

中华人民共和国国家标准

GB/T 47689—2026

网络安全技术 嵌入式操作系统安全技术规范

Cybersecurity technology—Security technical specification for embedded operating system

2026-05-25 发布

2026-12-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 通则 1

6 安全技术要求 2

 6.1 安全功能要求 2

 6.2 安全保障要求 5

7 测试方法 8

 7.1 安全功能测试 8

 7.2 安全保障评估 13

附录 A（规范性） 嵌入式操作系统典型应用场景安全技术要求 17

 A.1 工业控制场景 17

 A.2 网络通信场景 18

 A.3 消费物联网场景 19

 A.4 低空经济场景 21

参考文献 23

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。

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国网络安全审查认证和市场监管大数据中心、中国移动通信集团有限公司、公安部第三研究所、上海市信息安全测评认证中心、中国电子科技集团公司第十五研究所、国家信息技术安全研究中心、国家工业信息安全发展研究中心、中国信息安全测评中心、南京翼辉信息技术有限公司、北京天融信网络安全技术有限公司、中兴通讯股份有限公司、华为技术有限公司、新华三技术有限公司、中国信息通信研究院、北京中关村实验室、麒麟软件有限公司、北京智芯微电子科技有限公司、北京神州绿盟科技有限公司、北京梆梆安全科技有限公司、中国信息通信科技集团有限公司、宁波和利时信息安全研究院有限公司、OPPO 广东移动通信有限公司、广东为辰信息科技有限公司、中国电力科学研究院有限公司、中科方德软件有限公司、浪潮电子信息产业股份有限公司、郑州信大捷安信息技术股份有限公司、长扬科技(北京)股份有限公司、浙江望安科技有限公司、北京可信华泰信息技术有限公司、联想(北京)有限公司、深信服科技股份有限公司、鹿客科技(北京)股份有限公司、深圳供电局有限公司、宝德计算机系统股份有限公司。

本文件主要起草人：申永波、布宁、李蒙、王雷、李雪莹、张阳、袁泉、任永攀、李锋、严妍、杨明、董晶晶、李敏、缪皓、王峰、王宇航、刘继顺、宋好好、雷晓锋、安高峰、徐立锋、万晓兰、袁琦、路晔绵、辛伟、吴春光、赵峰、李德建、韩学宝、楚兵、李腾、刘哲、李东宏、卢佐华、吴国燕、赵焕宇、王也、郭海兵、贾玲、宋桂香、刘为华、王小松、胡杨、张峰、田健生、赵华、刘俊、孙政华、向阳、孙强强、邓克武。

网络安全技术 嵌入式操作系统安全技术规范

1 范围

本文件规定了嵌入式操作系统的通用安全技术要求,并描述了相应的测试方法。

本文件适用于指导工业控制、网络通信、消费物联网、低空经济等典型应用场景中嵌入式操作系统的设计、开发、测试和应用,其他应用场景参照使用。

本文件不适用于部署在台式微型计算机、便携式微型计算机、工作站、服务器等上的操作系统。

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 18336(所有部分) 网络安全技术 信息技术安全评估准则

GB/T 22033—2017 信息技术 嵌入式系统术语

GB/T 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 18336(所有部分)、GB/T 22033—2017 和 GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

嵌入式操作系统 embedded operating system

满足嵌入式系统应用环境特殊要求的操作系统软件。

[来源:GB/T 22033—2017,2.005]

4 缩略语

下列缩略语适用于本文件。

I/O:输入/输出(Input/Output)

MAC:媒体访问控制(Media Access Control)

5 通则

嵌入式操作系统一般运行于计算和存储能力有特定要求的计算机系统或硬件设备上,具有专用性强、系统精简、实时性高、多任务等特点。嵌入式操作系统通常包括基础功能和安全功能,基础功能一般包括硬件管理模块(驱动、板级支持包)、计算模块(任务管理、进程管理)、存储模块、通信模块、软件(系统软件、应用软件)管理模块、人机交互模块、用户管理模块等,安全功能一般包括网络接入安全、通信安

全、身份鉴别、访问控制等,嵌入式操作系统安全框架见图 1。嵌入式操作系统应用广泛,不同应用场景功能需求差异较大,通过对嵌入式操作系统的裁剪与配置,实现不同功能组合,能符合多种应用场景的需求。

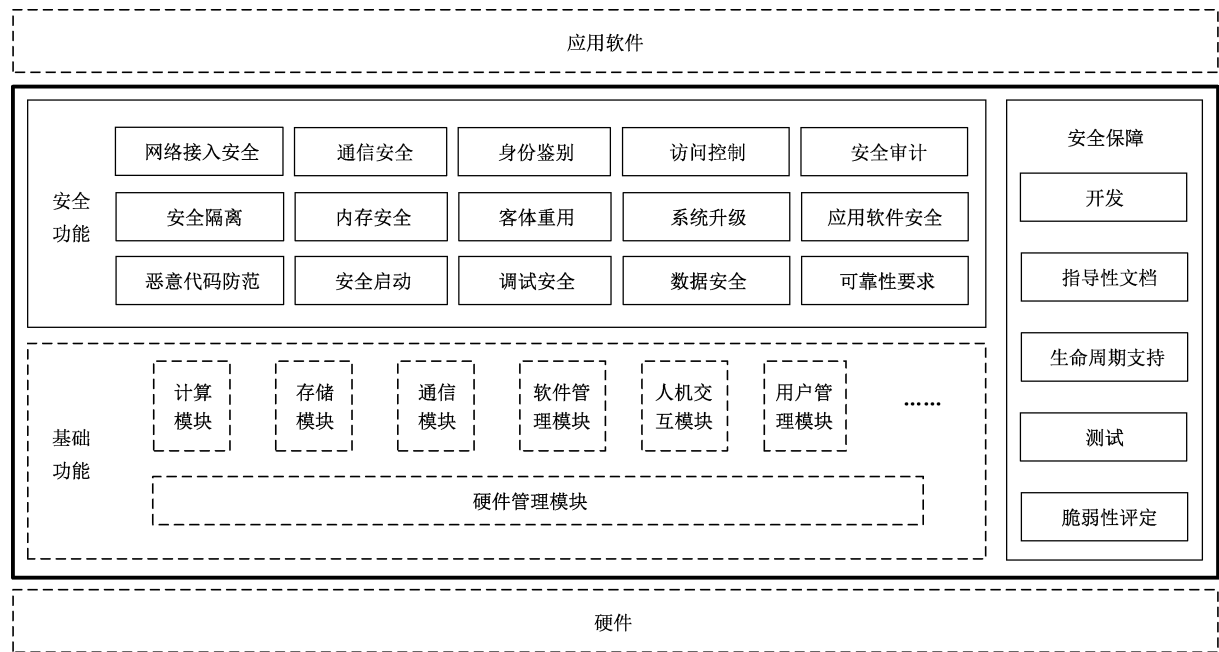


图 1 嵌入式操作系统安全框架

嵌入式操作系统的安全技术要求分为安全功能要求和安全保障要求。安全功能要求包括网络接入安全、通信安全、身份鉴别、访问控制、安全审计、安全隔离、内存安全、客体重用、系统升级、应用软件安全、恶意代码防范、安全启动、调试安全、数据安全、可靠性要求。安全保障要求包括开发、指导性文档、生命周期支持、测试和脆弱性评定。

