ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/SDEPI

团　　体　　标　　准

T/SDEPI XXXX—2023

工程机械设备网络管控安全要求

Security Specification on Management and Control of Construction Machinery over Networks

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

山东省 XXX 协会　　发 布

目　　次

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》以及 GB/T 20001《标准编写规则》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。

本文件由山东省装备制造业协会提出并归口。

本文件起草单位：临沂大学、山东润通科技有限公司、山东临工工程机械有限公司、临沂市中信信息技术有限公司、临沂智慧大数据研究院、 …

本文件主要起草人：武传坤、傅德谦、刘鸣涛、郭锋、荆长强、张问银、赵斌、张鑫、杜茜、王星、陈新疆、朱孔伟、蒋本帅、陈超伟、谢凡卿、赵玉伟、宋晓颖、王庆国、赵胜建、姜海涛、…

工程机械设备网络管控安全要求

1 范围

本文件规定了机械设备网络管控系统总体架构、设备定位信息采集、设备状态信息采集、数据传输、身份管理、设备的网络控制、数据管理的要求，以及网络管控平台建设技术、安全、安全管理、运维的要求。

本文件适用于（适用的领域和使用者）。

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 25069-2020 《信息安全技术 术语》

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

GB/T 36633-2018 《信息安全技术 网络用户身份鉴别技术指南》

3 术语和定义

3.1 术语和定义

GB/T 25069-2020界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本标准。

DDoS：分布式拒绝服务

4 机械设备网络管控系统总体架构

机械设备网络管控系统包括机械设备、通信系统、网络管控平台，其中机械设备一般由人工操作，而机械设备的操作多用于在某个小区域内施工作业，偶尔涉及远程运输问题；通信网络是数据传输网络，一般使用移动通信网络，如LTE或5G移动网络；网络管控平台则是设备管理者对设备进行网络管控和监督的数据和控制平台。它们之间的逻辑关系如图1所示：

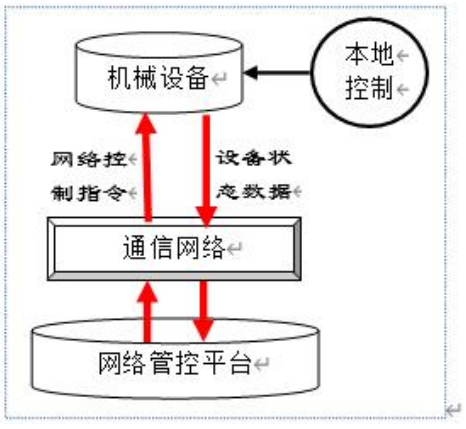

图 1 机械设备网络管控系统架构示意图

5 设备定位信息采集要求

5.1 设备定位模块要求

5.1.1 设备定位模块配置要求

本项要求包括：

a) 网络管控的机械设备须安装规范厂商生产的北斗导航定位模块；
b) 网络管控的机械设备应安装规范厂商生产的 GPS 定位模块。

5.1.2 设备定位模块精度要求

本项要求包括：

a) 网络管控的机械设备定位模块的位置数据精度应精确到 10 米以内；
b) 网络管控的机械设备定位模块的位置数据应能正确对应到电子地图上的位置。

5.1.3 设备定位模块安装要求

本项要求包括：

a) 网络管控的机械设备定位模块的安装应具有一定抗震、抗拆功能；
b) 网络管控的机械设备定位模块的工作状态应进行野外测试，确保能正常采集定位信息。

5.2 设备定位信息采集要求

5.2.1 开机关机位置采集要求

本项要求包括：

a) 网络管控的机械设备在开机时，应采集设备的位置信息，并与开机信息进行关联；
b) 后台网络管控平台在收到设备开机位置信息后，应予以回复确认。如果设备开机位置信息发送后未收到网络管控平台的回复确认，则再次发送位置信息，直至接收到网络管控平台的回复确认，或已经将开机位置信息发送了三次；
c) 网络管控的机械设备在关机时，应采集设备的位置信息，并与关机信息进行关联。

5.2.2 持续位置采集要求

本项要求包括：

a) 网络管控的机械设备在网络连接正常的情况下，应定期上传自己的位置信息；
b) 网络管控的机械设备在网络连接不正常的情况下，应提前获取授权，并在授权终止前通过网络连接上传设备的位置信息。

5.3 设备运动轨迹数据采集要求

5.3.1 设备移动时位置信息的采集要求

本项要求包括：

a) 网络管控的机械设备在移动状态中，根据移动速度可以调整位置信息的获取频率，使两次发送的位置距离不大于 1000 米；
b) 如果设备发送位置信息时没有网络连接，则在网络连接正常的情况下，第一时间启动位置信息的获取和发送任务。

