：参见图3和表1。

图中：

1——PE system部件；

2——非PE system部件。

图 3　安全装置

3.8

安全功能　safety function

针对特定的危险事件，为了达到或保持自动扶梯和自动人行道的安全状态，由安全相关系统实现的功能。

注1：参见表1。

注2：安全功能可包括非SIL相关安全状态要求，参见表2。

3.9

安全相关系统 safety-related system

执行一个或多个安全功能的一个或多个安全装置，可基于PE、电气、电子和/或机械的自动扶梯和自动人行道部件。

注：该术语包括执行安全功能所需的全部硬件、软件和支持服务（如电源等）。传感器、其他输入装置、最终元件（执行器）和其他输出装置也包括在安全相关系统中。

3.10

安全完整性等级 safety integrity level

SIL

一种离散的等级（四种可能等级之一），用于规定分配给可编程电子安全相关系统的安全功能的安全完整性要求。安全完整性等级4是最高的，安全完整性等级1是最低的。SIL表明了各种因素导致失效（随机硬件失效和系统性失效）的失效率，这些失效将导致不安全状态，如：硬件失效，软件导致的失效，电气干扰导致的失效。

注：对于本部分，SIL3为自动扶梯和自动人行道应用的最高安全完整性等级。

3.11

SIL相关安全状态要求 SIL-relevant safe-state requirement

安全相关系统的一部分，应符合安全功能所需的SIL。

注：参见图4和表2。

图中：

1——SIL相关安全状态要求；

2——非SIL相关安全状态要求。

图4 自动扶梯和自动人行道安全功能

3.12

系统响应时间 system reaction time

为下列两个数值之和：

a）从PESSRAE故障发生到开始对自动扶梯和自动人行道作出相应动作的时间；

b）自动扶梯和自动人行道响应上述动作以保持安全状态所需的时间。

4 符号与缩略语

EUC — 受控设备

MTTR — 平均修复时间

5 要求

5.1 总则

5.1.1 表1列出了自动扶梯和自动人行道的安全功能（装置）名称、安全功能描述和对该安全功能所要求的SIL。

5.1.2　表2列出了表1中安全功能动作后的安全状态要求。安全功能动作后，应使自动扶梯和自动人行道转入表2中的安全状态。

5.1.3　为了达到安全状态而不致发生危险，PESSRAE应考虑自动扶梯和自动人行道响应安全功能的时间以及检测到内部故障必要的时间。实现内部故障检测的方法应考虑SIL所要求的系统响应时间。

注：如果一个双通道系统在必要的系统响应时间内通过数据比较检测到一个内部故障，则可变内存区检测不必在系统响应时间内完成，因为安全完整性由双通道设计来保证。

5.2　扩展应用

5.2.1 总则

5.2.2到5.2.4中列举的要求用于验证自动扶梯和自动人行道安全功能的SIL和安全状态，这些自动扶梯和自动人行道安全功能是新的或不同于5.3和5.4提出的要求。

5.2.2 风险评价

如果在5.3和/或5.4的要求中不能找到相应条款，应按照GB/T 20438.5或GB 28526的方法决定所需安全完整性等级。对于新的PESSRAE功能和相应SIL，或与5.3和5.4要求不同的、修改的PESSRAE功能和/或SIL，应使用同样的方法建立理论依据。任何单一的潜在危险因素导致的最严重的程度，其平均目标失效量不应超过5E-7次/年，参见附录C。

5.2.3 确定 PESSRAE 的 SIL 的限制

5.2.3.1用于确定自动扶梯和自动人行道安全相关功能的PE system的目标失效量的要求不应低于SIL1也不应高于SIL3。如果某目标失效量的要求高于SIL3，则应考虑重新设计系统，使其所需的目标失效量满足SIL3或低于SIL3的规定。如果要求的SIL低于SIL1，可使用非SIL的PE system，但其不应归类于PESSRAE。即使将PESSRAE应用于低于SIL1要求的安全功能中，其SIL也不应低于SIL1。

5.2.3.2 对于自动扶梯和自动人行道，SIL4的单个安全功能的应用不是典型的需求。应避免这种应用，因为在安全装置的整个生命周期中，达到和保持这样的高等级是困难的。如果分析结果要求某个自动扶梯和自动人行道安全功能为SIL4或更高，应考虑对过程设计作出改变，如采用本质安全设计措施或增加额外层面的保护。这些改进有可能降低对自动扶梯和自动人行道安全功能的SIL要求。如果仍不能降低安全完整性等级，则应将该安全功能的目标失效量分散给多个充分独立的、实践应用验证过的低于或等于SIL3的PESSRAE。