根据可实现的安全功能和安全保障的强弱,嵌入式操作系统安全技术要求分为基本级和增强级。本文件中“**宋体加粗**”条款所描述的安全要求仅适用于增强级。

第 6 章规定的安全技术要求涵盖嵌入式操作系统多种场景,使用时应根据具体应用场景和实际安全需求确定适用条款。工业控制、网络通信、消费物联网、低空经济四种典型应用场景的嵌入式操作系统安全技术要求应符合附录 A 的规定。

6 安全技术要求

6.1 安全功能要求

6.1.1 网络接入安全

6.1.1.1 网络接入鉴别

功能要求如下：

- a) 应具备对终端设备进行唯一网络身份标识的功能；
- b) 应具备对终端设备网络接入的双向身份鉴别机制。

6.1.1.2 网络访问控制

功能要求如下：

- a) 应符合网络端口最小化暴露原则,禁用业务需求以外的通信端口;
- b) 应能设置网络访问控制策略,防止非授权的网络访问;
- c) 应具备对网络流量进行限制功能。

6.1.2 通信安全

功能要求如下:

- a) 应采用基于密码技术的安全机制,保证控制指令、鉴别数据、密钥数据等重要数据传输的完整性和保密性,采用的密码技术符合国家密码管理部门相关规定;
- b) 应采用安全措施,如使用序列码或时间戳等机制,防止重放攻击。

6.1.3 身份鉴别

对于具有用户登录操作系统的场景,系统具备身份鉴别功能,要求如下:

- a) 应对用户身份进行标识和鉴别;
- b) 使用口令鉴别方式时,应提供身份鉴别信息复杂度验证功能;
- c) 应提供登录失败处理功能,如采取限制连续登录失败次数等措施;
- d) 应采用二种或二种以上的组合鉴别技术对用户身份进行鉴别。

6.1.4 访问控制

功能要求如下:

- a) 在安全策略控制范围内,主体应对其创建的客体具有相应的访问操作权限,并能将这些权限的部分或全部授予其他主体;
- b) 应授权用户或进程完成任务所需的最小权限;
- c) 控制范围应覆盖所有主体、客体以及它们的操作;
- d) 应能对主、客体进行安全标记,并根据强制访问控制策略,控制主体对客体的访问。

6.1.5 安全审计

功能要求如下。

- a) 应提供安全审计机制,记录系统安全事件。
- b) 宜对与嵌入式操作系统安全相关的以下事件进行审计:
 - 1) 用户登录和退出;
 - 2) 增加、删除、修改用户账号和口令;
 - 3) 导入导出系统配置;
 - 4) 修改系统关键配置;
 - 5) 重启和升级系统;
 - 6) 修改系统时间;
 - 7) 系统运行时异常行为(如内存篡改、用户提权);
 - 8) 其他系统安全操作。
- c) 审计记录宜包括安全事件的主体、客体、时间、类型和结果等内容。
- d) 宜提供审计记录查询功能。
- e) 应提供审计记录保护功能,避免未经授权访问、修改或删除。

6.1.6 安全隔离

功能要求如下:

- a) 应具备操作系统程序与应用程序之间的隔离功能；
- b) 应具备应用程序之间的隔离功能；
- c) 应具备基于硬件的隔离机制；
- d) 宜具备 I/O 设备的访问控制和隔离机制，防止未授权访问；
- e) 宜能基于轻量级容器技术，实现应用程序的运行环境隔离。

6.1.7 内存安全

功能要求如下：

- a) 应具备进程之间的内存隔离功能；
- b) 应提供堆栈溢出检测和保护机制，避免堆栈溢出后破坏系统其他内存区域数据。

6.1.8 客体重用

功能要求如下：

- a) 在主体活动结束后，主体占用的存储客体中的信息不应被另一个主体使用；
- b) 对客体初始指定、分配或再分配一个主体之前，应撤销该客体所含信息的所有授权；
- c) 当主体获得对一个已被释放客体的访问权时，当前主体不应获得原主体活动所产生的任何信息。

6.1.9 系统升级

功能要求如下：

- a) 应具备操作系统更新升级机制，只有授权的操作系统版本才能更新；
- b) 升级时，应对更新文件的来源和完整性进行校验；
- c) 升级前后系统安全配置应保持一致；
- d) 在升级失败时，应能实现版本回滚，并保证系统完整性，且配置与更新升级前或出厂时一致；
- e) 应采取安全措施，对超级用户权限进行管控，保证安全更新。

6.1.10 应用软件安全

对于能进行应用软件安装的场景，系统应具备应用软件安全功能，功能要求如下。

- a) 应用软件的安装、卸载符合以下要求：
 - 1) 用户应能对应用软件的安装进行授权或禁止；
 - 2) 应具备应用软件白名单等安全标识机制，并宜将标识的应用软件纳入到强制访问控制机制范围；
 - 3) 应能对应用软件更新包来源进行真实性验证，更新前进行完整性校验；
 - 4) 应在应用软件卸载时删除由其生成的资源文件、配置文件和用户数据。
- b) 用户应能对应用软件使用的终端资源(包含通信资源和外设接口)和终端数据进行确认。

6.1.11 恶意代码防范

功能要求如下：

- a) 系统不应存在已公布的漏洞，或具备补救措施以防范漏洞安全风险；
- b) 预装软件、补丁包/升级包不应存在恶意代码；
- c) 应能安装恶意代码防护软件，并定期进行升级和更新。

6.1.12 安全启动

功能要求如下：

- a) 操作系统启动时应应对操作系统内核、可执行程序等进行完整性度量；
- b) 应对完整性度量基准值进行安全存储，防止其被篡改；
- c) 宜具有硬件可信根，并基于可信根实现系统的可信启动。