5.3.2 设备长时间不启动时位置信息的采集要求

本项要求包括：

a) 网络管控的机械设备长时间处于静止且不启动状态，上传位置信息时可以只上传未启动状态下最远一次同样位置的时间信息，并标注位置不变；
b) 网络管控的机械设备长时间处于静止且不启动状态，上传位置信息时，每隔一段时间，上传位置信息，以及未启动状态下最远一次同样位置的时间信息，并标注位置不变。

6 设备状态信息采集要求

6.1 设备停机状态信息采集要求

6.1.1 设备停机时应上传状态信息

网络管控的机械设备在停机时，应上传停机时间和位置信息。

6.1.2 设备停机状态下的信息采集

本项要求包括：

a) 网络管控的机械设备在停机状态，应定时采集并上传位置信息；如果位置信息与上次上传时相同，可以简略方式说明位置未发生变化；
b) 网络管控的机械设备在停机状态，若收到网络管控平台的位置询问，应以应答方式上传当前位置信息。

6.2 设备工作状态信息采集要求

6.2.1 设备开机时应上传状态信息

网络管控的机械设备在开机时，应上传开机时间和位置信息。

6.2.2 设备应定时采集并上传工作状态信息

本项要求包括：

a) 网络管控的机械设备应定时采集并上传当前的工作状态，包括功率输出百分百；
b) 网络管控的机械设备如果在工作状态，应定时采集并上传自开机以来输出功率的均值与方差。

6.2.3 设备应及时采集并上传异常状态信息

本项要求包括：

a) 当设备采集到异常数据时，应及时上传到网络管控平台，并附带预警信息；
b) 当设备电池容量低于 10%时，并在 1 分钟后仍然低于 10%时，应将此报警信息上传到网络管控平台；
c) 网络管控平台若发现设备上传的数据疑似异常且维持 10 分钟以上，或在 20 分钟内，异常数据占比超过 50%，或在 30 分钟内，异常数据占比超过 30%，应给设备发送报警信息，并控制设备逐渐停机。

7 数据传输要求

7.1 网络配置要求

7.1.1 数据传输模块配置要求

本项要求包括：

a) 网络管控的机械设备应配置移动通信模块，并保持通信模块可用；
b) 重要机械设备应配置至少两种通信方式，确保较高的通信成功率；
c) 需要通过网络实施控制的机械设备应配置至少两种独立通信模块。

7.1.2 数据传输安全配置要求

本项要求包括：

a) 网络管控的机械设备应与网络管控平台预置某个共享密钥；
b) 网络管控的机械设备应对上传的数据进行加密处理，保持设备身份标识以明文形式发送。

7.2 数据传输频次要求

7.2.1 正常网络配置下数据传输频次要求

本项要求包括：

a) 网络管控的机械设备在非工作状态下，应至少间隔 10 分钟上报一次当前的位置信息；
b) 网络管控的机械设备在工作状态下，应至少间隔 1 分钟上报一次当前的设备工作状态和位置信息。

7.2.2 网络连接失败时的异常处理要求

本项要求包括：
a) 网络管控的机械设备在上传数据时如果网络连接失败，则在网络连接恢复正常时第一时间上传当前的位置信息和工作状态；
b) 网络管控的机械设备在上传开机或关机状态信息时如果网络连接失败，则记录开机或关机状态信息、位置信息和开关机时间，并在网络连接恢复正常时第一时间上传所记录的信息。

7.2.3 辅助网络传输配置要求

本项要求包括：
a) 处在没有网络信号环境工作的网络管控机械设备，应配置辅助网络传输设备，通过移动通信模块，并保持通信模块可用；
b) 重要机械设备应配置至少两种通信方式，确保较高的通信成功率。

7.2.4 辅助网络传输配置下数据传输频次要求

本项要求包括：
a) 处在没有网络信号环境工作的网络管控机械设备，其辅助网络传输设备应在网络管控平台授权下，配置恰当的数据传输频次；
b) 处在没有网络信号环境工作的网络管控机械设备，其辅助网络传输设备如果在数据传输最大间隔时间两倍的时间内仍然不能成功连接网络，应通过人工方式获取临时解锁密码，以免设备因授权超时而锁死，影响设备的正常使用。

8 身份管理要求

8.1 设备身份管理要求

8.1.1 设备身份标识要求

本项要求包括：
a) 网络管控的机械设备身份标识在网络管控平台数据库内唯一；
b) 网络管控的机械设备身份标识应能体现设备的种类；
c) 网络管控的机械设备身份标识可以进行更新。

