ICS 91.140.90
Q 78

中华人民共和国国家标准

GB/T 35850.1—2018

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1部分：电梯（PESSRAL）

Programmable electronic systems in safety-related applications for lifts (elevators), escalators and moving walks—Part 1: Lifts (elevators) (PESSRAL)

(ISO 22201-1:2017, MOD)

2018-02-06 发布　　2018-09-01 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 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(PESSRAL)；

——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1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 22201-1:2017《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1部分：电梯(PESSRAL)》。

本部分与ISO 22201-1:2017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GB/T 4721、GB/T 4723、GB/T 4724、GB/T 4725代替了IEC 61249(所有部分)；
- 用修改采用国际标准的GB 4943(所有部分)代替了IEC 60950(所有部分)；
- 用GB/T 16261代替了IEC 62326-1；
- 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 20438.5代替了IEC 61508-5；
- 用等同采用国际标准的GB/T 20438.6代替了IEC 61508-6；
- 用等同采用国际标准的GB/T 20438.7代替了IEC 61508-7；
- 用等同采用国际标准的GB/T 24808代替了ISO 22200。

——基于GB 7588—2003＋XG1—2015中的表A.1和GB 21240—2007中的表A.1，并参考EN 81-20:2014，本部分做了以下修改：

- 在术语与定义中，删除了3.1和3.2，因为表1中相关内容已删除；
- 在表1中，删除了第1项、第3项、第6项、第8项、第10(a,b,c,…i)项、第10(i).1项、第10(a,d,g,h).2项、第10(e).3项、第26项、第34项、第35项、第37项、第43项、第45项、第51项，以便与GB 7588—2003＋XG1—2015和GB 21240—2007以及EN 81-20:2014一致；
- 在表1中，增加了下述电梯安全功能(装置)：第1项底坑停止装置、第2项滑轮间停止装置、第3项检查底坑梯子的存放位置、第4项检查通道门、安全门和检修门的关闭位置、第6项检查机械装置的非工作位置(轿厢内或轿顶上的工作区域)、第19项轿顶停止装置、第20项检查轿厢或对重的提升、第29项检查安全绳的断裂或松弛、第30项检查触发杠杆的收回位置、第35项检测门开启情况下轿厢意外移动保护装置的动作、第42项检查与检修运行配合使用的按钮、第45项检修运行停止装置、第46项电梯驱动主机上的停止装置、第47项紧急和测试操作屏上的停止装置、第49项检查液压缸柱塞位置传递装置的张紧(极限开关)，以便与相关标准一致；
- 在表1中，把电梯安全功能(装置)第39项检查减行程缓冲器的减速状况的安全完整性等

级(SIL)由 SIL2 提高为 SIL3,以便与相关标准一致;

- 在表 2 中,删除了第 1 项、第 3 项、第 6 项、第 8 项、第 10(a,b,c,…i)项、第 10(i).1 项、第 10(a,d,g,h).2 项、第 10(e).3 项、第 26 项、第 34 项、第 35 项、第 37 项、第 43 项、第 45 项、第 51 项,以便与 GB 7588—2003 + XG1—2015 和 GB 21240—2007 以及 EN 81-20:2014 一致;
- 在表 2 中,增加了下述电梯安全功能(装置):第 1 项底坑停止装置、第 2 项滑轮间停止装置、第 3 项检查底坑梯子的存放位置、第 4 项检查通道门、安全门和检修门的关闭位置、第 6 项检查机械装置的非工作位置(轿厢内或轿顶上的工作区域)、第 19 项轿顶停止装置、第 20 项检查轿厢或对重的提升、第 29 项检查安全绳的断裂或松弛、第 30 项检查触发杠杆的收回位置、第 35 项检测门开启情况下轿厢意外移动保护装置的动作、第 42 项检查与检修运行配合使用的按钮、第 45 项检修运行停止装置、第 46 项电梯驱动主机上的停止装置、第 47 项紧急和测试操作屏上的停止装置、第 49 项检查液压缸柱塞位置传递装置的张紧(极限开关)。同时增加了相应的安全状态要求;
- 在表 2 安全状态要求栏的第一列中,增加了强制式电梯,修改为“切断电机和制动器电源(曳引式电梯、强制式电梯)”,以提高适用性;
- 在表 2 安全状态要求栏中,删除了“阻止(防止)井道进入操作”,以便与相关标准一致;
- 在表 2 安全状态要求栏中,增加了“转换到紧急电动运行操作”,以便与相关标准一致;
- 在表 2 中,删除了 R1、R18、R19,因为其对应的电梯安全功能(装置)已删除;
- 在表 2 中,删除了 R10、R20、R25,因为与我国的实际应用不符;
- 在表 2 中,修改了 R17,改为 R12:

  当启用时,应允许下列一个或多个装置失效:

  a) 用于检查绳或链松弛的电气安全装置(序号 22);

  b) 轿厢安全钳上的电气安全装置(序号 25);

  c) 超速的电气安全装置(序号 26、序号 27);

  d) 轿厢上行超速保护装置上的电气安全装置(序号 33);

  e) 缓冲器上的电气安全装置(序号 36);

  f) 极限开关(序号 50)。
- 在表 2 中,修改了 R23,改为 R15“平层和再平层与预备操作时,忽略此项检查”,以便与相关标准一致;
- 在表 2 中,增加了 R26“仅当机械装置处于非工作位置时,忽略此项检查”;
- 在表 2 中,增加了 R27“轿厢速度不应超过 0.3 m/s”。

本部分与 ISO 22201-1:2017 相比还做了下列编辑性修改:

——删除了 ISO 22201-1:2017 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;

——对表 1 和表 2 中的电梯安全功能(装置)的序号进行了调整,对表 2 中的 R 注释的序号进行了调整,以便于应用;

——删除了附录 B(资料性附录)中表 B.1 中 ASME A17.1-2007/CSA B44-07 和日本建筑法规相关条款及内容,因为与我国的实际应用不符;

——在表 B.1 中增加了电梯安全功能对应 GB 7588—2003 + XG1—2015、GB 21240—2007 和 EN 81-20:2014 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)提出并归口。

本部分起草单位:上海新时达电气股份有限公司、中国建筑科学研究院建筑机械化研究分院、奥的

斯机电电梯有限公司、上海三菱电梯有限公司、日立电梯(中国)有限公司、江南嘉捷电梯股份有限公司、永大电梯设备(中国)有限公司、迅达(中国)电梯有限公司、通力电梯有限公司、上海交通大学、广东省特种设备检测研究院、上海市特种设备监督检验技术研究院、奥的斯高速电梯(上海)有限公司、苏州汇川技术有限公司、蒂森克虏伯电梯(上海)有限公司、广州广日电梯工业有限公司、康力电梯股份有限公司、国家电梯质量监督检验中心、华升富士达电梯有限公司、东芝电梯(中国)有限公司、巨人通力电梯有限公司、沈阳远大智能工业集团股份有限公司、苏州帝奥电梯有限公司、申龙电梯股份有限公司、东南电梯股份有限公司、上海爱登堡电梯集团股份有限公司、森赫电梯股份有限公司、菱王电梯股份有限公司、苏州莱茵电梯股份有限公司。

本部分主要起草人:王鹏、孙恩涛、陈凤旺、温爱民、翁彬、赖志鹏、赵碧涛、欧其斌、马光桦、王明凯、胡晖、代清友、方良、刘同秋、袁华佑、张伟伦、张研、黄维纲、李新龙、李旭征、姜华、张新华、王福强、唐林钟、唐志荣、蔡状、陈大华、茹晓英、江俊彪、黄波。

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地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子系统。

本部分阐述了对用于执行电梯安全功能的含有可编程电子部件的系统和可编程电子系统(PE system)产品的具体要求。本部分的目的在于对电梯安全相关的可编程电子系统(PESSRAL)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。对表1中每项安全功能的风险分析确定了PESSRAL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(SIL)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1部分：电梯（PESSRAL）

1 范围

1.1 GB/T 35850的本部分适用于乘客电梯和载货电梯，当可编程电子系统被用于执行电梯电气安全功能时，应采用本部分。当电梯规范、标准中所定义的电梯安全功能应用PESSRAL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PESSRAL。

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PESSRAL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) 应用于电梯的可编程电子系统（PE system），符合电梯相关标准（如：GB 7588等）的最低要求；

d) 明确了与GB/T 20438以及GB/T 24808之间的关系；

e) 说明了电梯安全功能与其安全状态条件之间的关系；

f) 适用于软件和相关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；

g) 要求PESSRAL制造商提供说明书，向实施该电梯组装、连接、调试、维护的组织详细说明如何保持PESSRAL的完整性；

h) 规定了与软硬件安全验证相关的要求；

i) 为具体的电梯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PESSRAL的风险降低的决策表；

l) 规定了要求的PESSRAL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；

b) 失效安全的概念，在失效模式定义良好和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PESSRAL复杂度很高，所以失效安全概念在此是不合适的；

c) 对电梯安全功能中的PESSRAL的完整运用所必需的其他相关要求，如开关、执行器件和传感器的机械结构、安装和标识等。这些要求应符合相关电梯标准；

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 4721 印制电路用覆铜箔层压板通用规则

GB/T 4723　印制电路用覆铜箔酚醛纸层压板

GB/T 4724　印制电路用覆铜箔复合基层压板

GB/T 4725　印制电路用覆铜箔环氧玻璃布层压板

GB 4943(所有部分)　信息技术设备　安全[IEC 60950(所有部分)]

