ICS 91.140.90
Q 78

中华人民共和国国家标准

GB/T ×××××—202×

电梯、自动扶梯和自动人行道的电气要求 信息传输与控制安全

Electrical requirements for lifts, escalators and moving walks—Information transmission and control security

(ISO 8102-20:2022, Electrical requirements for lifts, escalators and moving walks — Part 20: Cybersecurity, 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。

本文件使用重新起草法修改采用 ISO 8102-20:2022《电梯、自动扶梯和自动人行道的电气要求 第 20 部分：网络安全》。

本文件与 ISO 8102-20:2022 的技术差异及其原因如下：

——在范围中，用“本文件适用于按照 GB/T 7588、GB 16899 设计的电梯、自动扶梯和自动人行道” 代替了“本文件适用于按照 ISO 8100 系列标准设计的电梯、自动扶梯和自动人行道（EUC）”,以适合我国国情。

——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:

- 用修改采用国际标准的 GB/T 7588.1—2020 代替了 ISO 8100-1:2019；
- 增加引用了 GB 16899。

本文件做了下列编辑性改动：

——修改了标准名称；

——在引言和附录 C 中，用对应的国家标准代替了 IEC 62443 系列标准；

——更改了参考文献。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国电梯标准化技术委员会（SAC/TC 196）提出并归口。

本文件起草单位：（暂空）

本文件主要起草人：（暂空）

引　言

本文件是为了响应市场需求和日益增强的网络安全意识而制定的。在运营技术方面代表着最新技术水平的网络安全标准是 GB/T 35673—2017 、GB/T 42457—2023 等国家标准。本文件给出了电梯行业应用这些标准时所需的特定要求。

网络安全的基本原则是建立一个健全的网络安全过程生命周期。这个生命周期需要包含足够的培训、工具、资源和过程，以开发、加固及维护受控设备（EUC）在抵御网络攻击时的弹性。生命周期的方法也是各种网络安全标准和方法最佳实践的基本前提。

电梯、自动扶梯和自动人行道的电气要求 信息传输与控制安全

1 范围

本文件规定了新的电梯、自动扶梯和自动人行道信息传输与控制安全的要求，本文件适用于按照GB/T 7588、GB 16899 设计的电梯、自动扶梯和自动人行道，也可适用于与其相连的其他电梯相关设备。

本文件涵盖了与网络安全威胁相关的产品和系统在以下生命周期阶段中的要求：

——产品开发（过程和产品要求）；

——制造；

——安装；

——使用和维修；

——退役。

本文件涉及了 GB/T 42457—2023 的图 2 中的 EUC 产品供应商和系统集成商的角色。

本文件并未涉及 GB/T 42457—2023 的图 2 中的资产所有者的角色，但规定了 EUC 产品供应商和系统集成商建立文档的要求，以允许资产所有者（EUC 所有者）实现和维护 EUC 的安全。

本文件给出了下列功能的最低网络安全要求：

——基本功能；

——安全功能；

——报警功能。

本文件适用于能够连接到外部系统（如建筑物的网络、云服务或服务工具）的 EUC，其连接可以通过现场的永久设备或在安装、使用和维修以及退役阶段带到现场使用的临时设备来实现。

本文件包括 EUC 与外部系统和服务的接口，但未涉及接口之外的外部系统和服务。

本文件不适用于本文件实施日期之前安装的 EUC。

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 7588.1—2020 电梯制造与安装安全规范 第 1 部分：乘客电梯和载货电梯 （ISO 8100-1:2019 MOD）

GB 16899 自动扶梯和自动人行道的制造与安装安全规范

GB/T 35673—2017 工业通信网络 网络和系统安全 系统安全要求和安全等级（IEC 62443-3-3:2013 IDT）

GB/T 40211—2021 工业通信网络 网络和系统安全 术语、概念和模型（IEC/TS 62443-1-1:2009 IDT）

GB/T 42456—2023 工业自动化和控制系统信息安全 IACS 组件的安全技术要求（IEC 62443-4-2:2019 IDT）

GB/T 42457—2023 工业自动化和控制系统信息安全 产品安全开发生命周期要求（IEC 62443-4-1:2018 IDT）

IEC 62443-3-2:2020 工业自动化和控制系统的安全 第 3-2 部分：系统设计的安全风险评价（Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design）

3 术语、定义和缩略语

3.1 术语和定义

GB/T 7588.1—2020、GB 16899、GB/T 40211—2021、IEC 62443-3-2:2020 界定的以及下列术语和定义适用于本文件。

3.1.1

信息传输与控制安全 cybersecurity
网络安全
用于防止计算机或计算机系统受到未经授权的访问或攻击而采取的措施。

注 1：在本文件中，电梯、自动扶梯和自动人行道的控制系统被认为是计算机系统。

注 2：在本文件中，术语“安全”包括网络安全。

[来源：IEC 62443-3-2:2020，3.1.7，有修改]

3.1.2

受控设备 equipment under control
指电梯、自动扶梯和自动人行道。

3.1.3

EUC 所有者 EUC owner
对 EUC 负责的个人或组织。

注：EUC 所有者等同于 GB/T 42457—2023，3.1.6 中给出的术语“资产所有者”。

[来源：GB/T 42457—2023，3.1.6，有修改]

3.2 缩略语

下列缩略语适用于本文件。

CCSC 通用组件安全约束（common component security constraint）
DM 缺陷管理（defect management）
EDR 嵌入式设备要求（embedded device requirement）
EUC 受控设备（equipment under control）
FR 基本要求（foundational requirement）
HDR 主机设备要求（host device requirement）
IACS 工业自动化和控制系统（industrial automation and control systems）
NDR 网络设备要求（network device requirement）
RACI 责任人、负责人、被咨询人和被通知人 （responsible, accountable, consulted and informed）
RE 增强要求（requirement enhancement）
SAR 软件应用要求（software application requirement）
SD 安全设计（secure design）
SG 安全导则（security guideline）
SI 安全实施（security implementation）
SIL 安全完整性等级（safety integrity level）
SL 信息安全等级（security level）
SL-T 目标安全等级（target security level）

SM 安全管理（security management）
SR 安全要求（security requirement）
SUM 安全更新管理（security update management）
SVV 安全验证和确认（security verification and validation）

4 电梯、自动扶梯和自动人行道安全开发生命周期

4.1 通则

本条款的要求应用于组件开发和系统集成。有关安全开发生命周期的附加信息，参见附录 A。有关安全风险评估的附加信息，参见附录 B。有关安全实践的列表，参见附录 C。

4.2 安全管理

4.2.1 开发过程

应符合 GB/T 42457—2023 中“SM-1：开发过程”的要求。

4.2.2 明确职责

应符合 GB/T 42457—2023 中“SM-2：明确职责”的要求。

4.2.3 明确适用性

应符合 GB/T 42457—2023 中“SM-3：明确适用性”的要求。

4.2.4 安全专业知识

应符合 GB/T 42457—2023 中“SM-4：安全专业知识”的要求。
除网络安全外，培训计划还应包括 EUC 特定的安全专业知识。
注：ISO / TR 22100-4:2018 为设备制造商提供了与设备安全相关的、潜在的安全方面的指南。

4.2.5 过程范围界定

应符合 GB/T 42457—2023 中“SM-5：过程范围界定”的要求。

4.2.6 文件完整性

应符合 GB/T 42457—2023 中“SM-6：文件完整性”的要求。
使用信息应明确说明验证产品中包含的所有脚本、可执行文件和其他重要文件完整性的方法。

4.2.7 开发环境安全性

应符合 GB/T 42457—2023 中“SM-7：开发环境安全性”的要求。

4.2.8 私钥控制

应符合 GB/T 42457—2023 中“SM-8：私钥控制”的要求。

4.2.9 外部提供组件的安全需求

应符合 GB/T 42457—2023 中“SM-9：外部提供组件的安全需求”的要求。
使用信息应明确说明需要识别和管理在产品中使用的所有由外部提供的组件的安全风险。

