

T/CRSS

重庆市机器人学会团体标准

T/CRSS XXXX—XXXX

复合机器人应用身份标识与身份认证规范

Identity and identification specification for hybrid robot applications

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

XXXX - XX - XX 实施

重庆市机器人学会 发布

目 次

前言	II
引言	II
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 复合机器人应用系统框架	2
6 复合机器人应用身份安全风险	3
6.1 控制方身份被冒用风险	3
6.2 复合机器人身份被冒用风险	3
7 复合机器人应用身份安全要求	3
7.1 复合机器人应用身份标识	3
7.2 复合机器人应用身份标识安全	3
7.3 复合机器人数字证书格式	4
8 复合机器人应用身份认证要求	4

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。

本文件由重庆市机器人学会提出并归口。

本文件起草单位：

本文件主要起草人：

引 言

为了保障复合机器人所在生产线的安全，对复合机器人应用所涉对象身份标识和身份认证进行规范化，提升复合机器人应用身份认证的安全性，以便不同厂商的产品之间能安全互通对接。

本文件涉及密码管理的相关内容，按国家密码管理有关规定实施。

复合机器人应用身份标识与身份认证规范

1 范围

本文件规定了复合机器人及配合复合机器人协同工作的管控系统、云端系统、示教器等的安全要求，以及复合机器人应用各活动对象间的身份认证方法。

本文件适用于构建复合机器人安全应用系统。

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 15843.3-2023 《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》

GB/T 25064-2010 《信息安全技术 公钥基础设施 电子签名格式规范》

GB/T 32905-2016 《信息安全技术 SM3密码杂凑算法》

GB/T 32918.2-2016 《信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法》

GB/T 35276-2017 《信息安全技术 SM2密码算法使用规范》

GM/T 0005-2021 《随机性检测规范》

GM/T 0015-2023 《数字证书格式》

GM/Z 4001-2013 《密码术语》

3 术语和定义

GM/Z 4001-2013界定的以及下列术语和定义适用于本文件。

3.1

复合机器人 hybrid robot

复合机器人是一种集成移动机底盘、工业机械臂、视觉系统等功能为一体的新型机器人，具备“手、脚、眼、脑”等功能，用于接受控制指令、执行作业任务、返回执行过程及结果数据的设备。

3.2

复合机器人群 hybrid robots group

为完成某项任务而由若干台复合机器人组成的协同作业群。

3.3

控制方 controlling party

控制复合机器人正常作业，用于向复合机器人发送控制指令、布置作业任务、采集作业执行过程及结果的系统，包括但不限于：示教器、管控系统、云端系统等。

3.4

复合机器人应用系统 hybrid robot application system

协助生产过程自动化和无人化为目标的应用系统，包含：复合机器人群和控制方两大部分。

3.5

示教器 teach pendant

一种用于控制复合机器人的手持式装置。

3.6

管控系统 management and control system

一种用于管理和控制复合机器人的软件系统。

3.7

云端系统 cloud system

一种可通过互联网对复合机器人进行远程管理与控制的软件系统，部署在云端。

- 3.8
控制指令 control command
控制方发送给复合机器人用于控制复合机器人行为的数据。
- 3.9
作业任务 work task
控制方发送给复合机器人的工作任务数据。
- 3.10
作业任务过程 the process of work task
复合机器人发送给控制方的作业任务过程状态数据。
- 3.11
身份标识 identity
用于标识身份的编码，具有唯一性。
- 3.12
数字证书 digital certificate
用于证明身份的、不可篡改的电子文件，由CA中心签发。
- 3.13
身份密钥 identity key
与身份标识对应的、可用于密码计算来证明自己身份真实性的密钥。
- 3.14
数字签名 digital signature
被认证者用自己的身份密钥对认证数据进行计算的过程。
- 3.15
身份认证 identification
鉴别认证对象提交身份材料（包括：数字签名、数字证书）真伪的过程。
- 3.16
验证签名 authentication
对证书申请材料和申请者之间的关联性进行确定的活动。
- 3.17
Handle 编码
用Handle技术实现的标识解析编码。

4 缩略语

下列缩略语适用于本文件。

CA：认证服务机构(Certification Authority)

OID：对象标识符(Object Identifier)

UUID：通用唯一识别码 (Universally Unique Identifier)