GB/T 16261　印制板总规范(GB/T 16261—1996,IEC/PQC 88:1990,IDT)

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(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 20438.5　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 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(GB/T 20438.6—2006,IEC 61508-6:2000,IDT)

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(IEC 61508-7:1998,IDT)

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

IEC 61508-7:2010　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(Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 7: Overview of techniques and measures)

3　术语和定义

在GB/T 20438.4中给出的术语和定义适用于本文件,但是本文件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);

——专用集成电器(ASICs);

——可编程逻辑控制器(PLCs);和

——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

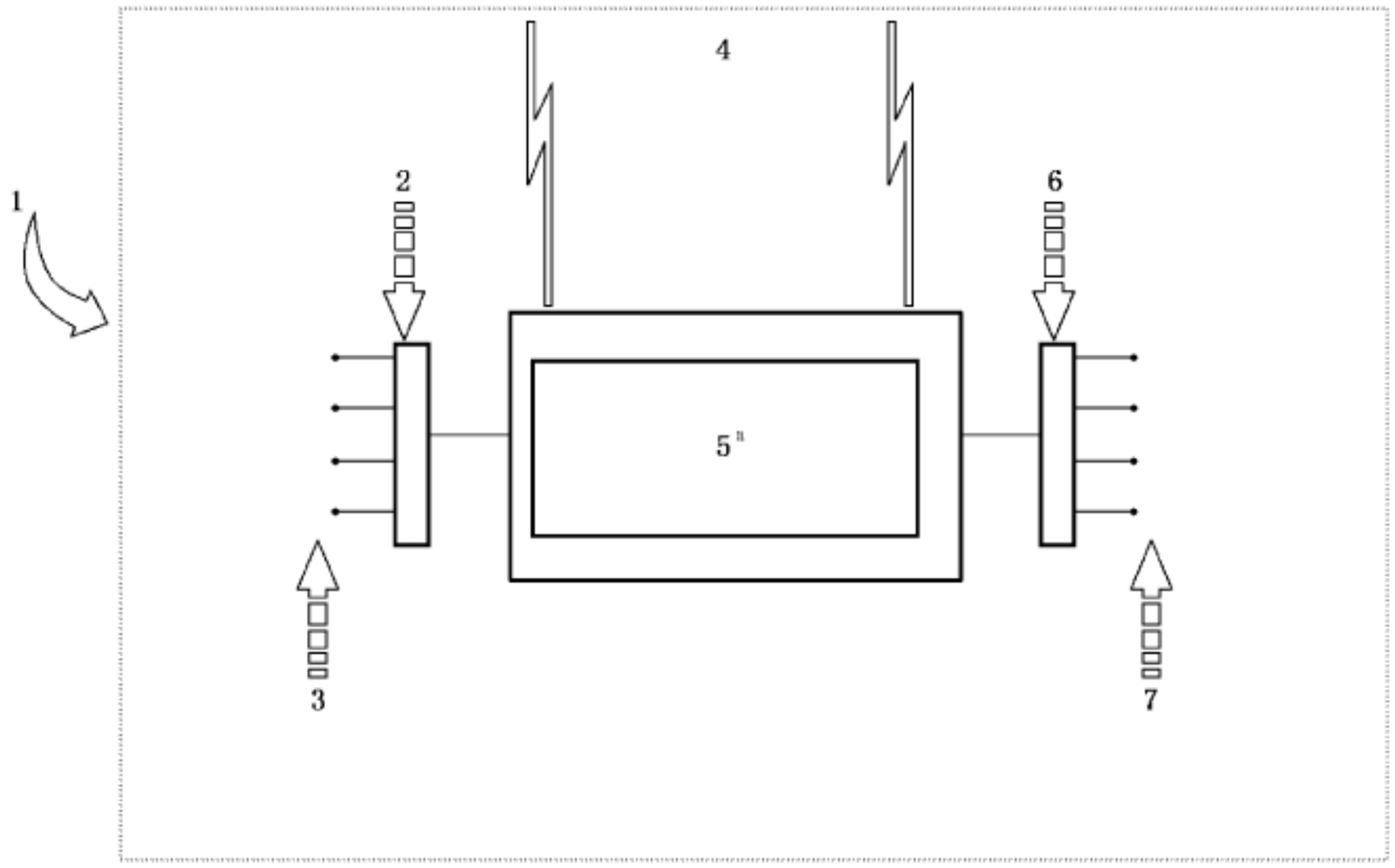
可编程电子系统　programmable electronic system

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，包括系统中所有单元，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 可包括执行 SIL 要求和非 SIL 要求的单元。SIL 分级仅对于执行 SIL 相关功能性要求的单元。



说明：

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(PEs)；

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

电梯安全相关的可编程电子系统　programmable electronic systems in safegy-related applications for lifts

PESSRAL

基于软件的 PE system 在电梯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。对于复杂的组件，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。

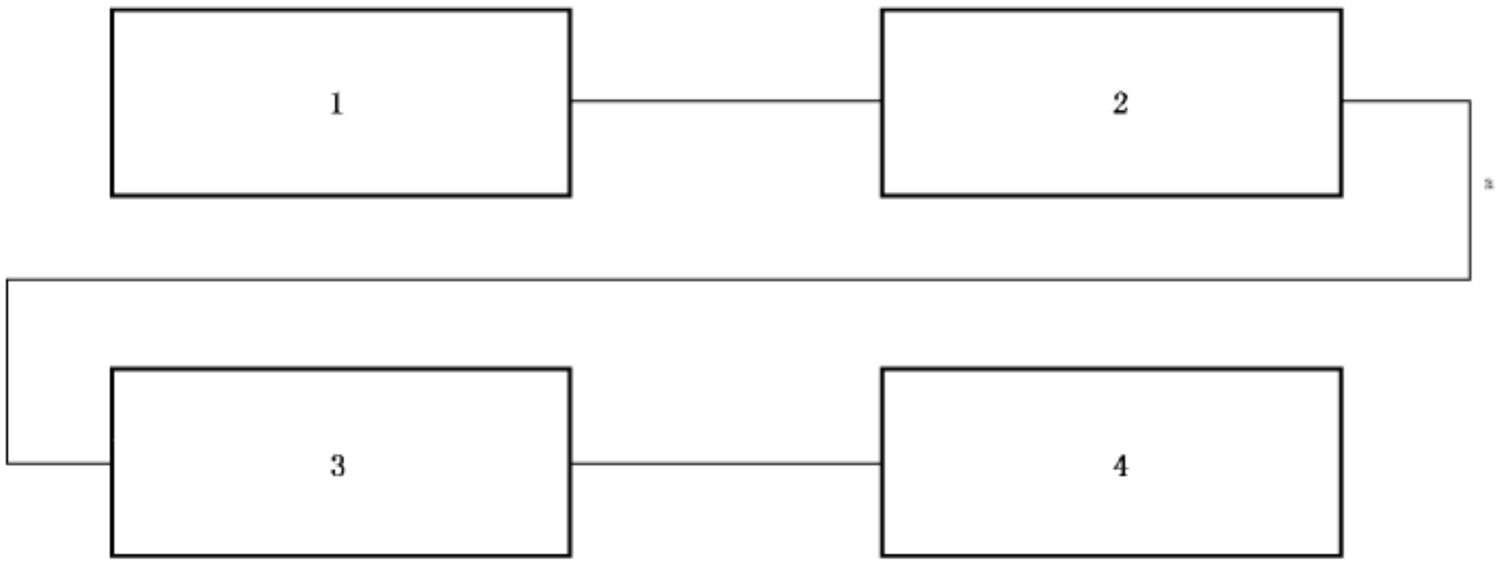
注 4：在检验测试期间，E/E/PE 安全相关系统可能部分或全部不能响应动作要求。仅在修复过程中 EUC 停机或使用其他等效的风险措施来代替时，用于 SIL 计算的 MTTR 可以忽略。

3.6

安全回路　safety chain

所有安全装置的组合，完成电梯的一组或所有安全功能。

注：参见图 2。



说明：

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] 一组或全部必要的电梯安全功能(参见表 1)。

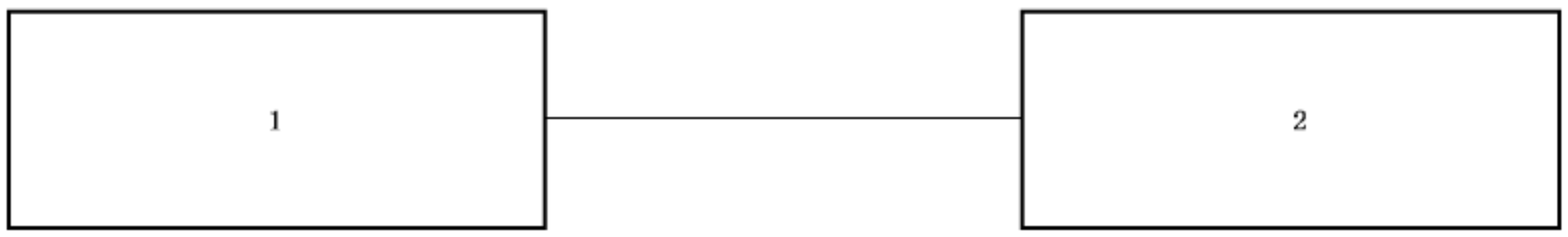
图 2　安全回路

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，用于独立地实现一个电梯安全功能，可由 PE 单元和非 PE 单元组成。

