ICS 91.140.90
Q 78

中　国　电　梯　协　会　标　准

T/CEA 703—202X

基于物联网的电梯、自动扶梯和自动人行道监测系统的网络安全标准通用要求

（征求意见稿）

202X-XX-XX 发布　　202X-XX-XX 实施

中国电梯协会　　发布

目　次

前　言

本标准按GB/T 1.1-2009给出的规则起草。

请注意本标准的某些内容可能涉及专利，本标准的发布机构不承担识别这些专利的责任。

本标准所要求达到的性能指标，应由采用本标准的制造企业在设计制造过程中自行进行验证测试，并对销售的产品作产品符合性声明。

本标准由中国电梯协会提出并归口。

本标准负责起草单位：

本标准参加起草单位：

本标准主要起草人：

引　言

电梯、自动扶梯和自动人行道的网络安全保护已成为现代电梯设备必不可少的要求。锁在机房门后面的独立旧系统已不复存在。如今的电梯是一种带有多个中央处理器（CPU）、可访问互联网的显示屏以及为笔记本电脑和手机服务工具提供Wi-Fi网络的复杂系统。由于配备语音、实时轿厢视频显示并且能够在疏散时与消防和生命安全系统进行复杂的交互，电梯、自动扶梯和自动人行道已成为紧急情况下的关键设备。通过网络向维修人员提供实时数据并且按需提供软件更新已成为一种常态。虽然电梯的计算机化提高了电梯的安全性和便捷性，但它们也容易受到计算机病毒和黑客的攻击。

本标准介绍了电梯连接到“外部”系统或互联网时的电梯网络安全最佳措施。

基于物联网的电梯、自动扶梯和自动人行道监测系统的网络安全标准通用要求

1 范围

本标准为电梯、自动扶梯和自动人行道制造商设计系统提供了一条途径，为基于网络的网络防护提供了可靠的保障和管理。本标准目标是关注电梯、自动扶梯和自动人行道系统与互联网、建筑区域网络和“不可信”系统之间的接口，包括技术人员使用的维护和服务工具，以上皆被视为不可信的系统

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB 7588—2003 电梯制造与安装安全规范

GB 21240 液压电梯制造与安装安全规范

GB/T 26465 消防电梯制造与安装安全规范

GB/T 7024 电梯、自动扶梯和自动人行道术语

GB/T 20900-2007 电梯、自动扶梯和自动人行道 风险评价和降低的方法

GB/T 22239 信息安全技术网络安全等级保护基本要求

JB/T 11960-2014 工业过程测量和控制安全网络和系统安全

ISO/IEC 27036-3:2013 信息技术 - 安全技术 - 供应商关系的信息安全

ISO 27005:2018 信息技术 - 安全技术 - 信息安全风险管理

3 术语和缩略语

本标准采用GB/T 26665中的术语及下列定义。GB/T 7024、GB 16899和GB/T 20900确定的以及下列术语和定义适用于本标准。

3.1

资产 asset

对组织有感知价值或实际价值的任何东西。

3.2

目的层调度系统 DDS（Destination Dispatching System）

3.3

电梯/自动扶梯管理系统 EMS（Elevator/escalator Management System）

3.4

安全控制 Security Control

为保证系统的整体网络安全，需要实施特定的过程、安装和组织控制，包括但不限于定期安全审核，持续的安全监测和事件管理过程。

3.5

安全措施 Security Measure

为满足特定的产品技术需求而实施的具体技术要求。包括使用最先进的认证协议、使用加密技术的加密程序、会话密钥、安全引导、代码签名、防火墙设置等。

3.6

建筑管理系统 BMS（Building Management System）

3.7

公用交换电话网 PSTN（Public Switched Telephone Network）

3.8

无机房电梯 MRL（Machine room-less elevator）

4 架构

本标准主要涉及电梯、自动扶梯和自动人行道系统与不可信设备进行通迅的接口。虽然本标准介绍了与其他系统的接口，但最佳策略是考虑内部功能间的通信。

以下章节中图1、图2和图3描述了电梯系统架构以及架构中存在风险的一些示例，这些示例同样适用于扶梯、自动人行道控制系统。

本标准包含但不限于如下接口：

a) 连接到互联网的有线或无线网络接口；
b) 连接到建筑物网络的有线或无线网络接口；
c) 连接到安防系统的串行通迅接口，物理隔离的接口除外；
d) 连接到智能服务工具的有线或无线接口；
e) 智能服务工具，例如计算机；
f) 能够下载软件或者能与电梯交互的被困乘客报警系统；
g) 连接电梯、自动扶梯和自动人行道的系统和外部的通信链路。

