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

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

非授权或意外的变更、破坏或者损失的系统资源的状态。基于 CU 的能力，能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能，同时保证授权人员和系统不被阻止。防止对 CU 的非法或有害的入侵，或者干扰其正确和计划的操作。

注 1：措施可以是与物理（网络）安全（控制物理访问 CU 的资产）或者逻辑（网络）安全（登录给定系统和应用的能力）相关的控制手段。

注 2：改写 GB/T 30976.1—2014，定义 3.1.14。

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）

CU：控制单元（Control Unit）

DoS：拒绝服务（Denial of Service）

ID：身份标识号码（Identification）

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 通信架构及关联性

5.1 工业机器人控制单元通信架构

工业机器人控制单元通信架构，如图 1 所示。

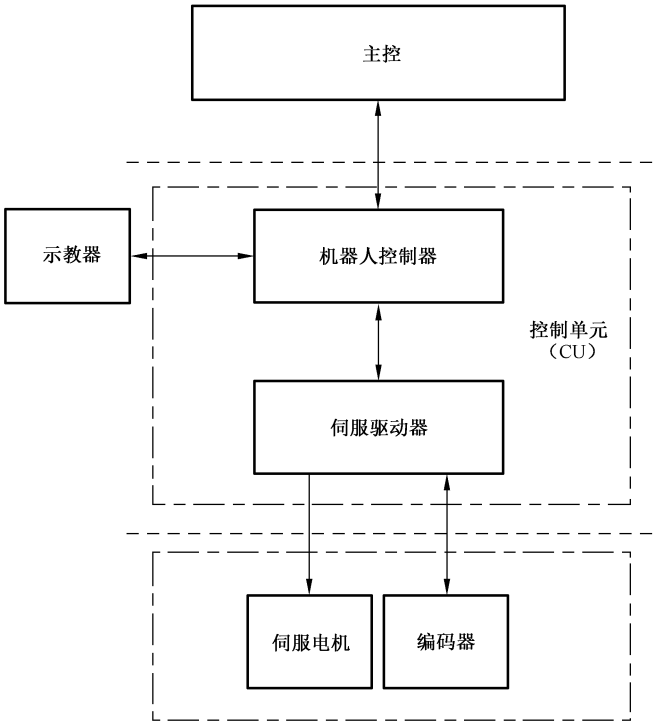

图 1 工业机器人控制单元通信架构

其中，CU 本体主要包括机器人控制器和伺服驱动器。

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) 同步串行通信；
b) 异步串行通信；
c) 以太网；
d) 总线。

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) 脉冲；
b) 模拟量；
c) 同步串行通信；
d) 异步串行通信；
e) 以太网和总线。

伺服驱动器与编码器和伺服电机之间的通信方式包括但不限于以下方式：

a) 脉冲；
b) 模拟量；
c) 同步串行通信；
d) 异步串行通信；
e) 以太网和总线。

机器人控制器模型见 GB/T 32197—2015 中图 1。

5.2 示教器与工业机器人 CU 之间的脆弱性

威胁源应包括但不限于以下内容：

a) 示教器未授权使用；
b) 示教器组态软件存在漏洞；
c) 示教器被误操作；
d) 通信缺少身份认证。

潜在的后果应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) 无法正常操作软件。

5.3 主控与工业机器人 CU 之间的脆弱性

威胁源应包括但不限于以下内容：

a) 主控的固有漏洞；
b) 主控抵御 DoS 攻击能力弱；
c) 主控开放不必要的远程服务端口；
d) 主控未经授权的下载安装程序；
e) 通信缺少身份认证、数据完整性、数据保密性的保护；
f) 接受错误指令。

潜在的后果应包括但不限于以下内容：

a) 非法查看、上传、下载、改变逻辑代码；
b) 非法读写、删除系统文件；
c) 非法改变文件权限；
d) 非法重启；

e) 非法恢复缺省设置；
f) 通信被阻塞，下发指令被干扰；
g) 通信数据被篡改、窃取。

5.4 机器人控制器与伺服驱动器之间的脆弱性

威胁源应包括但不限于以下内容：
a) 通信缺少身份认证、数据完整性、数据保密性的保护；
b) 机器人控制器固有漏洞；
c) 机器人控制器抵御 DoS 攻击能力弱。
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；
b) 机器人运行时意外停机；
c) 数据被篡改、删除、窃取。