注：参见图 3 和表 1。



说明：

1——PE 单元；

2——非 PE 单元。

图 3　安全装置

3.8

安全功能　safety function

针对特定的危险事件，为了达到或保持电梯的安全状态，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/或机械的电梯部件。

3.10

安全完整性等级；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。

注 1：SIL 表明了各种因素导致失效（随机的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。

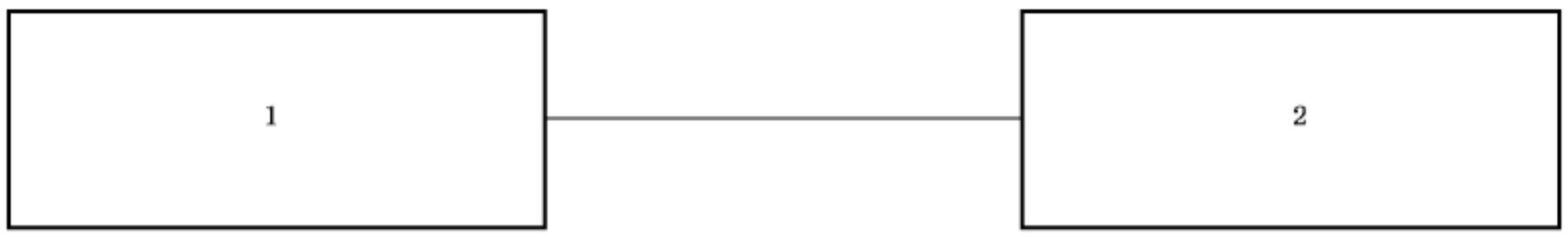
注 2：对于本部分，SIL3 为电梯应用的最高安全完整性等级。

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。



说明：

1——SIL 相关安全状态要求；

2——非 SIL 相关安全状态要求。

图 4　电梯安全功能

3.12

系统响应时间　system reaction time

为下列两个数值之和：

a）　从 PESSRAL 故障发生到开始对电梯作出相应动作的时间；

b）　电梯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

下列符号与缩略语适用于本文件。

EUC——受控设备。

MTTR——平均修复时间。

PCB——印制电路板。

5 要求

5.1 总则

5.1.1 表 1 列出了安全功能名称和对该安全功能 SIL 相关部分的 SIL 要求。当安全功能未动作时，允许电梯不中断运行。

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，使电梯转入表 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，PESSRAL 应考虑电梯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(参见示例)。

示例：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

5.2.2～5.2.4 中列举的要求用于确认电梯安全功能的 SIL 和安全状态，这些电梯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 的方法决定所需安全完整性等级。对于新的 PESSRAL 功能和相应 SIL，或与 5.3 和 5.4 要求不同的、修改的 PESSRAL 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 PESSRAL 的 SIL 的限制

5.2.3.1 用于确定电梯安全相关功能的 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 PESSRAL。即使将 PESSRAL 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 在电梯行业内 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电梯安全功能为 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电梯安全功能的 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 PESSRAL。

5.2.4 安全状态要求

对于新的或不同于 5.3 和 5.4 规定的电梯安全功能，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

电梯的安全功能所需要的 SIL 参见表 1 和表 B.1。

表 1　安全功能的 SIL 要求

序号	电梯安全功能(装置)	安全功能描述	SIL
1	底坑停止装置	检测底坑停止装置	3
2	滑轮间停止装置	检测滑轮间停止装置	3
3	检查底坑梯子的存放位置	检测底坑梯子的存放位置	1
4	检查通道门、安全门和检修门的关闭位置	检测通道门、安全门和检修门未关闭	2
5	检查轿门的锁紧状况	检测轿门未锁紧	2
6	检查机械装置的非工作位置(轿厢内或轿顶上的工作区域)	检测机械装置的非工作位置	3
7	检查检修门的锁紧位置	检测轿壁上的检修门的未锁紧	2
8	检查所有进入底坑的门的打开状态	检测进入底坑的门未关闭	2
9	检查机械装置的非工作位置(底坑内的工作区域)	检测机械装置的非工作位置	3
10	检查机械装置的工作位置(底坑内的工作区域)	检测机械装置的工作位置	3
11	检查工作平台的收回位置	检测工作平台的未完全收回	3
12	检查可移动止停装置的收回位置	检测可移动止停装置未完全收回	3
13	检查可移动止停装置的伸展位置	检测可移动止停装置未完全伸出	3
14	检查层门锁紧装置的锁紧位置	检测层门未锁紧	3
15	检查层门的关闭位置	检测层门未关闭	3
16	检查无锁门扇的关闭位置	检测无锁门扇未关闭	3
17	检查轿门的关闭位置	检测轿门未关闭	3
18	检查轿厢安全窗和轿厢安全门的锁紧状况	检测轿厢安全窗和轿厢安全门未锁紧	2
19	轿顶停止装置	检测轿顶停止装置	3
20	检查轿厢或对重的提升	检测轿厢或对重的提升	1
21	检查钢丝绳或链条的异常相对伸长(使用两根钢丝绳或链条时)	检测使用两根悬挂钢丝绳或链的松弛	1
22	检查强制式电梯和液压电梯的钢丝绳或链条的松弛	检测悬挂装置(如绳或链)的松弛	2
23	检查防跳装置	检测补偿装置的防跳装置超出其行程限制(防跳)	3
24	检查补偿绳的张紧	检测补偿绳的松弛	3
25	检查轿厢安全钳的动作	检测轿厢安全钳的动作	1
26	检查超速	检测轿厢超过设定的最大速度(不大于限速器触发速度)	2
27	检查限速器的复位	检测限速器不在复位状态	3
28	检查限速器绳的张紧	检测限速器绳的松弛	3
29	检查安全绳的断裂或松弛	检测安全绳的断裂或松弛	3

表 1（续）

序号	电梯安全功能(装置)	安全功能描述	SIL
30	检查触发杠杆的收回位置	检测触发杠杆未收回	2
31	检查棘爪装置的收回位置	检测棘爪装置未收回	1
32	采用具有耗能型缓冲装置的棘爪装置的电梯，检查缓冲装置恢复至其正常的伸出位置	检测棘爪装置的耗能型缓冲装置不在正常位置	3
33	检查轿厢上行超速保护装置	检测轿厢上行超速保护装置	2
34	检查门开启情况下轿厢的意外移动	检测门开启情况下轿厢的意外移动	2
35	检测门开启情况下轿厢意外移动保护装置的动作	检测门开启情况下轿厢意外移动保护装置	1
36	检查缓冲器恢复至其正常伸长位置	检测缓冲器不在正常位置	3
37	检查可拆卸盘车手轮的位置	检测可拆卸盘车手轮与驱动主机连接	1
38	采用接触器的主开关的控制	检测接触器装置的释放动作	2
39	检查采用减行程缓冲器时的减速状况	检测采用减行程缓冲器时的减速状况	3
40	检查平层、再平层和预备操作	检测门未关闭和未锁紧情况下的平层、再平层和预备操作控制	2
41	检修运行开关	检测检修运行开关	3
42	检查与检修运行配合使用的按钮	监测方向按钮和“运行”按钮的正确操作	1
43	紧急电动运行开关	检测紧急电动运行开关	3
44	层门和轿门旁路装置	检测层门和轿门旁路装置	3
45	检修运行停止装置	检测检修运行停止装置	3
46	电梯驱动主机上的停止装置	检测电梯驱动主机上的停止装置	3
47	紧急和测试操作屏上的停止装置	检测紧急和测试操作屏上的停止装置	3
48	检查轿厢位置传递装置的张紧(极限开关)	检测轿厢位置传递装置的张紧状态	1
49	检查液压缸柱塞位置传递装置的张紧(极限开关)	检测液压缸柱塞位置传递装置的张紧状态	1
50	极限开关	检测轿厢是否超越极限限位	1
51	检查轿厢位置传递装置的张紧(减速检查装置)	检测轿厢位置传递装置的张紧状态	2
52	检查轿厢位置传递装置的张紧(平层、再平层和防沉降)	检测轿厢平层区位置的连接装置的松弛	2
53	对接操作的行程限位装置	检测对接操作时轿厢超出限制区域	2
54	对接操作	检测处于对接操作状态	2