4.1 安全/可信区域

本标准未考的虑系统安全和可信部分，由图1、2、3中半透明绿色区域表示，大多数系统将包含多个受信任区域。

图1是安装的单部电梯，通过有线或无线与服务工具进行通迅，如下图所示。

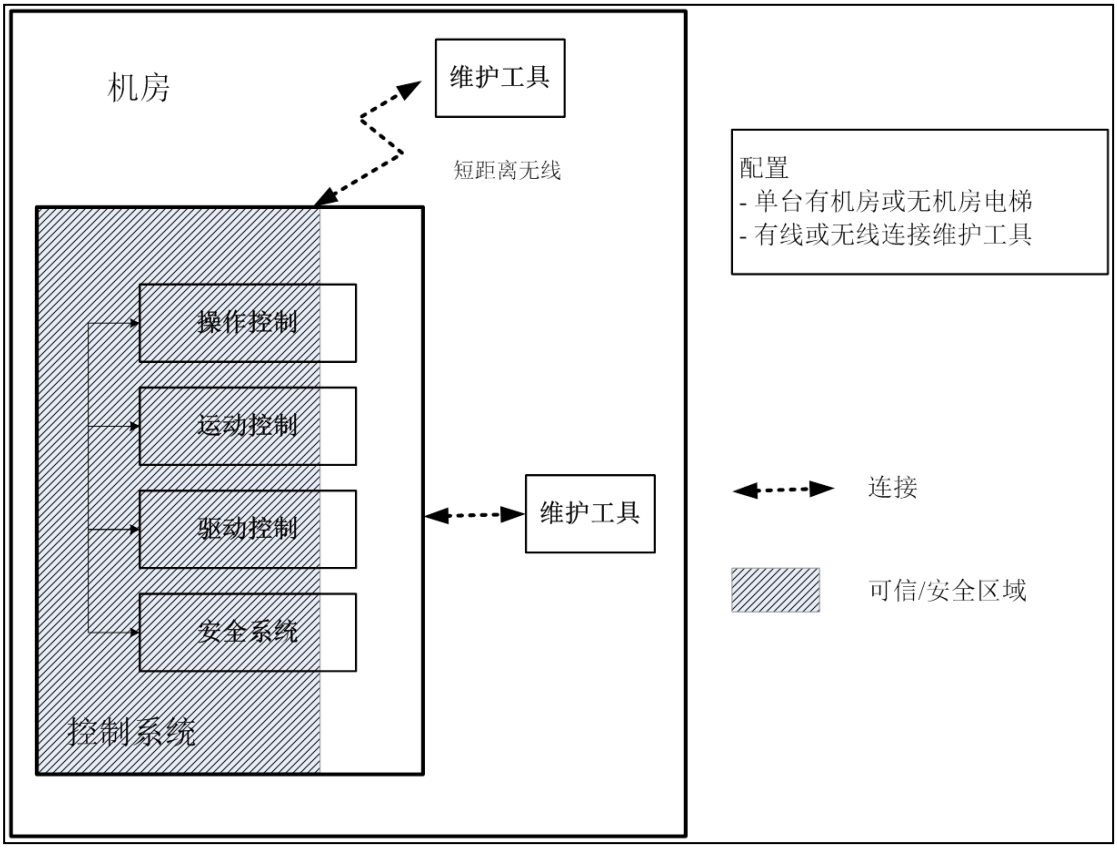

图 1

图 2 是较复杂的架构，目的层控制系统、电梯管理系统通过互联网和外部进行通讯，以及通过网关实现网络交互功能，如下图所示。

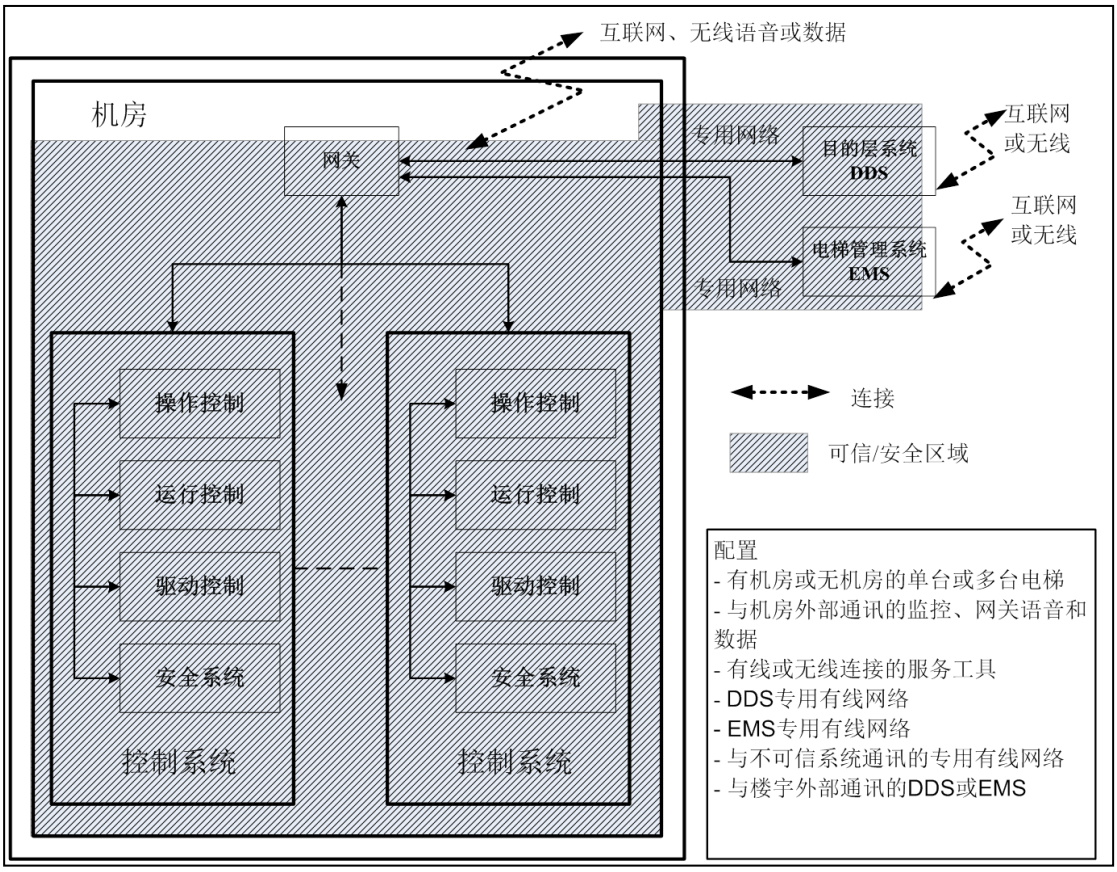

图 2

图3介绍了不受信任的建筑物网络的情况，如下图所示。

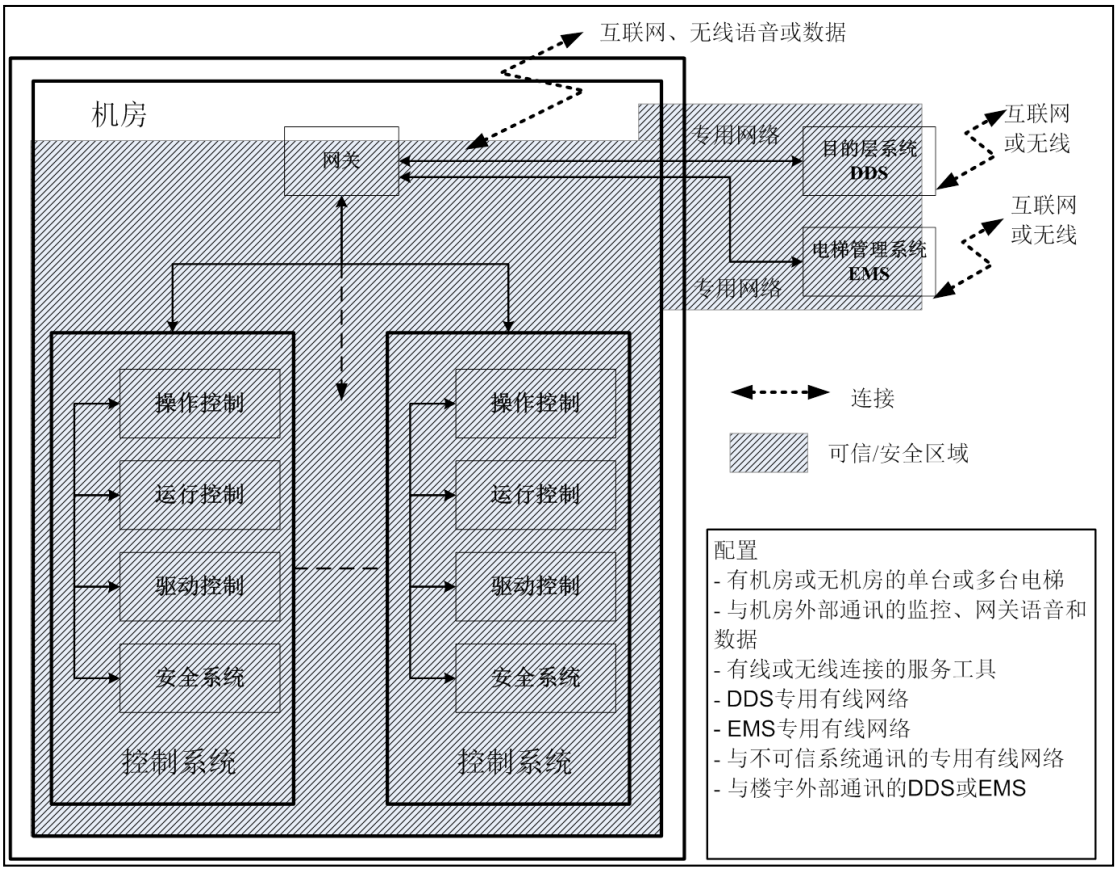

图 3

5 网络安全的生命周期

本标准定义网络安全的生命周期，该生命周期需要保证足够的培训、工具、资源和过程，以加强和维持电梯、自动扶梯和自动人行道系统抵御网络攻击的能力。生命周期的建立是保证是网络安全标准的方法和基本前提，生命周期包含七项功能，下面的章节将对其做进一步的描述。

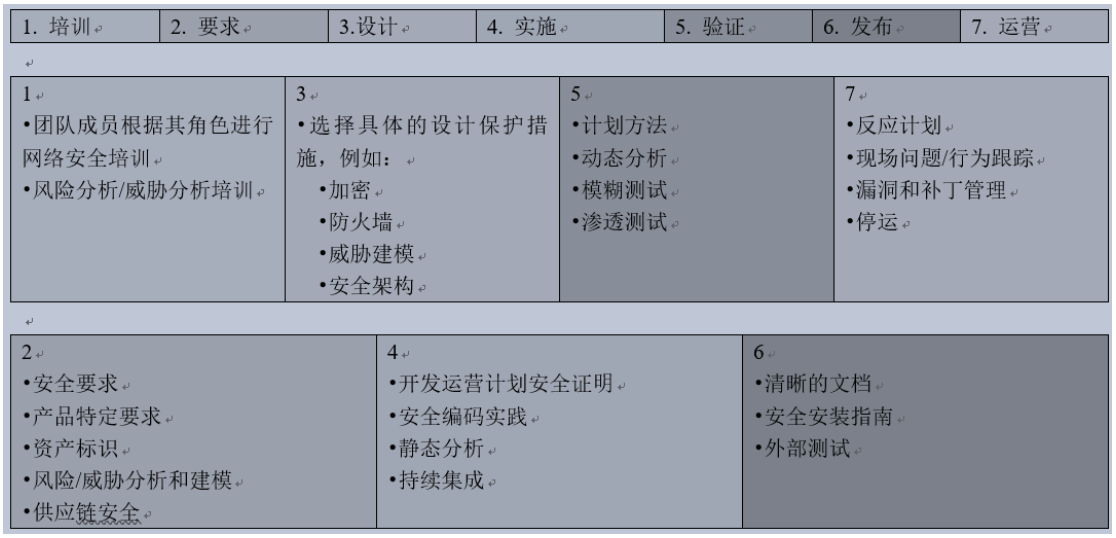

图 4

5.1 培训

参与网络安全生命周期的每个员工都应接受充分的培训，以确保电梯、自动扶梯和自动人行道达到相应的安全级别，包括但不限于高层管理人员、开发人员、生产线人员、维护人员和采购人员。

应根据员工的角色提供通用的网络安全培训内容和特定的专业知识。列举培训的内容如下：

参与网络安全生命周期的所有员工都需大致了解什么是网络安全、当前的最佳措施是什么以及如何应用，并了解需要保护的系统及网络安全威胁所引发的风险。建议培训团队包含网络安全专家。