6 信息安全要求

6.1 总则

工业机器人 CU 信息安全主要应包括：
a) 示教器/主控与 CU 的信息安全；
b) CU 内部的信息安全。
工业机器人 CU 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 对应条文的要求。

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 要求。

6.3 信息安全技术要求

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。同时，CU 应提供为以下事件生成审计记录的能力：
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。

6.3.1.2 中央管理的、系统范围的审计跟踪

中央管理的、系统范围的审计跟踪(SR2.8 RE(1))应符合 GB/T 30976.1—2014 中 6.3.8.1 的要求。同时，CU 应提供能力，对审计事件进行中央管理，并将来自整个 CU 内多个部件的审计记录汇聚为系统范围的、时间相关的审计跟踪。

6.3.1.3 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。同时,CU 应:

a) 根据日志管理和系统配置普遍认可的推荐值来分配足够的审计记录存储容量。提供审计机制减少超出容量的可能性;

b) 当分配的审计记录存储量达到最大审计记录存储容量的某个可配置比例时,CU 应提供发出警告的能力。

6.3.1.4 对审计流程失败时的响应

对审计流程失败时的响应(SR2.10)应符合 GB/T 30976.1—2014 中 6.3.10 的要求。同时,CU 应:

a) 在审计流程失败时,提供向人员告警并防止技术服务和功能丢失的能力;

b) 当审计流程失败时,提供停止生成审计记录的能力。

6.3.1.5 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。CU 应保护审计信息和审计工具不被未授权地访问、修改和删除。

6.3.1.6 一次性写入介质上的审计记录

一次性写入介质上的审计记录[SR3.9 RE(1)]应符合 GB/T 30976.1—2014 中 6.4.9.1 的要求。CU 应提供在基于硬件的、一次性写入介质上生成审计记录的能力。

6.3.1.7 审计日志的可访问性

审计日志的可访问性(SR6.1)应符合 GB/T 30976.1—2014 中 6.7.1 的要求。CU 应为已授权的人和(或)工具提供访问审计日志的能力。

6.3.1.8 对审计日志的编程式访问

对审计日志的编程式访问[SR6.1 RE(1)]应符合 GB/T 30976.1—2014 中 6.7.1.1 的要求。CU 应使用应用编程接口 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。CU 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。CU 应提供能力,采用密码学机制识别信息在通信过程中的变更,除非信息已被其他可替换的物理措施保护。

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。CU 应提供能力检测、记录和保护软件和信息不受未经授权的变更。

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。CU 应提供能力，使用自动化工具在完整性验证期间发现不符时通知人员。

6.3.2.5 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。CU 应验证任何输入的语法和内容，这些输入是作为工业过程控制输入或直接影响 CU 行为的输入。

6.3.2.6 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。CU 应提供能力，在遭受攻击无法保持正常运行时能够将输出设为预先定义的状态。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。

6.3.2.7 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。CU 应能够识别和处理错误条件的方式，应能够实施有效的补救，这一方式不能提供可能被利用来攻击 CU 的信息，除非泄露这一信息为及时发现并修理问题的必要条件。

6.3.2.8 会话完整性

会话完整性(SR3.8)应符合 GB/T 30976.1—2014 中 6.4.8 的要求。CU 应提供保护通信会话完整性的机制，能为通信会话的每一端提供端对端身份和传输信息正确性的信任。

6.3.2.9 会话终止后会话 ID 的失效

会话终止后会话 ID 的失效[SR3.8 RE(1)]应符合 GB/T 30976.1—2014 中 6.4.8.1 的要求。在用户登出或会话终止(包括浏览器会话)后，CU 应提供使其会话标识失效的能力。

6.3.2.10 唯一会话 ID 的产生和承认

唯一会话 ID 的产生和承认[SR3.8 RE(2)]应符合 GB/T 30976.1—2014 中 6.4.8.2 的要求。CU 应提供能力，为每个会话生成唯一的会话标识 ID，并且只认可系统生成的会话标识。

6.3.2.11 会话 ID 的随机性

会话 ID 的随机性[SR3.8 RE(3)]应符合 GB/T 30976.1—2014 中 6.4.8.3 的要求。CU 应提供使用普遍接受的随机源生成唯一的会话标识的能力。