5.4 SIL 相关和非 SIL 相关安全状态要求

电梯对表 1 中电梯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“○”的表示当安全功能被触发或 PESSRAL 检测到内部故障条件时，该安全状态条件需作出的响应。表 2 中未标注“○”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 2 中标注“-”的表示当安全功能被触发或 PESSRAL 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	电梯安全功能(装置)	安全状态要求																	
		切断电机和／或相关阀电源(曳引式电梯、强制式电梯) 切断电机和制动器电源(液压电梯)	阻止(防止)电梯自动运行(R14)	限制电梯运行范围	切断断路接触器的线圈供电电路	转换到检修操作	转换到紧急电动运行操作	限制轿厢速度	限制轿厢向一个方向的移动	需手动复位	忽略(检查轿门关闭和／或锁紧)	忽略(检查层门关闭和／或锁紧)	阻止(防止)门的自动操作	阻止(防止)对接操作	阻止(防止)紧急电动运行	阻止(防止)防沉降功能(仅液压电梯)	阻止(防止)轿内检修操作	允许按给定速度曲线启动和／或停止	启用信号装置
		SIL 相关				非 SIL 相关													
1	底坑停止装置	○	—	—	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—
2	滑轮间停止装置	○	—	—	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—
3	检查底坑梯子的存放位置	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
4	检查通道门、安全门及检修门的关闭位置	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
5	检查轿门的锁紧状况	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
6	检查机械装置的非工作位置(轿厢内或轿顶上的工作区域)	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
7	检查检修门的锁紧位置	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
8	检查所有进入底坑的门的打开状态	R21	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
9	检查机械装置的非工作位置(底坑内的工作区域)	R18	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
10	检查机械装置的工作位置(底坑内的工作区域)	R20	—	○	—	—	—	R4	—	—	—	—	—	—	—	—	—	—	—
11	检查工作平台的收回位置	R17	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
12	检查可移动止停装置的收回位置	R19	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
13	检查可移动止停装置的伸展位置	R20	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
14	检查层门锁紧装置的锁紧位置	R15	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—	—	—
15	检查层门的关闭位置	R15	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—	—	—

表 2（续）

序号	电梯安全功能(装置)	安全状态要求																	
		切断电机和／或相关阀电源(液压电梯)切断电机和制动器电源(曳引式电梯、强制式电梯)	阻止(防止)电梯自动运行(R14)	限制电梯运行范围	切断断路接触器的线圈供电电路	转换到检修操作	转换到紧急电动运行操作	限制轿厢速度	限制轿厢向一个方向的移动	需手动复位	忽略(检查轿门关闭和／或锁紧)	忽略(检查层门关闭和／或锁紧)	阻止(防止)门的自动操作	阻止(防止)对接操作	阻止(防止)紧急电动运行	阻止(防止)防沉降功能(仅液压电梯)	阻止(防止)轿内检修操作	允许按给定速度曲线启动和／或停止	启用信号装置
		SIL 相关				非 SIL 相关													
16	检查无锁门扇的关闭位置	R15	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—	—	—
17	检查轿门的关闭位置	R15	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—	—	—
18	检查轿厢安全窗和轿厢安全门的锁紧状况	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
19	轿顶停止装置	○	—	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—	—
20	检查轿厢或对重的提升	○	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—	—	—
21	检查钢丝绳或链条的异常相对伸长(使用两根钢丝绳或链条时)	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
22	检查强制式电梯和液压电梯的钢丝绳或链条的松弛	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
23	检查防跳装置	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
24	检查补偿绳的张紧	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
25	检查轿厢安全钳的动作	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
26	检查超速	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
27	检查限速器的复位	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
28	检查限速器绳的张紧	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
29	检查安全绳的断裂或松弛	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
30	检查触发杠杆的收回位置	R10	—	—	—	—	—	—	R11	—	—	—	—	—	—	—	—	—	—
31	检查棘爪装置的收回位置	R10	—	—	—	—	—	—	R11	—	—	—	—	—	—	—	—	—	—
32	采用具有耗能型缓冲装置的棘爪装置的电梯，检查缓冲装置恢复至其正常的伸出位置	R10	—	—	—	—	—	—	R11	—	—	—	—	—	—	—	—	—	—

表 2（续）

序号	电梯安全功能(装置)	安全状态要求																	
		切断电机和／或相关阀电源(液压电梯)切断电机和制动器电源(曳引式电梯、强制式电梯)	阻止(防止)电梯自动运行(R14)	限制电梯运行范围	切断断路接触器的线圈供电电路	转换到检修操作	转换到紧急电动运行操作	限制轿厢速度	限制轿厢向一个方向的移动	需手动复位	忽略(检查轿门关闭和／或锁紧)	忽略(检查层门关闭和／或锁紧)	阻止(防止)门的自动操作	阻止(防止)对接操作	阻止(防止)紧急电动运行	阻止(防止)防沉降功能(仅液压电梯)	阻止(防止)轿内检修操作	允许按给定速度曲线启动和／或停止	启用信号装置
		SIL 相关				非 SIL 相关													
33	检查轿厢上行超速保护装置	○	—	—	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—
34	检测门开启情况下轿厢的意外移动	○	—	—	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—
35	检测门开启情况下轿厢意外移动保护装置的动作	○	—	—	—	—	—	—	—	○	—	—	—	—	—	—	—	—	—
36	检查缓冲器恢复至其正常伸长位置	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
37	检查可拆卸盘车手轮的位置	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
38	用接触器的主开关的控制	—	—	—	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—
39	检查减行程缓冲器的减速状况	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	○	—
40	检查平层、再平层和预备操作	○	—	R3	—	—	—	R1	—	—	R2	R2	—	—	—	—	—	—	—
41	检修运行开关	○	○	R8	—	○	—	R4	R9	—	—	—	○	○	○	○	○	○	—
42	检查与检修运行配合使用的按钮	—	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
43	紧急电动运行开关	R12	○	—	—	—	○	R27	—	—	—	—	—	○	R13	○	—	○	—
44	层门和轿门旁路装置	—	○	—	—	—	—	○	—	R5	R6	R7	○	○	—	—	—	—	R22
45	检修运行停止装置	○	—	—	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—
46	电梯驱动主机上的停止装置	○	—	—	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—
47	紧急和测试操作屏上的停止装置	○	—	—	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—
48	检查轿厢位置传递装置的张紧(极限开关)	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

表 2（续）

序号	电梯安全功能(装置)	安全状态要求																	
		切断电机和／或相关阀电源(液压电梯)切断电机和制动器电源(曳引式电梯、强制式电梯)	阻止(防止)电梯自动运行(R14)	限制电梯运行范围	切断断路接触器的线圈供电电路	转换到检修操作	转换到紧急电动运行操作	限制轿厢速度	限制轿厢向一个方向的移动	需手动复位	忽略(检查轿门关闭和／或锁紧)	忽略(检查层门关闭和／或锁紧)	阻止(防止)门的自动操作	阻止(防止)对接操作	阻止(防止)紧急电动运行	阻止(防止)防沉降功能(仅液压电梯)	阻止(防止)轿内检修操作	允许按给定速度曲线启动和／或停止	启用信号装置
		SIL 相关				非 SIL 相关													
49	检查液压缸柱塞位置传递装置的张紧(极限开关)	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
50	极限开关	○	—	—	—	—	—	—	—	R16	—	—	—	—	—	—	—	—	—
51	检查轿厢位置传递装置的张紧(减速检查装置)	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
52	检查轿厢位置传递装置的张紧(平层、再平层和防沉降)	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
53	对接操作的行程限位装置	○	—	R24	—	—	—	—	—	—	R2	R2	—	—	—	—	—	—	—
54	对接操作	—	○	—	—	—	—	R23	R25	—	—	—	—	—	—	—	—	—	—

R1	将轿厢速度限制为：平层时最高 0.8 m/s，再平层时最高 0.3 m/s
R2	在目的层站的开锁区域忽略此项检查
R3	限制轿厢仅在开锁区域内运行
R4	轿厢速度不应超过 0.63 m/s
R5	仅能使用工具手动启用和复位
R6	轿门旁路操作时忽略此项检查
R7	层门旁路操作时忽略此项检查
R8	限定轿厢在端站限位内运行。液压电梯允许越过下极限
R9	当轿厢触及端站限位时，限定轿厢仅能向背离该端站的方向运行
R10	仅当向下运行时检查
R11	限制轿厢仅能向上运行