具体培训内容根据角色会有所差异：

a) 高层管理人员应了解网络安全对电梯、自动扶梯和自动人行道的重要性；

b) 管理层人员应建立安全生命周期过程来支持所有工作，分配必要的资源，使网络安全恢复能力达到合理水平；

c) 开发人员需要具备实现安全功能的专业知识（参见 5.3 章节：设计），并应通过培训掌握各自任务的最佳方法；

d) 电梯、自动扶梯和自动人行道维护人员也应接受培训，根据既定规程保障网络安全。

除上述网络安全培训外，风险或威胁分析的团队还必须掌握GB/T 20900等相关标准的最新知识,并根据最佳方法开展工作。

5.2 要求

5.2.1 概述

电梯、自动扶梯和自动人行道系统的网络安全要求的管理过程本质上是风险管理过程。

为获得具有可接受安全级别的产品，应创建有效的措施和控制过程，减轻威胁电梯、自动扶梯和自动人行道系统的各种风险。

确认资产和收集潜在的安全风险是一个多方合作的过程，如内部不具备专业知识的情况下，可寻求专业的外部支持，作为有效的补充，例如研讨会的评估。

与功能安全所面临的危险和风险分析一样，应组建风险分析团队，通过综合评估，逐渐完善已确定的威胁和风险列表。

电梯、自动扶梯和自动人行道系统的网络安全要求可分为两类：

a）基本安全要求

应在所有系统中使用最佳的安全措施，第7章节提供了推荐的安全基本要求。应多方面考虑和目标系统接口设备的安全要求。

b）特定系统的安全要求

在设计新系统或分析现有系统的安全时，应进行风险威胁分析以确认系统威胁并确定防范威胁的措施。尽管在某些情况下可以确认基本安全要求已经足够，但安全也不应只依赖于基本安全要求控制的实施。