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。CU 应提供能力，对有读授权的信息在静态和传输中进行保密性保护。CU 应：

a) 通过维护具有可控物理访问的可信网络来保护敏感信息的保密性；

b) 识别敏感信息；

c) 对敏感信息的访问和传输进行控制，以防止窃听和篡改。

示例：认证信息，例如用户名和口令应考虑保密。

6.3.3.2 静态和经由不可信网络传输的数据的保密性保护

静态和经由不可信网络传输的数据的保密性保护[SR4.1 RE(1)]应符合 GB/T 30976.1—2014 中 6.5.1.1 的要求。CU 应提供能力保护静态信息和穿越不可信网络的远程访问连接的保密性。CU 应加密敏感的 CU 信息，包括口令，在存储和穿过外部网络传输时是加密的。

6.3.3.3 区域边界的保密性保护

区域边界的保密性保护[SR4.1 RE(2)]应符合 GB/T 30976.1—2014 中 6.5.1.2 的要求。CU 应提供能力保护穿越所有区域边界的信息的保密性，敏感的 CU 数据包括口令在存储和穿越区域边界时应加密。

6.3.3.4 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。CU 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。

6.3.3.5 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。CU 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 CU 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。

6.3.3.6 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。当需要密码时，CU 应根据普遍接受的工业实践和推荐来使用密码算法、密钥长度以及密钥创建和管理机制。

6.3.4 通信信息安全要求

6.3.4.1 总线拓扑结构

CU 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

CU 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

CU 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

为保证 CU 中各站点的时间一致性、通信稳定性，CU 应进行时间同步。CU 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

CU 高速通信总线控制权的仲裁方式可采用主站管理从站、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

CU 应具备为工业机器人提供以下能力：

a) CU 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 持续监视

持续监视(SR6.2)应符合 GB/T 30976.1—2014 中 6.7.2 的要求。CU 应使用普遍接受的安全工业实践和推荐来提供持续监视所有安全机制的性能的能力，以及时检测、特征化、削减和报告对安全的违背。

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。CU 应对拒绝服务攻击有一定的防护能力。

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。CU 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 限制拒绝服务攻击对其他系统和网络的影响

限制拒绝服务攻击对其他系统和网络的影响[SR7.1 RE(2)]应符合 GB/T 30976.1—2014 中 6.8.1.2的要求。CU 应提供能力限制所有用户引发拒绝服务攻击事件的能力，这些事件可能影响其他 CU 和网络。

6.3.5.5 资源管理

资源管理(SR7.2)应符合 GB/T 30976.1—2014 中 6.8.2 的要求。CU 应对资源的使用提供安全功能，防止资源耗尽。

6.3.5.6 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。CU 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和系统级备份(包含系统状态信息)。CU 应提供以可配置的频率自动实现上述功能的能力。

6.3.5.7 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。CU 应提供验证备份机

制的可靠性的能力。

6.3.5.8 备份自动化

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

6.3.5.9 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，CU 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 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。CU 应提供能力，按照 CU 提供商规定的指南中描述的推荐网络和安全配置进行配置。CU 应提供与现有部署网络和安全配置设置之间的一个接口。CU 应具备为工业机器人提供以下能力：

a) 能为配置设置提供可调节的参数；

b) 能根据安全策略和规程对配置变更进行监视和控制。

6.3.6.2 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。CU 应提供必要的能力，明确禁止和(或)限制对非必要的功能、端口、协议和(或)服务的使用。

6.3.6.3 部件清单

部件清单(SR7.8)应符合 GB/T 30976.1—2014 中 6.8.8 的要求。CU 应提供报告当前已安装的部件及其关联属性的列表的能力。CU 应：

a) 提供报告已安装部件及其关联属性的方法；

b) 确保已安装部件在系统部件清单目录中是正确的；

c) 在部件增加、移除或部件属性变更时，正确更新系统部件清单目录。

6.4 主控与 CU 之间的信息安全要求

6.4.1 编程代码要求

6.4.1.1 编程代码

编程代码(SR2.4)应符合 GB/T 30976.1—2014 中 6.3.4 的要求。CU 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。

6.4.1.2 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。CU 应提供能力，在允许代码执行之前验证代码的完整性。

6.4.1.3 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。CU 应具备

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 CU；
c) 监视代码的使用。

6.4.2 并发连接控制

并发连接控制(SR2.7)应符合 GB/T 30976.1—2014 中 6.3.7 的要求。对任意给定用户，CU 应提供将每个接口的并发连接的数目限制为一个可配置的数目的能力。

