

ICS 25.040.30
J 28



中华人民共和国国家标准

GB/T 39404—2020

工业机器人控制单元的信息安全通用要求

Information security general requirement for control unit of industrial robot

2020-11-19 发布

2021-06-01 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	I
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 通信架构及关联性	2
5.1 工业机器人控制单元通信架构	2
5.2 示教器与工业机器人 CU 之间的脆弱性	3
5.3 主控与工业机器人 CU 之间的脆弱性	3
5.4 机器人控制器与伺服驱动器之间的脆弱性	4
6 信息安全要求	4
6.1 总则	4
6.2 信息安全物理要求	4
6.3 信息安全技术要求	4
6.3.1 审计要求	4
6.3.2 完整性要求	5
6.3.3 保密性要求	6
6.3.4 通信信息安全要求	7
6.3.5 可用性要求	8
6.3.6 系统要求	9
6.4 主控与 CU 之间的信息安全要求	9
6.4.1 编程代码要求	9
6.4.2 并发连接控制	10
6.4.3 时间要求	10
6.4.4 标识和认证要求	10
6.4.5 授权和访问要求	12
6.5 CU 内部的信息安全要求	13
6.5.1 标识和认证要求	13
6.5.2 恶意代码的防护要求	14
参考文献	15

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由中国机械工业联合会提出。

本标准由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本标准起草单位:中国科学院沈阳自动化研究所、机械工业仪器仪表综合技术经济研究所、中国电子技术标准化研究院、沈阳建筑大学、中国电子学会、珠海格力电器股份有限公司、重庆鲁班机器人技术研究院有限公司、沈阳新松机器人自动化股份有限公司、工业和信息化部电子第五研究所、沈阳通用机器人技术股份有限公司、伊之密机器人自动化科技(苏州)有限公司、北京机械工业自动化研究所有限公司、长春禹衡光学有限公司、博众精工科技股份有限公司、电力规划总院有限公司、中国科学院信息工程研究所、中国航空综合技术研究所、浙江明泉工业装备科技有限公司、成都飞机工业(集团)有限责任公司、华中科技大学、北京和利时智能技术有限公司、中国软件测评中心、北京神州绿盟信息安全科技股份有限公司、北京网御星云信息技术有限公司、湖南省产商品质量监督检验研究院、珠海格力智能装备有限公司、华南智能机器人创新研究院。

本标准主要起草人:尚文利、刘贤达、赵剑明、韩忠华、林硕、尹隆、陈春雨、王玉敏、范科峰、余文科、钟明生、何国田、邹风山、李丹、王圆星、韩刚、尹作重、褚旭升、孟健、张晋宾、石志强、吴灿辉、茅立安、雷沛、周纯杰、朱毅明、周峰、王晓鹏、于文凤、钟声、文辉、曹永军、郭海冰、詹永根、秦修功、王虹。

工业机器人控制单元的信息安全通用要求

1 范围

本标准规定了工业机器人控制单元的信息安全通用要求,以及 CU 与其他设备(包括示教器、主控、编码器)之间互联的信息安全通用要求。

本标准适用于工业机器人的设计、生产、集成以及评估等。

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 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

GB/T 32197—2015 机器人控制器开放式通信接口规范

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

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

自动控制的、可重复编程、多用途的操作机,可对三个或三个以上轴进行编程。它可以是固定式或移动式。在工业自动化中使用。

注1:工业机器人包括:

——操作机,含致动器;

——控制器,含示教盒或某些通信接口(硬件和软件)。

注2:这包括某些集成的附加轴。

[GB/T 12643—2013,定义 2.9]。

3.2

机器人控制器 robot controller

与机器人本体相连,接收用户指令,并控制机器人本体动作的装置。

[GB/T 32197—2015,定义 3.2]

3.3

控制单元 control unit; CU

能控制和监测机器人机械结构并与环境设备或使用者进行通信,包括控制器和伺服驱动器,以及各种接口的具有逻辑控制和动力功能的系统。

示例:接口包括主控、示教器、操作面板、存储设备、数字量和模拟量输入输出、打印机接口、视觉单元接口、声音和图像接口、网络接口等。

注:在本标准中使用缩略语 CU 代表控制单元(control unit),专指工业机器人的控制单元。

3.4

信息安全 information security

保护系统所采取的措施,由建立和维护保护系统的措施而产生的系统状态,能够免于非授权访问和