5.2.2 要求过程

应遵循以下过程来确定安全要求：

a) 确认资产和可接受的风险等级

b) 初步风险评估

1）确认资产威胁和风险；

2）确定风险事件的可能性和影响；

3）确定未缓解的网络安全风险；

4）定义系统安全等级。

c) 建立安全要求

d) 进行多轮风险评估

1）评估当前措施；

2）重新评估风险事件的可能性和影响；

3）确定剩余风险。

e) 记录网络安全要求、假设和约束

每当对系统进行更改或威胁情况发生显著的变化，例如发布新的软件漏洞时，应根据测试结果更新风险评估结果。

安全需求过程的每个步骤的标准见以下章节。

5.2.2.1 确认资产和系统

a) 确认资产以了解系统的哪些部分应受到保护，即哪些部分已被证明需要投入额外成本获得保护；

b) 从安全角度来看，对企业具有感知或实际价值的所有内容都是资产。资产可以是逻辑或物理对象，例如服务的可用性、乘客和服务技术人员的安全、安全系统的完整性等；

c) 必须考虑系统中的附加资产；

d) 对于电梯、自动扶梯和自动人行道系统，乘客和服务技术人员的安全应视为受保护的资产，并优先于其他保护方面。安全措施不应对电梯、自动扶梯和自动人行道系统的安全功能产生不良影响；

e) 在确认资产过程中，应确定可接受的风险级别。可接受级别取决于企业和当地法规规章以及社会价值等，例如安装在低风险住宅建筑中、安装在医院中、大使馆中的电梯、自动扶梯和自动人行道系统。如果需要进行风险评估，则应先定义电梯、自动扶梯和自动人行道系统的典型应用。

5.2.2.2 初始风险评估

a) 在风险评估过程中，应确定威胁资产的风险事件和风险威胁；

b) 初始风险评估的第一步是确定风险，但无需采取任何缓解措施；

c) 电梯、自动扶梯和自动人行道系统的安全威胁包括但不限于：

1）因软件错误引发的漏洞；

2）恶意软件，例如通过网络、可移动存储设备、临时连接的服务工具等传播的蠕虫和病毒；

3）非法访问；

4）员工或他人的未授权的行为；

5）工的无意行为；

6）拒绝服务攻击；

7）破坏、毁坏。

d) 关于其他潜在威胁，参见相关组织发布的最新威胁目录；

e) 评估威胁事件发生的概率，应在评估过程中考虑对方的能力和意图以及系统中存在的漏洞：

1）对方的能力：对方的专业程度和资源情况；

2）对方的意图：对方是专门针对具体目标还是寻找任何可以利用的系统；

3）系统漏洞和可访问性：系统是通过互联网公开还是在封闭网络中运行，例如电梯、自动扶梯和自动人行道控制系统的内部网络。

f) 与功能安全的危险和风险分析相比，安全风险评估更具有挑战性。会存在多方面的风险，而不是单方面，例如对人员或系统的伤害。根据具体的风险事件，后果可能有：

1）乘客受伤，例如：启动安全装置、电梯运行不受控制或电梯门驱动器不受控制等；

2）电梯、自动扶梯和自动人行道停止运行或运载能力下降；

3）越过访问控制，例如获得楼层的越权访问权限；

4）公司资产损失，例如失去知识产权或内部资料。

g） 在评估电梯、自动扶梯和自动人行道系统的风险时，可根据 GB/T 20900 确定概率和严重程度，并可使用该标准中的风险类别来评估风险等级。

h） 也可使用其他方法确定风险，但必须系统地实施。有关进行风险或威胁评估的其他指导可参见 IEC 62443-3-2，ISO 27005。

表 1 GB/T 20900-2007.C.2 风险概率示例

概率	单位系统概率	描述对方能力和意图与系统漏洞
A – 频繁	在生命周期中频繁发生	-系统在开放网络中，且未采取安全控制措施 -会被资源有限和缺乏专业知识的业余攻击者利用
B – 很可能	在生命周期中发生多次	-系统在开放网络中，已采取低效的最基本的安全控制措施 -只需较少的资源、专业知识和动机就能被利用
C - 偶尔	生命周期中至少发生一次	-系统在开放网络中，采取部分安全控制措施且部分有效 -只需普通的资源、专业的电梯、自动扶梯和自动人行道技能和一般的动机就能被利用
D - 极少	概率很低，但还是可能在生命周期中发生	-系统在开放网络中，绝大部分采取完整有效的安全控制措施 -需要大量资源、专业的电梯、自动扶梯和自动人行道技能和高度的动机才能被利用
E - 几乎不可能	在生命周期中几乎不可能发生	-系统在开放网络中，采取完整有效的安全控制措施 -需要非常尖端的专业知识、充足的资源，高度的动机和协作才能被利用
F - 不可能	概率几乎为零	无需担心，安全控制措施或其他措施已得到充分的评估、落实且有效
如果系统在封闭的网络中运行，则将概率降低一个等级。 如果系统在物理安全的位置上运行且只能在该位置访问，则将概率降低两个等级。		