6.1.13 调试安全

功能要求如下：

- a) 设备出厂时应禁用系统调试接口，对于确有需求的，应采取限制或控制措施；
- b) 系统应采取安全措施，防止动态加载或卸载内核模块。

6.1.14 数据安全

6.1.14.1 数据完整性

功能要求如下：

- a) 应对存储的重要数据（如鉴别数据、密钥数据、系统配置数据等）进行完整性校验；
- b) 应在检测到完整性错误时采用必要的恢复措施。

6.1.14.2 数据可用性

功能要求如下：

- a) 应能对重要数据（如保证系统正常运行的基本数据等）进行备份；
- b) 应具备数据丢失防护机制，检测到系统存储空间即将耗尽时，能采取必要的措施（如告警、开辟临时存储区域等），防止数据丢失。

6.1.14.3 数据保密性

应对鉴别数据、密钥数据、系统配置数据等重要数据进行加密存储保护。

6.1.15 可靠性要求

6.1.15.1 资源限制

系统应提供资源使用的检测和控制机制，防止应用程序因逻辑错误或恶意行为无限制消耗资源。

6.1.15.2 失效保护

系统应能自检出已定义的系统故障，并提供对应的保护措施，避免系统因故障处于失效状态。

6.1.15.3 可靠时钟

系统应提供手工设定系统时钟，或通过远程时钟服务自动同步时钟等系统时钟设置功能。

6.2 安全保障要求

6.2.1 开发

6.2.1.1 安全架构

开发者应提供嵌入式操作系统安全功能的安全架构描述，安全架构描述应符合以下要求：

- a) 与系统设计文档中对安全功能实施抽象描述的级别一致；
- b) 描述与安全功能要求一致的嵌入式操作系统安全功能的安全域；
- c) 描述嵌入式操作系统安全功能初始化过程为何是安全的；

- d) 证实嵌入式操作系统安全功能能防止被破坏；
- e) 证实嵌入式操作系统安全功能能防止安全特性被旁路。

6.2.1.2 功能规范

开发者应提供系统功能规范说明,功能规范说明应符合以下要求:

- a) 描述嵌入式操作系统的安全功能;
- b) 描述所有安全功能接口的目的与使用方法;
- c) 标识和描述每个安全功能接口相关的所有参数;
- d) 描述安全功能接口相关的安全功能实施行为;
- e) 描述由安全功能实施行为处理而引起的直接错误消息;
- f) 证实安全功能要求到安全功能接口的追溯。

6.2.1.3 实现表示

开发者应为全部安全功能提供实现表示,应符合以下要求:

- a) 实现表示按详细级别定义系统安全功能,且详细程度达到无需进一步说明就能生成系统安全功能的程度;
- b) 实现表示以开发人员使用的形式提供;
- c) 设计描述与实现表示示例之间的映射能证明它们的一致性。

6.2.1.4 系统设计

开发者应提供系统设计文档,系统设计文档应符合以下要求:

- a) 根据子系统描述嵌入式操作系统结构;
- b) 根据模块描述嵌入式操作系统安全功能;
- c) 标识和描述嵌入式操作系统安全功能的所有子系统;
- d) 描述安全功能所有子系统间的相互作用;
- e) 提供的映射关系能证实设计中描述的所有行为能映射到调用它的安全功能接口;
- f) 根据模块描述安全功能;
- g) 提供安全功能子系统到模块间的映射关系;
- h) 描述所有安全功能实现模块,包括其目的及与其他模块间的相互作用;
- i) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口;
- j) 描述所有安全功能的支撑或相关模块,包括其目的及与其他模块间的相互作用。

6.2.2 指导性文档

6.2.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南,操作用户指南与为评估而提供的其他所有文档保持一致,对每一种用户角色的描述应符合以下要求:

- a) 描述在安全处理环境中被控制的用户可访问的功能和特权,包含适当的警示信息;
- b) 描述如何以安全的方式使用嵌入式操作系统提供的可用接口;
- c) 描述可用功能和接口,尤其是受用户控制的所有安全参数,适当时指明安全值;
- d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件,包括改变安全功能所控制实体的安全特性;

- e) 标识嵌入式操作系统运行的所有可能状态(包括操作导致的失败或者操作性错误),以及它们与维持安全运行之间的因果关系和联系;
- f) 明确说明为实现安全目的所执行的安全策略。

6.2.2.2 准备程序

开发者应提供嵌入式操作系统及其准备程序,准备程序描述应符合以下要求:

- a) 描述与开发者交付程序相一致的安全接收所交付嵌入式操作系统必需的所有步骤;
- b) 描述安全安装嵌入式操作系统及其运行环境必需的所有步骤。

6.2.3 生命周期支持

6.2.3.1 配置管理能力

开发者的配置管理能力应符合以下要求:

- a) 为系统的不同版本提供唯一的标识;
- b) 使用配置管理系统对组成系统的所有配置项进行维护,并唯一标识配置项;
- c) 提供配置管理文档,配置管理文档描述用于唯一标识配置项的方法;
- d) 配置管理系统提供一种自动方式来支持系统的生产,通过该方式保证只能对系统的实现表示进行已授权的改变;
- e) 配置管理文档包括一个配置管理计划,配置管理计划描述如何使用配置管理系统开发系统;
- f) 配置管理计划描述用来接受修改过的或新建的作为系统组成部分的配置项的程序;
- g) 实施的配置管理与配置管理计划相一致。

6.2.3.2 配置管理范围

开发者应提供嵌入式操作系统配置项列表,配置项列表应符合以下要求:

- a) 包括系统、安全保障要求的评估证据和系统的组成部分;
- b) 实现表示、安全缺陷报告及其解决状态。

6.2.3.3 交付程序

开发者应使用一定的交付程序交付嵌入式操作系统,并将交付过程文档化。在给用户方交付嵌入式操作系统的各版本时,交付文档应描述为维护安全所必需的所有程序。

6.2.3.4 开发安全

开发者应提供开发安全文档,开发安全文档应描述在系统的开发环境中,为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.2.3.5 生命周期定义

开发者应建立一个生命周期模型对系统的开发和维护进行必要的控制,并提供生命周期定义文档描述用于开发和维护系统的模型。

6.2.3.6 工具和技术

开发者应明确定义用于开发系统的工具,并提供开发工具文档无歧义地定义实现中每个语句的含义和所有实现依赖选项的含义。

6.2.4 测试

6.2.4.1 覆盖证据

开发者应提供测试覆盖文档,测试覆盖描述应表明测试文档中所标识的测试与功能规范中所描述的嵌入式操作系统的安全功能间的对应性。

6.2.4.2 覆盖分析

开发者应提供测试覆盖文档,测试覆盖描述应符合以下要求:

- a) 表明测试文档中所标识的测试与功能规范中所描述的系统的的功能接口间的对应性;
- b) 表明上述对应性是完备的,并证实功能规范中的所有安全功能接口都进行了测试。

6.2.4.3 深度分析

开发者应提供测试深度分析,测试深度分析应符合以下要求:

- a) 论证测试文档中的测试与系统设计中的嵌入式操作系统安全功能子系统、安全功能要求执行模块之间的一致性;
- b) 论证系统设计中的所有嵌入式操作系统安全功能子系统都已经进行过测试;
- c) 论证系统设计中的安全功能要求执行模块都已经进行过测试。

6.2.4.4 功能测试

开发者应测试嵌入式操作系统安全功能,将结果文档化并提供测试文档。测试文档应包括以下内容:

- a) 测试计划,标识要执行的测试,并描述执行每个测试的方案,这些方案包括对于其他测试结果的任何顺序依赖性;
- b) 预期的测试结果,表明测试成功后的预期输出;
- c) 实际测试结果和预期的测试结果一致。

6.2.4.5 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源,以用于安全功能的抽样测试。

6.2.5 脆弱性评定

6.2.5.1 基本级脆弱性分析

基于已标识的潜在脆弱性,嵌入式操作系统能抵抗具有基本攻击潜力攻击者的攻击。

6.2.5.2 增强级脆弱性分析

基于已标识的潜在脆弱性,嵌入式操作系统能抵抗具有增强型攻击潜力攻击者的攻击。

7 测试方法

7.1 安全功能测试

7.1.1 网络接入安全

7.1.1.1 网络接入鉴别

网络接入鉴别的测试方法如下:

- a) 查看系统设计文档,确认系统是否具备对终端设备生成网络身份标识功能,查看其对终端设备进行网络身份标识的机制,并确认身份标识机制是否能保证标识唯一;
- b) 登录系统,使用工具或者查看源代码,验证是否按照设计文档描述的机制对终端设备生成网络身份标识,且标识唯一;
- c) 将终端设备与网络连接,使用工具抓包查看采用的身份鉴别机制,检查终端设备嵌入式操作系统侧是否能使用基于标识或密码技术的鉴别技术对平台侧进行鉴别,并确认终端设备是否提供凭证才能成功接入平台网络。

7.1.1.2 网络访问控制

网络访问控制的测试方法如下:

- a) 查看系统设计文档,确认系统是否默认仅开启业务需要的网络通信端口;
- b) 使用端口扫描工具进行验证,确认默认情况下系统是否仅开启了设计文档中声明的网络通信端口,禁用业务需求以外的通信端口;
- c) 查看系统设计文档,确认系统能实现的网络访问控制策略,如基于网络地址、MAC 地址、端口或协议相关访问控制策略;
- d) 配置相应的访问控制策略,逐一操作验证网络访问控制策略是否有效,只有符合策略的进程才能访问系统所在的终端设备以及只有符合策略的数据报文才能访问系统所在设备;
- e) 查看系统是否具有网络流量限制功能,配置流量限制策略,发送相应的流量,确认流量限制策略是否生效。

7.1.2 通信安全

通信安全的测试方法如下:

- a) 查看系统设计文档,确认操作系统对控制指令、鉴别数据、密钥数据等重要数据传输的完整性和保密性机制,确认其采用的密码技术是否符合国家密码管理部门相关规定;
- b) 使用抓包分析工具对系统传输完整性和保密性机制进行验证,确认系统是否能保证数据传输的完整性和保密性;
- c) 查看系统设计文档,确认系统实现的防止重放攻击的机制,如使用序列码或时间戳等;
- d) 使用抓包分析和重放工具验证系统是否实现了设计文档中描述的防止重放攻击机制,并确认是否能防止重放攻击。

7.1.3 身份鉴别

身份鉴别的测试方法如下:

- a) 对于具有登录操作系统场景的终端设备,执行新建用户操作,确认是否不能创建相同标识的用户;
- b) 使用用户标识和鉴别信息进行登录操作,确认系统身份鉴别机制是否有效;
- c) 对于使用口令鉴别的机制,检查系统是否提供身份鉴别信息复杂度验证功能,是否允许用户设置弱口令,如空口令、纯数字等;
- d) 尝试连续多次失败登录系统,确认系统是否触发登录失败处理功能,防止用户进一步登录尝试;
- e) 查看系统是否能应用二种或二种以上的组合鉴别技术对用户身份进行鉴别,并验证鉴别机制是否有效。

7.1.4 访问控制

访问控制的测试方法如下:

- a) 操作验证用户对其创建的客体是否具有相应的访问操作权限,验证其可执行的操作是否与安全策略一致;
- b) 尝试将这些权限部分或全部授予其他用户,检查其操作是否成功;
- c) 查看系统设计文档,在系统中验证用户或进程是否仅具有完成任务所需的最小权限;
- d) 使用系统不同的主体用户登录系统,验证其对客体的操作是否均与其访问控制策略一致;
- e) 验证系统是否具备强制访问控制功能,授权管理员是否能对主、客体进行安全标记;
- f) 使用不同标记的主体登录系统,尝试对不同安全标记的客体执行相应操作,确认其能执行的操作是否符合强制访问控制策略。

7.1.5 安全审计

安全审计的测试方法如下。

- a) 验证系统是否提供安全审计功能。
- b) 针对系统尝试执行如下操作,查看系统是否生成了相应的审计日志:
 - 1) 用户登录和退出;
 - 2) 增加、删除、修改用户账号和口令;
 - 3) 导入导出系统配置;
 - 4) 修改系统关键配置;
 - 5) 重启和升级系统;
 - 6) 修改系统时间;
 - 7) 系统运行时异常行为(如内存篡改、用户提权);
 - 8) 其他系统安全操作。
- c) 查看系统生成的审计记录,确认其是否包括安全事件的主体、客体、时间、类型和结果等内容。
- d) 以授权用户身份登录系统,查看系统是否提供审计记录查询功能。
- e) 查看系统设计文档,确认其是否提供了审计记录保护功能,登录系统验证系统提供的审计记录保护功能是否有效,是否能防止未授权访问、修改或删除审计记录。

7.1.6 安全隔离

安全隔离的测试方法如下:

- a) 查看系统设计文档,确认其是否具有操作系统程序与应用程序隔离、应用程序之间隔离的机制;
- b) 登录系统,验证系统对操作系统程序与应用程序隔离的机制是否有效;
- c) 登录系统,验证系统对应用程序之间隔离机制是否有效;
- d) 查看系统设计文档,确认系统是否具备基于硬件隔离机制、具备 I/O 设备的访问控制和隔离机制、具备轻量级容器技术实现应用程序运行环境隔离机制;
- e) 登录系统,使用测试工具或者查看源代码方式验证设计文档中描述的硬件隔离机制是否有效;
- f) 登录系统,使用测试工具验证设计文档中描述的 I/O 设备访问控制和隔离机制是否有效;
- g) 配置容器环境,验证设计文档中描述的轻量级容器技术实现应用程序运行环境隔离机制是否有效。

7.1.7 内存安全

内存安全的测试方法如下:

- a) 查看系统设计文档,确认其是否能在进程之间实现内存隔离;
- b) 使用测试工具或者查看源代码的方式,验证进程之间的内存隔离机制是否有效;

- c) 查看系统设计文档,确认其是否提供堆栈溢出检测和保护功能;
- d) 登录系统,开启堆栈溢出检测和保护功能,验证功能是否有效。

7.1.8 客体重用

客体重用的测试方法如下:

- a) 登录系统,测试验证一个主体活动结束后,主体占用的存储客体中的信息是否不能被另一个主体使用;
- b) 验证系统对客体初始指定、分配或再分配一个主体之前,是否撤销了该客体所含信息的所有授权;
- c) 验证系统在主体获得对一个已被释放客体的访问权时,当前主体是否不能获得原主体活动所产生的任何信息。

7.1.9 系统升级

系统升级的测试方法如下:

- a) 查看系统设计文档,确认系统更新升级机制;
- b) 配置环境,准备升级包,尝试进行系统升级,验证是否仅授权的操作系统版本能进行升级更新;
- c) 对授权的操作系统版本尝试进行升级操作,验证系统是否对更新文件来源和完整性进行校验;
- d) 对授权的操作系统版本尝试进行升级操作,验证升级前后的系统安全配置是否保持一致;
- e) 对授权的操作系统版本尝试进行升级操作,验证升级失败时系统是否能进行回滚,是否能保持系统完整性,安全配置与更新升级前或出厂时一致;
- f) 查看验证系统是否实现了严格控制超级用户权限的机制,如强制访问控制机制等,保证更新升级时的安全性。

7.1.10 应用软件安全

应用软件安全的测试方法如下。

- a) 查看并验证应用软件的安装、卸载是否符合以下安全要求:
 - 1) 用户能对应用软件的安装进行授权或禁止;
 - 2) 具备应用软件白名单等安全标识机制,若标识的应用软件纳入到强制访问控制机制范围,则进行强制访问控制机制验证;
 - 3) 能对应用软件更新包来源进行真实性验证,更新前进行完整性校验;
 - 4) 在应用软件卸载时删除由其生成的资源文件、配置文件和用户数据。
- b) 查看并验证用户是否能对应用软件使用的终端资源(包含通信资源和外设接口)和终端数据进行确认。

7.1.11 恶意代码防范

恶意代码防范的测试方法如下:

- a) 使用漏洞扫描工具对系统进行扫描,检查是否不存在已公布的安全漏洞,对于扫描存在的安全漏洞,是否具备补救措施以防范漏洞安全风险;
- b) 使用安全检测工具检查系统预装软件、补丁包/升级包,确认其是否存在恶意代码;
- c) 授权用户身份登录系统,尝试安装恶意代码防护软件,检查是否能成功;
- d) 恶意代码防护软件安装成功后,验证是否能定期进行升级和更新。

7.1.12 安全启动

安全启动的测试方法如下:

- a) 查看系统设计文档,确认系统启动时对操作系统内核、可执行程序等进行完整性度量的机制;
- b) 使用测试工具或者通过查看源代码的方式,验证系统启动时是否对操作系统内核、可执行程序进行了完整性度量;
- c) 使用测试工具或者通过查看源代码的方式,确认系统是否对完整性度量基准值进行了安全存储;
- d) 验证系统是否具有硬件可信根,并基于可信根实现系统可信启动。

7.1.13 调试安全

调试安全的测试方法如下:

- a) 查看系统设计文档,确认设备出厂时调试接口禁用情况,未禁用的调试接口查看其必要性说明;
- b) 使用端口扫描工具对系统进行扫描,检查是否存在调试接口(含远程),对于存在的调试接口,尝试对内核进行编译调试,检查是否禁用了对内核调试的相关命令或采取了相关限制措施;
- c) 查看系统设计文档,确认系统采取防止动态加载或卸载内核模块的机制;
- d) 使用测试工具或者查看源代码的方式,验证系统防止动态加载或卸载内核模块的机制是否有效。

7.1.14 数据安全

7.1.14.1 数据完整性

数据完整性的测试方法如下:

- a) 查看系统设计文档,确认对存储的重要数据(如鉴别数据、密钥数据、系统配置数据)进行完整性校验机制;
- b) 登录系统,使用测试工具验证系统对存储重要数据进行完整性校验机制是否有效;
- c) 使用测试工具验证系统在检测到完整性错误时是否采用必要的恢复措施。

7.1.14.2 数据可用性

数据可用性的测试方法如下:

- a) 查看系统设计文档,确认系统对重要数据(如保证系统正常运行的基本数据等)进行备份的机制;
- b) 登录系统,尝试对系统重要数据进行破坏,验证系统对重要数据备份机制能否生效;
- c) 登录系统,尝试耗尽系统存储空间,验证系统是否具有数据丢失防护机制,如告警、开辟临时存储区域等。

7.1.14.3 数据保密性

登录系统,使用工具分析存储的鉴别数据、密钥数据、系统配置数据等重要数据,验证其是否进行了加密保护。

7.1.15 可靠性要求

7.1.15.1 资源限制

资源限制的测试方法如下:

- a) 查看系统设计文档,确认系统提供的资源使用检测和控制机制;
- b) 登录系统,验证系统提供的资源使用检测和控制机制是否能防止因应用程序逻辑错误或恶意

行为无限制消耗资源。

7.1.15.2 失效保护

失效保护的测试方法如下：

- a) 查看系统设计文档，确认系统能自检出已定义的系统故障；
- b) 登录系统，尝试模拟系统设计文档中描述的能自检的系统故障，验证操作系统是否能检测出相应的故障，并提供相应的保护措施，如系统具有维护模式或通过减少功能、降低性能等方式提供基本服务，在系统不能正常启动且安全功能失效情况下，可通过启动维护模式，进行系统修复。