8.1.2 设备身份鉴别要求

本项要求包括：
a) 网络管控的机械设备在传输数据时，应对设备的身份标识进行一定的安全保护，使得设备身份标识不容易被伪造；
b) 网络管控的机械设备对身份标识的保护，应采用动态密码方法，避免重放攻击。

8.2 设备操作人员身份管理要求

8.2.1 设备操作人员授权要求

本项要求包括：
a) 网络管控的机械设备应由具有设备操控资质的人员进行操作；
b) 网络管控的机械设备操作人员的身份标识应提前在网络管控平台登记注册。

8.2.2 设备操作人员身份标识鉴别要求

本项要求包括：
a) 网络管控的机械设备在启动时，操作人员的身份标识应上传到网络管控平台进行备案；

b) 网络管控的关键机械设备，其操作人员的身份标识，应通过网络管控平台的身份鉴别，才能启动机械设备。

9 设备的网络控制要求

9.1 设备功率输出限制要求

9.1.1 设备功率定额限制要求

本项要求包括：

a) 网络管控平台应能够对其管控的机械设备通过网络指令限制其功率输出百分百，使得机械设备本地操控人员在作业时，设备的最大输出功率不超过网络控制平台设置的百分百；
b) 网络管控平台应能通过网络随时取消或修改对其管控的机械设备的功率输出限制。

9.1.2 设备渐停控制要求

本项要求包括：

a) 网络管控平台应能够对其管控的机械设备通过网络指令使其功率输出逐渐降低，并在预设的时间内最终停止运行；
b) 网络管控平台应能通过网络随时取消或修改对其管控的机械设备的功率输出限制。

9.2 没有网络连接的设备控制要求

9.2.1 设备的网络管控长时间授权功能要求

本项要求包括：

a) 网络管控平台应能够对其管控的机械设备通过网络指令使其在时间 T 内无须连接网络；
b) 网络管控的机械设备在无网环境下，应持续采集设备功率输出信息，并且在有网情况下将记录的数据上传到网络管控平台；
c) 网络管控的机械设备在无网环境下，如果超出授权时间 T 后仍然不能连接网络，则设备在关闭后不能再次启动。

9.2.2 设备的网络管控代理授权功能要求

本项要求包括：

a) 网络管控的机械设备在无网环境下，应该可以通过独立的移动设备进行代理授权。首先，代理授权的移动设备在有网络环境下与网络管控平台连接，网络管控平台将授权指令发送到代理授权的移动设备，移动设备再与机械设备进行近距离网络连接，将授权转发到机械设备；
b) 代理授权的移动设备应与机械设备有标注通信接口；
c) 代理授权的移动设备在使用前，应在网络管控平台进行注册登记和安全参数配置。

10 数据管理要求

10.1 机械设备的数据存储要求

10.1.1 机械设备的参数安全配置要求

本项要求包括：

a) 网络管控的机械设备的身份标识和密钥等配置参数，应由网络管理平台进行配置和管理；
b) 网络管控平台应能够对其管控的机械设备的配置参数进行修改，安全参数修改过程应在数据安全保护下进行；
c) 网络管控平台应掌握其管控的全部机械设备的关键配置参数，包括身份标识和共享密钥。

10.1.2 机械设备的业务数据存储要求

本项要求包括：

a) 网络管控的机械设备应能存储最长时间无网络连接期间所采集的数据；

b) 网络管控的机械设备应能存储最长时间连续开机状态下所采集的数据；
c) 长时间处在无网络环境下工作的机械设备，应能将设备采集的数据通过网络端口存储到外部存储设备。

10.2 网络管控平台的数据管理要求

10.2.1 机械设备的参数管理要求

网络管控平台应对其管控的全部机械设备建立数据库，记录设备的关键配置参数，包括身份标识和共享密钥。

10.2.2 机械设备使用者的账号管理要求

网络管控平台应给使用其管控机械设备的用户提供账号服务，使用户及时掌握自己所使用的设备情况。

11 网络管控平台建设技术要求

11.1 平台建设要求

11.1.1 硬件要求

本项要求包括：
a) 机械设备网络管控平台的硬件设备应安全可靠；
b) 机械设备网络管控平台应允许使用来自不同生产厂商的硬件设备。

11.1.2 软件要求

本项要求包括：
a) 机械设备网络管控平台的应用软件应安全可靠，并经过有资质的第三方测试评估；
b) 机械设备网络管控平台的应用软件应能在不间断服务的情况下进行更新。

