ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

高端智能装备远程运维数据加密传输规范 工业互联网应用

Specifications for Encrypted Data Transmission in Remote Operation and Maintenance of High-end Intelligent Equipment – Industrial Internet Application

（工作组讨论稿）

（本草案完成时间：2026-01-29）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据GB/T 1.1-2020《标准化工作导第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。
本文件由广西产学研科学研究院提出。
本文件由广西电子商务企业联合会归口。
本文件起草单位：
本文件主要起草人：
本文件为首次发布。

高端智能装备远程运维数据加密传输规范工业互联网应用

1 引言

随着工业互联网深度发展，高端智能装备远程运维已成为保障工业生产连续、提升设备管理水平的核心手段。其传输的设备状态、控制指令等敏感数据，直接关系工业控制系统与信息安全。为落实国家网络安全、数据安全及密码管理相关法律法规，规范加密传输行为，构建安全可控的传输体系，特制定本规范。结合我国工业互联网安全相关法规与标准，聚焦远程运维核心安全风险，明确数据加密传输的技术与管理要求，为相关主体开展系统设计、部署等工作提供技术遵循，也为监管工作奠定基础。

2 范围

本规范明确了高端智能装备在工业互联网环境下开展远程运维数据加密传输的总体安全目标、加密技术选型、传输协议标准、密钥全生命周期管理、身份认证与访问控制机制、安全审计与实时监测及系统整体安全防护等核心内容与技术要求。适用于全国范围内高端智能装备制造企业、远程运维服务商、工业互联网平台运营商、网络安全服务商等相关单位，在远程运维系统的设计、开发、测试、部署、运行、升级及评估等全流程中的数据加密传输工作；同时适用于各级工业和信息化、网络安全监管等部门开展高端智能装备远程运维数据传输安全的监督管理、合规检查与专项评估工作。

3 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，仅所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（包括所有修改单）适用于本文件。

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

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

GB/T 32918-2016 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 37033.1-2018 信息安全技术工业控制系统安全第 1 部分：评估规范

GB/T 39276-2020 信息安全技术网络产品和服务安全通用要求

GB/T 39786-2021 信息安全技术信息系统密码应用基本要求

GM/T 0024-2014 SSL VPN 技术规范

GM/T 0034-2014 基于 SM2 密码算法的证书认证系统密码协议规范

YD/T 3706-2020 工业互联网平台安全防护要求

《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）

《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）

《中华人民共和国密码法》（中华人民共和国主席令第三十五号）

《关键信息基础设施安全保护条例》（国务院令第 745 号）

4 术语和定义

下列术语和定义适用于本文件。

4.1 高端智能装备

面向航空航天、能源电力、智能制造、轨道交通、高端装备制造等国家重点产业领域，集成先进传感、精准控制、智能决策与高效执行功能，具备自感知、自诊断、自适应、自执行、自优化等核心能力，支撑工业生产高效协同与智能化升级的关键工业装备。

4.2 远程运维

通过工业互联网专用网络通道，对远端部署的高端智能装备开展状态监测、故障诊断、预测性维护、程序升级、参数配置、应急处置等全流程技术支持与运维服务的活动，是工业互联网服务化延伸的核心应用场景。

4.3 运维数据

远程运维全流程中产生、传输、处理的各类数据，包括但不限于设备运行状态数据、核心工艺参数、故障告警信息、控制指令、固件升级文件、运维日志记录、人员操作信息等，其中涉及国家核心工业秘密、关键生产数据的内容纳入国家重要数据管理范畴。