7.1.15.3 可靠时钟

登录系统，验证系统是否具有手工设定系统时钟或通过远程时钟服务自动同步系统时钟的功能。

7.2 安全保障评估

7.2.1 开发

7.2.1.1 安全架构

审查安全架构文档是否准确描述如下内容：

- a) 与系统设计文档中对安全功能实施抽象描述的级别一致；
- b) 描述与安全功能要求一致的嵌入式操作系统安全功能的安全域；
- c) 描述嵌入式操作系统安全功能初始化过程为何是安全的；
- d) 证实嵌入式操作系统安全功能能防止被破坏；
- e) 证实嵌入式操作系统安全功能能防止安全特性被旁路。

7.2.1.2 功能规范

审查功能规范文档是否准确描述如下内容：

- a) 完全描述嵌入式操作系统的安全功能；
- b) 描述所有安全功能接口的目的与使用方法；
- c) 标识和描述每个安全功能接口相关的所有参数；
- d) 描述安全功能接口相关的安全功能实施行为；
- e) 描述由安全功能实施行为处理而引起的直接错误消息；
- f) 证实安全功能要求到安全功能接口的追溯。

7.2.1.3 实现表示

审查系统设计文档是否准确描述如下内容：

- a) 以开发人员使用的形式提供；
- b) 按详细级别描述系统安全功能，详细程度达到无需进一步说明就能生成安全功能的程度；
- c) 提供系统设计描述与实现表示实例之间的映射，并证明其一致性。

7.2.1.4 系统设计

审查系统设计文档是否准确描述如下内容：

- a) 根据子系统描述嵌入式操作系统结构；
- b) 根据模块描述嵌入式操作系统安全功能；

- c) 标识和描述嵌入式操作系统安全功能的所有子系统；
- d) 描述安全功能所有子系统间的相互作用；
- e) 提供的映射关系能证实设计中描述的所有行为能映射到调用它的安全功能接口；
- f) 根据模块描述安全功能；
- g) 提供安全功能子系统到模块间的映射关系；
- h) 描述所有安全功能实现模块,包括其目的及与其他模块间的相互作用；
- i) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
- j) 描述所有安全功能的支撑或相关模块,包括其目的及与其他模块间的相互作用。

7.2.2 指导性文档

7.2.2.1 操作用户指南

审查操作用户指南是否准确描述如下内容：

- a) 描述在安全处理环境中被控制的用户可访问的功能和特权,包含适当的警示信息；
- b) 描述如何以安全的方式使用嵌入式操作系统提供的可用接口；
- c) 描述可用功能和接口,尤其是受用户控制的所有安全参数,适当时指明安全值；
- d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件,包括改变安全功能所控制实体的安全特性；
- e) 标识嵌入式操作系统运行的所有可能状态(包括操作导致的失败或者操作性错误),以及它们与维持安全运行之间的因果关系和联系；
- f) 明确说明为实现安全目的所执行的安全策略。

7.2.2.2 准备程序

审查准备程序文档是否准确描述如下内容：

- a) 描述与开发者交付程序相一致的安全接收所交付嵌入式操作系统必需的所有步骤；
- b) 描述安全安装嵌入式操作系统及其运行环境必需的所有步骤。

7.2.3 生命周期支持

7.2.3.1 配置管理能力

配置管理能力的评估方法如下：

- a) 审查开发者是否为不同版本的嵌入式操作系统提供唯一的标识；
- b) 现场检查配置管理系统是否对所有的配置项作出唯一的标识,且配置管理系统是否对配置项进行了维护；
- c) 审查开发者提供的配置管理文档,是否描述了对配置项进行唯一标识的方法；
- d) 配置管理系统是否提供一种自动方式来支持系统的生成,通过该方式保证只能对系统的实现表示进行已授权的改变；
- e) 配置管理文档是否包括一个配置管理计划,配置管理计划是否描述如何使用配置管理系统开发系统,实施的配置管理与配置管理计划是否相一致；
- f) 配置管理计划是否描述用来接受修改过的或新建的作为系统组成部分的配置项的程序；
- g) 实施的配置管理与配置管理计划是否一致。

7.2.3.2 配置管理范围

配置管理范围的评估方法如下：

- a) 检查系统提供者提供的配置项列表；
- b) 检查配置项列表是否描述了组成系统的全部配置项及相应的开发者；
- c) 检查系统提供者是否将实现表示、安全缺陷报告及其解决状态纳入配置管理范围，是否对安全缺陷进行跟踪。

7.2.3.3 交付程序

交付程序的评估方法如下：

- a) 现场检查开发者是否使用一定的交付程序交付嵌入式操作系统；
- b) 审查开发者是否使用文档描述交付过程，文档中是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

7.2.3.4 开发安全

审查开发者是否使用文档描述在系统的开发环境中，为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

7.2.3.5 生命周期定义

生命周期定义的评估方法如下：

- a) 审查开发者是否建立一个生命周期模型对系统的开发和维护进行必要的控制；
- b) 审查开发者是否提供生命周期定义文档描述用于开发和维护系统的模型。

7.2.3.6 工具和技术

工具和技术的评估方法如下：

- a) 现场检查开发者是否明确定义用于开发系统的工具；
- b) 审查开发者是否提供开发工具文档，无歧义地描述实现中每个语句的含义和所有依赖于实现的选项的含义。

7.2.4 测试

7.2.4.1 覆盖证据

审查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的嵌入式操作系统的安全功能间的对应性。

7.2.4.2 覆盖分析

覆盖分析的评估方法如下：

- a) 审查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的嵌入式操作系统的安全功能接口是对应的；
- b) 审查是否表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

7.2.4.3 深度分析

深度分析的评估方法如下：

- a) 审查开发者提供的测试深度分析文档,在测试深度分析中,是否表明测试文档中的测试与系统设计中的嵌入式操作系统安全功能子系统、安全功能要求执行模块之间的一致性;
- b) 审查是否表明系统设计中的所有嵌入式操作系统安全功能子系统都已经进行过测试;
- c) 审查是否标明系统设计中的所有安全功能要求执行模块都已经进行过测试。

7.2.4.4 功能测试

功能测试的评估方法如下:

- a) 审查开发者提供的测试文档,是否包括测试计划、预期的测试结果和实际测试结果;
- b) 审查测试计划是否标识了要测试的安全功能,是否描述了每个安全功能的测试方案(包括对其他测试结果的顺序依赖性);
- c) 审查期望的测试结果是否表明测试成功后的预期输出;
- d) 审查实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