4.2.10 来自第三方供应商定制开发的组件

应符合 GB/T 42457—2023 中“SM-10：来自第三方供应商定制开发的组件”的要求。

4.2.11 评估和解决安全相关的问题

应符合 GB/T 42457—2023 中“SM-11：评估和解决安全相关的问题”的要求。

4.2.12 过程验证

应符合 GB/T 42457—2023 中“SM-12：过程验证”的要求。

4.2.13 持续改进

应符合 GB/T 42457—2023 中“SM-13：持续改进”的要求。

4.3 安全需求规范

4.3.1 产品安全上下文

应符合 GB/T 42457—2023 中“SR-1：产品安全上下文”的要求。
使用信息应明确说明对 EUC 使用的假设。

4.3.2 威胁模型

应符合 GB/T 42457—2023 中“SR-2：威胁模型”的要求。
威胁模型应考虑 EUC 的全生命周期。

4.3.3 产品安全需求

应符合 GB/T 42457—2023 中“SR-3：产品安全需求”的要求。

4.3.4 产品安全需求内容

应符合 GB/T 42457—2023 中“SR-4：产品安全需求内容”的要求。

4.3.5 安全需求审查

应符合 GB/T 42457—2023 中“SR-5：安全需求审查”的要求。

4.4 安全设计

4.4.1 安全设计原则

应符合 GB/T 42457—2023 中“SD-1：安全设计原则”的要求。

4.4.2 纵深防御设计

应符合 GB/T 42457—2023 中“SD-2：纵深防御设计”的要求。

4.4.3 安全设计审查

应符合 GB/T 42457—2023 中“SD-3：安全设计审查”的要求。

4.4.4 安全设计最佳实践

应符合 GB/T 42457—2023 中“SD-4：安全设计最佳实践”的要求。

4.5 安全实施

4.5.1 安全实施审查

应符合 GB/T 42457—2023 中“SI-1：安全实施审查”的要求。

4.5.2 安全编码标准

应符合 GB/T 42457—2023 中“SI-2：安全编码标准”的要求。

4.6 安全验证和确认测试

4.6.1 安全需求测试

应符合 GB/T 42457—2023 中“SVV-1：安全需求测试”的要求。

4.6.2 威胁缓解措施测试

应符合 GB/T 42457—2023 中“SVV-2：威胁缓解措施测试”的要求。

4.6.3 脆弱性测试

应符合 GB/T 42457—2023 中“SVV-3：脆弱性测试”的要求。

4.6.4 渗透测试

应符合 GB/T 42457—2023 中“SVV-4：渗透测试”的要求。

4.6.5 测试人员的独立性

应符合 GB/T 42457—2023 中“SVV-5：测试人员的独立性”的要求。

4.7 安全相关问题管理

4.7.1 接收安全相关问题的通知

应符合 GB/T 42457—2023 中“DM-1：接收安全相关问题的通知”的要求。
使用信息应明确说明报告安全相关问题的方法。

4.7.2 安全相关问题的审查

应符合 GB/T 42457—2023 中“DM-2：安全相关问题的审查”的要求。

4.7.3 评估安全相关问题

应符合 GB/T 42457—2023 中“DM-3：评估安全相关问题”的要求。

4.7.4 解决安全相关的问题

应符合 GB/T 42457—2023 中“DM-4：解决安全相关的问题”的要求。
使用信息应明确说明需要解决 EUC 全生命周期内与安全相关的问题。

4.7.5 披露安全相关的问题

应符合 GB/T 42457—2023 中“DM-5，披露安全相关的问题”的要求。

4.7.6 定期审查安全缺陷管理实践

应符合 GB/T 42457—2023 中“DM-6：定期审查安全缺陷管理实践”的要求。

4.8 安全更新管理

4.8.1 安全更新合格条件

应符合 GB/T 42457—2023 中“SUM-1：安全更新合格条件”的要求。

4.8.2 安全更新文档

应符合 GB/T 42457—2023 中“SUM-2：安全更新文档”的要求。
使用信息应明确说明获取安全信息更新的方法。

4.8.3 依赖组件或操作系统安全更新文档

应符合 GB/T 42457—2023 中“SUM-3：依赖组件或操作系统安全更新文档”的要求。

4.8.4 安全更新交付

应符合 GB/T 42457—2023 中“SUM-4：安全更新交付”的要求。
使用信息应明确说明验证安全补丁真实性的方法。

4.8.5 安全补丁的及时交付

应符合 GB/T 42457—2023 中“SUM-5：安全补丁的及时交付”的要求。
使用信息应明确说明及时应用安全补丁的方法。

4.9 安全导则

4.9.1 产品纵深防御

应符合 GB/T 42457—2023 中“SG-1：产品纵深防御”的要求。
使用信息应在必要的范围内提供纵深防御策略的概述，以保持 EUC 的安全。

4.9.2 环境中可预期的纵深防御措施

应符合 GB/T 42457—2023 中“SG-2：环境中可预期的纵深防御措施”的要求。
使用信息应明确说明 EUC 的使用条件，以实现和保持 EUC 的安全。

4.9.3 安全加固指南

应符合 GB/T 42457—2023 中“SG-3：安全加固指南”的要求。
使用信息应包括在安装和维修期间加固 EUC 安全的指南。

4.9.4 安全废弃指南

应符合 GB/T 42457—2023 中“SG-4：安全废弃指南”的要求。
使用信息应包括用于停止使用 EUC 的网络安全指南。

4.9.5 安全操作指南

应符合 GB/T 42457—2023 中“SG-5：安全操作指南”的要求。
使用信息应包括用于操作 EUC 的网络安全指南。

4.9.6 账户管理指南

应符合 GB/T 42457—2023 中“SG-6：账户管理指南”的要求。
使用信息应记录操作 EUC 所需的管理账户、权限和特权。

4.9.7 文档审查

应符合 GB/T 42457—2023 中“SG-7：文档审查”的要求。

5 安全要求

5.1 通则

GB/T 35673—2017 和 GB/T 42456—2023 构成本文件中规定的安全要求的基础。

5.2 基本要求

GB/T 40211—2021 定义了七个基本要求（FRs），这些要求应适用于 5.3 至 5.6 中定义的 EUC 功能。

5.3 EUC 功能域

在本文件范围内，EUC 的功能划分为“安全”域、“基本”域和“报警”域。不属于上述域的功能应归为“其他”域。域的描述见表 1。

表 1 EUC 功能域

域	描述	功能示例
安全	SIL 等级的控制功能。	— 满足 SIL 等级的电气安全装置和电气保护装置 — 满足 SIL 等级的电机和制动器控制功能
基本	确保电梯、自动扶梯和自动人行道可用性的功能或能力，其符合安全规范，但不属于安全或报警功能域。	电梯： — 正常控制 — 轿厢和层站呼梯装置 — 访问控制 — 节能（轿厢照明、通风等） — 轿厢和层站指示器 — 驱动主机控制 — 门控制，包括其保护装置 — 负载控制 — 运转时间限制器 — 消防服务操作 — 电梯恢复正常运行 — 重开门 — 远程监视和交互 自动扶梯和自动人行道： — 启动和停止功能

域	描述	功能示例
		— 时间表和系统时钟操作 — 方向指示器 — 在超过允许制动距离时，防止启动 — 电机保护 — 自动运行：按预定方向启动 — 远程监视和交互
报警	用于在乘客被困情况下验证被困状态、呼救和救援的设备。	— 报警装置、对讲装置和视频设备 — 应急电源 — 疏散装置 — 用于救援的显示和语音装置
其他	与安全、基本或报警域无关的附加功能。	— 广告显示 — 音乐和游戏设备 — 其他应用

5.4 EUC 信息安全等级要求

每个 EUC 功能域应具有表 2 中规定的最低目标安全等级（SL-T）。SL-T 的要求被定义为 SL 矢量，并为 7 个 FR 中的每一个指定单独的 SL。

注 1：本文件未定义“其他”域的 SL-T。

使用信息应通过文档说明达到表 2 中定义的最低目标安全等级（SL-T）的方法。

注 2：信息安全等级矢量方法参见 GB/T 35673—2017 附录 A 中。

如果 EUC 的功能或组件是具有不同信息安全等级矢量的功能的一部分，则应采用其中最高信息安全等级矢量。

EUC 与外部系统和服务的接口以及 EUC 内部的服务功能应至少具有与之相关的报警、基本或安全功能的信息安全等级矢量。表 1 中的“其他”域的信息安全等级矢量在本文件中没有定义。将安全需求扩展到“其他”域的示例参见附录 D。