表 2 GB/T 20900-2007.C.1 风险严重程度示例

严重程度	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（对运营商）
1 - 高	死亡、系统损失或严重的环境损坏		
2 - 中	严重损伤、主要的系统或环境破坏		
3 - 低	较小损伤、次要系统损坏	服务中断，例如：电梯、自动扶梯和自动人行道停止服务且无其他运输工具可替代；电梯、自动扶梯和自动人行道失去访问控制A，B	数据完整性被破坏，例如：电梯、自动扶梯和自动人行道的管理系统数据被篡改A，B
4 – 可忽略	不会导致伤害、系	轻微服务中断，例如运载能	非关键数据丢失，例如电

	统或环境破坏	力下降A，B	梯管理系统数据A，B
注A 如果影响多个地点，则将严重程度提升一级。 注B 如果影响全国或全球，则将严重程度提高两级。			

根据初始风险分析结果确定未减轻的资产风险。基于风险矩阵，应确定哪些风险需要额外的缓解措施。安全等级参见第6章中的要求。

5.2.2.3 安全要求

a) 在初始风险评估之后，应选择有效的措施，以减轻超出先前定义的可接受风险等级的评估风险；
b) 创建、选择的措施最佳方法是“深度防御”。措施不应依靠单一的防护，而是需要利用多层保护，如果一种防护被突破，资产仍会受到其他几种防护的保护；
c) 补偿措施可被用于满足一个或多个安全要求，例如物理访问控制或检测控制等；
d) 有关措施的要求参见第 7 章。

5.2.2.4 进行多轮风险评估

a) 如初步风险评估一样进行多轮风险评估，但应落实先前选择的措施；
b) 检查之前定义的措施是否将已确认的网络安全风险降低到之前定义的可接受水平，还应检查措施是否会带来新的安全威胁，例如拒绝服务、新的攻击层面等。如果没有降低至可接受水平，应采取其他措施、缓解方法，并重新评估相关风险；
c) 当对现有产品或系统的风险评估结束时，应确定所需的缓解措施，以最大限度地降低初始评估期间发现的风险。

5.2.2.5 记录网络安全要求

记录网络安全要求如下：

a) 应包含在开发期间实施的满足安全要求的安全措施。安全要求应对之前确定的安全风险具有可追溯性；
b) 追踪并在开发结束时确认和验证所有其他安全要求。

5.2.2.6 外部开发的软件安全

上述方法应扩展到外部资源开发的组件，包括商务现货供应（COTS）软件、开源软件（OSS）和专门为公司开发的组件。

a) 无论风险评估、措施的选择以及安全概念是如何的完整，外部开发的组件中的不安全因素都会对系统造成危害；
b) 最佳措施包括对供应商的审核、仅从可靠的供应商处采购、仅外包给值得信赖的服务提供商，以及对要求遵守的过程进行合同保证；
c) 更多信息，参见 ISO/IEC 27036-3 和 IEC 62443-2-4。这个标准为供应商、服务提供商提供可能需要的安全建议。

在设计系统架构和分配其功能的同时，应检查和更新威胁模型。有几种方法是可行的，例如微软的STRIDE方法，这种方法通过筛选系统的每个组件来回答“我的系统可能出现什么问题？”：

a) 欺骗 – 伪装虚假身份；
b) 篡改 - 未经授权修改的数据或系统；
c) 否认 - 混淆了个人的行为责任；
d) 信息披露 - 未经授权披露有价值的数据；
e) 拒绝服务 - 将服务的可用性降低到几乎为零；
f) 提升权限 - 通过利用设计缺陷或漏洞获得比预期更高的权限。

如果威胁模型与系统的不断发展的体系结构保持同步，则可以获得可能存在威胁的综合目录。通过选择适当的措施来减轻威胁，这些措施可以合并到系统架构的后续迭代中。

5.3 设计

设计阶段的目标是开发系统架构。在该阶段，将确定有关高级设计选择和关键组件的所有决策。在架构开发过程中，为了实现符合所需功能的架构，应对产品的完整功能进行必要的描述。例如，这一描述可能包含所涉及的实体、由此所产生的数据流、已经分配的重要安全或非安全的属性。

由于在设计阶段确认的选择具有深远影响，因此该阶段特别容易出现安全漏洞。开发体系结构中的缺陷，可能直接或间接导致在此高级阶段中出现难以识别的漏洞，其原因是它们可能非常特殊或仅在较低等级阶段才能被发现。在设计阶段应尽早定性这些安全问题，这才是最为有效的措施。如果在后期阶段发现安全漏洞，例如在测试或运行期间，则处理会变得更加复杂，处理成本更加昂贵。因此，检测设计阶段已有的漏洞并采用行业标准最佳方法来减少暴露的攻击面是非常重要的。

方法如下：

a) 最小权限原则，即过程或用户在设计上不应拥有比完成其任务所需的更高权限；
b) 攻击层面的识别及最小化；
c) 模块化设计，以减少安全威胁的影响；
d) 深度防御，是指不应通过单一措施，而是通过多项分层措施减轻风险。即使其中一项措施失败，但其他措施仍然有效；
e) 限制用户的访问权限，仅对接那些满足相应功能的系统或任务所需的数据；
f) 优先使用简单、经过验证的概念或组件，而不是那些不必要的复杂的、专有或未经过充分测试的组件；
g) 定期执行安全设计审核，以检测当前设计尚未解决的安全要求，并检查系统当前架构是否符合最佳方法。

5.4 实施

至少应遵循以下与安全实施相关的主要属性：

a) 使用安全编码标准；
b) 使用静态分析工具；
c) 关键功能的单元测试；
d) 分析第三方和开源软件。

使用安全编码标准，标准应根据实际案例，列出可能被利用的编码结构或不应使用的设计。通常标准还应包括禁用、弃用功能列表。

使用静态分析工具，至少使用静态代码工具来分析满足以下条件的代码：

a) 侦听或连接到网络的代码，这些代码被规划连接到可信、安全区域外部的设备、系统或应用程序；
b) 已被确认的早期漏洞代码；
c) 需要高权限才能执行的代码，除非所有这些代码都需要高权限才能执行，例如系统最高权限、管理员账户、根账户等。以高权限运行的代码都应有正当理由；
d) 安全相关代码模块，例如身份验证、授权、加密和防火墙代码等；
e) 解析来自不可信来源的数据结构的代码；
f) 设置访问控制、处理加密密钥或密码的设置代码。