7.2.4.5 独立测试

独立测试的评估方法如下:

- a) 评价者应审查开发者提供的测试资源;
- b) 评价者应审查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

7.2.5 脆弱性评定

7.2.5.1 基本级脆弱性分析

从用户可能破坏安全策略的明显途径出发,按照安全机制定义的安全强度级别,对嵌入式操作系统进行脆弱性分析,能抵抗具有基本攻击潜力攻击者的攻击。

7.2.5.2 增强级脆弱性分析

从用户可能破坏安全策略的明显途径出发,按照安全机制定义的安全强度级别,对嵌入式操作系统进行脆弱性分析,能抵抗具有增强型攻击潜力攻击者的攻击。

附 录 A
(规范性)

嵌入式操作系统典型应用场景安全技术要求

A.1 工业控制场景

工业控制场景主要包括制造、能源、电力、交通等细分行业领域,嵌入式操作系统主要应用在制造过程使用到的各种工业控制设备,包括但不限于可编程逻辑控制器(PLC)、远程终端单元(RTU)、工业机器人、数控机床及其他工业装备等。

工业控制场景嵌入式操作系统应符合表 A.1 的安全要求。

表 A.1 工业控制场景嵌入式操作系统安全技术要求

安全技术要求			基本级	增强级
安全功能 要求	网络接入安全	网络接入鉴别	6.1.1.1 a)	6.1.1.1 a)
		网络访问控制	6.1.1.2 a)~b)	6.1.1.2
	通信安全		6.1.2	6.1.2
	身份鉴别		6.1.3 a)~c)	6.1.3
	访问控制		6.1.4 a)~c)	6.1.4
	安全审计		6.1.5 a)~d)	6.1.5
	安全隔离		6.1.6 a)~b)	6.1.6
	内存安全		6.1.7 a)	6.1.7
	客体重用		—	—
	系统升级		6.1.9 a)~c)	6.1.9
	应用软件安全		—	6.1.10 a)
	恶意代码防范		6.1.11 a)~b)	6.1.11 a)~b)
	安全启动		—	6.1.12
	调试安全		6.1.13 a)	6.1.13
	数据安全	数据完整性	6.1.14.1 a)	6.1.14.1
		数据可用性	6.1.14.2 a)	6.1.14.2
		数据保密性	6.1.14.3	6.1.14.3
安全保障 要求	开发	资源限制	6.1.15.1	6.1.15.1
		失效保护	6.1.15.2	6.1.15.2
		可靠时钟	—	6.1.15.3
		安全架构	—	6.2.1.1
	开发	功能规范	6.2.1.2	6.2.1.2
		实现表示	—	6.2.1.3
		系统设计	6.2.1.4 a)~e)	6.2.1.4

表 A.1 工业控制场景嵌入式操作系统安全技术要求（续）

安全技术要求			基本级	增强级
安全保障 要求	指导性文档	操作用户指南	6.2.2.1	6.2.2.1
		准备程序	6.2.2.2	6.2.2.2
	生命周期支持	配置管理能力	6.2.3.1 a)～c)	6.2.3.1
		配置管理范围	6.2.3.2 a)	6.2.3.2
		交付程序	6.2.3.3	6.2.3.3
		开发安全	—	6.2.3.4
		生命周期定义	—	6.2.3.5
		工具和技术	—	6.2.3.6
		测试	覆盖证据	6.2.4.1
	覆盖分析		—	6.2.4.2
	深度分析		—	6.2.4.3
	功能测试		6.2.4.4	6.2.4.4
	独立测试		6.2.4.5	6.2.4.5
	脆弱性评定	基本级脆弱性分析	6.2.5.1	—
		增强级脆弱性分析	—	6.2.5.2
注：“—”表示不适用。				

A.2 网络通信场景

网络通信场景，嵌入式操作系统主要应用在基于无线通信的基站、接入网设备、骨干网/城域网路由、光传输/交换网的通信设备等，也包括基于因特网部署的交换机、路由器、防火墙、负载均衡等通信及安全设备。

网络通信场景嵌入式操作系统应符合表 A.2 的安全要求。

表 A.2 网络通信场景嵌入式操作系统安全技术要求

安全技术要求			基本级	增强级
安全功能 要求	网络接入安全	网络接入鉴别	6.1.1.1 a)	6.1.1.1 a)
		网络访问控制	6.1.1.2 a)～b)	6.1.1.2
	通信安全		6.1.2	6.1.2
	身份鉴别		6.1.3 a)～c)	6.1.3
	访问控制		6.1.4 a)～c)	6.1.4
	安全审计		6.1.5 a)～d)	6.1.5
	安全隔离		6.1.6 a)～b)	6.1.6
	内存安全		6.1.7 a)	6.1.7
	客体重用		—	6.1.8

表 A.2 网络通信场景嵌入式操作系统安全技术要求（续）

安全技术要求			基本级	增强级
安全功能要求	系统升级		6.1.9 a)～c)	6.1.9
	应用软件安全		—	—
	恶意代码防范		6.1.11 a)～b)	6.1.11 a)～b)
	安全启动		—	6.1.12
	调试安全		6.1.13 a)	6.1.13
	数据安全	数据完整性	6.1.14.1 a)	6.1.14.1
		数据可用性	6.1.14.2 a)	6.1.14.2
		数据保密性	6.1.14.3	6.1.14.3
	可靠性要求	资源限制	6.1.15.1	6.1.15.1
		失效保护	6.1.15.2	6.1.15.2
可靠时钟		—	6.1.15.3	
安全保障要求	开发	安全架构	—	6.2.1.1
		功能规范	6.2.1.2	6.2.1.2
		实现表示	—	6.2.1.3
		系统设计	6.2.1.4 a)～e)	6.2.1.4
	指导性文档	操作用户指南	6.2.2.1	6.2.2.1
		准备程序	6.2.2.2	6.2.2.2
	生命周期支持	配置管理能力	6.2.3.1 a)～c)	6.2.3.1
		配置管理范围	6.2.3.2 a)	6.2.3.2
		交付程序	6.2.3.3	6.2.3.3
		开发安全	—	6.2.3.4
		生命周期定义	—	6.2.3.5
		工具和技术	—	6.2.3.6
	测试	覆盖证据	6.2.4.1	6.2.4.1
		覆盖分析	—	6.2.4.2
		深度分析	—	6.2.4.3
		功能测试	6.2.4.4	6.2.4.4
		独立测试	6.2.4.5	6.2.4.5
	脆弱性评定	基本级脆弱性分析	6.2.5.1	—
		增强级脆弱性分析	—	6.2.5.2
注：“—”表示不适用。				