6.4.3 时间要求

6.4.3.1 时间戳

时间戳(SR2.11)应符合 GB/T 30976.1—2014 中 6.3.11 的要求。CU 应提供时间戳用于生成审计记录。

6.4.3.2 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。CU 应提供以可配置的频率同步内部系统时钟的能力。

6.4.3.3 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。

6.4.4 标识和认证要求

6.4.4.1 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。CU 应具备为工业机器人提供以下能力：

a) 提供标识和认证所有用户(人)的能力。这一能力应在访问 CU 的所有访问接口上实施，以支持符合相应安全策略和规程的职责分离和最小特权原则；
b) 使用户标识符能在所有访问接口上被认证，无效用户标识符在所有访问接口上被拒绝。

6.4.4.2 非可信网络的多因子认证

非可信网络的多因子认证[SR1.1 RE(2)]应符合 GB/T 30976.1—2014 中 6.2.1.2 的要求。当人通过非可信网络访问 CU 时，系统应为其提供多因子认证的能力。对于经由非可信网络的远程访问的认证方法应多于一种。

示例：非可信网络访问，例如远程访问。

6.4.4.3 软件进程的标识和认证

软件进程的标识和认证(SR1.2)应符合 GB/T 30976.1—2014 中 6.2.2 的要求。CU 应提供标识和认证所有软件进程的能力。这一能力应在访问 CU 的所有访问接口上实施，以支持符合相应安全策略和规程的职责分离和最小特权原则。

6.4.4.4 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。CU 应具备为工

业机器人提供以下能力：

a) 对所有合法软件进程拥有唯一标识认证的能力；

b) 对所有用户(人)提供唯一标识和认证的能力。

6.4.4.5 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。CU 应提供对所有账号的管理，包括创建、激活、修改、禁用和移除账号的能力，当一个或多个号被修改或移除时，未被修改的账号保持激活和账号权限不变。

6.4.4.6 统一的账号管理

统一的账号管理[SR1.3 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.3.1 的要求。CU 应提供能力支持统一的账号管理。

6.4.4.7 标识符管理

标识符管理(SR1.4)应符合 GB/T 30976.1—2014 中 6.2.4 的要求。CU 应提供按照角色或 CU 接口管理标识符的能力。

示例：标识符，例如用户 ID。

6.4.4.8 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。CU 应具备为工业机器人提供以下能力：

a) CU 应提供能力定义初始的认证码内容；

b) CU 应提供能力周期的变更/更新认证码；

c) CU 应保护认证码存储和传输时不被未经授权的泄露和更改。

6.4.4.9 软件进程标识凭证的硬件安全

软件进程标识凭证的硬件安全[SR1.5 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.5.1 的要求。对于软件进程和设备用户，CU 应提供使用硬件机制保护相关认证码的能力。

6.4.4.10 口令认证

口令认证(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 CU，CU 应提供能力，实施可配置的基于最小长度和不同字符类型的口令强度。

6.4.4.11 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。CU 应为用户(人)提供口令重用次数、口令有效期可配置的能力，这些能力符合普遍接受的安全工业实践。

6.4.4.12 对所有用户的口令有效期的限制

对所有用户的口令有效期的限制[SR1.7 RE(2)]应符合 GB/T 30976.1—2014 中 6.2.7.2 的要求。CU 应为所有用户提供实施口令最小和最大有效期限制的能力。

6.4.4.13 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，CU应提供按照普遍接受的最佳实践运行公钥基础设施或从现有的PKI中获取公钥证书的能力。

6.4.4.14 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CU，CU应具备为工业机器人提供以下能力：

a) 系统应通过检查给定证书的签名的有效性来证实证书；
b) 通过可接受的证书认证机构(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) 建立用户对相应私钥的控制；
e) 将已认证的标识映射为用户。

6.4.4.15 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。CU应提供能力，按照普遍接受的安全工业实践和推荐，通过硬件机制保护相关的私钥。

6.4.4.16 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。CU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。

6.4.4.17 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。CU应具备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；
c) 不应允许关键服务或服务器运行的系统账号交互式登录。

