ICS 53.1
CCS P 97

T/SDZBZZ

团　　体　　标　　准

T/SDZBZZ 001—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

2023－10－26 发布　　2023－11－26 实施

山东省装备制造业协会　　发 布

目　　次

前言 III
引言 IV
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　工程机械设备网络管控系统的组成 1
5　设备身份和操作人员身份管理要求 2
5.1　网络管控的工程机械设备身份管理要求 2
5.2　网络管控的工程机械设备操作人员身份管理要求 2
6　设备定位信息采集要求 2
6.1　网络管控的工程机械设备定位模块要求 2
6.2　网络管控的工程机械设备定位信息采集要求 2
6.3　网络管控的工程机械设备运动轨迹数据采集要求 3
7　设备状态信息采集要求 3
7.1　网络管控的工程机械设备停机状态信息采集要求 3
7.2　网络管控的工程机械设备工作状态信息采集要求 3
8　数据传输要求 4
8.1　网络管控的工程机械设备的网络配置要求 4
8.2　网络管控的工程机械设备的数据传输频次要求 4
9　设备的网络控制要求 5
9.1　网络管控的工程机械设备输出功率限制要求 5
9.2　网络管控的工程机械设备在无网络连接情况下的控制要求 5
10　数据管理要求 5
10.1　网络管控的工程机械设备的数据存储要求 5
10.2　网络管控平台的数据管理要求 6
11　网络管控平台建设技术要求 6
11.1　网络管控平台建设要求 6
11.2　网络管控平台功能要求 6
12　网络管控平台安全要求 6
12.1　网络管控平台的网络安全保护能力 6
12.2　网络管控平台的数据安全保护要求 7
13　网络管控平台运维要求 7
13.1　网络管控平台的网络连接能力要求 7
13.2　网络管控平台的可扩展性要求 7
13.3　网络管控平台的可迁移性要求 7

14　网络管控平台安全管理要求 7
14.1　网络管控平台环境和人员管理要求 7
14.2　网络管控平台账号安全管理要求 7
14.3　网络管控平台的监管要求 8
14.4　网络管控平台的数据共享要求 8

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。

本文件的某些内容可能涉及专利。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、郭锋、蒋本帅、张树霞、荆长强、张问银、赵斌、刘鸣涛、张鑫、杜茜、王星、朱孔伟、陈超伟、曹仲明、谢凡卿、赵玉伟、宋晓颖、王庆国、赵胜建。

引　言

工程机械设备一般指服务于工程建设的机械设备，具有成本高、自身重、专业性强等特点，常用于具有定点施工，如钩机，铲车，推土机，平地机、混料机，桩机，摊铺机等。使用工程机械设备的用户常通过租赁方式，或分期付款方式购买。因此，出租方或出售方在所有权没有完全转移之前，需要有能力对设备进行网络管控，防止用户恶意拖欠钱款。

越来越多的工程机械设备具有网络管控功能。网络管控的主要目的是防止设备被非法使用。例如租赁设备使用过程中租户在恶意拖欠费用的情况下仍能继续使用设备。有些特殊设备则需要网络严格监控下运行，特别是一些自动运行或网络控制操作的设备，更需要严格的网络管控。

针对那些具有网络管控能力的工程机械设备，本文件规范了对这类设备进行网络管控的一些技术要求，提升网络环境下管控这类设备的数据安全性和控制安全性，确保设备所有人对设备的掌控权和对设备管控的可靠性。

本文件参与团队的分工大致如下：临沂大学团队主要负责标准的框架和信息安全技术相关条款的制定；山东润通科技有限公司团队主要负责标准体系在实际应用中可能遇到的问题；山东临工工程机械有限公司团队主要从当前机械设备的信息化程度分析设备能否实现标准条款对信息化要求；临沂市中信信息技术有限公司团队主要分析网络管控平台数据安全问题；临沂智慧大数据研究院团队主要研究标准在其他行业的应用。

工程机械设备网络管控安全要求

1 范围

本文件规定了通过网络管控的工程机械设备满足的规范性安全要求，包括设备定位信息采集要求、设备运动轨迹数据采集要求、数据传输要求、设备身份鉴别要求、设备操作人员资质要求、设备功率输出限制要求、设备操作人员授权要求、数据存储要求、平台安全管理要求等。

本文件适用于工程机械设备的生产行业、运营行业和终端用户。

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

3 术语和定义

GB/T 25069-2020界定的术语和定义适用于本文件。

4 工程机械设备网络管控系统的组成

工程机械设备网络管控系统包括工程机械设备、控制终端T-box、网络管控平台，其中工程机械设备一般由人工操作，而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；控制终端是安装在工程机械设备上的一个信息处理系统，具有数据处理和网络连接功能，与网络管控平台进行数据交换；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。工程机械设备网络管控系统的组成如图1所示（为叙述方便，本文件中在重复描述工程机械设备时，简称其为设备）：