4.4 加密传输

采用国家密码管理部门核准的密码算法与技术，对传输过程中的运维数据进行加密处理、完整性校

验与身份认证，确保数据在传输环节具备机密性、完整性、可用性与可认证性，防范数据窃取、篡改、伪造等安全风险的通信方式。

5 总体要求

5.1 安全目标

高端智能装备远程运维数据加密传输工作应围绕国家工业安全保障需求，实现以下核心安全目标：

5.1.1 机密性：确保传输过程中的运维数据（尤其是核心控制指令、敏感工艺参数等）不被未经授权的主体窃取、监听或泄露，保障国家工业核心信息安全；

5.1.2 完整性：防止运维数据在传输过程中被非法篡改、插入或删除，确保数据传输前后的一致性与真实性；

5.1.3 可用性：保障远程运维数据传输通道的稳定可靠，在极端场景下具备应急传输能力，支撑工业生产连续运行；

5.1.4 可认证性：实现通信双方（装备终端、运维平台、运维人员）的身份真实核验，防范假冒终端、假冒平台等恶意接入风险；

5.1.5 可追溯性：确保所有数据传输行为、密钥操作、身份认证等活动可审计、可追溯，为安全事件处置与责任认定提供支撑。

5.2 安全等级

依据《网络安全等级保护条例》及运维数据敏感程度、影响范围，结合工业控制系统安全防护要求，将高端智能装备远程运维数据加密传输安全等级划分为三级，实行分级防护、精准管控：

5.2.1 等级一（一般防护）：适用于非敏感运维数据（如公开设备型号信息、非核心运行状态数据等），应采用传输层加密机制，满足基本安全防护要求；

5.2.2 等级二（强化防护）：适用于重要运维数据（如一般工艺参数、设备故障信息、非核心操作指令等），应采用应用层加密或传输层+应用层双重加密机制，提升安全防护强度；

5.2.3 等级三（严格防护）：适用于核心运维数据与控制指令（如关键工艺参数、紧急停机指令、核心固件升级文件等），应采用端到端强加密、完整性校验与身份双向认证相结合的防护机制，落实最高级别安全管控要求。

5.3 合规性要求

远程运维数据加密传输系统的设计、建设、运行与管理，必须严格遵守《中华人民共和国网络安全

法》《中华人民共和国数据安全法》《中华人民共和国密码法》等国家法律法规，严格落实网络安全等级保护制度、关键信息基础设施安全保护制度与密码应用安全性评估制度；优先采用国家密码管理部门核准的 SM2、SM3、SM4 等国密算法，严禁使用未经核准的密码算法及境外密码产品，确保密码应用自主可控、安全合规。

6 加密技术与协议要求

6.1 密码算法选用

密码算法选用应遵循国家密码管理部门相关规定，满足密码应用安全性评估要求，确保算法合规、安全、可控：

6.1.1 对称加密算法：必须使用国家密码管理局核准的 SM4 分组密码算法，密钥长度不得小于 128 位，主要用于大批量运维数据（如设备状态数据、日志文件等）的加密传输，支持高效加密与解密运算，适配工业互联网实时传输需求。

6.1.2 非对称加密算法：必须使用国家密码管理局核准的 SM2 椭圆曲线公钥密码算法，主要用于密钥交换、数字签名与身份认证场景，支持密钥安全协商与通信双方身份核验，防范密钥泄露与假冒接入风险。

6.1.3 杂凑算法：必须使用国家密码管理局核准的 SM3 密码杂凑算法，哈希值长度为 256 位，主要用于运维数据完整性校验、数字签名生成与验证，确保数据在传输过程中未被非法篡改。

5.2 传输层加密协议

6.2.1 TLS/SSL 协议：传输层加密必须采用 TLS 1.2 及以上版本协议，严禁使用 SSLv2、SSLv3 等不安全协议版本及弱密码套件；密码套件应优先选用支持国密算法的组合，包括但不限于：TLS_SM4_GCM_SM3 TLS_ECDHE_SM2_WITH_SM4_SM3 所有加密会话应支持完美前向保密（PFS）机制，确保单个会话密钥泄露不影响其他会话数据安全。

6.2.2 证书要求：服务器与客户端数字证书必须由国家认可的合法电子认证服务机构（CA）签发，优先采用支持 SM2 算法的国密数字证书；证书应包含主体身份信息、公钥信息、有效期等核心字段，有效期不得超过 2 年；证书吊销列表（CRL）应实时更新，确保失效证书及时注销，防范证书冒用风险。

6.3 应用层加密协议

对于等级二、等级三的运维数据，必须在应用层额外实现加密防护，构建“传输层+应用层”双重加密体系；应用层加密应采用 GM/T 0034-2014 等国家密码行业标准定义的协议，实现端到端加密传输，