11.2 平台功能要求

11.2.1 网络管控平台的数据处理能力

本项要求包括：
a) 网络管控平台应能存储和处理不同类型的数据；
b) 网络管控平台应能判断数据的属性；
c) 网络管控平台应能判断数据是否异常。

11.2.2 网络管控平台的账号管理能力

本项要求包括：
a) 网络管控平台应能管理不同的账号，包括管理员账号、监督员账号；
b) 网络管控平台应能对不同账号赋予不同的数据访问权限。

12 网络管控平台安全要求

12.1 网络管控平台的网络安全保护能力

12.1.1 网络管控平台抵抗网络攻击能力要求

本项要求包括：
a) 网络管控平台应具有一定抵抗 DDoS 网络攻击的能力；
b) 网络管控平台应具有一定抵抗非法入侵的能力；
c) 网络管控平台应具有一定检测非法入侵的能力。

12.1.2 网络管控平台系统恢复能力要求

本项要求包括：

a) 网络管控平台应能在遭受网络攻击后，具有快速系统恢复能力，使其恢复到遭受网络攻击前的最后状态；
b) 网络管控平台应能在恢复系统正常工作状态后，应能选择使用不同时段备份的数据。

12.2 网络管控平台的数据安全保护要求

12.2.1 数据容灾备份要求

本项要求包括：

a) 机械设备网络管控平台的数据应实施多级备份机制，包括本地备份和异地或网络备份；
b) 机械设备网络管控平台的数据应能根据需要被重新装入系统。

12.2.2 数据恢复要求

本项要求包括：

a) 当数据遭到破坏或有错误时，系统管理员应能将平台数据恢复到最近一次备份的数据；
b) 如果恢复数据时指定某个特定时刻 t，则将系统恢复到时刻 t 之前最后一次备份的数据。

13 网络管控平台运维要求

13.1 网络管控平台的运维要求

13.1.1 网络管控平台的网络连接能力

本项要求包括：

a) 网络管控平台应能通过多种网络端口进行网络连接，包括有线连接、无线连接、物理连接；
b) 网络管控平台应能识别与其连接的设备和用户；
c) 网络管控平台应能鉴别与其连接的设备或用户身份，避免伪造和假冒；
d) 网络管控平台应能鉴别数据来源的合法性。

13.1.2 网络管控平台的可扩展性

本项要求包括：

a) 网络管控平台应具有可扩展性，包括存储空间可扩展、计算能力可扩展、服务内容可扩展；
b) 网络管控平台在进行功能和性能扩展时，应能持续提供现有服务，使已有的服务不受本质性影响。

13.1.3 网络管控平台的可迁移性

本项要求包括：

a) 网络管控平台应能进行数据迁移，迁移过程对用户的服务不造成严重影响；
b) 网络管控平台应能进行部分数据迁移，迁移过程对用户的服务不造成严重影响，迁移后仍能提供对剩余数据对应的设备和用户提供服务。

13.2 网络管控平台服务要求

13.2.1 网络管控平台的数据共享

本项要求包括：

a) 根据行业要求和管理要求，网络管控平台应能与其他数据平台进行数据共享；
b) 根据行业要求和管理要求，网络管控平台应能选择部分数据与其他数据平台共享；
c) 根据行业要求和管理要求，网络管控平台应能选择将其数据的部分访问权限分析给其他数据平台。

14 网络管控平台安全管理要求

14.1 网络管控平台环境和人员管理

本项要求包括：

a) 网络管控平台的物理环境应具有防火、防水、防盗功能；
b) 网络管控平台的物理环境应具有门禁系统或专职人员出入管理，避免非授权人员随意出入；
c) 网络管控平台的管理应安排专职人员。

14.2 网络管控平台账号安全管理

本项要求包括：

a) 网络管控平台的用户账号应使用口令密码或密码设备保护；
b) 网络管控平台用户账号的口令密码应包括至少 2 种类型的符号，长度为 8-16 个字符；；
c) 网络管控平台管理员账号的口令密码应包括至少 3 种类型的符号，长度为 8-16 个字符，且在 6 个月内更换；
d) 网络管控平台用户账号的口令密码在更新时，应避免与当前和之前用过的旧口令密码有超过50%的重复字段；
e) 如果网络管控平台管理员账号的口令密码超期未更新，每次登录后，系统提醒更新密码，并不断延长登录时长；
f) 网络管控平台的不同管理员使用不同的账号，同一管理员账号不允许多人使用。

14.3 网络管控平台的监管要求

本项要求包括：

a) 网络管控平台应能为行业主管机构提供所要求的数据；
b) 网络管控平台应能自动选取并转发给主管机构所要求的数据；
c) 网络管控平台在给主管机构转发数据时，应保护关键数据或数据关键字段的安全性。