表 2 EUC 功能域的信息安全等级矢量

基本要求（FR）	信息安全等级（SL）		
	报警	基本	安全
FR 1 – 标识和鉴别控制	1	2	3
FR 2 – 使用控制	1	2	2
FR 3 – 系统完整性	1	2	2
FR 4 – 数据保密性	1	2	2
FR 5 – 受限的数据流	1	1	1
FR 6 – 对事件的及时响应	1	1	1
FR 7 – 资源可用性	1	2	2

注 3：表 2 可用 GB/T 35673—2017, A.3.3 中描述的矢量格式表示，如：SL-T（基本）={2 2 2 2 1 1 2}。

5.5 安全控制和对抗措施选择

在选择了 EUC 功能域和表 2 中相应的信息安全等级矢量后，应根据需要从 GB/T 35673—2017 和 GB/T 42456—2023 中选择安全控制和对抗措施。但是，如果仅通过表 2 不能充分缓解 4.3.2 中要求的威胁模型，则应通过其他的安全控制和对抗措施来缓解剩余的威胁。

注 1：GB/T 35673—2017 描述了适用于所考虑的整个系统的系统要求和增强要求（REs）。

注 2：GB/T 42456—2023 描述了适用于系统组件的组件要求和增强要求（REs）。对于软件应用要求（SARs）、嵌入式设备要求（EDRs）、主机设备要求（HDRs）和网络设备要求（NDRs），还有特定的规定。

5.6 通用安全约束

5.6.1 通则

在实施系统要求和组件要求时，应符合 5.6.2 至 5.6.5 规定的通用组件安全约束（CCSCs）。

5.6.2 基本功能支持

应符合 GB/T 42456—2023 中“CCSC 1：基本功能的支持”的要求。

对于电梯、自动扶梯和自动人行道，CCSC 1 所述的基本功能包括 5.3 所示的安全、基本和报警功能。

GB/T 7588.1—2020 要求的报警功能的可用性应优先于保密性。

GB/T 7588.1—2020 要求的用于报警功能的控制系统网络在 GB/T 35673—2017 中被定义为关键控制系统网络。

5.6.3 补偿对抗措施

应符合 GB/T 42456—2023 中“CCSC 2：补偿对抗措施”的要求。

注：特定补偿对策示例参见 A.3.9。

5.6.4 最小权限

应符合 GB/T 42456—2023 中“CCSC 3：最小权限”的要求。

5.6.5 软件开发过程

应符合 GB/T 42456—2023 中“CCSC 4：软件开发过程”的要求。

6 使用信息

使用信息的目的是向 EUC 所有者、维修者和其他利益相关者提供有助于在 EUC 的安装场所实现和维护 EUC 安全的信息。

使用信息应说明如何集成、配置和维护 EUC 的安全。使用信息还应包括目标安全等级和必要的指南，以评估和保持已达到的信息安全等级。

使用信息应说明不同利益相关者的角色，包括生命周期中潜在的变更和所需的知识传播，例如变更维修供应商。

使用信息应列出并解释 EUC 系统中存在的所有安全配置选项，并记录它们的默认和可选设置。

如果 EUC 依赖外部系统或服务来实现和维护目标安全等级，则使用信息应定义适用于这些外部系统和服务的必要要求。

使用信息应包含报告安全脆弱性的规程，其方式不会对使用类似组件的其他装置造成风险，例如使

用电子邮件并通过密钥加密消息内容。

表 3 总结了除上述内容之外的对使用信息的要求。

注：关于不同利益相关方在整个生命周期内的合作与协调，参见 ISO/TR 22100- 4:2018。

表 3 使用信息的要求总结

本文件中的条款	参考	对使用信息的要求
4.2.6	GB/T 42457—2023 中的“SM-6：文件完整性”	使用信息应明确说明验证产品中包含的所有脚本、可执行文件和其他重要文件完整性的方法。
4.2.9	GB/T 42457—2023 中的“SM-9：外部提供组件的安全需求”	使用信息应明确说明需要识别和管理在产品中使用的所有由外部提供的组件的安全风险。
4.3.1	GB/T 42457—2023 中的“SR-1：产品安全上下文”	使用信息应明确说明对 EUC 使用的假设。
4.7.1	GB/T 42457—2023 中的“DM-1：接收安全相关问题的通知”	使用信息应明确说明报告安全相关问题的方法。
4.7.4	GB/T 42457—2023 中的“DM-4：解决安全相关的问题”	使用信息应明确说明需要解决 EUC 全生命周期内与安全相关的问题。
4.8.2	GB/T 42457—2023 中的“SUM-2：安全更新文档”	使用信息应明确说明获取安全信息更新的方法。
4.8.4	GB/T 42457—2023 中的“SUM-4：安全更新交付”	使用信息应明确说明验证安全补丁真实性的方法。
4.8.5	GB/T 42457—2023 中的“SUM-5：安全补丁的及时交付”	使用信息应明确说明及时应用安全补丁的方法。
4.9.1	GB/T 42457—2023 中的“SG-1：产品纵深防御”	使用信息应在必要的范围内提供纵深防御策略的概述，以保持 EUC 的安全性。
4.9.2	GB/T 42457—2023 中的“SG-2：环境中可预期的纵深防御措施”	使用信息应明确说明 EUC 的使用条件，以实现和保持 EUC 的安全。
4.9.3	GB/T 42457—2023 中的“SG-3：安全加固指南”	使用信息应包括在安装和维修期间加固 EUC 安全的指南。
4.9.4	GB/T 42457—2023 中的“SG-4：安全废弃指南”	使用信息应包括用于停止使用 EUC 的网络安全指南。
4.9.5	GB/T 42457—2023 中的“SG-5：安全操作指南”	使用信息应包括用于操作 EUC 的网络安全指南。
4.9.6	GB/T 42457—2023 中的“SG-6：账户管理指南”	使用信息应记录操作 EUC 所需的管理账户、权限和特权。

附 录 A
（资料性）
电梯、自动扶梯和自动人行道安全开发生命周期的附加信息

A.1 通则

网络安全的基本原则是拥有成熟的网络安全过程生命周期。这个生命周期需要包括足够的培训、工具、资源和过程，以加固和维护 EUC，提高其抵御网络攻击的能力。

推荐的网络安全过程生命周期实践见表 C.1 所示。

A.2 安全管理

A.2.1 过程范围

了解设备类型以及要部署设备的环境是很重要的。根据相关要求，为集成到 EUC 而开发的组件可能不包含外部连接，和/或物理隔离。但是，有些组件可能有外部连接，其不作为主要功能的要求，而是作为其操作的增强（如向服务系统提供数据或接受软件更新）。因此，重要的是要有一个健壮的过程来分析组件和/或对组件进行建模，并进行审查，以确定本文件的要求是否适用于该组件。

A.2.2 安全开发文档

表 A.1 列出了在安全开发生命周期中产生的典型文档。

表 A.1 典型的安全开发生命周期文档

文档	描述	本文件中的条款
威胁建模和风险评估	识别残余风险的威胁模型。	4.3.2
安全需求和安全设计	设计文档明确了每个安全需求和相关的安全控制。	4.3、4.4
安全测试计划	测试计划列出了如何测试每个安全控制，以确保其满足安全需求。	4.6.1
分析报告	报告总结了所执行的分析结果，并重点指出了发现的任何问题和不充分的安全控制。例如： —第三方代码/库分析报告； —动态安全分析报告； —静态代码分析报告。	4.5.1
测试报告	—模糊测试报告； —内部渗透测试报告； —外部渗透测试报告。	4.6.1—4.6.5
使用信息	见第 6 章。	第 6 章
事故响应计划	记录了在发生事件时结构化应对的规程，包括了有详细联系方式的责任人、负责人、被咨询人和被通知人（RACI）矩阵。	4.8