确保数据从源头加密到终端解密的全流程安全，不受传输链路中间节点影响。

6.4 数据封装格式

加密后的运维数据必须采用统一的标准化封装格式，确保不同厂商、不同类型的高端智能装备与运维平台之间的互联互通与安全兼容；封装格式应包含以下核心字段：版本号、加密算法标识、密钥标识、初始化向量（如算法需要）、密文数据、完整性校验值（SM3 哈希结果）、时间戳，封装后的数据应支持完整性自检与异常告警功能。

7 密钥管理要求

密钥管理应遵循“统一规划、分级负责、全生命周期管控”的原则，落实国家密码管理部门相关规定，确保密钥生成、存储、分发、使用、更新、归档与销毁全流程安全可控，严禁密钥明文传输与存储。

7.1 密钥生命周期管理

建立规范化的密钥生命周期管理机制，明确各环节责任主体与操作流程，实现密钥全生命周期的可追溯、可审计；密钥生命周期应覆盖生成、存储、分发、使用、更新、归档、销毁七个核心环节，每个环节均需落实安全防护措施与操作记录要求。

7.2 密钥生成

密钥必须在符合国家安全标准的安全环境（如密码机、硬件安全模块 HSM 等）中生成，随机数生成应符合 GM/T 0005《随机性检测规范》要求，确保密钥的随机性与唯一性；严禁在非安全环境中生成密钥，严禁使用固定密钥或弱随机性密钥。

7.3 密钥存储

密钥禁止明文存储，应采用加密存储、硬件隔离存储等方式进行保护，优先使用硬件安全模块（HSM）、可信执行环境（TEE）等专用设备存储核心密钥；密钥存储设备应符合国家密码管理部门相关认证要求，严禁将密钥存储在未加密的终端设备或网络服务器中。

7.4 密钥分发

密钥分发必须通过安全通道进行，优先采用基于 SM2 算法的密钥协商协议或数字信封机制实现密钥安全分发；分发过程中应进行身份认证与完整性校验，确保密钥仅被授权主体获取，严禁通过公共网络或非安全通道分发密钥。

7.5 密钥更新

建立密钥定期更新机制，严格控制密钥使用周期：对称加密密钥更新周期不得超过 90 天；数字证

书密钥对更新周期不得超过 2 年；当发生密钥泄露、设备丢失、人员离职等情况时，应立即启动应急更新流程，吊销旧密钥并生成新密钥，同时通知所有关联授权主体。

7.6 密钥归档与销毁

过期密钥应按照国家档案管理相关规定进行安全归档，归档期限不得少于数据保存期限，归档过程中应确保密钥完整性与保密性；废弃密钥应采用物理销毁或逻辑销毁（如多次覆写、粉碎性删除）的方式彻底销毁，确保无法被恢复，销毁过程应记录备案并可追溯。

8 身份认证与访问控制

身份认证与访问控制是远程运维数据加密传输安全的核心防护环节，应遵循“身份唯一、双向认证、分级授权、最小权限”的原则，构建设备、人员、平台三位一体的身份认证与访问控制体系。

8.1 设备身份认证

每台高端智能装备终端、运维平台节点均应具备唯一的设备身份标识，配备合法有效的国密数字证书；在建立远程运维通信连接前，必须进行设备双向认证（终端与平台相互认证），未通过认证的设备严禁接入远程运维网络；设备身份标识应纳入国家工业设备身份认证统一管理体系，实现设备身份的可追溯。

8.2 用户身份认证

远程运维人员应进行强身份认证，采用“用户名/密码+动态令牌”“数字证书”“生物识别”等两种及以上认证方式相结合的强认证机制；严禁使用弱密码或单一认证方式；运维人员身份信息应与岗位职责严格绑定，离职、调岗时应立即注销或调整其认证权限，防范身份冒用风险。

8.3 访问控制

建立基于角色的访问控制（RBAC）机制，结合数据敏感等级与运维岗位职责，对不同用户、不同设备的访问权限进行精细化划分与管控；明确各角色的权限边界，实现“谁授权、谁负责，谁操作、谁追溯”；严禁超权限访问运维数据，尤其是核心控制指令与敏感工艺参数。

9 安全审计与监测

建立全覆盖、全天候的安全审计与实时监测体系，及时发现、预警并处置远程运维数据加密传输过程中的安全风险与异常行为，为安全事件追溯与应急处置提供支撑，落实国家网络安全监测预警相关要求。

