中关村工业互联网产业联盟
团体标准

Zhongguancun industrial Internet Industry Alliance
Group standard

工业互联网数据安全传输技术要求

Security Technical Requirements for Data Transmission in the Industrial Internet

2022-11-01 发布　　2022-12-01 实施

中关村工业互联网产业联盟　　发布

目　次

前　言

本标准分为3个部分：

——术语与定义

——工业互联网中安全防护范围

——工业互联网数据安全传输技术要求

本标准起草单位：中国科学院信息工程研究所，神州数码系统集成服务有限公司，哈尔滨工业大学，索为技术股份有限公司，北京水木羽林科技有限公司

本标准主要起草人：王梓晗，操江峰，李沛南，赵路坦，李扬，张鼎，陈杉杉，王晨程，王宏志，丁小欧，刘锋，李远翼，孙锐

本标准为首次发布。

引　言

本标准描述了用于工业互联网的数据传输安全，下列文件对于本文件的应用是必不可少的。

GB/T3819-2020　工业互联网 数据采集结构化描述规范

GB/T37025-2018 信息安全技术 物联网数据传输安全技术要求

GB/T39786-2021 信息安全技术信息系统密码应用基本要求

工业互联网数据传输安全技术要求

1 术语与定义

1.1 定义

工业互联网（Industrial Internet of Things）
物联网在工业领域中的应用，其通过工业资源的网络互连、数据互通和系统互操作，实现制造原料的灵活配置、制造过程的按需执行、制造工艺的合理优化和制造环境的快速适应，达到资源的高效利用，从而构建服务驱动型的新工业生态体系，具有智能感知、泛在互联、精准控制、数字建模、 实时分析、迭代优化等特征。
[GB/T3819-2020]

传感器（Transducer/Sensor）：
能感受被测量并按照一定的规律转换成可用输出信号的器，或装置，通常由敏感元件和转换元件组成。
[GB/T7665-2005，定义 3.1.1]

感知设备（Sensing Device）：
能够获取对象信息的设备，并提供接入网络的能力。
[GB/T33745-2017，定义 2.1.9]
注：具备较高计算能力的感知设备还能对物或环境进行信息采集和/或执行操作。

传输安全（Transmission Security）：
保护网络中所传输信息的完整性、保密性、可用性及用户定制等特性。

隐私（Privacy）：
个人所具有的控制或影响与之相关信息的权限，涉及由谁收集和存储、由谁披露。
[GB/T25069-2010，定义 2.1.63]

敏感信息（Sensitive Information）：
一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。
[GB/T35273-2017，定义 3.2]

信任（Trust）：
两个元素之间的一种关系：元素 x 信任元素 y，当且仅当 x 确信 y 相对于一组活动，元素 y 将以良好定义的方式实施，且不违反安全策略。

[GB/T25069-2010，定义 2.1.51]

1.2 术语

IOT 物联网（Internet of Things）

ICS 工业控制系统（Industrial Control System)

DCS 分布式控制系统（Distributed Control System）

FCS 现场总线控制系统（Field bus Control System）

FTP 文件传输协议（File Transfer Protocol）

HTTP 超文本传输协议（Hyper Text Transport Protocol）

MQTT 消息队列遥感传输（Message Queuing Telemetry Transport）

PLC 可编程逻辑控制器（Programmable Logic Controller）

SCADA 数据采集与监视控制（Supervisory Control And Data Acquisition）

CAD 管理软件计算机辅助设计（Management Software Computer Aided Design）

MES 制造企业生产过程执行系统(Manufacturing Execution System)

SSL（Secure Sockets Layer）安全套接层。它是位于 HTTP 等各种应用层协议之下，TCP/IP 层之上的一个协议，为数据通信提高安全支持。主要任务是提供私密性，数据完整性和身份认证。