A.3 安全需求规范

A.3.1 通则

为 EUC 定义足够的安全需求是很重要的。这一过程包括识别和管理现有的风险，定义可容忍的风险等级，并形成安全需求文档。可采用以下过程：

——确定威胁建模的方法；

——识别和界定 EUC；

——识别 EUC 的特定资产；

——识别相关攻击者类型；

——识别危及已识别资产的威胁；

——识别个别风险事件；

——评估个别风险事件；

——创建安全要求；

——重复评估个别风险事件。

每个步骤的细节见 4.3.1 至 4.3.5，也参见附录 B。

A.3.2 威胁建模方法

建立威胁模型有助于识别 EUC 的资产。可采用不同的威胁建模方法：

——以攻击者为中心；

——以系统为中心；

——以资产为中心。

注：根据所选择的方法，使用了不同的起点，但如果操作正确，最终都会得出相同的结果。

A.3.3 识别 EUC 的具体资产

图 A.1 和图 A.2 给出了定义 EUC 资产的例子。图 A.1 和图 A.2 显示了 EUC 在使用环境中被划分为不同的资产，例如：安全功能。这些资产可以包括多个子资产，例如：音频连接和呼救功能是报警功能的两个子资产。

当 EUC 连接到外部系统时，EUC 接口需满足相应的信息安全等级要求。例如：用于报警功能的接口满足报警功能的信息安全等级。

根据设计的不同，资产可以被分组到不同的区，并通过管道相连。附录 D 给出了区和管道的应用指南。

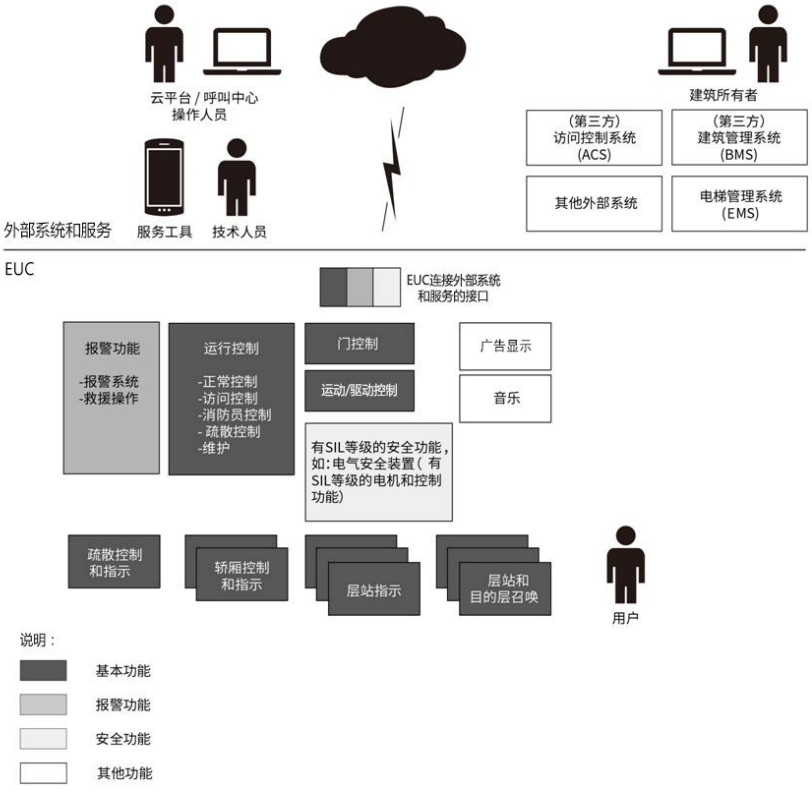

图 A.1 一个电梯系统资产的例子

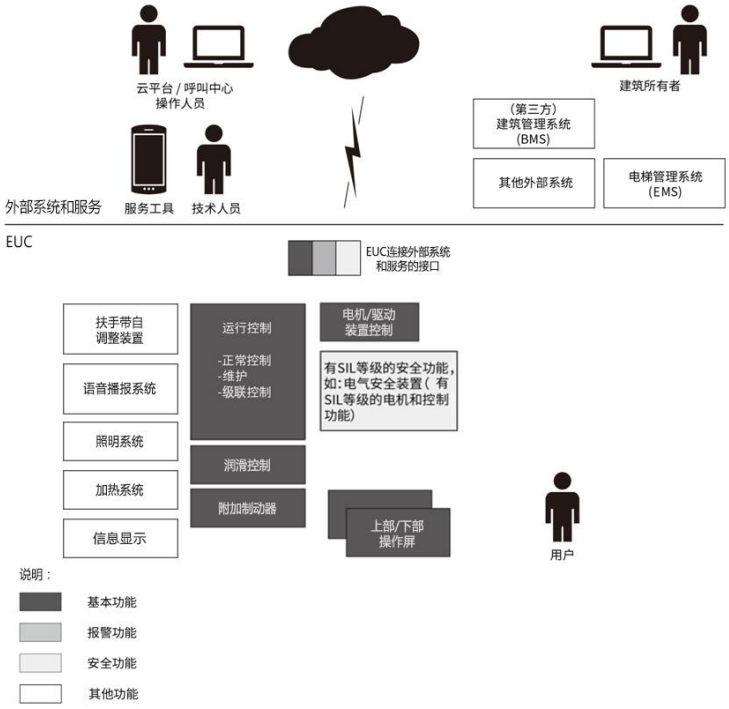

图 A.2 一个自动扶梯系统资产的例子

A.3.4 识别相关的攻击者类型

威胁模型和风险分析从识别相关的攻击者类型开始。

攻击者可以是通过恶意活动对资产实施破坏、暴露、更改、禁用、窃取、获取未经授权的访问或进行未经授权使用的个人或组织。这些攻击者从脚本小子、黑客主义者到网络犯罪分子和国家支持的攻击者，每个攻击者在能力、意图/动机和实施攻击的资源上都有所不同。

攻击者也可能是内部人员，例如：EUC 开发人员。

攻击向量的处理可能很复杂。根据攻击者和攻击的类型，实施攻击所需的活动范围可以从简单的侦察，包括识别和利用目标的一个被公开知晓的弱点，到蓄意尝试提取信息（即社会工程），以及更复杂和更有计划的活动，包括渗透到制造供应链和产品开发中。

本文件考虑了典型的攻击者。如果拥有巨大资源的攻击者（如有国家支持或是有大笔预算）与此相关，则进行专门的风险分析。

第五章中规定的网络安全要求是最低的。专业的建筑物、构筑物或特殊用途如政府设施、重症监护设施，可能需要考虑这些设施的应用场景，以确定是否需要更高的网络安全等级或与互联网完全隔离。例如：采取防护措施以防范可能导致电梯服务被拒绝的网络威胁。网络安全风险（威胁）评估指南见 GB/T 35673—2017 中的 4.2 的注。

攻击者对 EUC 的可访问性是另一个重要的方面。远程实施的攻击是传统网络攻击的主要来源。然而，也存在利用短距离无线通信（如 WLAN 和蓝牙），以及那些需要物理访问 EUC（如通过 JTAG 端口访问）的网络攻击。

A.3.5 个别风险事件识别

通过识别每个可评估的已定义资产的单个风险事件来定义第 4.3.2 条所述的威胁会如何发生。在此步骤中，定义 EUC 可接受的风险水平。在评估可接受的风险水平时，考虑资产清单以及对资产的影响。

A.3.6 评估个别风险事件

通过执行风险评估来评估先前识别的风险事件。风险评估是一个迭代过程，有时在 EUC 的开发阶段会重复多次。风险评估随着 EUC 设计的进展而成熟。至少在 EUC 或威胁现状的每次重大变化时重复风险评估。因此，需要记录可再现的结果。在编制文档时，可以使用以下问题：

——如何进行风险评估；

——做了哪些假设；

——可接受的风险水平。

初始风险评估在没有采取应对措施的假设下进行。在进行初始风险评估时，考虑以下几点：

——风险事件发生的可能性通常由发起攻击的意图/动机、必要的技能和资源以及发起攻击对受保护资产产生影响的概率组成；

——风险事件的发生可能会对一种或多种风险类型产生影响；

——将可能性和一个或多个已确定的严重程度相结合，以获得未降低的风险等级；

——将确定的风险等级与可接受的风险等级进行比较；

——如果确定的风险等级高于可接受的等级，则定义安全要求以管理此风险事件。

A.3.7 创建安全要求

在初始风险评估之后，选择有意义的对抗措施以降低评估出的超过先前定义的可接受风险等级的风险。定义对策时的最佳实践是被称为“纵深防御”的方法。对抗措施不依赖于单一防线，而利用多层防护。如果一条防线被打破，资产仍至少由另一层防线进行防御。补偿对抗措施，如物理访问控制或检测控制，也可用于满足一个或多个安全要求。

