ICS 25.040.30
CCS J 28

中华人民共和国国家标准

GB/T 45502—2025

服务机器人信息安全通用要求

General requirements for information security of service robots

宜器服务网 YIQIFUWU.COM

2025-03-28 发布　　2025-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

仪器服务网
YIQIFUWU.COM

目　　次

仪器服务网
YIQIFUWU.COM

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。

本文件由中国机械工业联合会提出。

本文件由全国机器人标准化技术委员会(SAC/TC 591)归口。

本文件起草单位：中国软件评测中心(工业和信息化部软件与集成电路促进中心)、北京人形机器人创新中心有限公司、中汽检测技术有限公司、烽台科技(北京)有限公司、北京猎户星空科技有限公司、北京机械工业自动化研究所有限公司、北京云迹科技股份有限公司、七腾机器人有限公司、福建汉特云智能科技有限公司、灵动智能机器人(河南)有限公司、锐趣科技(北京)有限公司、唐山清峰科技有限公司、赛迪检测认证中心有限公司、上海钛米机器人股份有限公司、乐聚(深圳)机器人技术有限公司、浙江大学、北京邮电大学、重庆凯瑞机器人技术有限公司、武汉理工大学、中国科学院沈阳自动化研究所、广州机械科学研究院有限公司、新石器慧通(北京)科技有限公司、北京三快在线科技有限公司、深圳市优必选科技股份有限公司。

本文件主要起草人：巩潇、梁学修、万彬彬、任容玮、曹懿莎、富显雯、苏永梓、吴璇、杨秋影、孙逊、支涛、朱冬、陈文强、李向明、黄维、尹啸峰、雷城炜、李梦玮、崔登祺、潘晶、孙冬冬、程鹏、李剑、张杰、刘冰艺、李志海、辛强、曾文达、李祖桥、王金芝、唐剑、马延辉、雷承霖。

仪器服务网
YIQIFUWU.COM

服务机器人信息安全通用要求

1 范围

本文件规定了服务机器人信息安全要求和测试方法。

本文件适用于服务机器人信息安全的设计、实施、测评和加固。

特种机器人和医疗机器人参考使用。

注：本文件适用于各类服务机器人，主要包括个人/家用服务机器人和公共服务机器人。

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 12643—2025 机器人 词汇

GB/T 25069—2022 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 12643—2025 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

服务机器人 service robot

个人使用或专业用途下，为人类或设备完成有用任务的机器人。

注 1：个人用途的任务包括物品的处理或提供、运输、身体的支撑、提供指引或信息、梳理、烹饪和食物处理，以及清洁。

注 2：专业用途的任务包括检查、监控、处理物品、人员运输、提供指导或信息、烹饪和食品处理，以及清洁。

[来源：GB/T 12643—2025，3.7]

3.2

调试接口 debug interface

预留用于机器人开发、维护、诊断等的物理接口。

3.3

操作终端 operating terminal

在移动中使用的与服务机器人交互的计算机设备，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行第三方应用软件。

3.4

主机系统 host system

协调机器人的各项功能，如导航、感知、决策、交互等，确保机器人能够有效地执行其任务的核心软件和硬件平台。

注：主机系统包括服务机器人本体、操作系统和传感器等模块。

3.5

凭证 credential

用于鉴别的身份代表。

注1：凭证通常是为了方便与它所代表的身份相关信息的数据鉴别。数据鉴别通常用于授权。

注2：例如，凭证表示的身份信息能打印在人类可读的媒体上，或者存储在物理令牌中。通常，这种信息能以一种旨在增强其感知有效的方式呈现。

注3：凭证可能是用户名、带口令的用户名、个人标识码(PIN)、证书、智能卡、令牌、指纹等。

[来源：GB/T 25069—2022，3.458，有修改]

3.6

重要数据　vital data

一旦泄露可能直接影响公共健康和安全的数据。

注：包括用户数据、凭证、系统配置、数据库内容、IP地址、密码、敏感文件路径、私钥、证书和API密钥等。

3.7

关键指令数据　key instruction data

用于指导服务机器人行为和决策的一系列指令和参数。

注：包括控制指令、任务指令、配置参数调整等。

4　缩略语

下列缩略语适用于本文件。

AES：高级加密标准(Advanced Encryption Standard)