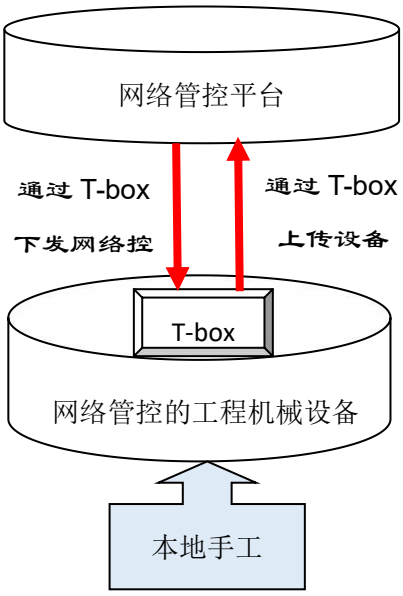

图 1 网络管控的工程机械设备网络管控系统架构示意图

5 设备身份和操作人员身份管理要求

5.1 网络管控的工程机械设备身份管理要求

5.1.1 设备身份标识要求

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

5.1.2 设备身份鉴别要求

本项要求包括：
——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；
——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。

5.2 网络管控的工程机械设备操作人员身份管理要求

5.2.1 设备操作人员授权要求

本项要求包括：
——设备应由具有设备操控资质的人员进行操作；
——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；

5.2.2 设备操作人员身份标识鉴别要求

本项要求包括：
——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；
——关键设备操作人员的身份标识，应通过网络管控平台的身份鉴别，才能启动设备。

6 设备定位信息采集要求

6.1 网络管控的工程机械设备定位模块要求

6.1.1 设备定位模块配置要求

本项要求包括：
——安装规范厂商生产的北斗导航定位模块；
——安装规范厂商生产的 GPS 定位模块；

6.1.2 设备定位模块精度要求

本项要求包括：
——定位模块的位置数据精度应精确到 10m 以内；
——定位模块的位置数据应能正确对应到电子地图上的位置。

6.1.3 设备定位模块安装要求

本项要求包括：
——安装应具有抗震、抗拆卸功能；
——工作状态应进行野外测试，确保能正常采集定位信息。

6.2 网络管控的工程机械设备定位信息采集要求

6.2.1 设备开机关机位置采集要求

本项要求包括：
——设备在开机时，应采集设备的位置信息并发送到网络管控平台；

——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；
——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。

6.2.2 设备持续位置采集要求

本项要求包括：
——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，两次上传信息的时间间隔不能大于 60min；
——在网络连接不正常的情况下，设备应提前获取授权，并在授权终止前通过网络连接上传设备的位置信息。

6.3 网络管控的工程机械设备运动轨迹数据采集要求

6.3.1 设备移动时位置信息的采集要求

本项要求包括：
——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 1000m；
——如果设备发送位置信息时没有网络连接，则应频繁尝试网络连接，一旦连接成功，在第一时间启动位置信息的获取和发送任务。

6.3.2 设备长时间不启动时位置信息的采集要求

本项要求包括：
——设备持续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；
——设备持续处于静止且不启动状态，两次上传位置信息的时间间隔不大于 60min；
——设备持续处于静止且不启动状态，若两次上传位置信息相同，则只上传最远一次同样位置的时间信息，并标注位置不变。

7 设备状态信息采集要求

7.1 网络管控的工程机械设备停机状态信息采集要求

7.1.1 设备转为停机状态时的信息采集和传输要求

本项要求设备在从运转状态变为停机状态时，应上传停机时间和位置信息；

7.1.2 设备停机状态下的信息采集和传输要求

本项要求包括：
——停机状态的设备应在上传上传位置信息后不大于 60min 内，重新采集并上传位置信息；
——如果位置信息与上次上传时相同，可以简单说明位置与某个时刻的位置未发生变化；
——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。

7.2 网络管控的工程机械设备工作状态信息采集要求

7.2.1 设备转为开机时的状态信息更新要求

设备由关机变为开机状态时，应上传开机时间和位置信息；

7.2.2 设备工作状态的信息采集和传输要求

本项要求包括：
——设备应定时采集并上传当前的工作状态，包括功率输出百分比；
——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；

7.2.3 设备异常状态信息的处理要求

本项要求包括：

——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；

——当设备电池容量低于 10%时应报警，并在 1min 后仍然低于 10%时，将此报警信息上传到网络管控平台；

——网络管控平台若发现设备上传的数据疑似异常，则向设备发送报警信息；如果上传异常数据状态维持 10min 以上，或在 20min 内异常数据占比超过上传数据总量的 50%，或在 30min 内异常数据占比超过上传数据总量的 30%，应首先给设备发送升级的报警信息，然后控制设备逐渐停机。

