ICS 91.140.90
Q 78

中华人民共和国国家标准化指导性技术文件

GB/Z 35850.3—202×

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3部分：PESSRAL和PESSRAE相关的可编程电子系统的生命周期指南

Programmable electronic systems in safety-related applications for lifts (elevators), escalators and moving walks—Part 3: Life cycle guideline for programmable electronic systems related to PESSRAL and PESSRAE

(ISO/TR 22201-3:2016, Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety related applications — Part 3: Life cycle guideline for programmable electronic systems related to PESSRAL and PESSRAE, MOD)

（征求意见稿）

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

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。

本文件是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》的第3部分，GB/T 35850已经发布了以下部分：

——第1部分：电梯（PESSRAL）；

——第2部分：自动扶梯和自动人行道(PESSRAE)；

本文件使用重新起草法修改采用ISO/TR 22201-3:2016《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3部分：PESSRAL和PESSRAE相关的可编程电子系统的生命周期指南》。

本文件与ISO/TR 22201-3:2016相比在结构上做了以下调整：

——在第4章中，增加了悬置段的编号和标题，即“4.1 概述”，并调整了后续条款的编号，以符合GB/T 1.1—2020的规定和便于应用。

——在第5章中，更改了a）项的分项层次，以符合GB/T 1.1—2020的规定。

本文件与ISO/TR 22201-3:2016的技术差异及其原因如下：

——关于规范性引用文件，本文件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：

- 用修改采用国际标准的GB/T 35850.1代替了ISO 22201-1；
- 用修改采用国际标准的GB/T 35850.2代替了ISO 8102-6。

本文件与ISO/TR 22201-3:2016相比还做了下列编辑性修改：

——在术语和定义中，删除了ISO和IEC维护用于标准化的术语数据库的链接地址，以符合GB/T 1.1—2020的规定。

——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。

本文件由全国电梯标准化技术委员会（SAC/TC 196）提出和归口。

本文件起草单位：（暂空）

本文件主要起草人：（暂空）

引　　言

本文件阐述了PESSRAL和PESSRAE的生命周期规划和安装后各个阶段的活动（如维护、修理、接口的更换和改造），以帮助确保系统在生命周期内的安全完整性等级（SIL）。

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3部分：PESSRAL和PESSRAE相关的可编程电子系统的生命周期指南

1 范围

本文件提供了编制GB/T 35850.1（PESSRAL）和GB/T 35850.2（PESSRAE）所要求说明书的附加信息和程序，供胜任的维护人员对可编程电子系统进行维护操作时使用的指南。

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 35850.1 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，ISO 22201-1:2017，MOD)

GB/T 35850.2 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）(GB/T 35850.2—2019，ISO 8102-6:2019，MOD)

3 术语和定义

在GB/T 35850.1和GB/T 35850.2中界定的以及下列术语和定义适用于本文件。

3.1

胜任的维护人员 competent maintenance person

已经过适当的培训，通过知识和实践经验方面的认定，并能得到其所在维护组织（3.4）必要的指导和支持以便能够安全进行所要求的维护操作的维护人员。

注：在维护组织中（3.4），维护人员的技能应当不断更新。

3.2

设计等效 design equivalent

原设备制造单位或者第三方的认证产品，其满足相同的SIL等级组件/子系统的设计规范，但是对PE系统的非SIL等级部分有着不同的规范。

3.3

功能等效 functional equivalent

产品具有与原认证产品不同的 SIL 等级组件/子系统设计规范，但满足相同的功能要求。

3.4

维护组织 maintenance organization

具备规定资格的，代表电梯设备的业主（3.7）并由胜任的维护人员（3.1）执行维护工作的法人或法人下属部门。

3.5

制造单位 manufacturer

负责电梯整机（电梯、自动扶梯和自动人行道）或安全部件的设计、制造和市场投放的法人。

[来源：GB/T 18775—2009，3.7，有修改]