AP：无线接入点(Access Point)

API：应用程序编程接口(Application Programming Interface)

CNNVD：中国国家信息安全漏洞库(China National Vulnerability Database of Information Security)

CNVD：国家信息安全漏洞共享平台(China National Vulnerability Database)

CPU：中央处理器(Central Processing Unit)

CRC：循环冗余校验(Cyclic Redundancy Check)

IP：网际互连协议(Internet Protocol)

MD5：消息摘要算法第五版(Message Digest Algorithm 5)

NVD：美国国家计算机通用漏洞数据库(National Vulnerability Database)

SQL：结构化查询语言(Structured Query Language)

SSL：安全套接层(Secure Sockets Layer)

TCP：传输控制协议(Transmission Control Protocol)

TLS：传输层安全性协议(Transport Layer Security)

USB：通用串行总线(Universal Serial Bus)

WAPI：无线局域网鉴别和保密基础结构(Wireless LAN Authentication and Privacy Infrastructure)

WPA：WPA：WAPI网络安全接入(WAPI Protected Access)

5　系统构成

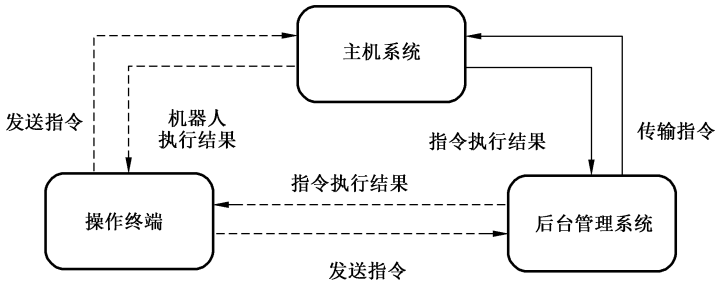
5.1　系统架构

服务机器人系统包括主机系统、操作终端和后台管理系统，系统架构见图1。

5.2　架构安全

主机系统与操作终端、后台管理系统之间的通信涉及用户指令、机器人执行结果等敏感信息的传输，应采用加密协议和安全通道，以防止信息泄露和篡改。操作终端与后台管理系统进行通信以实现

对机器人的控制和管理，应采用身份验证和权限控制，以保证通信的安全性和可靠性。主机系统、操作终端和后台管理系统中涉及个人信息收集、存储、使用和处理的部分应符合 GB/T 35273 的要求。



注：实线表示双方能够通信，虚线表示双方不一定能够通信。

图 1　服务机器人系统架构图

6　信息安全功能

6.1　具体功能

服务机器人信息安全主要包括主机系统安全、操作终端安全、后台管理系统安全，具体功能见图 2，对于不同类型、不同应用场景的服务机器人，其对信息安全关注程度的不同，安全防护能力等级可参考附录 A。

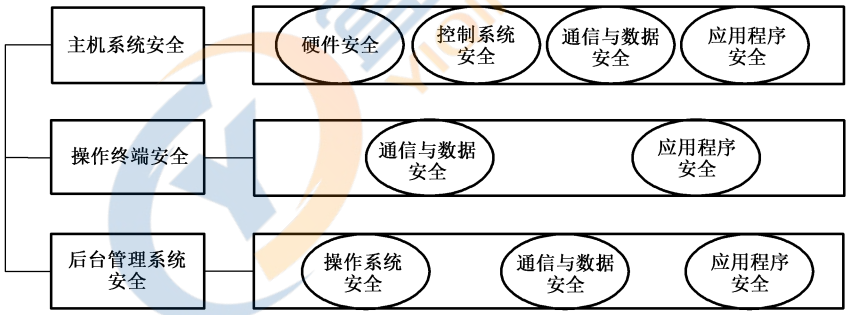


图 2　服务机器人信息安全功能图

6.2　主机系统安全功能

主机系统安全包括硬件安全、控制系统安全、通信与数据安全和应用程序安全，实现主机系统硬件、软件及相关数据的安全性、完整性和可用性，保障服务机器人主机系统的安全性和可靠性。

