ICS 25.040.30
CCS J 28

T/CRSS

重 庆 市 机 器 人 学 会 团 体 标 准

T/CRSS XXXX—XXXX

复合机器人应用安全通信规范

Security communication 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 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　复合机器人应用系统框架 2
6　复合机器人应用通信安全风险 2
7　复合机器人应用通信安全要求 3
7.1　复合机器人通信安全要求 3
7.2　控制方通信安全要求 3

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

在协同工作时，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间通信安全要求进行了规范化，提升复合机器人应用数据传输的安全性，以便不同厂商的产品之间能安全互通对接。本文件的对象为复合机器人应用所涉对象，包括：复合机器人、复合机器人管控系统、复合机器人云端系统，复合机器人示教器等。

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。

复合机器人应用安全通信规范

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、示教器等的安全通信要求。

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 32905-2016 《信息安全技术 SM3密码杂凑算法》

GB/T 32907-2016 《信息安全技术 SM4分组密码算法》

GM/T 0005-2021 《随机性检测规范》

GM/T 0028-2024 《密码模块安全技术要求》

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

身份认证 identification

鉴别认证对象提交的身份认证证明（包括：数字签名、数字证书）真伪的过程。

3.12

身份认证证明 the evidence of identification

为身份认证提供的证明数据（包括：数字签名、数字证书）。

4 缩略语

下列缩略语适用于本文件。

CA：认证服务机构(Certification Authority)

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群两大部分组成，见图 1 所示。

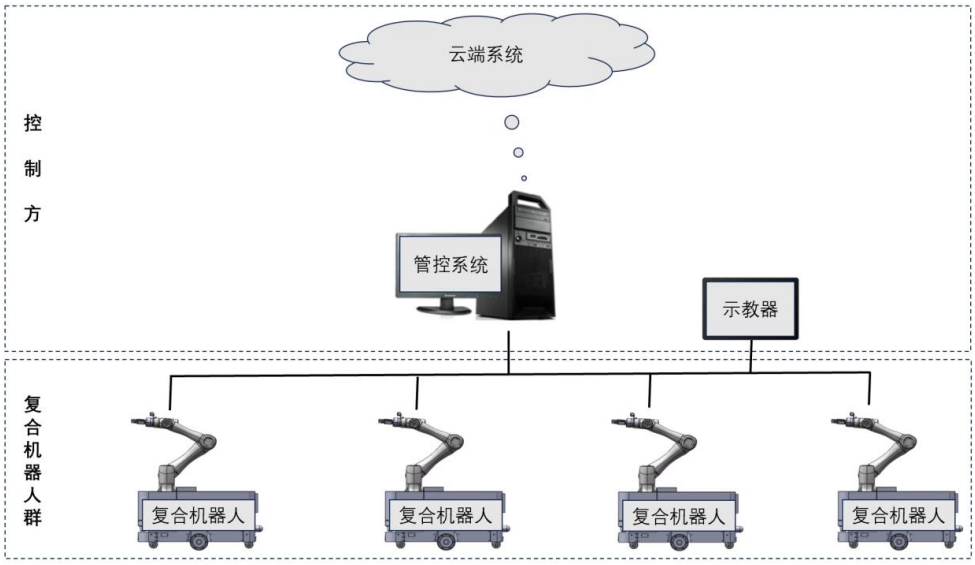

图1 复合机器人应用系统

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群进行管理和控制，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 复合机器人群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 复合机器人应用通信安全风险

6.1 控制方发送给复合机器人的控制指令可能被篡改，导致复合机器人失控，甚至出现生产事故。

6.2 控制方发送给复合机器人的作业任务可能被篡改，导致复合机器人未按照作业任务要求作业，进而导致生产线紊乱。
6.3 控制方发送给复合机器人的控制指令可能被非法截获、分析、寻找潜在漏洞，会对复合机器人应用形成潜在威胁。
6.4 控制方发送给复合机器人的作业任务可能被非法截获、分析，造成生产数据泄密。
6.5 复合机器人发送给控制方的作业任务过程可能被篡改，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。
6.6 复合机器人发送给控制方的作业任务过程可能被非法截获、分析，造成生产数据泄密。

7 复合机器人应用通信安全要求

7.1 复合机器人通信安全要求

7.1.1 复合机器人在接受控制方的控制指令、作业任务前应对控制方进行身份认证。
7.1.2 复合机器人在接受控制方的控制指令、作业任务后应对控制指令和作业任务进行数据完整性检测。
7.1.3 复合机器人在发送作业任务过程给控制方前宜提供身份认证证明。
7.1.4 复合机器人在发送作业任务过程给控制方前宜对作业任务过程进行数据完整性处理。
7.1.5 复合机器人在发送作业任务过程给控制方前宜对作业任务过程进行数据加密处理。
7.1.6 身份认证过程应符合 GB/T 15843.3-2023 要求。
7.1.7 数据完整性检测与数据完整性处理应符合 GB/T 32905-2016 要求。
7.1.8 数据加密处理应符合 GB/T 32907-2016 要求。
7.1.9 数据加密处理所用密钥随机性应符合 GM/T 0005-2021 要求。
7.1.10 进行身份认证、数据完整性检测、数据完整性处理、数据加密所用的密码模块应符合 GM/T 0028-2014 要求。
7.1.11 身份认证所使用的数字证书应为国家认可的第三方 CA 机构签发 。
7.1.12 身份认证、数据完整性处理、数据加密所使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

7.2 控制方通信安全要求

7.2.1 控制方在发送控制指令、作业任务给复合机器人前应提供身份认证证明。
7.2.2 控制方在发送控制指令、作业任务给复合机器人前应对控制指令和作业任务进行数据完整性处理。
7.2.3 控制方在发送控制指令、作业任务给复合机器人前宜对控制指令和作业任务进行数据加密处理。
7.2.4 控制方在接受复合机器人的作业任务过程前宜对复合机器人进行身份认证。
7.2.5 控制方在接受复合机器人的作业任务过程后宜对作业任务过程进行数据完整性检测。
7.2.6 身份认证过程应符合 GB/T 15843.3-2023 要求。
7.2.7 数据完整性检测与数据完整性处理应符合 GB/T 32905-2016 要求。
7.2.8 数据加密处理应符合 GB/T 32907-2016 要求。
7.2.9 数据加密处理所用密钥随机性应符合 GM/T 0005-2021 要求。
7.2.10 进行身份认证、数据完整性检测、数据完整性处理、数据加密所用的密码模块应符合 GM/T 0028-2014 要求。
7.2.11 身份认证所使用的数字证书应为国家认可的第三方 CA 机构签发。
7.2.12 身份认证、数据完整性处理、数据加密所使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。