3.6

维护 maintenance

设备安装后生命周期内的活动，包括预防性活动、更换、修理和改造。

3.7

业主 owner

具有设备的所有权或处置权，并对其操作和使用负责的自然人或法人。

3.8

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。

例如：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（如：智能传感器、智能变送器、智能执行器等）。

3.9

可编程电子系统 programmable electronic system

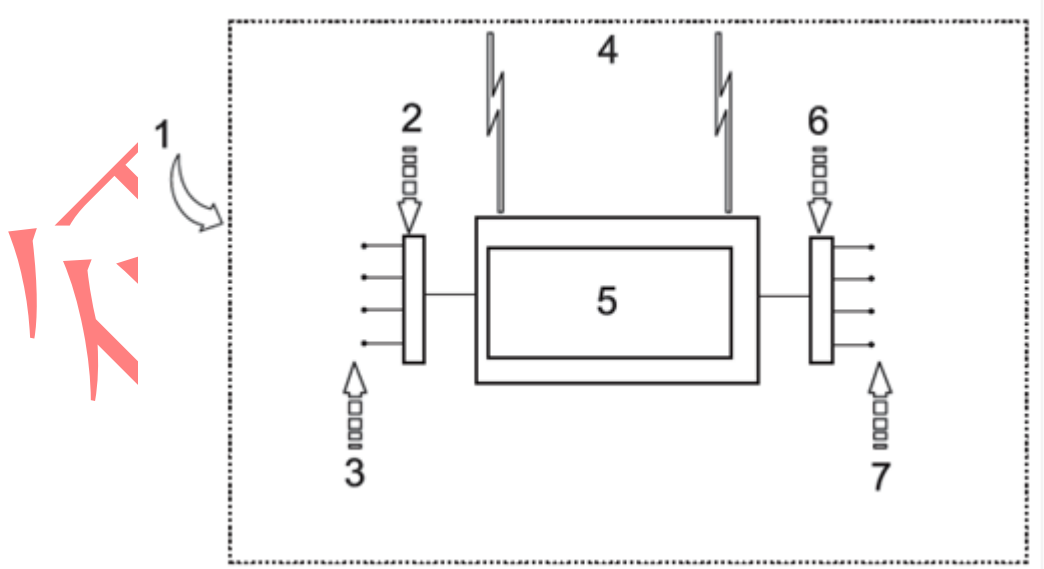
PE 系统 PE system

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，包括系统中所有组件，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系统可执行满足SIL要求或非SIL要求的功能。功能的SIL分级只需考虑PE系统中执行SIL相关功能要求的部分。

注3：图1中所示的可编程电子在中心位置，但是可以设置于PE系统的多个位置。



图中：

1——PE系统的范围；

2——输入接口（如：A/D转换器）；

3——输入装置（如：传感器）；

4——通信；

5——可编程电子（PE）；

6——输出接口（如：D/A转换器）；

7——输出装置/终端组件（如：执行装置）。

图 1　基本的 PE 系统结构

3.10

产品等效 product equivalent

原设备制造单位或第三方的认证产品，可在设计、制造、型号和版本（按相同的生产图纸制造）上直接替代原认证产品。

4 说明书内容

4.1 概述

本条款提供了对GB/T 35850.1和GB/T 35850.2所述的PE系统说明书的编制过程和附加内容的特殊考虑。

4.2 安全预防措施

在编制说明书时，开发人员应该进行风险评价，从而识别和消除PE系统生命周期中此阶段可能存在的危险（见GB/T 20900）。

4.3 标记、标志、象形图和书面警示

根据国家相关要求，含有SIL等级装置的装配组件宜进行标记或者标出识别信息，并指出维护人员应参考说明书，以获得详细的操作指南和预防措施。在可能的情况下，宜使用适用的国家标准中易理解的标记和图示，如GB/T 16273.1—2008中序号为167的“操作说明书”图形符号。