应通过静态分析工具降低违反编码标准的所有可识别的风险，除非这些违反标准是没有风险的。

最佳方法是在开发过程中进行持续的源代码分析，当开发人员输入代码时，会自动分析代码以查找任何可能的安全问题。

5.5 验证、计划方法

除了产品开发中的正常测试和验证过程之外，网络安全验证和测试计划也应成为系统验证阶段的正式过程。以下是与安全相关的关键活动：

a) 动态分析

对应用程序应执行动态测试，以识别存储损坏、竞争条件、用户权限问题以及任何其他严重的安全问题。

b) 模糊测试

对处理源自安全区域或组件外的数据的所有组件，应进行模糊测试。

应创建一个模糊测试计划，记录将要执行的模糊测试。该计划应包括将被模糊测试的所有组件的列表，如何进行模糊测试的描述，是否进行智能模糊测试或傻瓜模糊测试以及测试的通过和失败标准。

c) 渗透测试

除使用模糊测试工具外，建议在测试期间使用各种渗透测试工具。测试计划应包含使用渗透测试工具相关的详细的所有项目。

应定期考虑独立的（第三方）渗透测试。

d) 验证

以下是验证威胁模型的措施是否已正确实施：

1）应对所有组件执行破坏性测试和已知漏洞测试，并尝试利用已减少的威胁模型中确认的所有威胁；

2）确认威胁建模过程中未捕获的任何攻击面；

3）应仔细地记录结果；

4）应通过测试验证实施的安全措施的有效性，并应根据测试结果更新风险评估。

e) 独立的第三方分析

建议进行独立的第三方安全风险分析和测试，应由已通过充分审核的具有分析资质的机构，进行此类分析。

5.6 发布

在产品发布之前，下列文档和风险接受建议应是已完成并可交付的。

文件如下所列：

a) 威胁模型以及风险评估

威胁模型需要包含已确认的剩余风险。

b) 安全要求和安全设计

设计文件需要明确所有的安全需求及其相关的安全管控措施。

c) 安全测试计划

描述如果测试每项安全控制并确保其符合安全要求的测试计划。

d) 分析报告

报告总结已进行分析的结果并突出任何已发现的问题和不的安完善全管控措施。

1）第三方代码、库分析报告；

2）动态安全分析报告；

3）静态代码分析报告。

e） 测试报告

1）模糊测试报告；

2）内部渗透测试报告；

3）外部渗透测试报告。

f） 用户手册

用户手册包括用户、操作和维护手册等，应由相关专家进行审核，并应包括针对用户和管理员的安全指导部分，包括防止安全漏洞所必需的操作和约束。

管理员标准应包括产品安全操作所需的所有管理员职责,包括与产品安全环境声明中的相关的假设的管理员行为。

如果提供了可供开发人员创建应用程序的API（应用程序编程接口）、类、对象，则应为每个应用的函数或方法调用提供安全信息和最佳方法。

用户手册中的安全指南应包含安全漏洞报告过程。

文件应包括设计中假设的威胁配置文件以及与用户相关的高级安全功能，包括身份验证机制、身份验证和其他功能的默认策略，以及强制或可选的任何安全协议。

g） 安全系统安装指南

安装指南应列出并说明系统中存在的所有安全配置选项，并记录其默认和可选设置。因为无任何其他配置更改的默认配置被视为是安全的，所以安全系统的默认安装是安全的。

此外，安装手册应包含在调试之前要执行的所有现场、外部测试要求，从而完成安全的安装。

h） 事故响应计划

所有引起结构化程序的事件应被记录，包括带有联系方式的RACI模型矩阵a。

注[a]：RACI模型：谁负责responsible、谁批准accountable、咨询谁consulted、通知谁informed。

5.7 运营

在维护服务的情况下，暴露在威胁下的设备的运营要求应有追踪所有暴露的硬件和软件、监视安装和响应计划等措施。

应评估当前的安装风险,需了解可能暴露给攻击者的所有组件。以下资产清单应包括硬件以及软件：

a） 保持对正在使用的硬件、软件的库存和版本控制；

b） 持续监测漏洞数据库和现场问题；

c） 如果检测到软硬件资产的某个漏洞，则应分析该漏洞对资产造成的任何影响。

如果资产受到漏洞的影响，应通过实施针对此漏洞的更新、替换、减轻或接受风险，解决此问题的进一步过程。建议使用评分系统，来确定任何已确认的安全问题的优先级并进行评估。

5.8 响应计划

如果有事故发生，应提供书面程序来执行必要后续步骤即事故响应计划。事故响应计划应包含处理各种可能发生的事件的必要信息，并高度依赖于特定资产。事故响应计划至少应包含以下内容：

a） 联系方式、责任；

b） 资产组件；

c） 安装地点（如果适用）；

d） 预定义程序。

事件包括：

a） 网络流量异常；

b） 由于安全漏洞而意外关闭；

c） 电梯、自动扶梯和自动人行道显示器的失效。

应制定有关上述及其他需求的应急程序。在改变或更新时，应落实正确维护响应计划的过程。

应考虑如何处理电梯、自动扶梯和自动人行道系统的停运，因为敏感信息可能存储在某些组件上，如：身份凭证、证书、参数集等，这些组件可能被恶意使用或一旦披露会提供关于资产和其他连接资产信息的泄漏。可能需要删除信息或破坏资产。资产的停运应体现在资产清单中。

6 安全等级

电梯驱动主机的电磁式制动器应符合下列要求：如本标准第5.2章节所述，应在风险评估期间确定系统、组件或区域的安全等级目标，应通过测试验证系统、组件或区域所达到的安全等级。