8 数据传输要求

8.1 网络管控的工程机械设备的网络配置要求

8.1.1 设备的数据传输模块配置要求

本项要求包括：

——设备应配置移动通信模块，并保持通信模块可用；

——重要设备应配置至少两种通信方式，以主备模式进行切换，确保较高的通信成功率；

——如果设备的操作需要通过网络控制来实现，则应配置至少两种独立通信模块。

8.1.2 设备的数据传输安全配置要求

本项要求包括：

——设备应与网络管控平台预置某个共享密钥；

——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。

8.2 网络管控的工程机械设备的数据传输频次要求

8.2.1 设备在正常网络配置下数据传输频次要求

本项要求包括：

——设备在非工作状态下，应至少间隔 60min 上报一次当前的位置信息；

——设备在工作状态下，应至少间隔 10min 上报一次当前的设备工作状态和位置信息。

8.2.2 设备在网络连接失败时的异常处理要求

本项要求包括：

——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；

——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。

8.2.3 设备辅助网络传输配置要求

本项要求包括：

——处在没有网络信号环境工作的设备，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；

——重要设备应配置至少两种通信方式，确保较高的通信成功率。

8.2.4 设备在辅助网络传输配置下数据传输频次要求

本项要求包括：

——处在没有网络信号环境工作的设备，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；

——处在没有网络信号环境工作的设备，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。

9 设备的网络控制要求

9.1 网络管控的工程机械设备输出功率限制要求

9.1.1 设备输出功率限制要求

本项要求包括：

——网络管控平台应能够对其管控的设备通过网络指令限制其功率输出百分比，使得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比；

——网络管控平台应能通过网络随时取消或修改对其管控的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：

——网络管控平台应能够对其管控的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；

——网络管控平台应能通过网络随时取消或修改对其管控的设备的功率输出限制。

9.2 网络管控的工程机械设备在无网络连接情况下的控制要求

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：

——网络管控平台应能够对其管控的设备通过网络指令使其在时间 T 内无须连接网络；

——设备在无网络环境下，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；

——设备在无网络环境下，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：

——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，移动设备再与工程机械设备进行近距离网络连接，将授权转发到工程机械设备；

——代理授权的移动设备应与工程机械设备有标准通信接口；

——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 网络管控的工程机械设备的数据存储要求

10.1.1 设备的参数安全配置要求

本项要求包括：

——设备的身份标识和密钥等配置参数，应由网络管控平台进行配置和管理；

——网络管控平台应能够对其管控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；

——网络管控平台应掌握其管控的全部设备的关键配置参数，包括身份标识和共享密钥。

10.1.2 设备的业务数据存储要求

本项要求包括：

——设备应能存储最长时间无网络连接期间所采集的数据；
——设备应能存储最长时间连续开机状态下所采集的数据；
——长时间处在无网络环境下工作的设备，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 网络管控的工程机械设备参数管理要求

网络管控平台应对其管控的全部设备建立数据库，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 网络管控的工程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 网络管控平台建设要求

11.1.1 硬件要求

本项要求包括：
——设备网络管控平台的硬件设备应安全可靠；
——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：
——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；
——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 网络管控平台功能要求

11.2.1 网络管控平台的数据处理能力要求

本项要求包括：
——网络管控平台应能存储和处理不同类型的数据；
——网络管控平台应能判断数据的属性；
——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要求

本项要求包括：
——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；
——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：
——网络管控平台具有抵抗 DDoS 网络攻击的能力；
——网络管控平台具有抵抗非法入侵的能力；
——网络管控平台具有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：

——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；

——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：

——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；

——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：

——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；

——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。

12.2.3 安全等级保护要求

网络管控平台应满足国家安全等级保护标准的第3级或以上要求。

13 网络管控平台运维要求

13.1 网络管控平台的网络连接能力要求

本项要求包括：

——网络管控平台应能通过多种端口进行网络连接，包括有线连接、无线连接、物理连接；

——网络管控平台应能识别与其连接的设备和用户；

——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；

——网络管控平台应能鉴别数据来源的合法性。

13.2 网络管控平台的可扩展性要求

本项要求包括：

——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；

——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。

13.3 网络管控平台的可迁移性要求

本项要求包括：

——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；

——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。

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要求

本项要求包括：

——网络管控平台的物理环境应具有防火、防水、防盗功能；

——网络管控平台的物理环境应有门禁系统或专职人员出入管理，避免非授权人员出入；

——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要求

本项要求包括：

——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；

——网络管控平台用户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；

——网络管控平台管理员账号的口令密码应包括至少 4 种类型的符号，长度为 8-16 个字符，且在 6 个月内更换；

——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；

——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；

——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：

——网络管控平台应能为行业主管机构提供所要求的数据，或允许行业主管机构在其权限范围内访问平台的数据；

——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；

——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。

14.4 网络管控平台的数据共享要求

本项要求包括：

——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；

——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；

——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。