如果风险评价表明，为了维护而需要使用附加的特定警示，那么这些警示宜直接粘贴在设备或部件上面，如果无法操作，可以在其附近的地方粘贴。标记、标志、象形图和书面警示应是明确和易于理解的。不宜使用只含有“危险”字样的标志或书面警示。直接粘贴在设备或部件上的信息需要清晰且永久。

4.4 说明书内容需考虑的要素

以下列出的是需要在说明书内容中考虑的要素。另外的考虑要素见附录A的A.1。

a)所有的必要操作，以确保在安装完成后以及整个生命周期内设备及其部件的安全和预期功能；

b)修理或更换可能发生磨损或损坏的部件时不能影响其设备的特性；

c)设备的改造，包括改变设备的任何特性（速度、负载等）；

d)消防队和应急人员采取的救援行动；

e)设备的规格和预期用途（设备类型、性能、运输的货物类型，用户类型等）；

f)设备及其部件安装的环境（气候条件，故意破坏行为等）；

g)任何的使用限制；

h)对每项任务和每个工作区域风险评价（见4.1）的结果；

i)安全组件制造单位提供的具体维护说明。

5　程序

在PE系统投入市场时，制造单位应提供其维护说明。这些维护说明应是风险评价的结果，并以应用设备使用地的国家官方语言编写。在编写维护说明的内容时，应在说明书中考虑以下要素：

a) 控制文件---识别和维护包含SIL等级硬件或软件的PE系统的生命周期的控制文件。这些文件包括下列功能需求：

1）设计规范（系统和组件/子系统）；

2）生产规范；

3）版本识别和版本控制。

b）维护活动和保存维护活动记录---由业主在PE系统装置的生命周期中记录并保存下列PE系统维护活动的事项、日期和原因说明：

1）安全装置的预防性维护（有计划的安全性功能动作、检验测试等）；

2）安全装置的失效事件；

3）PE系统装置的改造（如：报废、升级、可靠性改进等）；

4）对安全装置的接口或其环境的改造。

c）更换或改造过程的确认---在（b）项的维护活动中进行的更换或者改造，应按照A.2中所述的过程进行，并且不宜修改该功能所需要的最低SIL。如果PE系统的SIL等级设计中包含了SIL相关和非SIL相关功能（GB/T 35850.1和GB/T 35850.2中列明的,由SIL等级部分驱动或与SIL等级部分通讯的电路中的功能），那么非SIL相关功能的软件或硬件的改动应按PE系统中SIL相关部分的改动的同样方式进行处理。