表 2（续）

序号	电梯安全功能(装置)	安全状态要求																	
		切断电机和／或相关阀电源(液压电梯) 切断电机和制动器电源(曳引式电梯、强制式电梯)	阻止(防止)电梯自动运行(R14)	限制电梯运行范围	切断断路接触器的线圈供电电路	转换到检修操作	转换到紧急电动运行操作	限制轿厢速度	限制轿厢向一个方向的移动	需手动复位	忽略(检查轿门关闭和／或锁紧)	忽略(检查层门关闭和／或锁紧)	阻止(防止)门的自动操作	阻止(防止)对接操作	阻止(防止)紧急电动运行	阻止(防止)防沉降功能(仅液压电梯)	阻止(防止)轿内检修操作	允许按给定速度曲线启动和／或停止	启用信号装置
		SIL 相关				非 SIL 相关													
R12	当启用时，应允许下列一个或多个装置失效： a) 用于检查绳或链松弛的电气安全装置(序号 22)； b) 轿厢安全钳上的电气安全装置(序号 25)； c) 超速的电气安全装置(序号 26、序号 27)； d) 轿厢上行超速保护装置上的电气安全装置(序号 33)； e) 缓冲器上的电气安全装置(序号 36)； f) 极限开关(序号 50)																		
R13	仅允许一个紧急电动运行，任何启用的检修运行操作均应优先于紧急电动运行，如平台上、轿内、底坑内等																		
R14	任何类型的自动运行，包括单台的、集选的、群控的、火灾情况下的电梯运行、紧急电源运行等																		
R15	平层和再平层与预备操作时，忽略此项检查																		
R16	仅液压电梯需要手动复位																		
R17	当工作平台和可移动止停装置处于完全伸展位置时，忽略此项检查																		
R18	仅当机械止停装置处于工作位置且底坑检修操作启用时，忽略此项检查																		
R19	仅当可移动止停装置处于完全伸展位置时，忽略此项检查																		
R20	仅当装置处于完全收回位置和非工作位置时，忽略此项检查																		
R21	仅当启用底坑检修且底坑机械保护装置处于工作位置(序号 10)时，忽略此项检查																		
R22	启用轿厢听觉和视觉信号																		
R23	轿厢速度限制为检修速度																		
R24	轿厢仅能在相应平层位置以上不大于 1.65 m 的区域内运行																		
R25	轿厢仅能通过持续按压方向按钮和运行按钮运行																		
R26	仅当机械装置处于非工作位置时，忽略此项检查																		
R27	轿厢速度不应超过 0.3 m/s																		

5.5 SIL 符合性验证的实现和证明

5.5.1 总则

应按照 5.5 要求验证 PESSRAL 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～SIL3 的实施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电梯安全功能中的最高 SIL。

5.5.3 PESSRAL 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 PESSRAL 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)，PESSRAL 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 PESSRAL 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

实现和证明 PESSRAL 的 SIL 符合性所需的技术和措施应满足以下任意一项：

a） 运用 A.2 规定的技术和措施；

b） 运用 A.3 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。

在电梯正常运行中，无法进行 PESSRAL 的功能验证时，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 PESSRAL 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 PESSRAL 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） PESSRAL 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；

——维护及故障的报告要求。

A.1.3 维护或可维护性的设计要求

PESSRAL 的设计应允许端到端或分部测试。

注：术语“端到端”是指从传感器端到进入安全状态。

当预计的计划检验时间间隔大于用以决定 PESSRAL 的 SIL 的检验测试时间间隔时，应对试验作适当的规定。当需进行自动检验测试时，试验项目应成为 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，PESSRAL 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“一般功能电路”和“所有电路”测试等级。

A.2 实现和验证 SIL 符合性的特定技术和措施

A.2.1 总则

按照本附录设计的可编程电子系统，不必对两个或两个以上故障组合的后果进行进一步的评价。

表 A.1～表 A.3 列出了所有 SIL 通用的安全功能的最低要求。表 A.4、表 A.5 和表 A.6 分别列出了 SIL1、SIL2 和 SIL3 所需的更多的特定措施。

注：表 A.1～表 A.6 列出的 IEC 61508-7:2010 条款是针对 GB/T 20438.2 和 GB/T 20438.3 中的相关要求。

为避免不安全的修改，应提供阻止访问程序代码和 PESSRAL 安全相关数据的措施，如：采用 EPROM，访问密码等。

A.2.2 硬件要求

A.2.2.1 印制电路板(PCB)

如满足下列条件，可不考虑短路的可能性：

a) PCB 的通用技术条件符合 GB/T 16261 的要求；

b) 基板的材料符合 GB/T 4721 的要求，以及 GB/T 4723、GB/T 4724 和/或 GB/T 4725 的要求；

c) PCB 的结构符合上述要求，而且各最小值根据 GB/T 16935.1—2008 中的表，满足以下条件：

——污染等级是 3；

——材料类别是Ⅲ；

——非均匀电场。

不使用 GB/T 16935.1—2008 的表 F.4 中“印制线路材料”栏。

对于 250 V 的有效电压值，爬电距离为 4 mm，电气间隙为 3 mm。

对于其他电压值，应参考 GB/T 16935.1—2008。

如果 PCB 的防护等级不低于 IP5X，或者材料有更高的质量，爬电距离可以减小到电气间隙值要求，如：对于 250 V 的有效电压值，爬电距离可以为 3 mm。对于至少有 3 层经预浸处理的聚酯胶片或其他绝缘薄片组成的多层板，短路故障可以排除(见 GB 4943)。

A.2.2.2 共用硬件

如果 PESSRAL 和非安全相关系统共用了同一块 PCB，应按下列要求隔离这两个系统：

a) 如果保护外壳的防护等级不高于 IP4X，则其电气间隙不应小于 3 mm，爬电距离不应小于 4 mm；

b) 如果保护外壳的防护等级高于 IP4X，则其爬电距离可降至 3 mm。

如果 PESSRAL 和非安全相关系统共用了同一硬件，则该硬件应满足 PESSRAL 的要求。

A.2.2.3 其他要求

与硬件设计相关的避免和检测失效的通用措施见表 A.1。

A.2.3 软件要求

A.2.3.1 与软件设计相关的避免和检测失效的通用措施见表 A.2。

A.2.4 设计过程要求

A.2.4.1 设计和实现过程的通用措施见表 A.3。

A.2.5 与 SIL 相关的特定措施

A.2.5.1 符合 SIL1 的特定措施见表 A.4。

A.2.5.2 符合 SIL2 的特定措施见表 A.5。

A.2.5.3 符合 SIL3 的特定措施见表 A.6。

A.2.6 符合性验证的测试程序

A.2.6.1 一般规定

A.2.6.1.1 本部分所规定的试验单位是一个经批准的机构。

A.2.6.1.2 测试样品的选送应由实验室和申请人商定。申请人可以参加测试。

A.2.6.1.3 除非有特殊规定,仪器的精确度应满足下列测量精度的要求:

a) 质量、力、距离、速度:±1%;

b) 加速度:±2%;

c) 电压、电流:±5%;

d) 温度:±5℃;

e) 记录仪器:应能检测到 0.01 s 内变化的信号。

A.2.6.2 对印制电路板或其等效组件的规定

申请者应向实验室说明:

a) 印制电路板裸板/印制电路板的标识;

b) 工作条件;

c) 使用的元件清单;

d) 印制电路板裸板/印制电路板布置图;

e) 混合电路布置图及用于安全电路的布线标志;

f) 功能描述;

g) 布线图等电气数据,如果可能,还应有印制电路板裸板/印制电路板的输入输出定义;

h) 与表 A.3 所列措施相关的文件和描述;

i) 使用软件的总体描述,如:编程规则、语言、编译器、模块等;

j) 功能描述,包括软件架构和硬/软件配合;

k) 功能块、模块、数据、变量和接口的描述;

l) 软件清单。

A.2.6.3 功能和安全测试

除采用表 A.1～表 A.6 中定义的措施进行验证外,还应确认:

a) 软件设计和编码:使用例如形式化设计检查、范根(FAGAN)检查法或测试用例等方法检查全部代码语句;

b) 软件和硬件检查：使用例如故障插入测试法等方法（基于 GB/T 20438.2 和 GB/T 20438.7）来验证表 A.1 和表 A.2 中所有措施及所选择的措施（如从表 A.7 中选择）。

A.2.7 可用措施描述

失效控制的可用措施描述见表 A.7。

A.2.8 符合性验证

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。

表 A.1 避免和检测故障的通用措施——硬件设计

序号	对象	措施	参见 IEC 61508-7：2010 条款
1	处理单元	使用看门狗	A.9
2	元器件选择	仅按元器件的技术要求使用	—
3	I/O 单元和接口，包括通讯链接	在电源失效或复位情况下进入规定的安全状态	—
4	电源	在过电压或欠电压情况下进入规定的安全断电状态	A.8.2
5	可变存储区	仅使用固态存储器	—
6	可变存储区	启动过程中对可变数据存储器进行读写测试	—
7	可变存储区	远程访问仅适用于信息类数据（如统计数据）	—
8	不可变存储区	程序代码不能被远程干预更改或系统自动更改	—
9	不可变存储区	启动过程中对程序代码存储器和不可变数据存储器进行测试，测试方法至少等同于和数校验	A.4.2

表 A.2 避免和检测故障的通用措施——软件设计

序号	对象	措施	参见 IEC 61508-7：2010 条款（除序号 13 外）
1	结构	依照现有技术水平（见 GB/T 20438.3）的程序结构（即模块化、数据操作、接口定义）	B.3.4/C.2.1 C.2.9/C.2.7
2	启动过程	启动过程中应保持电梯的安全状态	—
3	中断	有限地使用中断； 仅当所有可能的中断序列可预测时，才能使用中断嵌套	C.2.6.5
4	中断	中断过程不得触发看门狗，除非在与其他程序序列组合的条件下	A.9.4
5	断电	对于安全相关功能无断电处理程序，如保存数据	A.8.3
6	内存管理	硬件和/或软件中带有相应反应过程的堆栈管理器	C.2.6.4/C.5.4
7	程序	迭代循环时间应短于系统响应时间，如通过限制循环次数或检查执行时间	—
8	程序	如果使用的编程语言没有包括数组指针偏移量检查，则应进行此项检查	C.2.6.6

