



中华人民共和国国家标准

GB/T 39404—2026

代替 GB/T 39404—2020

工业机器人控制单元的信息 安全通用要求

General security requirements for control unit of industrial robot

2026-04-30 发布

2026-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

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 2

5 通信架构 2

6 信息安全要求 3

 6.1 通则 3

 6.2 信息安全物理要求 3

 6.3 信息安全总体技术要求 3

 6.4 主控与控制单元之间的信息安全要求 7

 6.5 控制单元内部的信息安全要求 8

附录 A (资料性) 工业机器人控制单元风险分析 11

 A.1 工业机器人控制单元的脆弱性 11

 A.2 示教器/编程软件与机器人控制器之间通信的脆弱性 11

 A.3 主控与机器人控制器之间通信的脆弱性 11

 A.4 机器人控制器与伺服驱动器之间通信的脆弱性 12

附录 B (资料性) 系统能力(技术)评估列表 13

参考文献 16

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。

本文件代替 GB/T 39404—2020《工业机器人控制单元的信息安全通用要求》，与 GB/T 39404—2020 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了“信息安全”的定义(见 3.4, 2020 年版的 3.4)；
- b) 更改了工业机器人控制单元通信架构图(见第 5 章, 2020 年版的 5.1)；
- c) 删除了“示教器与工业机器人 CU 之间的脆弱性”“主控与工业机器人 CU 之间的脆弱性”“机器人控制器与私服驱动器之间的脆弱性”(见 2020 年版的 5.2、5.3、5.4)；
- d) 更改了审计存储容量描述(见 6.3.1.2, 2020 年版的 6.3.1.3)、审计信息的保护(见 6.3.1.4, 2020 年版的 6.3.1.5)，增加了“达到审计记录存储容量上限时发出警告”(见 6.3.1.3)，删除了“中央管理的、系统范围的审计跟踪”“对审计流程失败时的响应”“一次性写入介质上的审计记录”“审计日志的可访问性”(见 2020 年版的 6.3.1.2、6.3.1.4、6.3.1.6、6.3.1.7)；
- e) 更改了通信完整性描述(见 6.3.2.1, 2020 年版的 6.3.2.1)、基于密码技术的完整性保护描述(见 6.3.2.2, 2020 年版的 6.3.2.2)、软件和信息完整性描述(见 6.3.2.3, 2020 年版的 6.3.2.3)、对破坏完整性进行自动通知描述(见 6.3.2.4, 2020 年版的 6.3.2.4)，删除了“会话完整性”“会话终止后会话 ID 的失效”“唯一会话 ID 的产生和承认”“会话 ID 的随机性”(见 2020 年版的 6.3.2.8、6.3.2.9、6.3.2.10、6.3.2.11)；
- f) 更改了信息保密性描述(见 6.3.3.1, 2020 年版的 6.3.3.1)、密码的使用(见 6.3.3.5, 2020 年版的 6.3.3.6)，增加了“加密协议安全”(见 6.3.3.2)，删除了“静态和经由不可信网络传输的数据的保密性保护”“区域边界的保密性保护”(见 2020 年版的 6.3.3.2、6.3.3.3)；
- g) 更改了拒绝服务的防护(见 6.3.5.2, 2020 年版的 6.3.5.2)、数据备份描述(见 6.3.5.4, 2020 年版的 6.3.5.6)，删除了“持续监视”“限制拒绝服务攻击对其他系统和网络的影响”“资源管理”(见 2020 版的 6.3.5.1、6.3.5.4、6.3.5.5)；
- h) 更改了网络和安全配置设置(见 6.3.6.2, 2020 年版的 6.3.6.1)；
- i) 增加了“数据安全要求”(见 6.3.7)；
- j) 更改了主控的标识和认证(见 6.4.2.1, 2020 年版的 6.4.4.1)，删除了“并发连接控制”(见 2020 版的 6.4.2)；
- k) 删除了“非可信网络的多因子认证”“软件进程的标识和认证”“统一的账号管理”“标识符管理”“软件进程标识凭证的硬件安全”“对所有用户的口令有效期的限制”(见 2020 版的 6.4.4.2、6.4.4.3、6.4.4.6、6.4.4.7、6.4.4.9、6.4.4.12)；
- l) 删除了“经由非可信网络的访问”“授权的执行”“无线使用控制”“对未授权的无线设备进行识别和报告”(见 2020 版的 6.4.5.1、6.4.5.3、6.4.5.4、6.4.5.5)；
- m) 删除了“非可信网络的多因子认证”“软件进程的标识和认证”“唯一标识和认证”(见 2020 版的 6.5.1.3、6.5.1.4、6.5.1.5)；
- n) 删除了“在入口和出口点防护恶意代码”“SR 3.2 RE(2) 恶意代码防护的集中管理和报告”(见 2020 年版的 6.5.2.2、6.5.2.3)；
- o) 更改了“恶意代码的防护”(见 6.5.4.4, 2020 年版的 6.5.2.1)，增加了“编程代码加密”(见 6.5.4.5)；