9.1 审计内容

安全审计应覆盖远程运维数据加密传输全流程，重点记录以下事件并留存完整日志：

9.1.1 身份认证事件：包括设备认证、用户认证的成功与失败记录（含认证主体、时间、地点、方式等信息）；

9.1.2 加密会话事件：包括加密会话的建立、终止、协议版本、密码套件选用等信息；

9.1.3 密钥管理事件：包括密钥生成、存储、分发、使用、更新、归档、销毁等全流程操作记录；

9.1.4 数据传输事件：包括运维数据的传输方向、传输量、加密算法、完整性校验结果等异常信息；

9.1.5 权限变更事件：包括用户权限、设备接入权限、策略配置等变更操作记录。

9.2 日志保护

审计日志应进行完整性保护与加密存储，采用 SM3 算法进行日志哈希校验，防止日志被篡改、伪造或非法删除；日志保存时间不得少于 6 个月，涉及核心控制指令、重要敏感数据的审计日志保存时间不得少于 1 年；日志数据应支持按事件类型、时间范围等条件快速查询，为安全事件追溯提供支撑。

9.3 实时监测

建立远程运维数据加密传输实时监测机制，部署专用监测设备与系统，对加密连接状态、协议版本合规性、密码套件选用、密钥使用周期、数据传输异常等情况进行 24 小时不间断监测；对异常加密连接、密钥重复使用、协议版本降级、数据篡改尝试等风险行为及时发出告警，并自动触发应急处置流程；监测数据应定期上报至国家工业互联网安全态势感知平台，支撑全国范围内的安全风险统筹研判。

10 系统安全要求

高端智能装备远程运维数据加密传输系统的整体安全防护，应落实“终端加固、网络隔离、平台防护、全流程管控”的原则，结合网络安全等级保护三级及以上要求，构建纵深防御体系，确保终端、网络、平台各环节安全可控。

10.1 终端安全

高端智能装备终端应具备安全启动、固件完整性校验、安全存储、恶意代码防护等核心安全功能；终端固件应采用加密方式存储与升级，升级过程中进行身份认证与完整性校验，防范固件被篡改或植入恶意代码；终端应禁用不必要的端口与服务，定期进行安全漏洞扫描与修复，确保终端自身安全；终端安全功能应符合 GB/T 37033.1-2018《信息安全技术工业控制系统安全第 1 部分：评估规范》要求。

10.2 通信网络安全

远程运维通信通道应与企业生产控制网络、公共互联网严格隔离，采用工业防火墙、网闸、入侵防御系统（IPS）等专用安全设备构建网络边界防护体系；优先使用工业专用网络（如工业以太网、5G 工业专网等）传输运维数据，严禁通过公共互联网传输核心控制指令与敏感运维数据；网络设备应进行安全配置，禁用弱密码、关闭不必要的服务，定期进行安全审计与漏洞修复，确保通信网络传输安全。

10.3 平台安全

工业互联网运维平台应严格满足 YD/T 3706-2020《工业互联网平台安全防护要求》，具备漏洞管理、入侵防范、恶意代码防护、数据安全防护等核心安全能力；平台应采用分布式架构与冗余备份机制，确保服务连续可用；平台数据存储应采用加密存储方式，对敏感数据进行分类分级管理；平台应定期开展安全测评与密码应用安全性评估，及时整改安全隐患，确保平台整体安全合规，支撑远程运维数据加密传输全流程安全管控。

11 附则

本标准由广西电子商务企业联合会负责解释。本标准自发布之日起试行，试行期为一年。试行期满后，根据实施反馈情况进行修订和完善。各相关单位可依据本标准制定具体的实施细则。若本标准与国家新颁布的法律法规或强制性标准有不一致之处，应以国家法律法规和强制性标准为准。本标准所引用的规范性引用文件如有更新，其最新版本适用于本标准。广西电子商务企业联合会将根据技术发展和应用需求，适时组织对本标准的复审与修订工作，以保障其持续的先进性和适用性。本标准的有效实施，有赖于各级医疗机构、主管部门、技术服务商和各相关方的共同努力，通过规范智慧医院数据互联互通共享技术，推动医疗健康数据资源有效整合与安全共享，提升医疗服务质量和效率，促进智慧医院建设规范化发展，为推进健康中国建设提供技术支撑。