5.2.4 安全状态要求

对于新的或不同于5.3和5.4规定的自动扶梯和自动人行道安全功能，设计者可按照表2所描述的类似方式识别安全状态要求。

5.3 安全功能的SIL要求

自动扶梯和自动人行道的安全功能所需要的SIL参见表1，也参见表B.1。

表1　安全功能的SIL要求

序号	自动扶梯和自动人行道 安全功能（装置）	功能描述	SIL
1	检查超速	检测自动扶梯或自动人行道的超速	2
2	检查非操纵逆转	当运行方向为上行时，检测非操纵逆转	2
3	检查附加制动器的动作	检测附加制动器的动作	1
4	检查梯级链断裂	检测直接驱动梯级、踏板或胶带的元件断裂或过分伸长	1
5	检查驱动装置与转向装置之间的距离伸长或缩短	检测驱动装置与转向装置之间的距离伸长或缩短	1
6	检查梳齿板的位移	检测梯级、踏板或胶带进入梳齿板处有异物夹住	1
7	检查出口限制	检测多台连续且无中间出口的自动扶梯或自动人行道中的一台停止运行或自动扶梯和自动人行道出口被建筑结构阻挡	2
8	检查扶手带入口夹入异物	检测扶手带入口有异物或者身体部位夹入	1
9	检查梯级或踏板的下陷	检测梯级或踏板的向下移位	2
10	检查梯级或踏板的缺失	检测梯级或踏板的缺失	2
11	检查工作制动器未提起	启动后，检测工作制动器未提起	1
12	检查扶手带速度偏差	检测扶手带速度偏差	1
13	检查检修盖板和楼层板的打开	检测打开桁架区域的检修盖板和（或）移去或打开楼层板	1
14	检查手动盘车装置	检测可拆卸的手动盘车装置装上驱动主机之前或装上时的动作	1
15	检查紧急停止开关的动作	检测紧急停止装置的动作	1
16	检查维护和修理用停止开关	检测维修区域的停止开关的动作	2
17	检查检修控制装置上的停止开关	检测检修控制装置上的停止装置的动作	2
18	检查检修控制装置的动作	检测检修控制装置的动作	2
注：控制和操作电路的SIL不低于安全回路中的最高SIL。			

5.4　SIL相关和非SIL相关安全状态要求

自动扶梯和自动人行道对表1中自动扶梯和自动人行道安全功能所需作出的响应，以及该功能动作导致的每个响应的SIL和非SIL相关要求，参见表2。表2中标注“〇”的表示当安全功能被触发或PESSRAE检测到内部故障条件时，该安全状态条件需作出的响应。表中未标注“〇”而是使用了注解编号的，可查看相应编号所对应的注释以获取所需作出响应的更详细的说明。表中标注“-”的表示当安全功能被触发或PESSRAE检测到内部故障条件时，该安全状态条件不必作出的响应。

表2　安全状态要求

序号	自动扶梯和自动人行道安全功能（装置）	安全状态要求				
		切断主机和工作制动器电源	阻止任何其他启动	手动复位（R5）	旁路安全功能	切断附加制动器电源
		SIL 相关				非SIL相关
1	检查超速	R1	–	○	–	R2
2	检查非操纵逆转	○	–	○	–	○
3	检查附加制动器的动作	○	–	–	–	–
4	检查梯级链断裂	○	–	○	–	–
5	检查驱动装置与转向装置之间的距离伸长或缩短	○	–	–	–	–
6	检查梳齿板的位移	○	–	–	–	–
7	检查出口限制	○	–	–	–	–
8	检查扶手带入口夹入异物	○	–	–	–	–
9	检查梯级或踏板的下陷	○	–	○	–	–
10	检查梯级或踏板的缺失	○	–	○	–	–
11	检查工作制动器未提起	○	–	○	–	–
12	检查扶手带速度偏差	○	–	–	–	–
13	检查检修盖板和楼层板的打开	○	–	–	–	–
14	检查手动盘车装置	○	–	–	–	–
15	检查紧急停止开关的动作	○	–	–	–	–
16	检查维护和修理用停止开关	○	–	–	–	–
17	检查检修控制装置上的停止开关	○	–	–	–	–
18	检查检修控制装置的动作	–	R3	–	R4	–
R1	当速度超过名义速度的1.2倍之前起作用。					
R2	当速度超过名义速度的1.4倍之前起作用。					
R3	所有其他启动，包括所有其他的检修操作装置。					
R4	当装置连接时，下列保护可以无效： 1）出口限制； 2）梯级或踏板下陷； 3）梯级或踏板缺失； 4）工作制动器未提起； 5）附加制动器未动作； 6）扶手带速度； 7）检修盖板和楼层板的打开。					
R5	故障锁定的手动复位：严格要求人工手动来复位安全功能，以启动自动扶梯和自动人行道。使用钥匙启动自动扶梯和自动人行道不是手动复位。 注：手动复位的要求不是一个SIL的功能，而是为了应对事件发生后可能产生的危险情况的功能。					