p) 增加了“漏洞管理要求”(见 6.5.5);

q) 增加了“防重放”(见 6.5.6)。

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:中国科学院沈阳自动化研究所、珞石(山东)智能科技有限公司、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)、浙江大学、大连理工大学、北京机械工业自动化研究所有限公司、沈阳新松机器人自动化股份有限公司、中国电子技术标准化研究院、山东大学、北京交通大学、上海擎标信息技术服务有限公司、深圳市朗宇芯科技有限公司、深圳库玛科技有限公司、湖北三江博力智能装备有限公司、布谷鸟同创科技(天津)有限公司、江西云杉智能科技有限公司。

本文件主要起草人:赵剑明、刘贤达、纪磊、李梦玮、冯博、刘燕、李志海、郭成、刘颖、周川、赵绍祥、李邦宇、宋斌、巩潇、宋锐、金一、李琳、邵士亮、夏冀、贺毅、崔登祺、雷城炜、罗梦、盛川、夏旭升、章林、张华森、吴化格、焦见伟、徐征鹏。

本文件及其所代替文件的历次版本发布情况为:

——2020 年首次发布为 GB/T 39404—2020;

——本次为第一次修订。

工业机器人控制单元的信息 安全通用要求

1 范围

本文件确立了工业机器人控制单元的通信架构,规定了工业机器人控制单元的信息安全物理要求、信息安全总体技术要求,以及主控与控制单元之间、控制单元内部的信息安全要求。

本文件适用于工业机器人控制单元信息安全组件的设计、开发、集成以及评估。

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 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 33008.1—2016 工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分:系统要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业机器人 industrial robot

自动控制且可重复编程的多用途操作机,能对三个或更多的轴进行编程,能固定在某一位置或固定在移动平台上,在工业自动化中使用。

注:工业机器人包括:

- 操作机,由机器人控制器控制的机器人致动器;
- 机器人控制器;
- 对机器人进行示教和/或编程的方法,包括任何通信接口(硬件和软件)。

[来源: GB/T 12643—2025, 3.6, 有修改]

3.2

机器人控制器 robot controller

一套能实现逻辑控制和动力控制以及其他功能的硬件和软件组件,允许监测和控制机器人的行为,以及机器人与环境中其他物体及人类的交互和通信。

[来源: GB/T 12643—2025, 3.4]

3.3

控制单元 control unit; CU

能控制和监测机器人机械结构,与环境设备或使用者进行通信,并且具有逻辑控制和动力功能的

系统。

3.4

信息安全 information security

保护系统资源,防范非授权访问、变更、破坏或意外损失及非法入侵、操作干扰,确保授权主体依法依规使用系统功能而形成的安全状态及相关防护措施。

注:措施包括与物理(网络)安全或者逻辑(网络)安全相关的控制手段。

[来源:GB/T 30976.1—2014,3.1.14,有修改]

4 缩略语

下列缩略语适用于本文件。

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

CA:数字证书认证中心(Certificate Authority)

CL:能力等级(Capability Level)