A.3.8 重复评估个别风险事件

使用选定的对抗措施重复初始风险评估。重复此过程，直到剩余风险低于可接受的风险。

A.3.9 补偿对抗措施应用实例

A.3.9.1 可能的措施

EUC 采用的标准中定义的措施可用于 4.3.2 中要求的威胁模型。此类措施包括但不限于：

——物理访问限制：

——授权人员的进入（见 GB/T 7588.1—2020 中的 5.2.2.1）；

——紧急开锁装置（见 GB/T 7588.1—2020 中的 5.3.9.3 和 5.12.1.5.2.2）；

——上锁的机器柜或检修门（见 GB/T 7588.1—2020 中的 5.2.6.4.3.4、5.2.6.4.4.1 和 5.12.1.5.2.2）；

——单向或有限的连接：

——与电气安全装置并联（见 GB/T 7588.1—2020 中的 5.11.2.1.2）；

——通过用途受限和带宽受限的连接装置连接的轿厢控制和指示以及层站指示；

——系统完整性：

——远程报警系统的可靠性符合 GB/T 24475（见 GB/T 7588.1—2020 中的 5.12.3）。

在威胁分析中确定补偿对抗措施缓解的充分性。按照第 4 章中的安全开发生命周期记录假设和结论。

以下示例说明了如何应用 5.6.3 中定义的补偿对抗措施。

A.3.9.2 远程报警系统电话号码

按照 GB/T 7588.1 设计的电梯需要配置远程报警系统。这通常包括与救援服务的电话连接（见 GB/T 7588.1—2020 中的 5.12.3.1）。为了建立此连接，需要定义救援服务的电话号码。

允许不受控制的访问来更改报警电话号码对于实现 SL1 是不可接受的。

如果修改此类电话号码需要进入井道、机房和滑轮间，或者上锁的控制柜，而只有授权人员才能够进入，那么这种修改电话号码的方式就能达到 FR 1（识别和鉴别控制）的 SL1。

如果可以通过在井道、机房和滑轮间，或者上锁的控制柜之外的通讯修改电话号码，则需要采取额外措施才能达到 SL1。

在井道、机房和滑轮间，或者上锁的控制柜的范围内的通讯，这一类对抗措施可适用。

此外，如果在三天内能检测到电话号码的错误修改（见 GB/T 24475 中的 4.2.1），就能达到 FR 3（系统完整性）的 SL1。

A.3.9.3 读取安全回路状态

按照 GB/T 7588.1 设计的电梯有安全回路。对于电梯的操作，控制系统通常会连接到安全回路，以读取其不同位置的状态。

为了实现 SL2，不允许不受限制的电气连接直接连到安全回路。

GB/T 7588.1—2020 中的 5.11.2.1.2 允许使用特定方法进行连接。这种方法可确保即使连接到安全回路的控制系统发生失效或故障，也能保持安全回路的完整性。这些方法可能用到的技术可以在 GB/T 7588.2 中 5.15 中找到。这就能让读取安全回路状态的功能达到 FR 3（系统完整性）的 SL2。

另一方面，GB/T 7588.2 中的 5.15 中的方法不限制信息流，因此不是符合 FR 4（数据保密性）的技术措施。

A.3.9.4 固件升级

安全更新 EUC 软件或固件的能力是一项重要功能，与所有 EUC 功能域相关。执行远程更新功能的方式是考虑风险的一个关键方面。例如，如果 EUC 软件或固件更新功能允许通过开放互联网进行，而不是需要物理访问来执行或触发更新，则 EUC 功能域的网络风险会大大增加。补偿对抗措施（如控制柜上锁）可进一步降低风险，因此可用于替代支持不同信息安全等级对应的安全要求所需的等效安全控

制。

A.3.9.5 EUC 集成到更大的系统

对建筑物的风险评估有时表明需要比本文件中为典型电梯定义的信息安全等级更高的安全等级。例如，对保密性或可用性的要求可能会更高。

如果建筑物采取对抗措施，典型的电梯仍然可能达到更高的安全水平。例如，该建筑物可以提供现场人员长期驻场的救援服务，可以在电梯和现场救援服务之间安装报警装置，以确保建筑安全所要求的保密性。

A.3.10 识别危及已识别资产的威胁

威胁分为故意和意外。

EUC 面临的安全威胁包括但不限于：

——由于软件错误而导致的脆弱性被利用；

——恶意软件，例如：通过网络、可移动介质（如 U 盘）和临时连接（如服务工具）传播的蠕虫和病毒；

——未经授权的访问；

——员工或他人未经授权的行为；

——员工的无意行为；

——拒绝服务攻击；

——蓄意破坏/故意破坏。

A.4 安全设计

在设计产品时，重要的是使用过程来确保产品安全设计。

设计阶段的目标是系统架构的开发。在此阶段，将做出所有有关概要设计选择和关键组件使用的决策。此外，在系统架构的开发过程中，将产品的完整功能概括到必要的程度，以实现适合所需功能的系统架构。例如，这个框架可以包括所涉及的实体、产生的数据流以及已经分配的重要的安全或非安全属性。

由于在设计阶段所做的选择影响深远，因此这个阶段特别容易引入安全脆弱性。开发的系统架构中的缺陷可能会直接或间接地导致脆弱性，这些脆弱性在概要阶段是难以识别的，因为脆弱性可能隐藏很深或者仅能在详细设计阶段被识别出来。在设计阶段尽早识别需解决的安全问题是最有效的。如果安全缺陷只能在后期发现，如在测试或投入运行期间，那么处理他们就会变得越来越复杂和昂贵。因此，在设计阶段尝试检测脆弱性，并使用行业标准最佳实践来减少暴露的攻击面是非常重要的。

最佳实践包括：

——最小权限原则，意味着通过设计使过程或用户不会拥有超过完成任务所需的权限；

——攻击面识别和最小化；

——模块化设计方法，以减少安全威胁的影响；

——纵深防御，意味着不通过单一措施，而通过一组分层措施来降低风险，即使其中一项单独的措施失效了，这组措施仍有效；

——将用户、接口系统或任务的访问权限限制为各自功能所需的数据；

——优先选择简单的、经过验证的概念或组件，而不是那些过于复杂的、专有的或测试不充分的概念或组件；

——定期进行安全设计审查，以检测当前设计尚未解决的安全要求，并检查系统的当前体系架构是否符合最佳实践。

有关安全最佳实践的更多信息，参见参考文献中的[10]~[18]。

A.5 安全实施

A.5.1 实施活动和审查

安全实施是指确保安全开发产品的过程和指南。EUC 的供应商被要求建立这样的过程和指南，如GB/T 42457—2023 实践 4 中的“SI-1：安全实施审查”和“SI-2：安全编码标准”。

与安全实施相关的主要属性至少包括：

——安全编码指南的使用；

——静态分析工具的使用；

——关键功能的单元测试；

——第三方和开源软件分析。

除了针对不同编程语言的良好编码实践之外，指南还需列出不推荐使用有潜在可被利用风险的编码结构或设计，这些实践来自实例。指南通常还包含一个禁用/弃用函数列表。

至少满足以下条件的代码需使用静态代码分析工具来分析：

——监听或连接到设备、系统或应用程序可信区之外网络的代码；

——先前已识别出脆弱性的代码；

——以高级权限执行的代码（例如：系统、管理员、根）；

——安全相关代码模块（例如：认证、授权、密码、防火墙代码等）；

——从外部源解析数据结构的代码；

——从外部源获取的代码；

——用于配置访问控制、处理加密密钥或密码的设置代码。

所有由静态分析工具识别的违反编码标准的风险都需修复，除非可以证明风险是不相关的。

最佳实践是在开发过程中进行持续的源代码分析，而不是在代码开发阶段结束时进行。当开发人员更新代码时，可以自动分析代码是否存在可能的安全问题。

A.5.2 系统组件的集成

电梯、自动扶梯和自动人行道均被设计成系统来运行。EUC 系统制造商和/或安装公司可能将多个组件集成为系统的一部分。因此，重要的是要考虑在系统集成中如何指定上下文中的组件，以便获得需求、实施设计和验证安全措施。