6.3　操作终端安全功能

操作终端安全包括通信与数据安全和应用程序安全，实现操作终端设备的数据安全，确保应用程序使用安全的配置、具有安全防护策略，以保护操作终端免受安全威胁的侵害。

6.4　后台管理系统安全功能

后台管理系统安全包括操作系统安全、通信与数据安全和应用程序安全，实现操作系统的安全管理，提供可靠的服务，防止恶意活动或网络攻击的发生，提高系统的安全性和可靠性。

7 信息安全要求

7.1 主机系统安全

7.1.1 硬件安全

7.1.1.1 物理接口安全

硬件不应暴露物理接口，如果调试接口是物理可访问的，则不应在软件中启用，或者配备健全的授权访问机制以验证操作者的合法性。

7.1.1.2 数据存储安全

主板芯片应具备安全存储机制。

7.1.1.3 防海豚音攻击

人机交互所使用的送话器识别的频率应限定在人耳适应的正常范围内(20 Hz～20 000 Hz)，以防范海豚音攻击。

7.1.1.4 第三方外设身份验证

第三方外设如摄像头、激光雷达等，应具备身份验证机制，并具有抵御身份验证攻击的能力。

7.1.2 控制系统安全

7.1.2.1 身份验证

应具备身份验证机制，并具有抵御身份验证攻击的能力。

7.1.2.2 权限划分

应对用户权限进行划分，不同用户只能使用其所拥有的权限。

7.1.2.3 最少服务原则

在满足正常工作要求前提条件下宜尽量减少服务或运行所需的功能。

7.1.2.4 防火墙

应开启防火墙，对潜在的网络攻击进行过滤。

7.1.2.5 非必要接口安全

应关闭所有未使用的网络和逻辑接口，如果接口是可访问的，则配备健全的授权访问机制验证操作者的合法性。

7.1.2.6 安全审计

应记录安全事件，以便及时发现异常行为。

7.1.2.7 系统可靠

应及时修复已知安全漏洞，操作系统和中间件不存在 NVD、CNVD 或 CNNVD 所披露的 6 个月

以前的高危及以上漏洞。

7.1.2.8 可信验证

应具备可信验证机制，对主机系统中的引导加载程序、信任根和应用程序进行可信验证。

7.1.3 通信与数据安全

7.1.3.1 数据传输安全

主机系统通过网络传输的数据应采用加密机制。

7.1.3.2 双向身份验证

使用安全套接字层协议证书的场景应采用双向验证方式。

7.1.3.3 无线安全

主机系统对外提供无线信号时，应采用安全的配置。

7.1.3.4 数据备份

应具备数据备份机制，确保在意外发生后能及时准确恢复数据。

7.1.3.5 重要数据防输出

重要数据不应被明文输出到日志中。

7.1.4 应用程序安全

7.1.4.1 漏洞管理

应及时修复已知安全漏洞，不存在 NVD、CNVD 或 CNNVD 所披露的 6 个月以前的高危及以上漏洞。

7.1.4.2 固件完整性校验

应保障固件更新的完整性。

7.1.4.3 固件真实性校验

应保障固件更新的真实性。

7.1.4.4 更新异常回滚

更新异常时，应确保固件能够恢复到更新前的版本，保障应用的可用性。

7.1.4.5 关键指令数据防重放

接收的外部关键指令数据宜避免被重放成功。

7.2 操作终端安全

7.2.1 通信与数据安全

7.2.1.1 通信安全

通过网络传输的数据应采用加密机制。

7.2.1.2 数据安全

不应明文显示或输出重要数据。

7.2.2 应用程序安全

7.2.2.1 访问控制

应具备授权访问机制，以满足正常功能的最小权限运行。

7.2.2.2 异常验证防护

应具备抵御对身份验证机制进行攻击的能力。