5.5 SIL符合性验证的实现和证明

5.5.1 总则

应按照本节要求验证PESSRAE的安全完整性等级。

5.5.2 实现和验证PE system符合本部分规定的安全完整性等级所需的技术和措施

5.5.2.1 符合SIL1到SIL3的实现和验证所需的技术和措施见附录A。

5.5.2.2 如果在安全回路中，两个或两个以上的安全功能由共用的电路实现，则该共用电路的SIL应至少达到该电路所实现的自动扶梯和自动人行道安全功能中的最高SIL。

5.5.3 PESSRAE装置启用后的失电

5.5.3.1 对于不需要手动复位的功能，在电源恢复后应允许PESSRAE恢复正常工作模式，其输出状态应由电源恢复后的输入条件决定。

5.5.3.2 对于需要手动复位的功能（参见表2），PESSRAE应恢复到其失电前的输出状态。

附录 A
（规范性附录）
实现、验证和保持 SIL 符合性的技术和措施

A.1 总则

本附录规定了对实现、验证和保持PESSRAE的SIL符合性的要求。

A.1.1 用于满足本部分SIL要求的技术和措施

实现和验证PESSRAE的SIL符合性所需的技术和措施应满足A.2中规定的使用GB/T 20438.2和 GB/T 20438.3的技术和措施。

A.1.2 说明书

制造商应提供说明书。

当PESSRAE的功能验证无法在自动扶梯和自动人行道正常运行时进行，说明书应说明如何实施功能验证。说明书还应提供下列活动的信息，以便这些活动能够安全有效地实施：

a）组装；
b）连接；
c）调试；
d）维护和修理；
e）识别、标记、标识、证书和清单；
f）功能验证的周期。

A.1.2.1说明书中对维护和修理的一般要求

制造商提供的说明书应包含下列有关PESSRAE维护和修理的内容：

a）用于培训维护人员的特别要求和/或注意事项，以使PESSRAE的所有功能运行维持在其相应的SIL；
b）检验测试、预防性维护和故障维修的活动；
c）用于维护的特定技术和措施；
d）维护活动的验证和文档要求；
e）维护活动的周期；
f）确保日常维护中所用的检测设备经正确地校验和维护；
g）PESSRAE发生故障或失效时所需进行的维护和修理活动，包括：
—— 故障诊断和修理；
—— 重新确认；
—— 维护及失效的报告要求。

A.1.3 维护或可维护性设计要求

PESSRAE的设计应当允许端到端或分部测试。当预计的计划检验时间间隔大于用以保持PESSRAE的SIL的检验测试时间间隔时，应对试验作适当的规定。

注：“端到端”是指从传感器端到进入安全状态。当需进行自动检验测试时，试验项目应当成为SIL设计的必备部分，以测试未检测到的失效。

A.1.4 EMC抗扰度

对于SIL相关安全状态要求，PESSRAE应达到GB/T 24808中规定的“安全电路”测试等级；对于非SIL相关安全状态要求，应达到GB/T 24808中的“所有电路”测试等级。

A.2 使用GB/T 20438.2和 GB/T 20438.3实现和证明SIL符合性的技术和措施

A.2.1 一般要求

本节规定了应用GB/T 20438的要求，可用于实现和证明PESSRAE的SIL符合性。

A.2.1.1 对于本部分，SIL代表了对工作在低要求模式中装置的要求，以及在要求时执行安全功能的失效概率（见GB/T 20438.1-2006中的表2）。然而，PESSRAE是以持续控制的方式来保持安全功能的，SIL应代表对工作在高要求模式中PESSRAE的要求，并使用每小时危险失效概率（见GB/T 20438.1-2006中的表3）。

注：如果存在子系统输出状态的组合会直接导致危险事件的可能性，需将子系统中危险故障的检测视为工作在连续模式的安全功能。

A.2.1.2 用于执行非SIL相关要求的装置和软件不应用于实现PESSRAE的SIL相关要求，除非这些装置和软件已经包含在安全相关功能SIL的分级中。

A.2.1.3 在任何能容许单一故障的PESSRAE子系统中，一旦检测出危险故障（通过诊断测试、检验测试或任何其他方式），应进入表2中定义的安全状态。为了在同一子系统中可导致危险状况的第二个故障出现之前保持PESSRAE的完整性和安全状态条件，如果有必要，应采取手动复位使PESSRAE脱离安全状态条件。