表 A.2 （续）

序号	对 象	措 施	参见 IEC 61508-7:2010 条款(除序号 13 外)
9	程序	定义强制系统进入所规定的安全状态的异常处理(如除零、溢出、变量范围检查等)	—
10	程序	除非在良好可靠的标准库中、或在被认可的操作系统中、或在高级语言编译器中，不使用递归编程。对于上述例外，应为每个包含递归编程的任务提供独立的堆栈，并由内存管理单元控制	C.2.6.7
11	程序	程序库接口和操作系统的说明文件应至少和用户程序本身一样详尽	—
12	程序	应对安全功能相关数据进行似真性检查，如输入模式、输入范围、内部数据	C.2.5/C.3.1
13	程序	如果任何操作模式被用于测试或验证，直到该模式终止，电梯才能正常运行	GB/T 20438.1—2006，7.7.2.1
14	通讯系统(内部和外部)	在具有安全功能的总线通讯系统内，如果发生通讯错误或总线上节点的故障，应达到安全状态，并考虑系统响应时间	A.7/A.9
15	总线系统	除启动过程外不得再配置 CPU 总线系统 **注**：周期性刷新 CPU 总线系统不认为是再配置	C.3.10
16	I/O 口操作	除启动过程外不得再配置 I/O 口 **注**：周期性刷新 I/O 配置寄存器不认为是再配置	C.3.10

表 A.3 设计和实现过程的通用措施

序号	措 施	参见 IEC 61508-7:2010 条款
1	所应用的功能、环境和接口方面的评价	A.14/B.1
2	要求规范，包括安全要求	B.2.1
3	所有规范的检查	B.2.6
4	除 A.2.6.2 要求的设计文档外，还应有： ——功能描述，包括系统架构和软/硬件配合； ——软件文档，包括功能和程序流程描述	C.5.9
5	设计评审报告	B.3.7/B.3.8，C.5.16
6	可靠性检查，可使用失效模式和影响分析(FMEA)等方法	B.6.6
7	制造商的测试规范、测试报告及现场测试报告	B.6.1
8	说明文件，包括对预期使用的限制	B.4.1
9	如果产品发生变更，应重复上述步骤并更新文件	C.5.23
10	实施软硬件及其兼容性的版本控制	C.5.24

表 A.4　符合 SIL1 的特定措施

部件和功能	要　　求[a]	措　　施	表 A.7 中措施序号	参见 IEC 61508-7:2010 条款
结构	结构应为:任意单独的随机失效被检出,系统应进入安全状态	带自检的单通道结构,或 带比较的双通道或多通道结构	M1.1 M1.3	A.3.1 A.2.5
处理单元	应能检测到导致错误结果的处理单元失效。 如果失效会导致危险情况,系统应进入安全状态	失效纠正硬件,或 软件自检,或 双通道结构比较器,或 双通道结构下利用软件相互比较	M2.1 M2.2 M2.4 M2.5	A.3.4 A.3.1 A.1.3 A.3.5
不可变存储区	错误的信息修改,即所有单个位或 2 位的失效以及一些 3 位和多位的失效,最迟应在电梯下次运行之前被检出	以下措施仅涉及单通道结构: 一位冗余(校验位),或 带单字冗余的块安全处理	M3.5 M3.1	A.5.5 A.4.3
可变存储区	寻址、写入、存储、读取过程中的全局失效,以及所有单个位或 2 位失效以及一些3 位和多位失效,最迟应在电梯下次运行之前被检出	以下措施仅涉及单通道结构: 带多位冗余(校验位),或 通过测试模式检查静态或动态故障	M3.2 M4.1	A.5.6 A.5.2
I/O 单元和接口,包括通讯链接	I/O 线上的静态失效和串扰,以及数据流中的随机和系统失效,最迟应在电梯下次运行之前被检出	代码安全,或 测试模式	M5.4 M5.5	A.6.2 A.6.1
时钟	处理单元的时钟发生器失效,如:频率改变或停顿,最迟应在电梯下次运行之前被检出	具有分离时基的看门狗,或 相互监视	M6.1 M6.2	A.3.5 A.9.1 A.9.2
程序序列	安全相关功能的错误的程序序列和不恰当的执行时间,最迟应在电梯下次运行之前被检出	程序序列的时序和逻辑监视组合	M7.1	A.9.4

[a] 检测出失效之后,电梯应保持在安全状态。

表 A.5　符合 SIL2 的特定措施

部件和功能	要　　求[a]	措　　施	表 A.7 中措施序号	参见 IEC 61508-7:2010 条款
结构	结构应为:在考虑了系统响应时间的条件下,任意单独的随机失效被检出,则系统进入安全状态	带自检和监视的单通道结构,或 带比较的双通道或多通道结构	M1.2 M1.3	A.3.3 A.2.5
处理单元	在考虑系统响应时间的条件下,应能检测到导致错误结果的处理单元失效。 如果失效会导致危险情况,系统应进入安全状态	失效纠正硬件的单通道结构,和 由硬件支持的软件自检的单通道结构,或 双通道结构的比较器,或 双通道结构下利用软件相互比较	M2.1 M2.3 M2.4 M2.5	A.3.4 A.3.3 A.1.3 A.3.5
不可变存储区	在考虑系统响应时间的条件下,错误的信息修改,即所有单个位或 2 位失效以及一些 3 位和多位失效,应被检出	以下措施仅涉及单通道结构: 带单字冗余的块安全处理,或 带多位冗余的字保存	M3.1 M3.2	A.4.3 A.5.6
可变存储区	在考虑系统响应时间的条件下,寻址、写入、存储、读取过程中的全局失效,以及所有单个位或 2 位失效以及一些 3 位和多位失效,应被检出	以下措施仅涉及单通道结构: 带多位冗余的字保存,或 通过测试模式检查静态或动态故障	M3.2 M4.1	A.5.6 A.5.2
I/O 单元和接口,包括通讯链接	在考虑系统响应时间的条件下,I/O 线上的静态失效和串扰,以及数据流中的随机和系统失效,应被检出[b]	代码安全,或 测试模式	M5.4 M5.5	A.6.2 A.6.1
时钟	在考虑系统响应时间的条件下,处理单元的时钟发生器失效,如频率改变或停顿,应被检出	具有分离时基的看门狗,或 相互监视	M6.1 M6.2	A.3.5 A.9.1 A.9.2
程序序列	在考虑系统响应时间的条件下,安全功能的错误的程序序列和不恰当的执行时间,应被检出	程序序列的时序和逻辑监视组合	M7.1	A.9.4

[a] 检测出失效之后,电梯应保持在安全状态。

[b] 该项不适用于执行装置,如安全回路中的安全继电器或同等的电气装置。

表 A.6　符合 SIL3 的特定措施

部件和功能	要求[a]	措施	表 A.7 中措施序号	参见 IEC 61508-7:2010 条款
结构	结构应为:在考虑了系统响应时间的条件下,任意单独的随机失效被检出,则系统进入安全状态	带比较的双通道或多通道结构	M1.3	A.2.5
处理单元	在考虑系统响应时间的条件下,应能检测到导致错误结果的处理单元失效。 如果失效会导致危险情况,系统应进入安全状态	双通道结构的比较器,或 双通道结构下利用软件相互比较	M2.4 M2.5	A.1.3 A.3.5
不可变存储区	在考虑系统响应时间的条件下,错误的信息修改,即所有单个位或多位失效,应被检出	有复制块的块安全处理,或 带多字冗余的块安全处理	M3.3 M3.4	A.4.5 A.4.4
可变存储区	在考虑系统响应时间的条件下,寻址、写入、存储、读取过程中的全局失效,以及静态位失效和动态耦合,应被检出	带复制块的块安全处理,或 巡视检查,如“galpat”法	M4.2 M4.3	A.5.7 A.5.3
I/O 单元和接口,包括通讯链接	在考虑系统响应时间的条件下,I/O 线上的静态失效和串扰,以及数据流中的随机和系统失效,应被检出[b]	多通道并行输入,和 多通道并行输出,或 输出回读,或 代码安全,或 测试模式	M5.1 M5.3 M5.2 M5.4 M5.5	A.6.5 A.6.3 A.6.4 A.6.2 A.6.1
时钟	在考虑系统响应时间的条件下,处理单元的时钟发生器失效,如频率改变或停顿,应被检出	具有分离时基的看门狗,或 相互监视	M6.1 M6.2	A.3.5 A.9.1 A.9.2
程序序列	在考虑系统响应时间的条件下,安全功能的程序序列错误和不恰当的执行时间,应被检出	程序序列的时序和逻辑监视组合	M7.1	A.9.4