7.2.2.3 身份验证

应具备用户身份验证机制。

7.2.2.4 防反汇编

应具备反汇编防范措施。

7.2.2.5 软件完整性校验

应保障软件更新的完整性。

7.2.2.6 软件真实性校验

应保障软件更新的真实性。

7.2.2.7 更新异常回滚

更新异常时，应确保软件能够恢复到更新前的版本，保障应用的可用性。

7.2.2.8 防硬编码

代码包中不应含重要数据。

7.2.2.9 应用可靠

应及时修复已知安全漏洞，不存在 NVD、CNVD 或 CNNVD 所披露的 6 个月以前的高危及以上漏洞。

7.3 后台管理系统安全

7.3.1 操作系统安全

7.3.1.1 安全审计

应具有安全审计机制，记录关键事件和用户活动，以便及时检测和响应潜在的安全威胁。

7.3.1.2 身份验证

应具备身份验证功能，并具有抵御身份验证攻击的能力。

7.3.1.3 防格式化

应具备物理写保护或逻辑写保护等防格式化保护机制，防止病毒和入侵者恶意格式化存储单元。

7.3.1.4 权限划分

应根据角色对用户权限进行划分，不同角色用户只能使用本角色权限。

7.3.1.5 系统监测

应具备系统资源监控与报警功能，包括对系统的 CPU、内存、存储单元、网络资源进行监控。

7.3.1.6 威胁检测

应具备木马文件检测和病毒检测功能。

7.3.2 通信与数据安全

7.3.2.1 加密协议安全

应保证数据加密算法的安全性，不存在弱密钥、随机数可被预测、身份伪造等安全风险和 NVD、CNVD 或 CNNVD 所披露的 6 个月以前的高危及以上漏洞。

7.3.2.2 防重放

应能够防止重放攻击。

7.3.2.3 数据机密性

应保证数据在网络传输过程中的机密性。

7.3.2.4 数据备份

应具备数据备份与恢复功能。

7.3.3 应用程序安全

7.3.3.1 身份验证

应能够对登录用户进行身份标识和认证，并具有抵御身份验证攻击的能力。

7.3.3.2 输入验证

应验证通过 API 和用户界面输入的数据的正确性。

7.3.3.3 漏洞管理

应及时修复已知安全漏洞，不存在 NVD、CNVD 或 CNNVD 所披露的 6 个月以前的高危及以上漏洞。

7.3.3.4 权限管理

应具备权限划分机制，并保证用户仅拥有被授予的权限。

8 测试方法

8.1 主机系统安全

8.1.1 硬件安全

8.1.1.1 物理接口安全

物理接口安全测试方法如下：

a) 检查服务机器人是否暴露物理接口；

b) 查看服务机器人设置菜单、配置文件或串口管理器等信息，检查服务机器人硬件调试接口是否在软件中被禁用；

c) 使用接口对应的协议，采用软件或工具连接服务机器人硬件调试接口检查其是否配备了健全的授权访问机制。

8.1.1.2 数据存储安全

查看主板芯片的详细信息及安全功能，检查是否具备安全存储机制，如加密算法、访问控制、防篡改等。

8.1.1.3 防海豚音攻击

防海豚音攻击测试方法如下：

a) 在背景噪声低于 20 dB 的环境下，模拟正常频段(20 Hz、1 kHz、10 kHz、20 kHz)的信号，查看人机交互所使用的送话器是否能够正常识别；

b) 在背景噪声低于 20 dB 的环境下，模拟次声波(15 Hz、10 Hz)信号，查看人机交互所使用的送话器是否无法识别；

c) 分别在背景噪声低于 20 dB/40 dB/60 dB/80 dB 的环境下，模拟攻击频段(25 kHz、30 kHz、40 kHz)的信号，查看人机交互所使用的送话器是否无法识别。