DoS:拒绝服务(Denial of Service)

PKI:公钥基础设施(Public Key Infrastructure)

RE:增强要求(Requirement Enhancement)

SR:系统要求(System Requirement)

5 通信架构

工业机器人控制单元通信架构,见图 1。

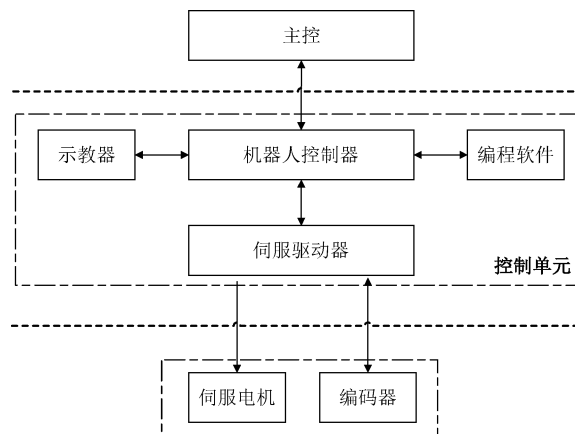


图 1 工业机器人控制单元通信架构

其中,控制单元主要包括机器人控制器、伺服驱动器、示教器及编程软件。

主控与机器人控制器之间的通信方式包括但不限于以下方式:

- a) 输入输出(IO)信号;
- b) 串行通信;
- c) 现场总线;
- d) 工业以太网;
- e) 其他专用或标准协议。

机器人控制器与伺服驱动器之间的通信方式包括但不限于以下方式:

- a) 模拟量与脉冲指令；
- b) 现场总线；
- c) 工业以太网。

工业机器人控制单元的风险分析见附录 A。

6 信息安全要求

6.1 通则

工业机器人控制单元信息安全主要应包括：

- a) 主控与控制单元之间的信息安全；
- b) 控制单元内部的信息安全。

工业机器人控制单元信息安全要求包括系统要求(SR)和系统增强要求(RE),应符合 GB/T 30976.1—2014 和 GB/T 33008.1—2016 的相关要求。工业机器人控制单元信息安全分级要求见附录 B。

6.2 信息安全物理要求

信息安全物理要求应符合 GB/T 32919—2016 中 B.7 的要求。

6.3 信息安全总体技术要求

6.3.1 审计要求

6.3.1.1 可审计的事件

可审计的事件(SR2.8)应符合 GB/T 30976.1—2014 中 6.3.8 的要求。控制单元应为以下事件生成审计记录：

- a) 访问控制；
- b) 请求错误；
- c) 系统事件；
- d) 备份和存储事件；
- e) 配置变更；
- f) 潜在的侦查行为和审计日志事件。

注：可审计的事件在示教器、编程软件或其他人机接口查看。

6.3.1.2 审计存储容量

审计存储容量(SR2.9)应符合 GB/T 30976.1—2014 中 6.3.9 的要求。控制单元应根据日志管理和系统配置推荐值来分配足够的审计记录存储容量。控制单元应提供审计机制减少超出该容量的可能性,可根据包括但不限于保存策略、应执行的审计等因素提供足够的审计存储容量。

6.3.1.3 达到审计记录存储容量上限时发出警告

达到审计记录存储容量上限时发出警告[SR2.9 RE(1)]应符合 GB/T 30976.1—2014 中 6.3.9.1 的要求。当分配的审计记录存储量达到最大审计记录存储容量的可配置比例时,控制单元应发出警告,并具备将审计记录备份至独立外部存储空间的能力,以确保其完整性。同时,警告信息及备份操作状态应能通过人机接口进行查看。

6.3.1.4 审计信息的保护

审计信息的保护(SR3.9)应符合 GB/T 30976.1—2014 中 6.4.9 的要求。控制单元应保护审计信息不被未经授权地访问、增加、修改和删除。

6.3.1.5 对审计日志的程式化访问

对审计日志的程式化访问[SR6.1 RE(1)]应符合 GB/T 30976.1—2014 中 6.7.1.1 的要求。控制单元应使用 API 提供对审计记录的访问。