[a] 检测出失效之后,电梯应保持在安全状态。

[b] 该项不适用于执行装置,如安全回路中的安全继电器或同等的电气装置。

表 A.7　失效控制的可用措施描述

部件和功能	措施序号	措　施　描　述
结构	M1.1	带自检的单通道结构 **描述：** 即使结构由单通道组成，也应提供冗余输出途径以确保安全切断。循环的自检可按应用要求的间隔时间在 PESSRAL 的子单元内执行。这些检查（如 CPU 或存储器检查）用以检测独立于数据流的潜在失效。 检测到失效应使系统进入安全状态
	M1.2	带自检和监视的单通道结构 **描述：** 带自检和监视的单通道结构包含独立的硬件监视单元，该单元独立于具体应用、周期性地从系统接受自检过程产生的测试数据。如果数据错误，系统应进入安全状态。 应至少有两个独立的切断路径，可通过处理单元本身或者监视装置实施切断
	M1.3	带比较的双通道或多通道结构 **描述：** 双通道安全相关设计应由两个独立的无反馈功能单元组成。特定的功能在每个通道内独立地实现。对于一个专为安全装置的功能而设计的双通道 PESSRAL，各通道的设计在软硬件方面可以是相同的。若双通道 PESSRAL 用于复杂的解决方案（如多个安全功能的组合），且过程或条件无法明确验证，应考虑软硬件的多样化。 该结构具有对与安全功能相关的内部信号（如总线比较）和/或输出信号进行比较的功能，以便失效检测。 至少需要两个独立的切断路径，可由通道本身或比较器实施切断。比较本身的失效也应被识别出
处理单元	M2.1	失效纠正硬件 **描述：** 可使用专门的失效识别或失效纠正电路技术来实现。对于简单结构这些技术是已知的
	M2.2	软件自检 **描述：** 用于安全相关应用的所有处理单元功能都应进行循环测试。 这些测试可与其他子部件的测试组合，如存储器、I/O 等
	M2.3	由硬件支持的软件自检 **描述：** 支持自检功能的用于失效检测的专用硬件。如一个检查某个位模式的周期性输出的监视单元

表 A.7（续）

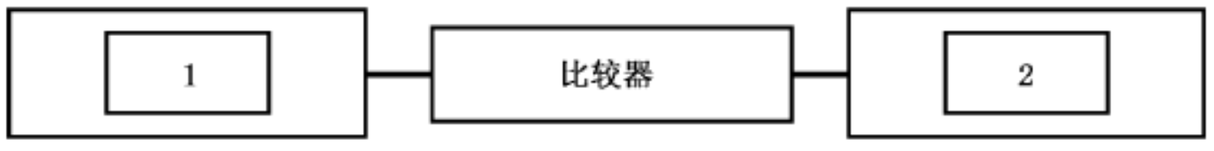
部件和功能	措施序号	措　施　描　述
处理单元	M2.4	双通道结构的比较器 **描述：**  带硬件比较器的双通道： a）　使用硬件单元循环地或持续地对两个处理单元的信号进行比较。比较器可以是一个外部验证过的单元或被设计为一个自监视装置；或 b）　使用处理单元对两个通道的信号进行比较。比较器可以是一个外部验证过的单元或被设计为一个自监视装置
	M2.5	双通道的相互比较 **描述：**  使用两个冗余处理单元，二者相互交换安全相关数据。每个处理单元内都对数据进行比较
不可变存储区（ROM，EPROM...）	M3.1	带单字冗余的块安全处理（如 ROM 中的一个字长的签名） **描述：** 在该测试中，ROM 的内容被特定算法压缩为至少一个存储字。该类算法，如循环冗余校验（CRC），可使用软件或硬件实现
	M3.2	带多位冗余的字保存，如改进的海明码（hamming code） **描述：** 存储器的每个字被扩展若干冗余位以容纳一个海明距至少为 4 的改进的海明码。每读一个字时，通过校验冗余位可以确定是否发生了错误。若发现差异，系统应进入安全状态
	M3.3	有复制块的块安全处理 **描述：** 地址空间被划分到两个存储器中。第一个存储器以正常方式工作，第二个存储器包含同样的信息并同第一个并行存取。比较两者的输出，当检测到差异时就认为失效。为检测某些类型的位错误，应对其中的一个存储器中的数据取反后存储，读取时再次取反。在软件执行过程中，应通过一个程序对两个存储区域的内容进行循环比较
	M3.4	带多字冗余的块安全处理 **描述：** 使用 CRC 算法来计算一个签名，而结果值至少有两个字长，扩展的签名如同单字的情况中被存储、重新计算和比较。当存储的和重新计算的签名之间有差异时就产生失效信息
	M3.5	一位冗余的字保存（如带奇偶校验位的 ROM 监视） **描述：** 把存储器的每个字都扩展一位（奇偶校验位），此位给每个字补齐偶数个或奇数个逻辑“1”。每次读数据字时检验它的奇偶性。若发现“1”的个数有错，产生失效信息。应这样选择偶或奇的奇偶性，使得在一次失效中，无论是 0 字（全 0）还是 1 字（全 1）都不是有效的，此时字也不是有效代码。当数据字和它的地址串联计算奇偶性时，奇偶校验也可用来检测寻址错误

表 A.7（续）

部件和功能	措施序号	措　施　描　述
可变存储区	M4.1	通过测试模式检查静态或动态故障，如 RAM 测试“漫步路径”(walkpath)法 **描述：** 用一个均匀的位流初始化要测试的存储范围，第一个单元被反向并检查其余的存储区以确保后台是正确无误的。此后第一单元再次反向从而使它回复到它的初始值，对下一个单元也重复整个操作过程。在反向的后台预赋值情况下执行“漫游位模型”的第二次运行。如果有差异发生，系统应进入安全状态
	M4.2	带复制块的块安全处理，如：带硬件或软件比较的双重 RAM **描述：** 地址空间被划分到两个存储器中。第一个存储器以正常方式工作，第二个存储器包含同样的信息并同第一个并行存取。比较两者的输出，当检测到差异时就认为失效。为检测某些类型的位错误，应对其中的一个存储器中的数据取反后存储，读取时再次取反。在软件执行过程中，应通过一个程序对两个存储区域的内容进行循环比较
	M4.3	对静态和动态失效检查的检视，如“galpat”法 **描述：** a) RAM 测试“galpat”：在标准预赋值的存储空间中，先对第一个存储单元取反，并检查所有剩余单元以确保它们内容的正确。每读取一个剩余单元后，都检查一次被取反的单元。然后对第二个存储单元取反后执行上述操作，以此类推对每个单元重复这样的操作。在存储空间预赋与第一轮相反的值后执行第二轮。出现差异就认为存在失效；或 b) 透明的“galpat”测试：开始测试时，考虑要测试的存储范围的内容，用软件或硬件产生“签名”，把它存入寄存器中。这对应“galpat”法中的预赋值。然后把要测试的单元取反后写入，并检测剩余单元的内容，每读取一个剩余单元后也验证该取反的测试单元。由于剩余单元的内容是未知的，它们的内容不能被单独地测试，但是可以通过再一次产生一个“签名”来实现。对第一个单元的第一次运行之后，该单元的内容取反数次(即内容再次为真)后又启动了第二次运行。这样，存储器的原始内容被重建了。按同样的方法测试所选存储范围内的所有单元。出现差异就认为存在失效
I/O 单元和接口	M5.1	多通道并行输入 **描述：** 符合规定的容差范围(时间、值)的一种与数据流有关的独立输入的比较
	M5.2	输出回读(输出监视) **描述：** 符合规定的容差范围(时间、值)的一种与数据流有关的输出和独立输入的比较。检测到的失效不总是与有缺陷的输出有关
	M5.3	多通道并行输出 **描述：** 一种依赖于数据流的输出冗余。通过技术处理或外部比较器直接识别失效
	M5.4	代码安全 **描述：** 保护输入和输出信息免受随机失效和系统失效的影响。它通过信息冗余和/或时间冗余实现了依赖于数据流的输入和输出单元的失效识别

表 A.7（续）

部件和功能	措施序号	措　施　描　述
I/O 单元和接口	M5.5	测试模式(模型) **描述：** 一种不依赖于数据流的输入和输出单元的循环测试，用一种定义的测试模式来比较观测值和相应预期值。测试模式的信息、接收和评价是相互独立的。假定所有可能的输入模型均被测试
时钟	M6.1	具有分离时基的看门狗 **描述：** 具有分离时基的硬件定时器，由程序的正确操作来触发
	M6.2	相互监视 **描述：** 具有分离时基的硬件定时器，由其他处理器程序的正确操作触发
程序序列	M7.1	程序序列的时序和逻辑监视组合 **描述：** 仅当各程序段的顺序执行正确时，一个基于时序的程序序列监视装置才会被重新触发

A.3　使用 GB/T 20438.2 和 GB/T 20438.3 实现和验证 SIL 符合性的技术和措施

A.3.1　一般要求

A.3 规定了采用 GB/T 20438 的要求，可用于实现和验证 PESSRAL 的 SIL 符合性。

A.3.1.1　本部分中的 SIL 表示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(参见 GB/T 20438.1—2006 的表 2)。然而，PESSRAL 是以持续控制的方式来保持安全功能时，SIL 应表示对工作在高要求模式中 PESSRAL 的要求，并应使用每小时危险失效概率(参见 GB/T 20438.1—2006 的表 3)。