作为组件设计实施的一部分，制造商提供文档来规定组件开发人员和系统集成商之间的职责。组件的安全使用条件需记录在案。

作为系统实施的一部分，集成商遵循组件制造商确定的安全要求。

记录组件在系统中应用时所期望的条件。

记录确保安全性（如密钥或证书管理）的过程等级要求。

组件假设作为系统集成设计中的安全要求考虑（这可能是必要的，以确保组件声明的安全是完整的）。

例如：为了实现特定的 SL，组件可能需要在系统级别实现特定的安全要求。

A.6 安全确认

A.6.1 通则

除了作为产品开发一部分的正常测试和确认过程之外，网络安全验证和测试计划也是产品验证阶段正式化过程的一部分。A.6.2 至 A.6.6 中的与安全相关的关键活动是重要的。

A.6.2 动态分析

需要对应用程序执行动态分析，以识别任何内存损坏、资源竞争、用户特权问题和任何其他关键安全问题。

A.6.3 模糊测试

对于所有处理来自安全区域或组件外部数据的组件，需进行模糊测试。

创建一个模糊测试计划，记录将要进行的模糊测试。该计划包括将进行模糊测试的所有组件的列表、如何进行模糊测试的描述、智能模糊测试或非智能模糊测试的选择，以及测试通过/失败的标准。

A.6.4 渗透测试

除了使用模糊测试工具外，还建议在测试期间使用各种渗透测试工具。测试计划包含与使用渗透测试工具相关的特定项目。

需要定期考虑独立的（第三方）渗透测试。

A.6.5 验证威胁建模结果的对策是否正确实施

对所有组件进行滥用用例测试和已知脆弱性测试，在测试中尝试利用威胁模型中确定的所有已缓解的威胁。

识别在威胁建模过程中未捕获的任何攻击面。记录研究结果。

通过测试验证已实施的安全应对措施的有效性，并根据测试结果更新风险评估结果。

A.6.6 独立的第三方分析

根据制造商的网络安全过程和技术成熟度，进行独立的第三方安全脆弱性分析和渗透测试。特别建议在目标安全等级为 2 或更高的区和管道中使用。或者，使用红蓝攻防演练的测试方法，以验证整个系统的安全性。参见参考文献[12]。

A.7 产品生命周期内的安全管理

A.7.1 安全相关问题的管理

虽然解决测试过程中出现的脆弱性是安全开发过程的一部分，但也需要解决制造商或任何外部组织（例如产品用户或安全研究人员）在产品安装后发现的任何其他安全问题或脆弱性。这从收集威胁情报或者提供从内部和外部接收安全问题信息途径的过程开始。最佳实践建议通过定义良好的过程对这些安全问题或脆弱性进行审查、解决和跟踪，直至结束。这个过程通常包括分析和验证阶段、影响评估、必要时对客户的通知、开发更新和发布。

在不同的装置中使用的硬件和软件的清单、安装环境的假设或细节、任何特殊配置等都有助于有效地验证问题以及更好地进行影响评估。检查并理解潜在影响，以支持决策与如何通知和解决问题相关。在此基础上，进一步确定通过更新、更换或使用补偿控制来解决问题。建议产品制造商和集成商保持书面规程，概述事件响应过程的不同方面。

有关更多指南，参考 GB/T 42457—2023（DM1-DM6）和其他来源。

注：事件应急响应和安全团队（FIRST）。将产品事件应急响应团队（PSIRT）和计算机事件应急响应团队（CSIRT）定义为制造商和维保商的两种良好实践，以涵盖其产品交付时的两个事件响应计划。

A.7.2 安全更新管理

A.7.2.1 通则

一旦系统能够跟踪、发现和接收潜在的脆弱性，设备制造商就有责任制定有效的安全更新流程。制造商验证该脆弱性的存在，并根据设备的预期使用情况来评估对 EUC 使用者的潜在安全风险。此

外，设备制造商制定相关流程，以便告知 EUC 所有者其已安装产品的安全脆弱性以及解决这些问题的说明。由于 EUC 所有者并非总是设备服务提供商，EUC 制造商向 EUC 服务提供商提供补丁或修复方法。制造商、服务提供商和 EUC 所有者的角色见表 A.2。

表 A.2 安全文档

GB/T 42457—2023 实践 7		制造商/集成商	EUC 所有者/服务提供商
SUM-1	安全更新合格资格	执行	/
SUM-2	安全更新文档	传递	采取行动
SUM-3	依赖组件或操作系统安全更新文档	传递	采取行动
SUM-4	安全更新交付	传递	采取行动
SUM-5	安全补丁的及时交付	执行	/
A.7.2.2	检查对影响大的情节的安全更新的实施	执行	采取行动

A.7.2.2 检查安全补丁

如果由产品风险分析确定的安全脆弱性影响很大，则制造商需确保与客户进行后续沟通，以验证该安全脆弱性是否已被修复。

A.7.2.3 关于电梯、自动扶梯和自动人行道交付安全补丁的注意事项

提供安全补丁更新时，重要的是遵守适用的电梯、自动扶梯和自动人行道的标准要求。系统中的组件类型及其功能可能导致无法自动提供安全更新。在这种情况下，需提供替代方法以确保可以更新应用，例如使用可用的服务设备下载和应用补丁的说明，在安全的物理设备中传输软件，或用包含安全补丁的组件替换有安全脆弱性的组件。

A.8 退役行动

制造商和/或系统提供商还需考虑如何处理电梯、自动扶梯和自动人行道系统的退役，因为敏感信息可能存储在某些组件上（例如：ID、凭证、参数集、证书），如果这些信息被泄露，可能会被恶意使用或被洞察资产和其他相关资产的情况。从物理上删除信息或销毁资产是必要的。资产的退役需反映在资产清单中。

附 录 B
（资料性）
如何应用风险评估的一般方法的附加信息

B.1 安全风险评估的附加信息

本附录提供了关于如何应用附录 A 中定义的风险评估的一般方法的附加信息。

在处理特定产品时，考虑以下几点：

——通过附加风险来扩展风险评估（因此可能需要额外的对抗措施）；

——通过额外资产扩展风险评估（因此可能有额外的风险）；

——修改本文件中假定的功能分组；

——如果给定的要求不适用，或可以证明在某种风险情况下不需要满足这些要求，则可以与给定的要求有差异。

在本文件发布时，尚未有专门针对电梯、自动扶梯和自动人行道的安全方法、威胁目录和最佳实践，且经证实的在用生态系统，因此本附录旨在提供行业特定的指南。

在评估电梯、自动扶梯和自动人行道的安全风险时，考虑以下要点：

——虽然表 2 中规定了最低安全要求，但在其他情况下，可接受的风险等级需与利益相关者达成一致。这个等级取决于法律方面、组织、EUC 的预期使用情况和（当地）社会价值。

——对比 GB/T 20900 等功能安全标准的风险评估，宜考虑多个行业特定的信息安全风险影响维度。表 B.1 给出了一个可能的系统风险类型的示例。

——建议创建一个风险评级系统，用于比较不同类型的风险。

——在安全风险评估中，通常无法对风险概率进行定量评估。使用一种定性的方法来代替。表 B.2 给出了基于对手能力和意图以及系统脆弱性的风险概率定性评级的示例。

——每项风险降低措施都是成本（包括单位成本和工作量）与安全效益之间的权衡。因此，对不切实际的威胁的保护既不必要，在经济上也不合理。实施不必要的风险降低措施甚至可能会适得其反，例如，风险降低措施通常会对产品的可用性产生影响，如果造成合法的终端用户使用不便，可能会试图绕过或禁用它们，而且每一种风险降低措施也可能会单独引入额外的脆弱性。在任何情况下，风险事件的发生不能因疏忽而对人员造成任何伤害。

——网络安全不是功能安全的子集，因此网络安全风险评估不宜在功能安全人员的职责下进行。功能安全和网络安全是不同的领域，需要不同的方法和知识。例如，风险评估方法和必要的思维方式是根本不同的，几个核心区别如下：