附录A
（资料性）
说明书的要素和确认过程

A.1 编制说明书的附加要素

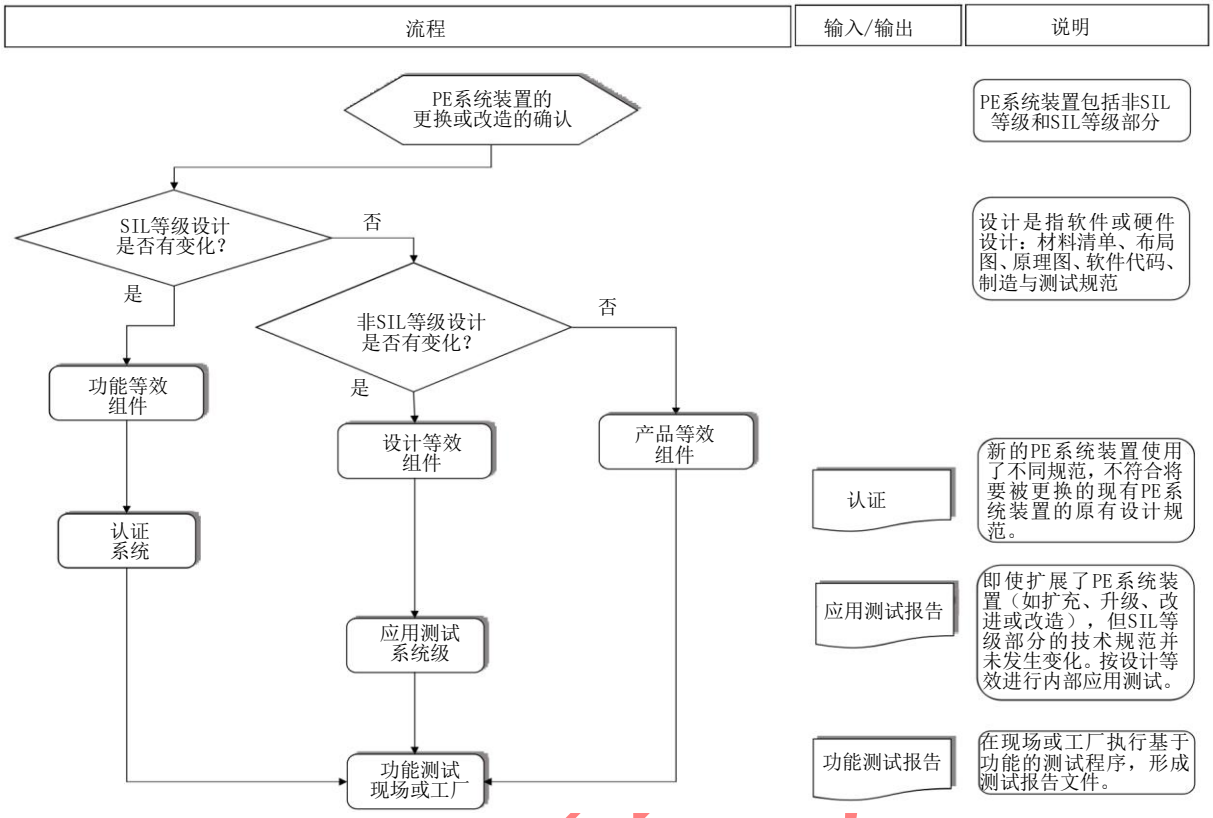
编制说明书的附加要素见表A.1。

表A.1 编制说明书的附加要素

序号	考虑要素
1	对诊断和已识别的失效模式的考虑
2	明确如何进行检验测试
3	明确如何获取PE组件
4	明确如何更换PE组件
5	识别包括软件在内的物理组件
6	识别文件中的PE组件
7	PE系统装置和相关软件的版本及配置管理
8	与PE系统装置相连的系统接口的版本及配置管理
9	装置对外界环境变化（如气压、温度、湿度、ESD、EMI和接地）敏感性的预防措施
10	维护工作（含检验测试）的周期
11	因测试模拟设置/参数而导致意外故障的预防措施
12	因测试条件而导致意外故障的预防措施
13	因软件工具（配置，编程和测试工具）或其不兼容导致意外故障的预防措施
14	因误用软件工具（配置，编程和测试工具）或其不兼容导致误导性结果的预防措施

A.2 PE系统装置更换或改造的确认过程

PE系统装置更换或改造的确认过程见图A.1。



图A.1 PE系统装置更换或改造的确认过程

A.3 应用于安全功能的PE系统装置的SIL等级相关的验证和/或认证类别

应用测试（系统级）：由注册或许可的专业工程师、实验室或认证机构进行测试或见证，以确保符合规范的要求。这些测试不涉及其他标准可能要求的认证符合性，例如EMC。

认证（系统）：由一个独立的机构进行的过程，且该机构被授权评估装置的SIL等级是否符合适当的标准。

功能测试（现场或工厂）：验证现场安装不会引起失效。这些测试不涉及其他标准可能要求的认证符合性，例如EMC。

参考文献

[1] GB/T 16273.1-2008 设备用图形符号 第1部分：通用符号（ISO 7000:2004，NEQ）
[2] GB/T 20900 电梯、自动扶梯和自动人行道 风险评价和降低的方法