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，应将子系统中危险故障的检测视为一个工作在连续模式的安全功能。

A.3.1.2　用于执行非 SIL 相关要求的装置和软件不得用于实现 PESSRAL 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.3.1.3　在任何能容许单一故障的 PESSRAL 子系统中，一旦检出一个危险故障(通过诊断测试、检验测试或任何其他方式)，应进入本部分表 2 中的安全状态。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 PESSRAL 的完整性和安全状态条件，如果有必要，应采取手动复位使 PESSRAL 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，则报警本身应被认为是该 PESSRAL 的 SIL 相关功能的一部分。

A.3.2　SIL 符合性的实现

PESSRAL 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。见 GB/T 20438.7，它包含了 GB/T 20438.2 和 GB/T 20438.3 相关的各种安全技术和措施的概述。

注：假如若干个低安全完整性等级系统能达到足够等级的独立性，且在应用中被证明，则可用来满足一个更高安全完整性等级功能的需求。

A.3.3 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。

附 录 B
（资料性附录）
适用的电梯规范和标准

本部分中的电梯安全功能（装置）参考了 GB 7588—2003＋XG1—2015、GB 21240—2007 和 EN 81-20：2014 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 中的电梯安全功能（装置）之间的关系。

表 B.1 适用的电梯标准对照表

序号	电梯安全功能（装置）	GB 7588—2003＋XG1—2015 的条款号	GB 21240—2007 的条款号	EN 81-20：2014 的条款号
1	底坑停止装置	5.7.3.4a)	5.7.2.5a)	5.2.1.5.1a)
2	滑轮间停止装置	6.4.5	6.4.5	5.2.1.5.2c)
3	检查底坑梯子的存放位置	—	—	5.2.2.4
4	检查通道门、安全门及检修门的关闭位置	5.2.2.2.2	5.2.2.2.2	5.2.3.3
5	检查轿门的锁紧状况	11.2.1c)	11.2.1c)	5.2.5.3.1c)
6	检查机械装置的非工作位置（轿厢内或轿顶上的工作区域）	—	—	5.2.6.4.3.1b)
7	检查检修门的锁紧位置	—	—	5.2.6.4.3.3e)
8	检查所有进入底坑的门的打开状态	—	—	5.2.6.4.4.1d)
9	检查机械装置的非工作位置（底坑内的工作区域）	—	—	5.2.6.4.4.1e)
10	检查机械装置的工作位置（底坑内的工作区域）	—	—	5.2.6.4.4.1f)
11	检查工作平台的收回位置	—	—	5.2.6.4.5.4a)
12	检查可移动止停装置的收回位置	—	—	5.2.6.4.5.5b)
13	检查可移动止停装置的伸展位置	—	—	5.2.6.4.5.5c)
14	检查层门锁紧装置的锁紧位置	7.7.3.1	7.7.3.1	5.3.9.1
15	检查层门的关闭位置	7.7.4.1	7.7.4.1	5.3.9.4.1
16	检查无锁门扇的关闭位置	7.7.6.2	7.7.6.2	5.3.11.2
17	检查轿门的关闭位置	8.9.2	8.9.2	5.3.13.2
18	检查轿厢安全窗和轿厢安全门的锁紧状况	8.12.4.2	8.12.4.2	5.4.6.3.2
19	轿顶停止装置	8.15b)	8.15b)	5.4.8b)
20	检查轿厢或对重的提升	—	—	5.5.3c)2)
21	检查钢丝绳或链条的异常相对伸长（使用两根钢丝绳或链条时）	9.5.3	9.3.3	5.5.5.3a)
22	检查强制式电梯和液压电梯的钢丝绳或链条的松弛	12.9	12.13	5.5.5.3b)
23	检查防跳装置	9.6.2	—	5.5.6.1c)
24	检查补偿绳的张紧	9.6.1e)	—	5.5.6.2f)

表 B.1（续）

序号	电梯安全功能(装置)	GB 7588—2003＋XG1—2015 的条款号	GB 21240—2007 的条款号	EN 81-20:2014 的条款号
25	检查轿厢安全钳的动作	9.8.8	9.8.8	5.6.2.1.5
26	检查超速	9.9.11.1	9.10.2.10.1	5.6.2.2.1.6a)
27	检查限速器的复位	9.9.11.2	9.10.2.10.2	5.6.2.2.1.6b)
28	检查限速器绳的张紧	9.9.11.3	9.10.2.10.3	5.6.2.2.1.6c)
29	检查安全绳的断裂或松弛	—	9.10.4.4	5.6.2.2.3e)
30	检查触发杠杆的收回位置	—	—	5.6.2.2.4.2h)
31	检查棘爪装置的收回位置	—	9.11.9	5.6.5.9
32	采用具有耗能型缓冲装置的棘爪装置的电梯,检查缓冲装置恢复至其正常的伸出位置	—	9.11.10	5.6.5.10
33	检查轿厢上行超速保护装置	9.10.5	—	5.6.6.5
34	检测门开启情况下轿厢的意外移动	9.11.7	—	5.6.7.7
35	检测门开启情况下轿厢意外移动保护装置的动作	9.11.8	—	5.6.7.8
36	检查缓冲器恢复至其正常伸长位置	10.4.3.4	10.4.3.3	5.8.2.2.4
37	检查可拆卸盘车手轮的位置	12.5.1.1	—	5.9.2.3.1a)3)
38	采用接触器的主开关的控制	13.4.2	13.4.2	5.10.5.2
39	检查减行程缓冲器的减速状况	12.8.5	—	5.12.1.3
40	检查平层、再平层和预备操作	14.2.1.2a)2)	14.2.1.2a)2)	5.12.1.4a)
41	检修运行开关	—	—	5.12.1.5.1.2a)
42	检查与检修运行配合使用的按钮	—	—	5.12.1.5.2.3b)
43	紧急电动运行开关	—	—	5.12.1.6.1
44	层门和轿门旁路装置	—	—	5.12.1.8.2
45	检修运行停止装置	14.2.1.3c)	14.2.1.3c)	5.12.1.11.1d)
46	电梯驱动主机上的停止装置	—	—	5.12.1.11.1e)
47	紧急和测试操作屏上的停止装置	—	—	5.12.1.11.1f)
48	检查轿厢位置传递装置的张紧(极限开关)	10.5.2.3b)	—	5.12.2.2.3
49	检查液压缸柱塞位置传递装置的张紧(极限开关)	—	10.5.2.2b) 10.5.2.3b)	5.12.2.2.4 5.12.2.2.5
50	极限开关	10.5.3.1b)2)	10.5.3.1	5.12.2.3.1b)
51	检查轿厢位置传递装置的张紧(减速检查装置)	12.8.4c)	—	—
52	检查轿厢位置传递装置的张紧(平层、再平层和防沉降)	14.2.1.2a)3)	14.2.1.2a)3)	—
53	对接操作的行程限位装置	14.2.1.5b)	14.2.1.4b)	—
54	对接操作	14.2.1.5	14.2.1.4	—

附 录 C
（资料性附录）
风险降低决策表的示例

表 C.1 给出 PESSRAL 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	灾难性的(Ⅰ)	严重的(Ⅱ)	轻微的(Ⅲ)	可忽略的(Ⅳ)
$F_I \geqslant$1E-3(A)	>0.5E-2	ⅠA	ⅡA	ⅢA	ⅣA
1E-4$\leqslant F_I <$1E-3(B)	0.5E-3	ⅠB	ⅡB	ⅢB	ⅣB
1E-5$\leqslant F_I <$1E-4(C)	0.5E-4	ⅠC	ⅡC	ⅢC	ⅣC
1E-6$\leqslant F_I <$1E-5(D)	0.5E-5	ⅠD	ⅡD	ⅢD	ⅣD
1E-7$\leqslant F_I <$1E-6(E)	0.5E-6	ⅠE	ⅡE	ⅢE	ⅣE
$F_I <$1E-7	<0.5E-7	不考虑	不考虑	不考虑	不考虑

表 C.2 纠正措施——风险降低的要求

ⅠA，ⅠB，ⅠC，ⅡA，ⅡB，ⅢA	应采取纠正措施减轻后果，且如果可以，消除风险
ⅠD，ⅡC，ⅢB	应采取纠正措施降低影响
ⅠE，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
ⅢE，ⅣC，ⅣD，ⅣE	不需要任何措施

参 考 文 献

[1] GB 7588—2003+XG1—2015 电梯制造与安装安全规范

[2] GB 21240—2007 液压电梯制造与安装安全规范

[3] EN 81-20:2014 Safety rules for the construction and installation of lifts—Lifts for the transport of persons and goods—Part 20: Passenger and goods passenger lifts

[4] GB/T 16935.1—2008 低压系统内设备的绝缘配合 第1部分:原理、要求和试验(IEC 60664-1:2007,IDT)

[5] 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)

中 华 人 民 共 和 国
国 家 标 准
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 1 部分：电梯（PESSRAL）
GB/T 35850.1—2018
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2018 年 2 月第一版
*
书号：155066・1-59436

GB/T 35850.1-2018