TLS（Transport Layer Security）安全传输层协议。用于在两个通信应用程序之间提供保密性和数据完整性。

2 工业互联网

2.1 工业互联网系统架构

工业互联网不是互联网在工业的简单应用，而是工业间互联的网。它以工业级网络为基础、平台为中枢、数据为要素、安全为保障。能够把工业生产过程中的人、数据、机器连接起来，使工业生产流程数字化、自动化、智能化和网络化，进而提高生产效率，降低生产成本。

工业互联网系统架构主要分为 5 层，包括设备层、网络层、平台层、软件层、应用层，如图 1 所示。

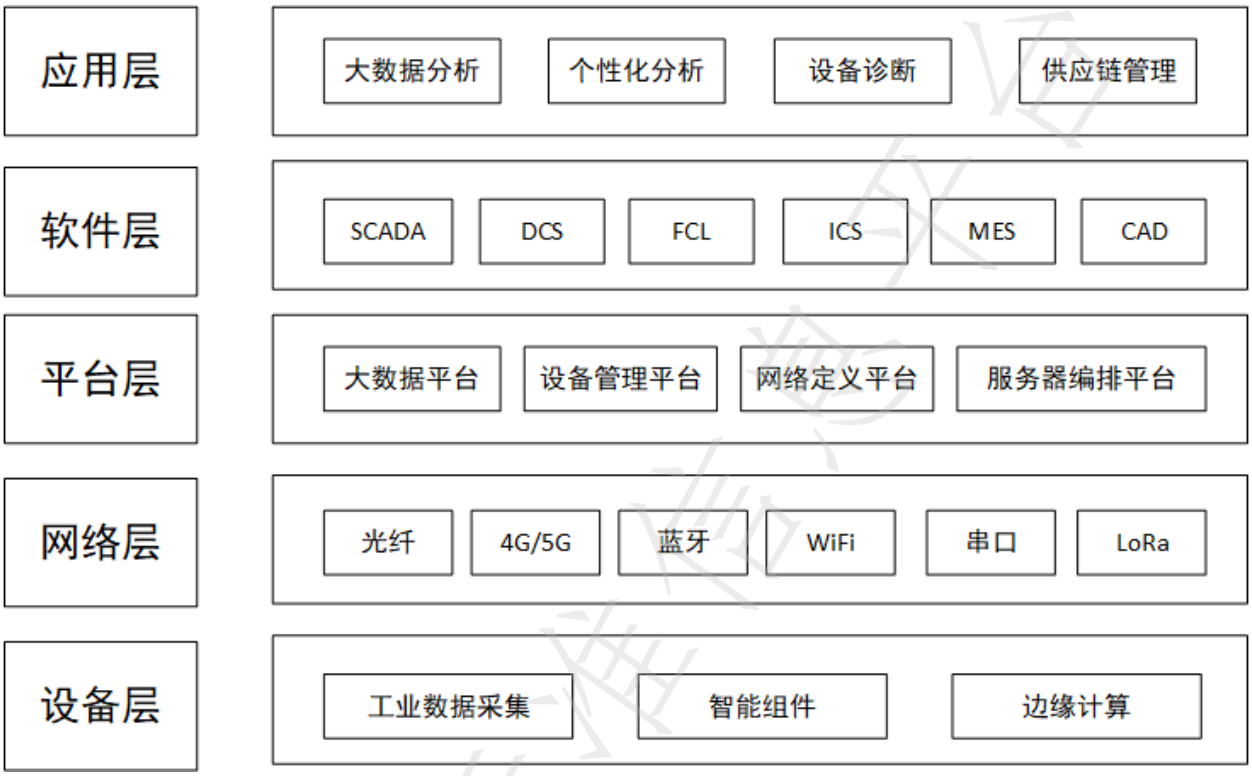

图 1 — 工业互联网系统架构图

设备层包括工业数据采集组件，智能组件及边缘计算组件，主要负责数据的采集和初步计算，直接执行工业生产动作。网络层负责工业互联网各层设备间信息的传输与转发。平台层包括工业互联网大数据平台、设备管理平台、网络定义平台、服务器编排平台等，负责网络、数据存储、计算等基础设施的编排。软件层通过总线控制系统、过程执行系统等软件刺痛，负责工业生产过程中的研发设计，生产控制和信息管理等。应用层通过大数据分析等应用手段，抽象出工业互联网的价值，并在各个不同的垂直领域与行业中形成针对性解决方案。