——统计上可忽略不计的双重或多重故障与攻击向量之后的一系列有针对性的行动的区别；

——随机（无动机）故障与智能威胁源的区别；

——单个估计因素的可能性与通常为难以估计的多个估计因素相结合下的可能性的区别。

——一个多样化的团队有利于利用不同的经验和观点。建议至少包括具有功能安全、制造、安装和维修维护背景的人员。

——可能的威胁者会基于具体产品及其威胁现状而有显著差异。例如基于产品具体使用情形、安装地点、预期乘客以及安装环境中预期的安全措施。

表 B.1 映射不同风险维度的严重级别的示例

严重程度	风险类型		
	对安全、系统或环境的影响	对服务可用性的影响（对用户）	对信息的影响（对操作员）
1—高	死亡、系统损失或严重的环境损害	不适用	不适用
2—中	严重损伤、主要的系统或环境损害	不适用	不适用
3—低	较小的损伤或次要的系统损害	服务中断（例如：当没有其他运输工具或失去访问控制时，电梯停止服务）	数据的完整性受损（例如：电梯管理系统数据被篡改）
4—可忽略	不会引起伤害、系统或环境损害	较小的服务中断（例如：传输能力减弱）	非关键数据（例如：电梯管理系统数据）的丢失

表 B.2 概率等级的示例

概率等级	使用寿命内发生的概率	对手能力和意图与系统脆弱性的描述
A—频繁	在使用寿命内很可能经常发生	系统暴露于网络，没有实施安全控制，也没有计划；可被资源和专业知识有限的普通攻击者利用
B—很可能	在使用寿命内很可能发生数次	系统暴露于网络，实施最低限度的安全控制，效率最低；利用少的资源、专业知识和较低动机
C—偶尔	在使用寿命内很可能至少发生一次	系统暴露于网络，实施部分的安全控制，有些有效；利用适度的资源、一些 EUC 系统的特定技能和适度的动机
D—极少	未必发生，但在使用寿命内可能发生	系统暴露于网络，安全控制大多被实施并有效；利用大量的资源、EUC 系统的特定技能和较高的动机
E—不大可能	在使用寿命内很不可能发生	系统暴露于网络，安全控制得到充分实施并有效；利用非常复杂的专业知识、大量的资源、高度的动机和协作
F—几乎不可能	概率几乎为零	不考虑，安全控制或其他措施已得到充分实施、评估和起效。
注：如果系统在封闭网络中运行，或存在其他补偿对抗措施，则可认为概率更低。		

确定风险的概率和严重程度后，可将风险分组到风险矩阵中（见表 B.3 示例）。由此得出的风险等级将表明不采取行动是否可以接受，或是否需要额外的对策或缓解措施。

如 A.3.5 和 A.3.7 所述，确定应对措施后，重复进行风险评估。

表 B.3 6×4 风险矩阵的示例

概率等级	严重程度			
	1—高	2—中	3—低	4—可忽略
A—频繁	高	高	高	中
B—很可能	高	高	高	中
C—偶尔	高	高	中	低
D—极少	高	中	中	低
E—不大可能	中	中	低	低
F—几乎不可能	低	低	低	低

B.2 进一步的指南

由于没有现成的方法评估电梯、自动扶梯和自动人行道的安全风险，通用标准需与电梯的特定专业知识一起使用。

在进行安全风险评估时，以下文件可能提供有价值的输入，予以考虑：

——附录 D，区和管道的应用指南；

——IEC 62443-3-2:2020 描述了将 EUC 划分为区和管道、评估每个区和管道的风险以及为每个区和管道建立目标安全等级（SL-T）的过程；

——ISO 27005:2022 描述实施风险评估和风险处理过程所必需的一般活动，但没有规定具体的方法；

——NIST SP 800-30 描述一种成熟的风险评估方法，该方法已被各种行业完全采用或部分采用。

对于可能出现的其他威胁输入，可在列出可能的威胁、最常见的攻击类型或典型的攻击模式的多个目录中找到。这些目录保持最新状态，并由多个相关组织分发。可参考的文档包括：

——OWASP Top 10 列出了与 web 应用程序最相关的风险类型。虽然电梯是一种与 web 应用程序非常不同的产品，但所有这些风险都可能适用于电梯系统（考虑配置 GUI 或诊断接口）；

——OWASP API Top 10 包含类似的列表，特别是针对有关 API 最常见的风险类型；

——OWASP IoT Top 10 包含类似的列表，特别是针对有关 IoT 设备最常见的风险类型；

——CWE Top 25 最危险的软件弱点；

——BSI ICS 安全概要概述了工业控制系统环境中可能存在的威胁和最佳实践；

——CAPEC 提供了不同抽象层次的攻击机制和攻击模式的列表。

附 录 C
（资料性）
安全实践的列表

表 C.1 概括了第 4 章中列出的适用要求。除 GB/T 35673—2017 、GB/T 42457—2023 等标准中的相关子条款外，本文件还规定了部分子条款的附加要求，在相应子条款的最右栏中标记为“是”。

表 C.1 安全实践的列表

序号	实践	条款号	需求编号	需求名称	附加要求
1	安全管理	4.2.1	SM-1	开发过程	否
		4.2.2	SM-2	明确职责	否
		4.2.3	SM-3	明确适用性	否
		4.2.4	SM-4	安全专业知识	是
		4.2.5	SM-5	过程范围界定	否
		4.2.6	SM-6	文件完整性	是
		4.2.7	SM-7	开发环境安全性	否
		4.2.8	SM-8	私钥控制	否
		4.2.9	SM-9	外部提供组件的安全需求	是
		4.2.10	SM-10	来自第三方供应商定制开发的组件	否
		4.2.11	SM-11	评估和解决与安全相关的问题	否
		4.2.12	SM-12	过程验证	否
		4.2.13	SM-13	持续改进	否
2	安全需求规范	4.3.1	SR-1	产品安全上下文	是
		4.3.2	SR-2	威胁模型	是
		4.3.3	SR-3	产品安全需求	否
		4.3.4	SR-4	产品安全需求内容	否
		4.3.5	SR-5	安全需求审查	否
3	安全设计	4.4.1	SD-1	安全设计原则	否
		4.4.2	SD-2	纵深防御设计	否
		4.4.3	SD-3	安全设计审查	否
		4.4.4	SD-4	安全设计最佳实践	否
4	安全实施	4.5.1	SI-1	安全实施审查	否
		4.5.2	SI-2	安全编码标准	否
5	安全验证和确认测试	4.6.1	SVV-1	安全需求测试	否
		4.6.2	SVV-2	威胁缓解措施测试	否
		4.6.3	SVV-3	脆弱性测试	否
		4.6.4	SVV-4	渗透测试	否
		4.6.5	SVV-5	测试人员的独立性	否
6	安全相关问题管理	4.7.1	DM-1	接收安全相关问题的通知	是
		4.7.2	DM-2	安全相关问题的审查	否
		4.7.3	DM-3	评估安全相关问题	否
		4.7.4	DM-4	解决安全相关的问题	是
		4.7.5	DM-5	披露安全相关的问题	否
		4.7.6	DM-6	定期审查安全缺陷管理实践	否

序号	实践	条款号	需求编号	需求名称	附加要求
7	安全更新管理	4.8.1	SUM-1	安全更新合格条件	否
		4.8.2	SUM-2	安全更新文档	是
		4.8.3	SUM-3	依赖组件或操作系统安全更新文档	否
		4.8.4	SUM-4	安全更新交付	是
		4.8.5	SUM-5	安全补丁的及时交付	是
8	安全导则	4.9.1	SG-1	产品纵深防御	是
		4.9.2	SG-2	环境中可预期的纵深防御措施	是
		4.9.3	SG-3	安全加固指南	是
		4.9.4	SG-4	安全废弃指南	是
		4.9.5	SG-5	安全操作指南	是
		4.9.6	SG-6	账户管理指南	是
		4.9.7	SG-7	文档审查	否

附 录 D
（资料性）
区和管道的应用指南

区是一组网络资产，对于每个 FR，它们共享相同的信息安全等级（SL），而管道则是专门用于通信的资产组成，并为每个 FR 共享相同的信息安全等级。就本文件而言，每个区可以包括分区，管道不宜具有子管道。区和子分区可以有多个管道来相互通信。

注：有关区和管道的更多信息，参见 IEC 62443-3-2:2020。

每个 FR 的信息安全等级都是通过获取该区功能定义的每个 FR 的最高信息安全等级来定义的。

图 D.1 示例系统中 Z1 和 Z2 区内的功能，使用表 D.1 的“Z1 和 Z2”列定义的信息安全等级矢量。由于安全组件对每个 FR 具有最高的信息安全等级矢量要求，同一区的所有资产包括基本域和报警域都遵循此要求。