A.3 消费物联网场景

消费物联网场景,以提升消费者自身体验为主导,面向消费者或以消费者为最终用户的物联网应用

领域。嵌入式操作系统主要应用在智能家居、智能门锁、智能可穿戴、智能安防、智能医疗等消费物联网领域的智能终端设备。

消费物联网场景嵌入式操作系统应符合表 A.3 的安全要求。

表 A.3 消费物联网场景嵌入式操作系统安全技术要求

安全技术要求			基本级	增强级
安全功能要求	网络接入安全	网络接入鉴别	6.1.1.1	6.1.1.1
		网络访问控制	6.1.1.2 a)～b)	6.1.1.2
	通信安全		6.1.2	6.1.2
	身份鉴别		6.1.3 a)～c)	6.1.3
	访问控制		6.1.4 a)～c)	6.1.4
	安全审计		6.1.5 a)～d)	6.1.5
	安全隔离		6.1.6 a)～b)	6.1.6
	内存安全		6.1.7 a)	6.1.7
	客体重用		—	—
	系统升级		6.1.9 a)～c)	6.1.9
	应用软件安全		—	6.1.10
	恶意代码防范		6.1.11 a)～b)	6.1.11
	安全启动		—	6.1.12
	调试安全		6.1.13 a)	6.1.13
	数据安全	数据完整性	6.1.14.1 a)	6.1.14.1
		数据可用性	6.1.14.2 a)	6.1.14.2
		数据保密性	6.1.14.3	6.1.14.3
	可靠性要求	资源限制	6.1.15.1	6.1.15.1
		失效保护	6.1.15.2	6.1.15.2
		可靠时钟	—	6.1.15.3
安全保障要求	开发	安全架构	—	6.2.1.1
		功能规范	6.2.1.2	6.2.1.2
		实现表示	—	6.2.1.3
		系统设计	6.2.1.4 a)～e)	6.2.1.4
	指导性文档	操作用户指南	6.2.2.1	6.2.2.1
		准备程序	6.2.2.2	6.2.2.2
	生命周期支持	配置管理能力	6.2.3.1 a)～c)	6.2.3.1
		配置管理范围	6.2.3.2 a)	6.2.3.2
		交付程序	6.2.3.3	6.2.3.3
		开发安全	—	6.2.3.4
		生命周期定义	—	6.2.3.5
		工具和技术	—	6.2.3.6

表 A.3 消费物联网场景嵌入式操作系统安全技术要求（续）

安全技术要求			基本级	增强级
安全保障 要求	测试	覆盖证据	6.2.4.1	6.2.4.1
		覆盖分析	—	6.2.4.2
		深度分析	—	6.2.4.3
		功能测试	6.2.4.4	6.2.4.4
		独立测试	6.2.4.5	6.2.4.5
	脆弱性评定	基本级脆弱性分析	6.2.5.1	—
		增强级脆弱性分析	—	6.2.5.2
注：“—”表示不适用。				

A.4 低空经济场景

低空经济场景,指以民用航空器为主,以载人、载货及其他作业等低空飞行活动为应用场景。嵌入式操作系统主要应用在无人机、电动垂直起降飞行器以及机库、起降场站、空中交通管理设备等低空基础设施。

低空经济场景嵌入式操作系统应符合表 A.4 的安全要求。

表 A.4 低空经济场景嵌入式操作系统安全技术要求

安全技术要求			基本级	增强级
安全功能 要求	网络接入安全	网络接入鉴别	6.1.1.1	6.1.1.1
		网络访问控制	6.1.1.2 a)~b)	6.1.1.2 a)~b)
	通信安全		6.1.2	6.1.2
	身份鉴别		6.1.3 a)~c)	6.1.3
	访问控制		6.1.4 a)~c)	6.1.4
	安全审计		6.1.5 a)~d)	6.1.5
	安全隔离		6.1.6 a)~b)	6.1.6
	内存安全		6.1.7 a)	6.1.7
	客体重用		—	—
	系统升级		6.1.9 a)~c)	6.1.9
	应用软件安全		—	—
	恶意代码防范		6.1.11 a)~b)	6.1.11 a)~b)
	安全启动		—	6.1.12
	调试安全		6.1.13 a)	6.1.13
	数据安全	数据完整性	6.1.14.1 a)	6.1.14.1
		数据可用性	6.1.14.2 a)	6.1.14.2
		数据保密性	6.1.14.3	6.1.14.3

表 A.4 低空经济场景嵌入式操作系统安全技术要求（续）

安全技术要求			基本级	增强级
安全功能要求	可靠性要求	资源限制	6.1.15.1	6.1.15.1
		失效保护	6.1.15.2	6.1.15.2
		可靠时钟	—	6.1.15.3
安全保障要求	开发	安全架构	—	6.2.1.1
		功能规范	6.2.1.2	6.2.1.2
		实现表示	—	6.2.1.3
		系统设计	6.2.1.4 a)～e)	6.2.1.4
	指导性文档	操作用户指南	6.2.2.1	6.2.2.1
		准备程序	6.2.2.2	6.2.2.2
	生命周期支持	配置管理能力	6.2.3.1 a)～c)	6.2.3.1
		配置管理范围	6.2.3.2 a)	6.2.3.2
		交付程序	6.2.3.3	6.2.3.3
		开发安全	—	6.2.3.4
		生命周期定义	—	6.2.3.5
		工具和技术	—	6.2.3.6
	测试	覆盖证据	6.2.4.1	6.2.4.1
		覆盖分析	6.2.4.2	6.2.4.2
		深度分析	—	6.2.4.3
		功能测试	6.2.4.4	6.2.4.4
		独立测试	6.2.4.5	6.2.4.5
	脆弱性评定	基本级脆弱性分析	6.2.5.1	—
		增强级脆弱性分析	—	6.2.5.2
注：“—”表示不适用。				

参 考 文 献

- [1] GB/T 20272—2019 信息安全技术 操作系统安全技术要求
 - [2] GB/T 20276—2016 信息安全技术 具有中央处理器的 IC 卡嵌入式软件安全技术要求
 - [3] GB/T 30284—2020 信息安全技术 移动通信智能终端操作系统安全技术要求
 - [4] GB/T 34976—2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法
 - [5] GB/T 36951—2018 信息安全技术 物联网感知终端应用安全技术要求
 - [6] GB/T 39680—2020 信息安全技术 服务器安全技术要求和测评准则
 - [7] GB 40050—2021 网络关键设备安全通用要求
 - [8] GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求
-