在以下情况中，应在系统生命周期内重新进行安全等级的确认：

a) 对系统进行更改；

b) 检测到与系统相关的新漏洞；

c) 供应商或开源社区发布了系统组件新的安全补丁；

d) 定期，由机构政策决定。

安全等级（SL）用于描述为抵御网络攻击的技术等级和动机。

6.1 SL0

SL0定义：无特定要求或必需的安全保护措施

通过风险评估，确定系统不需要特定的安全要求，例如：因为误用的后果被确定为可以忽略不计。

在评估是否已达到安全等级时，SL0可表示已实施SL1的一部分措施，但未满足完整的SL1的等级。

6.2 SL1

SL1定义：能够抵御业余或偶尔的入侵

应能保护系统免受低技能攻击或无意、误用的攻击。应采取基本的安全控制措施以确保数据的保密性、完整性和可用性，并实施访问身份的验证、授权和记录。例如根据SL1所采取的安全控制，不需要对用户和设备进行唯一性认证。

本标准中引用的ISA / IEC 62443-3-3标准中提供了一组推荐的SL1控件。

6.3 SL2

SL2定义：防止使用需要少量资源、通用技能和低动机的简单方式的故意入侵。

系统应能抵御具有盗用通用信息技术系统的工具和技能的攻击，例如：基于网络的应用程序。但攻击者不具备电梯、自动扶梯和自动人行道系统的专业知识，且不专门针对这些系统进行攻击。攻击者的动机可能是获得金钱收益或声誉收益等，例如勒索软件。与SL1的不同之处在于，SL2保护措施是更细致的安全控制措施。例如应对用户和设备的唯一性进行身份验证。

本标准第7章描述了SL2的建议控制措施。

6.4 SL3

SL3定义：防止使用需要中等资源、特定电梯、自动扶梯和自动人行道的技能和中等动机的复杂手段的故意入侵。

系统应能够抵御技能高超、了解安全措施和电梯、自动扶梯和自动人行道系统并且专门针对此类系统的攻击者。以SL3系统为目标的攻击者可能会使用针对特定目标系统定制的攻击媒介。攻击者的动机可能是勒索、报复或破坏，例如心怀不满的前雇员、行业竞争对手等。

SL3的控制措施超出了本标准的范围。

6.5 SL4

SL4定义：防止使用需要扩展资源、特定电梯、自动扶梯和自动人行道的技能和强烈动机的故意入侵。

系统应能够抵御技能高超、了解安全措施及电梯、自动扶梯和自动人行道系统并且专门针对具有扩展资源和强烈动机的系统的攻击者。这与SL3类似，但SL4的攻击者动机更高并准备花更长的时间、资源来规划和执行攻击。

SL4的控制措施超出了本标准的范围。

7 安全措施

本章节建议根据ISA/IEC 62443-3-3标准表6a）中定义的系统要求（SR），对安全级别1和2使用的安全措施。可以在该标准中找到要求的详细描述。

7.1 服务工具的安全

用于服务电梯、自动扶梯和自动人行道的工具应采取有效的安全措施。服务工具大致可分为三类：

a） 可从互联网上的任何地方与电梯、自动扶梯和自动人行道进行远程通迅的服务工具；

b） 基于近、中范围近距离无线技术的服务工具，例如 Wi-Fi 和蓝牙等；

c） 要求硬件靠近设备并且插入电线电缆的服务工具，例如 USB 或串行电缆等。

有效的网络安全方法包含深度防御策，该策略根据设备的可访问性等级实施多种安全措施。如果系统受到损坏，这些措施则会受到影响。在这方面，上述三种情况中的可访问性应采取不同类型的安全控制措施，具体取决于通过服务工具对系统控制的程度。例如：如服务工具能够从网络远程更改配置，则建议至少实施多重身份验证，包括同时使用证书、预共享唯一密钥、密码和白名单等。当需要物理访问时，至少应采取基于密码的唯一方法。

强化电脑端，除了用于认证和加密的安全控制措施之外，对于服务工具的一项重要要求是确保运行工具的机器得到充分强化，例如电脑、移动设备等，并采取与机器使用相关的适当访问控制措施。

强化标准中的关键要素包括对所有用户帐户使用强密码、对防病毒和反间谍软件进行良好的维护、及时更新补丁、打开软件防火墙选项、将机器的使用限制在设计范围内。此类强化标准由NIST和其他组织发布，建议任何使用服务工具或参与电梯维护的第三方遵守此类标准。