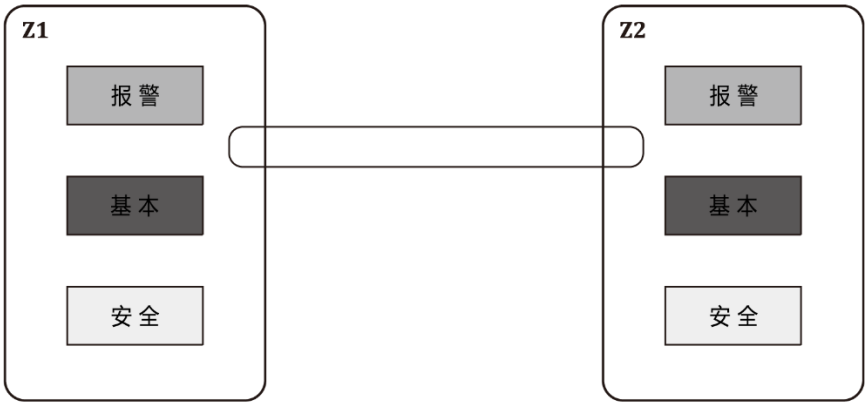

图 D.1 显示两个区和一个将之连接的管道的示例

表 D.1 图 D.1 中的系统的信息安全等级矢量示例

基本要求（FR）	信息安全等级（SL）			
	报警	基本	安全	Z1 和 Z2
FR 1—识别和鉴别控制	1	2	3	3
FR 2—使用控制	1	2	2	2
FR 3—系统完整性	1	2	2	2
FR 4—数据保密性	1	2	2	2
FR 5—受限的数据流	1	1	1	1
FR 6—对事件的及时响应	1	1	1	1
FR 7—资源可用性	1	2	2	2

同样，图 D.2 示例系统中 Z1a 和 Z2a 区内的功能，使用表 D.2 的“Z1a 和 Z2a”列定义的信息安全等级矢量。按照相同的方法，位于 Z1b 和 Z2b 区内的功能使用“Z1b 和 Z2b”列中定义的信息安全等级矢量。然而，Z1 和 Z2 区域没有最低信息安全等级要求，因为安全、基本和报警组件已经被满足相应分区信息安全等级要求的应对措施所保护。Z1b 和 Z2b 区的其他功能与报警功能共享信息安全等级矢量

要求。

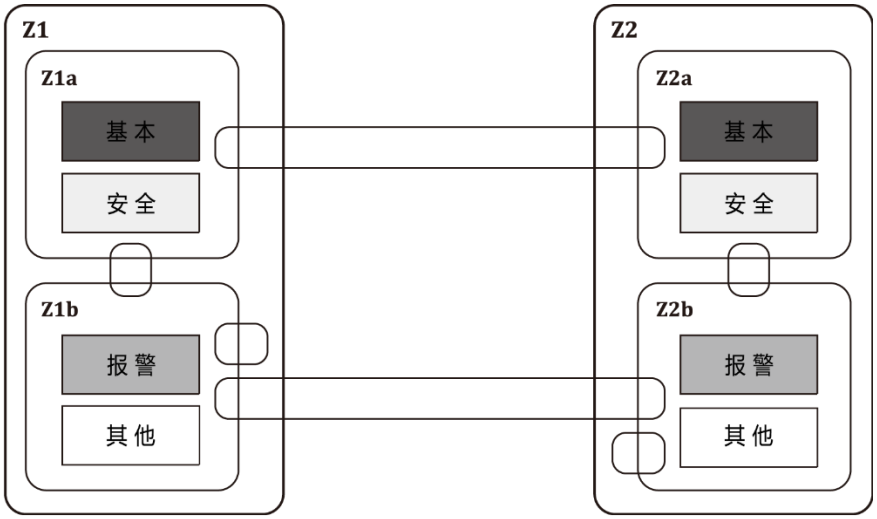

图 D.2 显示六个区域和连接管道的示例

表 D.2 图 D.2 中的系统的信息安全等级矢量示例

基本要求	信息安全等级（SL）				
	报警	基本	安全	Z1a 和 Z2a	Z1b 和 Z2b
FR 1—识别和鉴别控制	1	2	3	3	1
FR 2—使用控制	1	2	2	2	1
FR 3—系统完整性	1	2	2	2	1
FR 4—数据保密性	1	2	2	2	1
FR 5—受限的数据流	1	1	1	1	1
FR 6—对事件的及时响应	1	1	1	1	1
FR 7—资源可用性	1	2	2	2	1

图 D.3 所示的示例系统，使用表 D.3 中“Z1b”列所定义的信息安全等级矢量。位于区域 Z1a 和 Z2a 中的功能使用“Z1a 和 Z2a”列中定义的信息安全等级矢量。区域 Z1 和 Z2 中的其他域中的组件不存在安全等级要求。

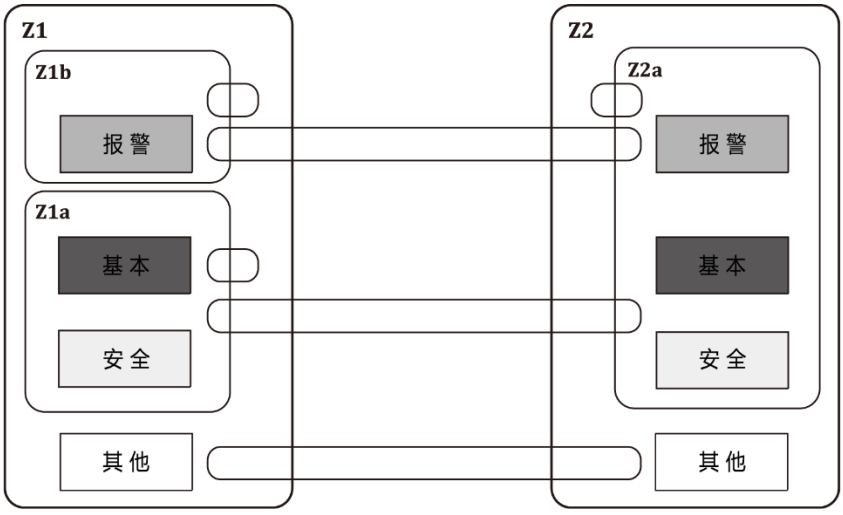

图 D.3 显示五个区和连接管道的示例

表 D.3 图 D.3 中的系统的信息安全等级矢量示例

基本要求	信息安全等级（SL）				
	报警	基本	安全	Z1b	Z1a 和 Z2a
FR 1—识别和鉴别控制	1	2	3	1	3
FR 2—使用控制	1	2	2	1	2
FR 3—系统完整性	1	2	2	1	2
FR 4—数据保密性	1	2	2	1	2
FR 5—受限的数据流	1	1	1	1	1
FR 6—对事件的及时响应	1	1	1	1	1
FR 7—资源可用性	1	2	2	1	2

参考文献

［1］GB/T 7588.2 电梯制造与安装安全规范 第 2 部分:电梯部件的设计原则、计算和检验

［2］GB/T 20900—2007 电梯、自动扶梯和自动人行道 风险评价与风险降低的方法

［3］GB/T 24475—2023 电梯远程报警系统

［4］GB/T 24476—2023 电梯物联网 企业应用平台基本要求

［5］GB/T 40682—2021 工业自动化和控制系统安全 IACS 服务提供商的安全程序要求

［6］IEC Guide 120:2018 Security aspects — Guidelines for their inclusion in publications

［7］ISO/TR 22100-4:2018 Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

［8］ ISO/IEC 27005:2022 Information technology — Security techniques — Information security risk management

［9］ ISO 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

［10］CAPEC, https://capec.mitre.org

［11］NIST SP 800-82

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

［12］NIST 计算机安全资源中心：

https://csrc.nist.gov/glossary/term/Red_Team_Blue_Team_Approach

［13］BSI ICS 安全概要：

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICSSecurity_compendium.pdf?__blob=publicationFile&v=3ISO

［14］OWASP https://owasp.org

［15］NIST SP 800-30, 2012

［16］安全编码实践快速参考指南 OWASP, Version 2.0, 2010, https://owasp .org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

［17］事件响应和安全团队论坛(FIRST), 网址: https://www.first .org/

［18］CWE https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html