6.4.5 授权和访问要求

6.4.5.1 经由非可信网络的访问

经由非可信网络的访问(SR1.13)应符合GB/T 30976.1—2014中6.2.13的要求。CU应能监视和控制所有经由不可信网络对CU的访问，拒绝来自不可信网络的访问，除非被指定角色批准。

6.4.5.2 明确地对访问请求的批准

明确地对访问请求的批准[SR1.13 RE(1)]应符合GB/T 30976.1—2014中6.2.13.1的要求。默认的访问，CU应提供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。

6.4.5.3 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。在所有接口上，CU应提供能力执行分配给所有用户(人)的授权，按照职责分离和最小特权来控制对CU的使用。

CU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) 浏览权限用户；
b) 操作员；
c) 控制应用工程师；
d) 系统管理员；
e) 操作主管。

6.4.5.4 无线使用控制

无线使用控制(SR2.2)应符合 GB/T 30976.1—2014 中 6.3.2 的要求。CU 应提供能力，对 CU 的无线连接应依据普遍接受的安全工业实践进行授权、监视和限时使用，CU 应具备为工业机器人提供以下能力：

a) 能授权、监视和限制对 CU 的无线访问；
b) 能使用适当的认证机制保护无线访问。

6.4.5.5 对未授权的无线设备进行识别和报告

对未授权的无线设备进行识别和报告[SR2.2 RE(1)]应符合 GB/T 30976.1—2014 中 6.3.2.1 的要求。CU 应提供识别和报告未授权的与 CU 相关的无线设备在 CU 物理环境内发射信号的能力。

6.5 CU 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。CU 应提供标识和认证所有用户(人)的能力，这一能力应在访问 CU 的所有访问接口上实施，以支持符合相应安全策略的规程的职责分离和最小特权原则。

6.5.1.2 唯一标识和认证

唯一标识和认证[SR1.1 RE(1)]应符合 GB/T 30976.1—2014 中 6.2.1.1 的要求。CU 应对所有用户(人)提供唯一标识和认证的能力。

6.5.1.3 非可信网络的多因子认证

非可信网络的多因子认证[SR1.1 RE(2)]应符合 GB/T 30976.1—2014 中 6.2.1.2 的要求。当人通过非可信网络访问 CU 时，系统应为其提供多因子认证的能力。对于经由非可信网络的远程访问的认证方法要求多于一种。

示例：非可信网络访问，例如远程访问。

6.5.1.4 软件进程的标识和认证

软件进程的标识和认证(SR1.2)应符合 GB/T 30976.1—2014 中 6.2.2 的要求。CU 应提供标识和认证所有软件进程的能力。这一能力应在访问 CU 的所有访问接口上实施，以支持符合相应安全策略和规程的职责分离和最小特权原则。

6.5.1.5 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。CU 应对所有合法软件进程拥有唯一标识认证的能力。

6.5.2 恶意代码的防护要求

6.5.2.1 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。CU 应采用防护机制来防止、检测、报告和消减恶意代码或非授权软件的影响。CU 应具备为工业机器人提供以下能力：

a) 采用一定的防护机制以防护恶意代码；
b) 配置、启用防护产品；
c) 更新防护产品到软件最新版本；
d) 提供防护产品防护的恶意代码类型的列表或说明。

6.5.2.2 在入口和出口点防护恶意代码

在入口和出口点防护恶意代码[SR3.2 RE(1)]应符合 GB/T 30976.1—2014 中 6.4.2.1 的要求。CU 应提供在所有入口和出口点上采用恶意代码防护机制的能力。CU 应具备为工业机器人提供以下能力：

a) 在区域边界提供恶意代码的防护；
b) 配置和启用防护产品；
c) 更新防护产品到软件最新的版本；
d) 提供防护产品防护的恶意代码类型的列表或说明。

6.5.2.3 SR 3.2 RE(2) 恶意代码防护的集中管理和报告

恶意代码防护的集中管理和报告[SR3.2 RE(2)]应符合 GB/T 30976.1—2014 中 6.4.2.2 的要求。CU 应提供集中管理恶意代码防护机制的能力。

参 考 文 献

[1] GB/T 12643—2013 机器人与机器人装备 词汇
[2] GB/T 25069—2010 信息安全技术 术语
[3] GB/T 30976.2—2014 工业控制系统信息安全 第2部分:验收规范
[4] GB/T 33266—2016 模块化机器人高速通用通信总线性能