6.3.2 完整性要求

6.3.2.1 通信完整性

通信完整性(SR3.1)应符合 GB/T 30976.1—2014 中 6.4.1 的要求。机器人控制器与示教器、编程软件之间应保护通信信道上传输的信息的完整性。

6.3.2.2 基于密码技术的完整性保护

基于密码技术的完整性保护[SR3.1 RE(1)]应符合 GB/T 30976.1—2014 中 6.4.1.1 的要求。控制单元应采用密码学机制识别信息在通信过程中的变更,对信息已被其他可替换的物理措施保护的通信链路,不适用此要求。

注 1: 密码学机制包括但不限于消息摘要算法、消息认证码、数字签名等技术。

注 2: 物理保护措施包括但不限于专用线缆、物理隔离的网络、封闭的通信背板。

6.3.2.3 软件和信息完整性

软件和信息完整性(SR3.4)应符合 GB/T 30976.1—2014 中 6.4.4 的要求。控制单元应具备软件、固件不受未经授权变更的能力。

6.3.2.4 对破坏完整性进行自动通知

对破坏完整性进行自动通知[SR3.4 RE(1)]应符合 GB/T 30976.1—2014 中 6.4.4.1 的要求。控制单元应在完整性验证期间发现不符时进行通知。

6.3.3 保密性要求

6.3.3.1 信息保密性

信息保密性(SR4.1)应符合 GB/T 30976.1—2014 中 6.5.1 的要求。控制单元应确保信息在存储和传输中的保密性。

6.3.3.2 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。

6.3.3.3 信息存留

信息存留(SR4.2)应符合 GB/T 30976.1—2014 中 6.5.2 的要求。控制单元应提供退役能力,清除被在用服务所释放的部件中所有与安全相关的资料。

6.3.3.4 共享内存资源的清除

共享内存资源的清除[SR4.2 RE(1)]应符合 GB/T 30976.1—2014 中 6.5.2.1 的要求。控制单元应

防止借助易失性存储资源进行的未经授权的和无意的信息传输,当易失性共享存储释放回控制单元供不同用户使用时,所有的特有数据及特有数据的关联都应从资源中清除,从而使新用户对其不可见和不可访问。

6.3.3.5 密码的使用

密码的使用(SR4.3)应符合 GB/T 30976.1—2014 中 6.5.3 的要求。控制单元应采用符合 GM/T 系列标准或国家密码管理部门核准的密码算法,其安全强度与密钥管理策略应符合 GB/T 39786 中相应安全等级的规定。

6.3.4 通信可靠性要求

6.3.4.1 总线拓扑结构

控制单元通信采用的高速通信总线可组成的站点网络结构应符合树状、链式、星形或环状等网络结构中的一种或一种以上。

6.3.4.2 差错检查

控制单元高速通信总线数据链路层协议应包含对传输的数据的检错和纠错功能。

6.3.4.3 最大通信延迟

控制单元高速通信总线的最大通信延迟应满足具体应用的实时通信要求。

6.3.4.4 时间同步精度

控制单元应实现各站点间的时间同步。其高速通信总线的时间同步精度应满足具体应用的实时通信要求。

6.3.4.5 总线仲裁

控制单元高速通信总线控制权的仲裁方式可为主站管理从站、无主站协调管理多从站、无主站管理的多站点抢占等方式。

6.3.4.6 网络容错与自愈

控制单元为工业机器人提供以下能力:

- a) 控制单元高速通信总线应具有网络容错功能,在偶然性外部干扰影响下,通信总线应能对数据传输过程中造成的数据错误进行容错处理,不因偶发性错误造成通信过程的中断或停止;
- b) 在通信站点短时异常造成网络通信中断情况下,在站点恢复正常后,高速通信总线应具有自愈功能,恢复通信总线正常通信所需的时间应满足具体应用要求。

6.3.5 可用性要求

6.3.5.1 确定性的输出

确定性的输出(SR3.6)应符合 GB/T 30976.1—2014 中 6.4.6 的要求。控制单元应在遭受攻击无法保持正常运行时,将输出设置为预先定义的安全状态。这些状态包括:

- a) 未上电状态;
- b) 可知最后的确定值;
- c) 由资产属主或应用确定的固定值。

6.3.5.2 拒绝服务的防护

拒绝服务的防护(SR7.1)应符合 GB/T 30976.1—2014 中 6.8.1 的要求。控制单元应具备抗 DoS 攻击能力,确保在 DoS 的攻击下,关键控制回路仍能维持基本功能。

6.3.5.3 管理通信负荷

管理通信负荷[SR7.1 RE(1)]应符合 GB/T 30976.1—2014 中 6.8.1.1 的要求。控制单元应提供管理通信负荷的能力来消减信息泛洪类的拒绝服务攻击事件。

示例:管理通信负荷的能力,例如使用限速。

6.3.5.4 数据备份

数据备份(SR7.3)应符合 GB/T 30976.1—2014 中 6.8.3 的要求。控制单元应在不影响系统正常运行情况下,支持识别和定位关键文件,并有能力执行用户级备份(包含状态信息)。

6.3.5.5 备份验证

备份验证[SR7.3 RE(1)]应符合 GB/T 30976.1—2014 中 6.8.3.1 的要求。控制单元应提供检测备份数据被破坏的能力。

6.3.5.6 备份自动化

备份验证[SR7.3 RE(2)]应符合 GB/T 30976.1—2014 中 6.8.3.2 的要求。控制单元应提供按照可配置的频率自动备份的能力。

6.3.5.7 恢复和重构

恢复和重构(SR7.4)应符合 GB/T 30976.1—2014 中 6.8.4 的要求。当遭受攻击而造成系统故障后,控制单元应提供恢复和重构到已知的安全状态的能力。

6.3.6 系统要求

6.3.6.1 错误处理

错误处理(SR3.7)应符合 GB/T 30976.1—2014 中 6.4.7 的要求。控制单元应能识别和处理错误条件的方式,应能实施有效的补救,这一方式不应提供可能被利用来攻击控制单元的信息,除非泄漏这一信息为及时发现并修理问题的必要条件。

6.3.6.2 网络和安全配置设置

网络和安全配置设置(SR7.6)应符合 GB/T 30976.1—2014 中 6.8.6 的要求。控制单元应支持网络与安全配置,并提供接口用于查看和修改当前已部署的配置。

6.3.6.3 最小功能化

最小功能化(SR7.7)应符合 GB/T 30976.1—2014 中 6.8.7 的要求。控制单元应限制使用非必要的端口、协议及服务。

6.3.6.4 组件清单

组件清单(SR7.8)应符合 GB/T 30976.1—2014 中 6.8.8 的要求。控制单元应提供报告当前已安装

的组件及其关联属性的能力。控制单元应：

- a) 提供报告已安装组件及其关联属性的方法；
- b) 确保已安装组件在系统部件清单目录中是正确的；
- c) 在部件增加、移除或组件属性变更时，正确更新系统部件清单目录。

6.3.7 数据安全要求

控制单元应具备对数据进行分类分级的能力，设定数据敏感度级别。

6.4 主控与控制单元之间的信息安全要求

6.4.1 时间要求

6.4.1.1 时间戳

时间戳(SR2.11)应符合 GB/T 30976.1—2014 中的 3.11 的要求。控制单元应提供时间戳用于生成审计记录。

6.4.1.2 内部时间同步

内部时间同步[SR2.11 RE(1)]应符合 GB/T 30976.1—2014 中 6.3.11.1 的要求。控制单元应提供以可配置的频率同步内部系统时钟的能力。

6.4.1.3 时间源的完整性保护

时间源的完整性保护[SR2.11 RE(2)]应符合 GB/T 30976.1—2014 中 6.3.11.2 的要求。时间源应被保护不受未授权的变更，其变更应触发审计事件。