8.1.1.4 第三方外设身份验证

第三方外设身份验证测试方法如下：

a) 查看机器人与第三方外设通信方式，确认是否为网络连接；

b) 对通过网络连接的第三方外设通信进行流量分析，检查是否具备身份验证机制；

c) 使用口令爆破、字典攻击等攻击手段，检查是否具有抵御身份验证攻击的能力。

8.1.2 控制系统安全

8.1.2.1 身份验证

身份验证测试方法如下：

a) 访问控制系统远程登录服务，检查是否具备密码策略、数字证书、安全令牌等身份验证机制；

b) 通过检查身份验证策略或者暴力破解、证书伪造等攻击方式检查是否具有强密码、限制尝试次数、账户锁定等抵御身份验证攻击的能力。

8.1.2.2 权限划分

使用普通用户，越权访问该用户所不具有权限访问的资源，查看是否能够被拒绝。

8.1.2.3 最少服务原则

了解服务机器人的运行环境、使用场景、功能特点等相关信息，查看控制系统运行的服务，检查是否开启与业务服务无关的系统服务和网络服务。

8.1.2.4 防火墙

检查控制系统是否开启了防火墙并设置了规则。

8.1.2.5 非必要接口安全

非必要接口安全测试方法如下：

a） 对接口进行安全扫描，查看是否存在未使用的接口；

b） 对可访问的接口模拟未授权的访问，检查系统是否能够拒绝。

8.1.2.6 安全审计

检查控制系统是否能够记录关键操作的日志，如用户访问、配置更改、网络活动、异常事件等。

8.1.2.7 系统可靠

查询 NVD、CNVD、CNNVD 等相关资料，查看控制系统采用的操作系统和中间件是否存在已披露的 6 个月以前的高危及以上漏洞。

8.1.2.8 可信验证

可信验证测试方法如下：

a） 检查主机系统是否存在可信验证机制；

b） 模拟可信验证异常情况，主机系统是否能够正常启动。

8.1.3 通信与数据安全

8.1.3.1 数据传输安全

通过数据包捕获工具捕获主机系统网络通信数据包，检查其是否采用数据加密机制，如数字签名、SSL 协议、AES 等。

8.1.3.2 双向身份验证

双向身份验证测试方法如下：

a） 检查主机系统是否具有安全套接字层协议证书；

b） 使用无效证书或伪造证书等方式，检查系统是否具备检测证书有效性的能力；

c） 模拟客户端和服务器之间的双向验证过程，检查系统是否能够正确地验证客户端和服务器的身份。

8.1.3.3 无线安全

检查主机系统开放的 WAPI、蓝牙、紫蜂(Zigbee)等是否采用了安全的配置，如强密码、协议加密、服务集标识隐藏或物理地址过滤等。

8.1.3.4 数据备份

数据备份测试方法如下：

a） 查看主机系统是否具有数据备份功能，将数据备份到本地或远程存储设备上；

b） 模拟数据损坏或丢失等情况，检查系统是否能够通过备份文件进行数据恢复。

8.1.3.5 重要数据防输出

查看系统生成的日志，检查系统是否会将用户身份信息、系统配置等重要数据明文输出到日志中。

8.1.4 应用程序安全

8.1.4.1 漏洞管理

查询 NVD、CNVD、CNNVD 等相关资料，查看应用程序是否存在已披露的 6 个月以前的高危及以上漏洞。

8.1.4.2 固件完整性校验

固件完整性校验测试方法如下：

a） 查看主机系统是否具备固件更新系统；

b） 通过代码审计或逆向工程等方式分析更新程序，查看是否具有 MD5 校验、哈希校验或 CRC 校验等完整性校验机制。

8.1.4.3 固件真实性校验

固件真实性校验测试方法如下：

a） 查看主机系统是否具备固件更新系统；

b） 通过代码审计或逆向工程等方式分析更新程序，查看主机系统与更新服务器之间是否使用了数字签名技术。

8.1.4.4 更新异常回滚

在固件更新的过程中，模拟设备断电、网络中断、强制重启等异常情况，待系统恢复后查看固件是否能够恢复到更新前的版本。

8.1.4.5 关键指令数据防重放

通过捕获通信数据包或逆向工程等方式分析服务机器人关键指令数据的数据结构，构造存在关键指令数据的数据包，模拟重放攻击，查看是否能够重放成功。

8.2 操作终端安全

8.2.1 通信与数据安全

8.2.1.1 通信安全

通过数据包捕获工具检查操作终端通过网络传输数据时是否采用加密算法，如 AES、加密算法、数字签名等。

8.2.1.2 数据安全

对已有功能进行测试，检查操作终端是否明文显示或输出用户身份数据、系统配置、会话令牌、API 密钥等重要数据。