2.2 安全防护范围

工业互联网数据传输安全防护范围包括：工业互联网系统架构中层内、层间数据传输通信接口的安全保障以及安全性支持，作用于全生命周期（规划设计、开发建设、运维管理、废弃退出）

3 工业互联网数据安全传输技术要求

工业互联网涉及到传输的数据包括设备层的控制指令数据、传感器采集数据（振波、温度、湿度、红外、紫外、磁场、图像、声波流、视频流）、平台业务数据等，在保障基础的数据安全传输前提下，不同类型的数据传输可以采用不同安全策略。一个安全的数据传输系统包括以下几个方面，数据保密性、数据完整性、数据可用性、身份认证、数据隐私、安全审计。如果采用行业标准的传输协议（比如 FTP、HTTP），应当使其相关配置选项符合以上几个方面的要求。

3.1 数据保密性

工业互联网各个模块之间通信需要具备数据传输保密性保护功能，比如对传输的数据进行加密，相应的加密算法需要符合国家标准 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》。

对控制指令数据、传感器采集数据、平台业务数据可以采用不同安全级别的加密算法。传感器采集数据涉及原始的工业现场数据，应该具有更高的加密等级。对于加密密钥的协商、保存、传输、更新都应符合国家标准 GB/T39786-2021。

3.2 数据完整性

工业互联网各个模块之间传输数据时支持信息完整性校验机制,实现管理数据、鉴别信息、敏感信息、重要业务数据等重要数据的传输完整性保护(比如校验码、消息摘要、数字签名等)，防止信息被破坏、篡改，并在信息被破坏、篡改之后能够检测出来。特别是工业环境控制指令数据，应当充分验证其完整性，防止设备被劫持、非法访问。

3.3 数据可用性

应保障工业互联网各个模块之间数据传输时数据的时效性、准确性。具体包括以下两个方面：

1) 时效性：一方面需要对传输的数据添加时间戳，能够识别历史数据或超出时限的数据。应保障数据来源与系统采用统一时间分配/矫正机制。另一方面，应保证数据及时传输到目标设备/对象。比如，工业环境设备控制指令数据应当保证时效性，数据传输延迟过大可能导致设备控制失败，造成生产事故。
2) 准确性：保障传输和接收的数据误差在可接受的范围内,建立容错机制（比如哈希检验、错误重传）保障系统正常运行。

3.4 身份认证

工业互联网各个模块之间对发送方和接收方进行身份鉴别，建立信任关系。在建立连接前，利用密码技术进行初始化会话验证。

1) 确认彼此身份的合法性，防止中间人等安全攻击行为。
2) 协商密钥，为后续加解密、签名等提供支持。
3) 提供可以信赖的第三方，保障建立信任的基础。

3.5 数据隐私

工业互联网各个模块之间进行数据传输时,应标明传输的数据是否涉及隐私,同时标明可能的隐私收集与存储部分,保护用户隐私。

1) 对于传输双方的敏感数据，例如用户口令、生物特征、私钥、对称密钥等，不能以明文的形式显示或存储。
2) 需要时,对数据传输双方身份进行隐私保护。可采用数据脱敏算法等进行敏感信息保护。用户应能选择安全协议(例如 SSL、TLS 等)对传输的数据进行保护。

3.6 安全审计

工业互联网传输系统应对以下安全事件记录日志并进行审计，日志内容应至少包含日期和时间、事

件双方身份、事件类型、事件描述、设备类型、设备 ID，成功/失败的信息。日志记录应至少覆盖以下事件：

1） 双方数据传输建立成功与失败；
2） 传输设备在线监测异常与告警事件；
3） 数据破坏、篡改等恶意程序入侵警报事件；
4） 日志管理系统登录、修改、退出事件。