6.4.2 标识和认证要求

6.4.2.1 主控的标识和认证

控制单元应为工业机器人提供以下能力：

- a) 提供标识和认证主控的能力；
- b) 使主控标识符能在访问接口上被认证，无效主控标识符在访问接口上被拒绝。

6.4.2.2 唯一标识和认证

唯一标识和认证[SR1.2 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.2.1 的要求。控制单元应对主控提供唯一标识和认证的能力。

6.4.2.3 公钥基础设施证书

公钥基础设施证书(SR1.8)应符合 GB/T 30976.1—2014 中 6.2.8 的要求。当使用公钥基础设施 PKI 时，控制单元应提供能力按照最佳实践运行公钥基础设施或从现有的 PKI 中获取公钥证书。

6.4.2.4 公钥认证的加强

公钥认证的加强(SR1.9)应符合 GB/T 30976.1—2014 中 6.2.9 的要求。对于使用公钥认证的控制单元，控制单元应提供以下能力：

- a) 通过检查给定证书的签名的有效性来证实证书；
- b) 通过可接受的 CA 证实证书，或在自签名证书情况下，以某种事先定义的方式证实证书；

- c) 通过给定证书的撤销状态证实证书；
- d) 建立对私钥的控制；
- e) 将已认证的标识映射为设备。

6.4.2.5 公钥认证的硬件安全

公钥认证的硬件安全[SR1.9 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.9.1 的要求。控制单元应通过硬件机制保护相关的私钥。

6.4.3 明确的对访问请求的批准

明确的对访问请求的批准[SR1.13 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.13.1 的要求。控制单元应提供能力拒绝来自不可信网络的访问,除非被指定角色批准。

示例: 拒绝来自不可信网络的访问,例如限制未授权的 IP 地址接入。

6.5 控制单元内部的信息安全要求

6.5.1 标识和认证要求

6.5.1.1 用户(人)的标识和认证

用户(人)的标识和认证(SR1.1)应符合 GB/T 30976.1—2014 中 6.2.1 的要求。控制单元应对所有用户(人)提供基于角色的标识和认证能力。

6.5.1.2 唯一标识和认证

唯一标识和认证[SR1.2 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.2.1 的要求。控制单元应对所有用户(人)提供唯一标识和认证的能力。

6.5.1.3 账号管理

账号管理(SR1.3)应符合 GB/T 30976.1—2014 中 6.2.3 的要求。控制单元应提供对所有账号的管理,包括创建、修改和移除账号的能力。当一个或多个号被修改或移除时,未被修改的账号保持账号权限不变。

6.5.1.4 认证码管理

认证码管理(SR1.5)应符合 GB/T 30976.1—2014 中 6.2.5 的要求。控制单元应:

- a) 提供能力定义初始的认证码内容；
- b) 提供不被未经授权的变更/更新认证码的能力。

6.5.1.5 口令认证的强度

口令认证的强度(SR1.7)应符合 GB/T 30976.1—2014 中 6.2.7 的要求。对于使用口令认证的控制单元,控制单元应实施可配置的基于最小长度和不同字符类型的口令强度。

6.5.1.6 对用户(人)的口令生成和口令有效期的限制

对用户(人)的口令生成和口令有效期的限制[SR1.7 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.7.1 的要求。控制单元应为用户(人)提供口令重用次数、口令有效期可配置的能力。

6.5.1.7 认证反馈

认证反馈(SR1.10)应符合 GB/T 30976.1—2014 中 6.2.10 的要求。控制单元将认证信息的反馈模

糊化,使得当一个或多个凭证无效时,失败的认证尝试不提供任何合法凭证有效性的信息。

示例:合法凭证有效性的信息,例如用户名和口令。

6.5.1.8 失败的登录尝试

失败的登录尝试(SR1.11)应符合 GB/T 30976.1—2014 中 6.2.11 的要求。控制单元应为工业机器人提供以下能力:

- a) 对任何用户在可配置的时间周期内连续无效访问尝试的次数限制为一个可配置的数目;
- b) 在可配置时间周期内未成功尝试次数超过上限时,在指定时间内拒绝访问直到由管理员解锁。