8.2.2 应用程序安全

8.2.2.1 访问控制

访问控制测试方法如下：

a） 通过授权、限制访问权限等方式，检查应用程序是否具备授权访问机制；

b） 通过查看系统资源权限使用情况，检查应用程序是否以满足正常功能的最小权限运行。

8.2.2.2 异常验证防护

采用口令破解工具或手工测试的方式，检查应用程序是否能够有效的抵御。

8.2.2.3 身份验证

查看注册表单、登录流程或证书认证等方式，检查应用程序是否具备用户身份验证机制。

8.2.2.4 防反汇编

通过反汇编工具，如 IDA Pro、dex2jar、apktool 等，对应用程序进行反汇编，检查应用程序是否具备反汇编防范措施，如代码混淆、加密、加壳等。

8.2.2.5 软件完整性校验

软件完整性校验测试方法如下：

a） 查看操作终端是否具备软件更新系统；

b） 通过代码审计或逆向工程等方式分析更新程序，查看是否具有 MD5 校验、哈希校验或 CRC 校验等完整性校验机制。

8.2.2.6 软件真实性校验

软件真实性校验测试方法如下：

a） 查看操作终端是否具备软件更新系统；

b） 通过代码审计或逆向工程等方式分析更新程序，查看操作终端与更新服务器之间是否使用了数字签名技术。

8.2.2.7 更新异常回滚

在软件更新的过程中，模拟设备断电、网络中断、强制重启等异常情况，待系统恢复后查看软件是否能够恢复到更新前的版本。

8.2.2.8 防硬编码

通过逆向工程、程序文件解析等方式，检查应用程序代码包是否包含用户数据、凭证、API 密钥和证书等重要数据。

8.2.2.9 应用可靠

查询 NVD、CNVD、CNNVD 等相关资料，查看应用程序是否存在已披露的 6 个月以前的高危及

以上漏洞。

8.3 后台管理系统安全

8.3.1 操作系统安全

8.3.1.1 安全审计

模拟恶意入侵行为，如端口扫描、暴力破解、非法数据篡改等，检查系统是否能够及时准确地记录该事件。

8.3.1.2 身份验证

身份验证测试方法如下：

a) 访问后台管理系统远程登录服务，检查是否具备密码策略、双因素认证或智能卡等身份验证机制；

b) 通过暴力破解、身份伪造等攻击方式检查是否具有抵御身份验证攻击的能力。

8.3.1.3 防格式化

在真实系统环境或者通过虚拟化技术模拟真实系统环境，查看系统配置，检查系统是否具有物理写保护或逻辑写保护等防格式化保护机制。

8.3.1.4 权限划分

权限划分测试方法如下：

a) 查看系统是否存在根据角色的用户权限划分；

b) 通过查看系统配置检查不同角色的用户是否仅具有完成任务所必需的最小权限集合；

c) 通过越权访问等攻击方式检查用户权限划分是否存在安全风险。

8.3.1.5 系统监测

查看系统功能，检查是否具有对 CPU、内存、存储单元、网络资源等系统资源进行监控的功能。

8.3.1.6 威胁检测

威胁检测测试方法如下：

a) 在真实系统环境或者通过虚拟化技术模拟真实系统环境，传输一个木马文件，检查系统是否能够及时检测到该文件的存在并进行报警；

b) 在真实系统环境或者通过虚拟化技术模拟真实系统环境，传输一个病毒文件，检查系统是否能够及时检测到该病毒的存在并进行报警。

8.3.2 通信与数据安全

8.3.2.1 加密协议安全

加密协议安全测试方法如下：

a) 使用数据包捕获工具捕获后台管理系统网络通信数据包，查看数据交互是否使用了加密算法；

b) 查询 NVD、CNVD、CNNVD 等相关资料，查看使用的加密算法是否存在已披露的 6 个月以前的高危及以上漏洞；

c） 通过代码审计、黑盒测试等方式查看使用的加密算法是否存在弱密钥、随机数可被预测、身份伪造等安全风险。

8.3.2.2 防重放

通过数据包捕获工具，捕获后台管理系统网络通信数据包检查系统是否对接收的请求数据加入时间戳、随机数、序列号、令牌等。

8.3.2.3 数据机密性

通过数据包捕获工具，捕获后台管理系统网络通信数据包，检查系统在通信时是否采用加密机制。

8.3.2.4 数据备份

通过数据备份功能将数据备份到本地或异地存储设备上，模拟数据损坏或丢失，检查系统是否能够通过备份文件进行数据恢复。

8.3.3 应用程序安全

8.3.3.1 身份验证

身份验证测试方法如下：

a） 在系统中使用已授权的用户和非法的用户进行登录，检查该已授权用户是否能够成功登录系统，非法用户是否被拒绝登入；