8 示例

以下是关于风险评估和安全要求选择的简化版本的示例，示例中的电梯将远程监测集成到电梯控制系统中。

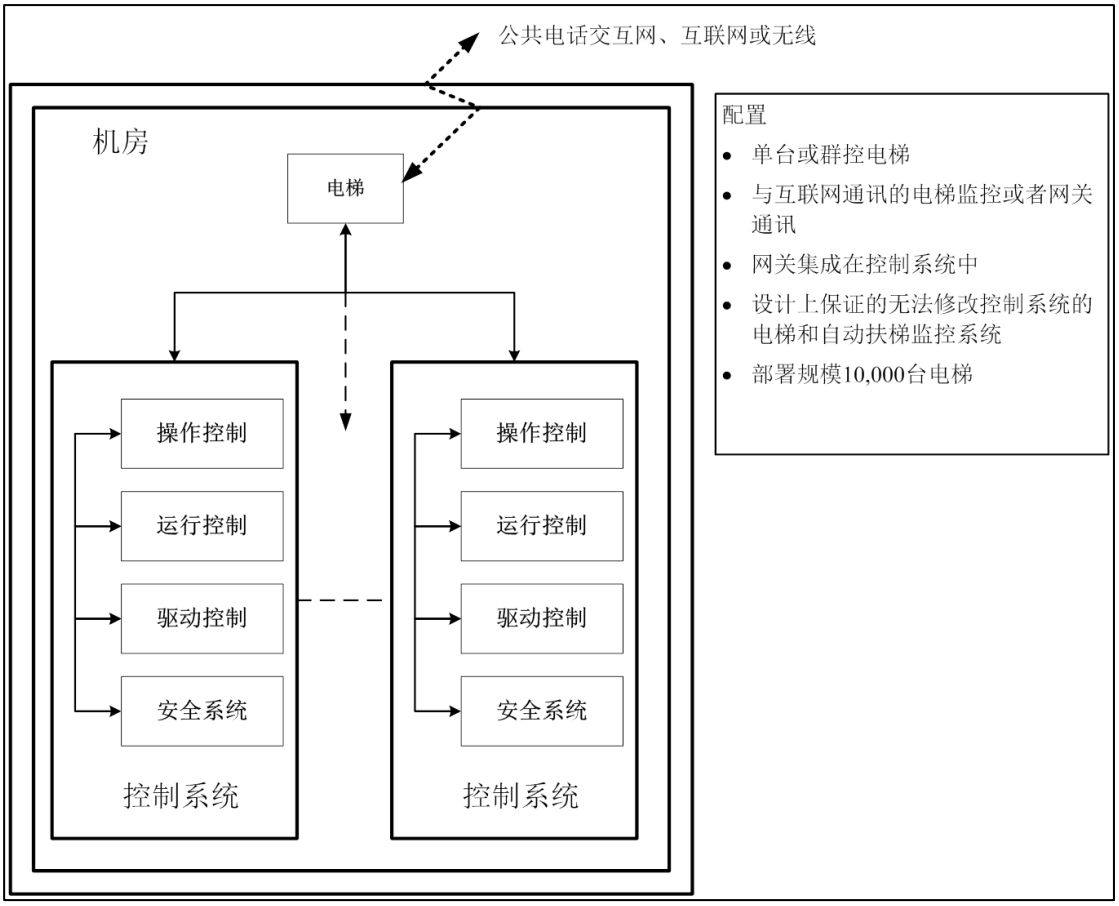

图 5

8.1 过程要求

a) 确认资产：

1）监测系统不能修改控制系统的功能；

2）监测系统完整性；

3）监测系统发送数据的完整性；

4）监测系统的可用性。

b) 可接受的风险

1）不允许因特网上的可扩展攻击；

2）无需考虑通过物理访问发起的本地攻击，因为这种攻击只会影响单个设备。

c) 初步风险评估

1）确认资产威胁和风险

(1) 对监测系统的拒绝服务攻击；

(2) 篡改监测系统发送的数据；

(3) 伪装成监测系统发送数据；

(4) 获得监测系统的所有权；

(5) 通过监测系统攻击控制系统。

2）确定可能性和影响（见下表3）

表 3 风险评估

运行事故风险	可能性	影响	注
i.对监测系统的拒绝服务攻击	A	4（单一） 3（可扩展）	工具通常可用于执行DoS攻击，并且它们经常发生在公开互联网的系统上。单个站点的影响可能微不足道，因为监测数据的暂时丢失不是严重事件。
ii.篡改监测系统发送的数据	D	3（单一） 2（可扩展）	修改监测数据需要专业技能。如果成功，对单个节点的影响很小，因为合法的服务需求可能会被忽略，导致间接的安全风险。
iii. 伪装成监测系统发送数据	B	3（单一） 2（可扩展）	对于不受保护的通信，很容易受到欺骗攻击。盗窃数据对单个节点的影响很小。
iv.取得监测系统的所有权	C	3（单一） 2（可扩展）	如果监测系统不受保护，取得所有权并不难。但是，监测不被视为关键功能，因此对单个节点的影响较小。
v.通过监测系统攻击控制系统	E	2 （单一） 1（可扩展）	即使在监测系统遭到破坏之后，攻击控制系统也需要全面的专业技能。如果攻击成功，则对单个节点的影响可能是中等的。

3）确定未缓解的网络安全风险

由于监测系统将通过互联网连接，因此可扩展攻击是一个需要考虑的安全威胁。因此，风险评估必须假设攻击者可以同时攻击多个节点，如下表所示。

表 4：可扩展攻击的网络安全风险

概率等级	严重级别描述			
	1 -- 高	2 -- 中	3 -- 低	4 -- 可忽略
A - 非常可能			i	
B - 可能		iii		
C - 偶然		iv		
D. 不太可能		ii		
E - 不可能	v			
F - 非常不可能				

4）定义安全级别

某些风险处于不可接受的级别，所以应采取安全措施来降低风险。出于示例的目的，我们选择根据IEC 62443-3-3实现安全级别1要求。安全级别1应足以阻止临时攻击者。

5）创建安全要求

在SL 1要求中，以下内容将降低初始风险：

(1) 拒绝服务防护；

(2) 通讯完整性；

(3) 通讯完整性和信息机密性；

(4) 用户的身份识别和验证、强制授权执行，可追溯和统计的事件，软件和信息完整性

(5) 区域边界保护，应用程序分区。

6）进一步迭代风险评估

在应用安全级别SL1后，风险评估将重新执行，见下表。

表 5

风险事件	概率	影响	减轻说明
i.对监测系统的拒绝服务攻击	C	4（单个） 3 （扩展）	实施DoS保护会使攻击更加困难,如:数据包过滤。
ii.篡改监测系统发送的数据	E	3（单个） 2 （扩展）	实现通信完整性，如使用TLS将使篡改攻击不可能。但并非完全不可能，因为可能出现新的和未知的漏洞。
iii. 伪装成监测系统发送数据	E	3（单个） 2 （扩展）	实现通信完整性和机密性，例如使用具有相互身份验证的TLS将使欺骗攻击不可能。但并非完全不可能，因为可能会出现新的和未知的漏洞。
iv.取得监测系统的所有权	E	3（单个） 2 （扩展）	在监测系统上实施身份验证、账户管理和审核将使远程攻击无法获得所有权
v.通过监测系统攻击控制系统	F	2（单个） 1（扩展）	从控制系统对监测系统进行分区将使攻击变得极不可能

表 6

概率	严重程度			
	1-高	2-中	3-低	4- 可忽略
A - 频繁				
B - 很可能				
C - 偶尔			i	
D - 极少				
E - 几乎不可能		ii,iii,iv		
F - 不可能	v			

以上风险评估表明，某些风险仍需要利益相关方进行评审。如果风险被认为是不可接受的，则需要定义额外的保护层。

中国电梯协会标准

基于物联网的电梯、自动扶梯和自动人行道监测系统的网络安全标准通用要求

T/CEA 703-202X

*

中国电梯协会

地址：065000 河北省廊坊市金光道 61 号

Add：61 Jin-Guang Ave.，Langfang，Hebei 065000，P.R. China

电话/Tel：（0316）2311426，2012957

传真/Fax：（0316）2311427

电子邮箱/Email：info@cea-net.org

网址/URL：http://www.elevator.org.cn