如果上述动作依赖于对危险故障报警执行特定动作的操作人员或远程子系统，则报警本身应被视为该PESSRAE的SIL相关功能的一部分。

A.2.2 SIL符合性的实现

PESSRAE的SIL符合性的实现，应与GB/T 20438.2和GB/T 20438.3的原则和措施一致

注：假如几个低SIL系统能达到足够等级的独立性，且在应用中被证实，则可用来满足一个更高SIL功能的需求。

A.2.3 符合性的验证

本部分所规定的符合性验证由经批准的机构执行，该机构同时承担试验和签发合格证工作。

型式试验申请应由部件制造商或其委托的代理商提出，并应提交给被认可的实验室。

附录 B
（资料性附录）
自动扶梯和自动人行道适用的规范和标准

本部分中的自动扶梯和自动人行道安全功能（装置）参考了GB 16899—2011和EN 115-1:2017所定义的安全功能（装置）。为了便于对照和应用，表B.1给出了这些规范和标准与表1中的自动扶梯和自动人行道安全功能（装置）之间的关系。

表B.1 适用的自动扶梯和自动人行道标准对照表

序号	自动扶梯和自动人行道安全功能（装置）	GB 16899-2011的条款号	EN 115-1:2017的条款号
1	检查超速	5.4.2.3.1	5.12.2.7.2
2	检查非操纵逆转	5.4.2.3.2	5.12.2.7.3
3	检查附加制动器的动作	5.4.2.2.4	5.12.2.7.4
4	检查梯级链断裂	5.4.3.3	5.12.2.7.5
5	检查驱动装置与转向装置之间的距离伸长或缩短	5.4.3.3	5.12.2.7.6
6	检查梳齿板的位移	5.7.3.2.6	5.12.2.7.7
7	检查出口限制	A.2.6	5.12.2.7.8
8	检查扶手带入口夹入异物	5.6.4.3	5.12.2.7.9
9	检查梯级或踏板的下陷	5.7.2.5	5.12.2.7.10
10	检查梯级或踏板的缺失	5.3.6	5.12.2.7.11
11	检查工作制动器未提起	5.4.2.1.1	5.12.2.7.12
12	检查扶手带速度偏差	5.6.1	5.12.2.7.13
13	检查检修盖板和楼层板的打开	5.2.4	5.12.2.7.14
14	检查手动盘车装置	5.4.1.5	5.12.2.7.16
15	检查紧急停止开关的动作	5.12.2.2.3	5.12.2.7.15
16	检查维护和修理用停止开关	5.8.4	5.12.2.7.17
17	检查检修控制装置上的停止开关	5.12.2.5.3	5.12.2.7.18
18	检查检修控制装置的动作	5.12.2.5.4	5.12.3.13.4

附录 C
（资料性附录）
风险降低决策表的示例

表C.1给出PESSRAE应用的一个风险降低决策表的示例，相应的纠正措施列在表C.2。关于后果的定义如下：

Ⅰ 灾难性的： 在标准的范围内丧失所有的安全目标；

Ⅱ 严重的： 在标准的范围内永久性地失去部分安全目标；

Ⅲ 轻微的： 在标准的范围内临时性地失去部分安全目标；

Ⅳ 可忽略的： 在标准的范围内可忽略的或安全目标无任何损失。

表 C.1 风险降低决策表

后果的频率(*F*) (次/年)		潜在的安全危险后果			
范围	平均值	1 灾难的	2 严重的	3 轻微的	4 可忽略的
F≥0.01	0.01	ⅠA	ⅡA	ⅢA	ⅣA
0.001≦ *F* <0.01	0.005	ⅠB	ⅡB	ⅢB	ⅣB
0.0001≦ *F* <0.001	0.0005	ⅠC	ⅡC	ⅢC	ⅣC
0.00001≦ *F* <0.0001	0.00005	ⅠD	ⅡD	ⅢD	ⅣD
0.000001≦ *F* <0.00001	0.000005	ⅠE	ⅡE	ⅢE	ⅣE
F <0.000001	4.16667E-7	ⅠF	ⅡF	ⅢF	ⅣF

表C.2 纠正措施—风险降低的要求

ⅠA，ⅠB，ⅠC，ⅠD，ⅠE，ⅡA，ⅡB，ⅡC，ⅢA，ⅢB	应采取纠正措施减轻后果，且如果可以，消除风险。
ⅡD，ⅡE，ⅢC，ⅢD，ⅣA，ⅣB	检查并决定进一步地降低损失在技术上是否可行
ⅠF，ⅡF，ⅢE，ⅢF，ⅣC，ⅣD，ⅣE，ⅣF	不需要任何措施

参考文献

[1] GB 16899—2011 自动扶梯和自动人行道的制造与安装安全规范
[2] EN115-1:2017 Safety of escalators and moving walks - Part 1: Construction and installation
[3] GB/T 20438.6　电气/电子/可编程电子安全相关系统的功能安全 第6部分：GB/T 20438.2和GB/T 20438.3的应用指南
[4] GB/T 20438.7　电气/电子/可编程电子安全相关系统的功能安全 第7部分：技术与措施概述