5 复合机器人应用系统框架

- 5.1 复合机器人应用系统由控制方和复合机器人两大组成部分组成，见图 1。

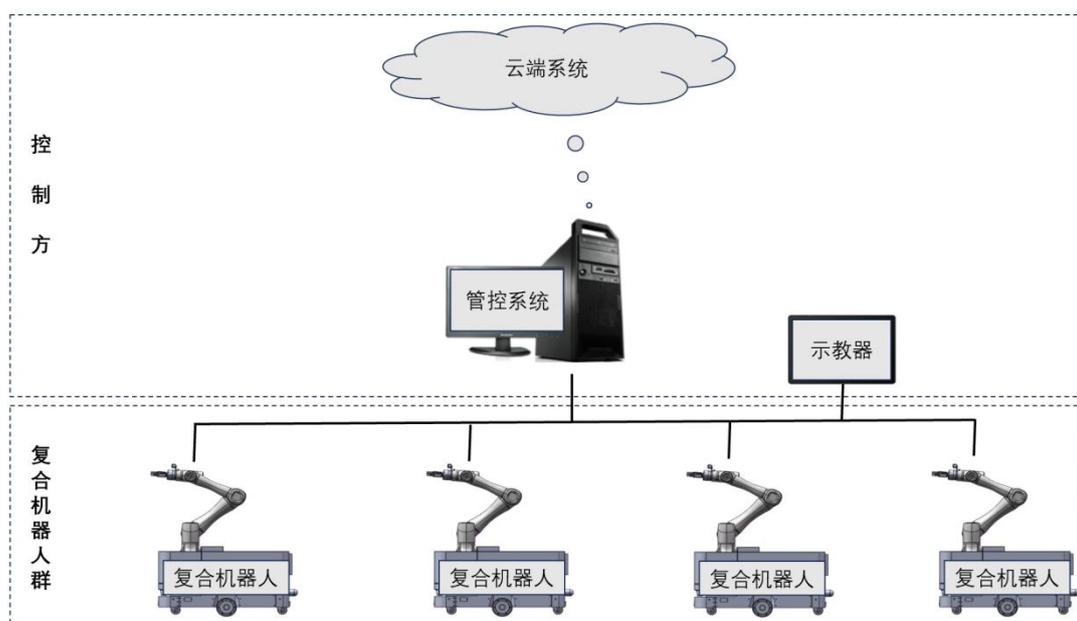


图1 复合机器人应用系统

5.2 控制方包括但不限于：示教器、管控系统、云端系统。控制方用于对复合机器人进行管理和控制，包括：发送控制指令、布置作业任务、采集作业任务过程等。

5.3 复合机器人包含至少一台复合机器人，用于接受控制方的控制指令、作业任务，向控制方提供作业任务过程等。

5.4 对于简单的只有一台复合机器人的应用场景，一台示教器和一台复合机器人，或者一套管控系统和一台复合机器人即可满足应用场景需求。

5.5 对于多机协同的应用场景，需一套管控系统和若干台复合机器人来满足应用场景。

5.6 对于需要通过云端控制的场景，需要增加云端系统。

6 复合机器人应用身份安全风险

6.1 控制方身份被冒用风险

6.1.1 复合机器人接受了非法控制方发送的控制指令、作业任务，导致复合机器人作业紊乱、出现故障或生产事故。

6.1.2 复合机器人向非法控制方发送作业任务过程，导致生产数据泄密。

6.2 复合机器人身份被冒用风险

6.2.1 控制方接受了非法复合机器人发送的作业任务过程，导致控制方生产调度与决策紊乱，对正常生产造成干扰，甚至出现生产事故。

6.2.2 控制方向非法复合机器人发送控制指令、作业任务，导致控制指令和作业任务数据泄密。

7 复合机器人应用身份安全要求

7.1 复合机器人应用身份标识

7.1.1 复合机器人和控制方应采用全球唯一编码来形成自己的身份标识，应采用 Handle 编码、OID 编码、UUID 之一进行编码。

7.1.2 复合机器人和控制方的身份标识应以安全的方式在对方系统中进行注册。

7.2 复合机器人应用身份标识安全

7.2.1 复合机器人和控制方应采用数字证书对表示自己身份的身份标识进行绑定，数字证书格式应复

合本规范 7.3 的要求

7.2.2 复合机器人和控制方应从国家认可的第三方 CA 机构获取代表身份的数字证书，以供复合机器人应用各活动对象间进行身份认证。

7.2.3 复合机器人和控制方应采用国家密码管理局许可的密码模块对代表身份的身份密钥进行保存和使用。

7.3 复合机器人数字证书格式

数字证书主题格式应采用：

——C=CN；

——ST=厂商所在省；

——L=厂商所在市；

——O=厂商名称；

——OU=设备/系统名称；

——CN=身份标识。

注：数字证书其它部分格式应符合GM/T 0015-2023的要求。

8 复合机器人应用身份认证要求

8.1 复合机器人在初始化启动时，应对其控制方进行身份认证。

8.2 复合机器人控制方在采集复合机器人数据时宜对其进行身份认证。

8.3 复合机器人与控制方在进行身份认证时应采用数字证书进行身份认证。

8.4 复合机器人与控制方的身份认证流程应符合 GB/T 15843.3-2023 要求。

8.5 复合机器人与控制方在身份认证过程中用到的随机数应符合 GM/T 0005-2021 要求。

8.6 复合机器人与控制方在身份认证过程中用到的数字签名应符合 GB/T 25064-2010 要求。

8.7 复合机器人与控制方在身份认证过程中用到的数字签名算法应符合 GB/T 32918.2-2016 要求。

8.8 复合机器人与控制方在身份认证过程中用到的数字签名格式应符合 GB/T 35275-2017 要求。

8.9 复合机器人与控制方在身份认证过程中用到的杂凑算法应符合 GB/T 32905-2016 要求。