6.5.2 授权的执行

授权的执行(SR2.1)应符合 GB/T 30976.1—2014 中 6.3.1 的要求。控制单元应具有执行分配给所有用户(人)的授权的能力,按照职责分离和最小特权来控制对控制单元的使用。

控制单元应为资产所有者提供修改许可到角色的映射的能力。包括但不限于:

- a) 操作员;
- b) 工程师;
- c) 管理员。

6.5.3 输入验证

输入验证(SR3.5)应符合 GB/T 30976.1—2014 中 6.4.5 的要求。示教器和编程软件应验证输入的语法和内容,这些输入是作为工业过程控制输入或直接影响控制单元行为的输入。

6.5.4 编程代码要求

6.5.4.1 编程代码授权

编程代码(SR2.4)应符合 GB/T 30976.1—2014 中 6.3.4 的要求。控制单元应提供对编辑、修改编程代码的人员进行权限管理和身份认证。

6.5.4.2 编程代码的完整性检查

编程代码的完整性检查[SR2.4 RE(1)]应符合 GB/T 30976.1—2014 中 6.3.4.1 的要求。控制单元应在允许代码执行之前验证代码的完整性。

6.5.4.3 编程代码的使用限制

编程代码的使用限制[SR2.4 RE(2)]应符合 GB/T 33008.1—2016 中 5.3.2.8 的要求。控制单元应为工业机器人提供以下能力:

- a) 对代码源要求适当的认证和授权;
- b) 限制代码传入/传出控制单元;
- c) 监视代码的使用。

6.5.4.4 恶意代码的防护

恶意代码的防护(SR3.2)应符合 GB/T 30976.1—2014 中 6.4.2 的要求。控制单元应能检测编程语言代码潜在的安全风险,提示告警或阻止执行,防止恶意软件攻击与利用。

6.5.4.5 编程代码加密

控制单元应采用代码混淆、加密或加壳等加固防护措施。

6.5.5 漏洞管理要求

控制单元应提供漏洞管理机制,无已公开 6 个月以上的高危及以上的漏洞。

注:漏洞信息来源包括但不限于 CNVD、CNNVD、NVD、CVE。

6.5.6 防重放

控制单元所使用的通信协议应能防范重放攻击。

附录 A

(资料性)

工业机器人控制单元风险分析

A.1 工业机器人控制单元的脆弱性

威胁源包括但不限于以下内容：

- a) 示教器/编程软件未授权使用；
- b) 示教器/编程软件/机器人控制器存在漏洞；
- c) 示教器/编程软件被误操作；
- d) 示教器/编程软件存在非法设备接入风险；
- e) 机器人控制器抵御 DoS 攻击能力弱；
- f) 机器人控制器开放不必要的远程服务端口；
- g) 机器人控制器未经授权的下载安装程序。

潜在的后果包括但不限于以下内容：

- a) 越权操作，出现错误；
- b) 程序或数据被修改、删除、窃取；
- c) 设备损坏，出现故障；
- d) 非法注入后门。

A.2 示教器/编程软件与机器人控制器之间通信的脆弱性

威胁源包括但不限于以下内容：

- a) 通信缺少身份认证、完整性、保密性的保护；
- b) 非法设备接入通信信道；
- c) 侧信道攻击。

潜在的后果包括但不限于以下内容：

- a) 下发错误的指令；
- b) 越权操作，出现错误；
- c) 程序或数据被修改、删除、窃取；
- d) 设备损坏。

A.3 主控与机器人控制器之间通信的脆弱性

威胁源包括但不限于以下内容：

- a) 通信缺少身份认证、完整性、保密性的保护；
- b) 非法设备接入通信信道；
- c) 侧信道攻击。

潜在的后果包括但不限于以下内容：

- a) 非法操作系统配置、逻辑代码和敏感数据；
- b) 非法注入后门；
- c) 非法关机或重启；
- d) 通信被阻塞，下发指令被干扰；
- e) 通信数据被篡改、窃取。