b） 通过字典攻击、证书伪造等手段，检查系统是否具有抵御身份验证攻击的能力。

8.3.3.2 输入验证

输入验证测试方法如下：

a） 模拟 SQL 注入、命令注入等攻击方式，发送异常的 API 数据请求，检查应用程序是否能够拒绝请求或返回错误信息；

b） 模拟 SQL 注入、命令注入等攻击方式，通过用户界面输入异常情况，检查应用程序是否能够拒绝请求或提示错误。

8.3.3.3 漏洞管理

查询 NVD、CNVD、CNNVD 等相关资料，查看应用程序是否存在已披露的 6 个月以前的高危及以上漏洞。

8.3.3.4 权限管理

权限管理测试方法如下：

a） 检查系统是否能够对不同的用户进行权限划分；

b） 使用不同的用户账号登录系统，执行当前角色所不具有的权限，检查系统是否能够限制。

附 录 A
（资料性）
信息安全防护能力分级

根据服务机器人信息安全防护能力不同，划分为五个等级，具体防护能力分级见表 A.1，其中：

a） L1：对软硬件接口设计有一定的安全要求，重要数据防输出；

b） L2：具备应用和系统的安全初始化配置，能够抵御部分攻击；

c） L3：在 L2 基础上要求数据的机密性和完整性、系统可信验证、应用防重放、权限划分和具有抵御身份验证攻击的能力；

d） L4：在 L3 的基础上对数据的安全性提出更高要求，实现应用的输入验证和系统的可审计性，能够抵御复杂的攻击行为；

e） L5：在 L4 的基础上对系统进行多重防护，防海豚音攻击，确保应用的真实性和机密性。

表 A.1 服务机器人信息安全防护能力分级

服务机器人信息安全防护能力等级		L1	L2	L3	L4	L5
8.1 主机系统	8.1.1 硬件安全	7.1.1.1	7.1.1.1	7.1.1.1、7.1.1.4	7.1.1.1、7.1.1.2、7.1.1.4	7.1.1.1～7.1.1.4
	8.1.2 控制系统安全	7.1.2.5	7.1.2.1、7.1.2.3、7.1.2.5	7.1.2.1、7.1.2.2、7.1.2.3、7.1.2.5、7.1.2.8	7.1.2.1、7.1.2.2、7.1.2.3、7.1.2.5、7.1.2.6、7.1.2.8	7.1.2.1～7.1.2.8
	8.1.3 通信与数据安全	—	7.1.3.4、7.1.3.5	7.1.3.1、7.1.3.3、7.1.3.4、7.1.3.5	7.1.3.1～7.1.3.5	7.1.3.1～7.1.3.5
	8.1.4 应用程序安全	—	7.1.4.1、7.1.4.4	7.1.4.1、7.1.4.2、7.1.4.4、7.1.4.5	7.1.4.1、7.1.4.2、7.1.4.4、7.1.4.5	7.1.4.1～7.1.4.5
8.2 操作终端	8.2.1 通信与数据安全	7.2.1.2	7.2.1.2	7.2.1.1～7.2.1.2	7.2.1.1～7.2.1.2	7.2.1.1～7.2.1.2
	8.2.2 应用程序安全	—	7.2.2.1、7.2.2.3、7.2.2.7、7.2.2.9	7.2.2.1、7.2.2.2、7.2.2.3、7.2.2.5、7.2.2.7、7.2.2.8、7.2.2.9	7.2.2.1、7.2.2.2、7.2.2.3、7.2.2.5、7.2.2.7、7.2.2.8、7.2.2.9	7.2.2.1～7.2.2.9
8.3 后台管理系统	8.3.1 操作系统安全	—	7.3.1.2	7.3.1.2、7.3.1.4	7.3.1.1、7.3.1.2、7.3.1.4、7.3.1.5	7.3.1.1～7.3.1.6
	8.3.2 通信与数据安全	—	7.3.2.4	7.3.2.2、7.3.2.3、7.3.2.4	7.3.2.1～7.3.2.4	7.3.2.1～7.3.2.4
	8.3.3 应用程序安全	—	7.3.3.1、7.3.3.3	7.3.3.1、7.3.3.3、7.3.3.4	7.3.3.1～7.3.3.4	7.3.3.1～7.3.3.4

参 考 文 献

[1] GB/T 39575—2020 具有融合功能的移动终端安全能力技术要求

[2] GB 44495—2024 汽车整车信息安全技术要求

[3] ETSI EN 303645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

仪器服务网 YIQIFUWU.COM