A.4 机器人控制器与伺服驱动器之间通信的脆弱性

威胁源包括但不限于以下内容：

- a) 通信缺少身份认证、完整性、保密性的保护；
- b) 非法设备接入通信信道；
- c) 侧信道攻击。

潜在的后果包括但不限于以下内容：

- a) 机器人未按预定逻辑运行，出现故障；
- b) 机器人运行时意外停机；
- c) 非法注入后门；
- d) 存在数据泄漏风险；
- e) 通信被阻塞，下发指令被干扰；
- f) 通信数据被篡改、窃取。

附 录 B
(资料性)
系统能力(技术)评估列表

信息安全总体技术要求下的安全等级映射见表 B.1。

表 B.1 信息安全总体技术要求下的安全等级的映射

SR 和 RE	CL1	CL2	CL3	CL4
审计要求				
可审计的事件	√	√	√	√
审计存储容量	√	√	√	√
达到审计记录存储容量上限时发出警告			√	√
审计信息的保护		√	√	√
对审计日志的编程式访问	√	√	√	√
完整性要求				
通信完整性	√	√	√	√
基于密码技术的完整性保护			√	√
软件和信息完整性		√	√	√
对破坏完整性进行自动通知			√	√
保密性要求				
信息保密性	√	√	√	√
加密协议安全	√	√	√	√
信息存留		√	√	√
共享内存资源的清除				√
密码的使用	√	√	√	√
通信可靠性要求				
总线拓扑结构	√	√	√	√
差错检查	√	√	√	√
最大通信延迟	√	√	√	√
时间同步精度	√	√	√	√
总线仲裁		√	√	√
网络容错与自愈		√	√	√

表 B.1 信息安全总体技术要求下的安全等级的映射（续）

SR 和 RE	CL1	CL2	CL3	CL4
可用性要求				
确定性的输出	√	√	√	√
拒绝服务的防护				√
管理通信负荷		√	√	√
数据备份	√	√	√	√
备份验证		√	√	√
备份自动化				√
恢复和重构	√	√	√	√
系统要求				
错误处理		√	√	√
网络和安全配置设置	√	√	√	√
最小功能化	√	√	√	√
组件清单		√	√	√
数据安全要求			√	√
注：“√”表示对应安全等级下的条款规定。				

主控与控制单元之间的信息安全要求下的安全等级映射见表 B.2。

表 B.2 主控与控制单元之间的信息安全要求下的安全等级映射

SR 和 RE	CL1	CL2	CL3	CL4
时间要求				
时间戳		√	√	√
内部时间同步			√	√
时间源的完整性保护				√
标识和认证要求				
主控的标识和认证	√	√	√	√
唯一标识和认证		√	√	√
公钥基础设施证书		√	√	√
公钥认证的加强				√
公钥认证的硬件安全			√	√
明确的对访问请求的批准				√
注：“√”表示对应安全等级下的条款规定。				

控制单元内部的信息安全要求下的安全等级映射见表 B.3。

表 B.3 控制单元内部的信息安全要求下的安全等级映射

SR 和 RE	CL1	CL2	CL3	CL4
标识和认证要求				
用户(人)的标识和认证	√	√	√	√
唯一标识和认证		√	√	√
账号管理	√	√	√	√
认证码管理		√	√	√
口令认证的强度	√	√	√	√
对用户(人)的口令生成和口令有效期的限制		√	√	√
认证反馈				√
失败的登录尝试				√
授权的执行		√	√	√
输入验证				√
编程代码要求				
编程代码授权		√	√	√
编程代码的完整性检查			√	√
编程代码的使用限制		√	√	√
恶意代码的防护				√
编程代码加密				√
漏洞管理要求	√	√	√	√
防重放			√	√
注：“√”表示对应安全等级下的条款规定。				

参 考 文 献

- [1] GB/T 12643—2025 机器人 词汇
 - [2] GB/T 39360—2020 工业机器人控制系统性能评估与测试
 - [3] GB/T 39405—2020 机器人分类
 - [4] 龚仲华.工业机器人编程与操作[M].北京:机械工业出版社, 2016.
-

