ICS 35.030
CCS L 70

YD

中华人民共和国通信行业标准

YD/T XXXXX—XXXX

工业互联网安全隔离与信息交换系统技术要求

Technical requirements of security isolation and information ferry system for Industrial Internet

（报批稿）

（本稿完成时间：2023 年 2 月 23 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　　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》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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：北京天融信网络安全技术有限公司、中国信息通信研究院、国家工业信息安全发展研究中心、中国科学院信息工程研究所、新华三技术有限公司、北京东方通网信科技有限公司、北京奇虎科技有限公司、郑州信大捷安信息技术股份有限公司、长扬科技（北京）股份有限公司、奇安信科技集团股份有限公司、北京神州绿盟科技有限公司、施耐德电气（中国）有限公司。

本文件主要起草人：李雪莹、寇增杰、董悦、王冲华、雷晓锋、安高峰、于广琛、余果、闫兆腾、王进法、万晓兰、袁留记、马霄、金忠龙、张有慧、王龑、崔婷婷、刘为华、张屹、姚一楠、汪义舟、张亚京、赵华、崔君荣、王弢、程潞样、毕继华。

工业互联网安全隔离与信息交换系统技术要求

1 范围

本文件规定了工业互联网安全隔离与信息交换系统的功能要求、系统管理要求和性能要求。

本文件适用于工业互联网安全隔离与信息交换系统的设计、开发和测试。

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 20279 信息安全技术 网络和终端隔离产品安全技术要求

GB/T 25069 信息安全技术 术语

GB/T 32919 信息安全技术 工业控制系统安全控制应用指南

GB/T 42021-2022 工业互联网 总体网络架构

3 术语和定义

GB/T 20279、GB/T 25069、GB/T 32919和 GB/T 42021-2022界定的以及下列术语和定义适用于本文件。

3.1

工业互联网 industrial Internet

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系。

[来源：GB/T 42021-2022，3.1]

3.2

工业互联网安全隔离与信息交换系统 industrial Internet security isolation and information ferry system

位于工业互联网不同安全域之间，在工业互联网络上实现安全域安全隔离与信息交换的产品。

4 缩略语

下列缩略语适用于本文件。

CIFS 通用网络文件系统（Common Internet File System）

CPU 中央处理器（Central Processing Unit）

DA 数据访问（Data Access）

FTP 文件传输协议（File Transfer Protocol）

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

ICMP 互联网控制报文协议（Internet Control Message Protocol）

IP	网际互连协议（Internet Protocol）
MAC	媒体存取控制（Media Access Control）
MQTT	消息队列遥测传输协议（Message Queuing Telemetry Transport）
MSTP	多生成树协议（Multiple Spanning Tree Protocol）
NFS	网络文件系统（Network File System）
OPC	对象链接与嵌入的过程控制（OLE for Process Control）
PLC	可编程逻辑控制器（Programmable Logic Controller）
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol）
STP	生成树协议（Spanning Tree Protocol）
TCP	传输控制协议（Transmission Control Protocol）
UA	统一架构（Unified Architecture）
UDP	用户数据报协议（User Datagram Protocol）

5 工业互联网安全隔离与信息交换系统描述

工业互联网安全隔离与信息交换系统通常部署在工业互联网不同安全域之间，保护工业互联网平台或网络中的资产。

如图1所示，工业互联网安全隔离与信息交换系统通常由两个独立处理单元和一个专用隔离模块组成。其中，两个处理单元分别连接不同的安全域，同时经隔离模块实现数据摆渡，专用隔离部件可以是采用包含电子开关并固化信息摆渡控制逻辑的专用隔离芯片构成的隔离交换板卡，也可以是经过安全加固并运行专用信息传输逻辑控制程序的主机。专用隔离部件是两个安全域之间唯一的可信物理通道。

工业互联网安全隔离与信息交换系统用于连接两个不同的安全域，实现工业互联网的两个安全域之间的访问控制、协议转换、内容过滤和信息交换等功能。

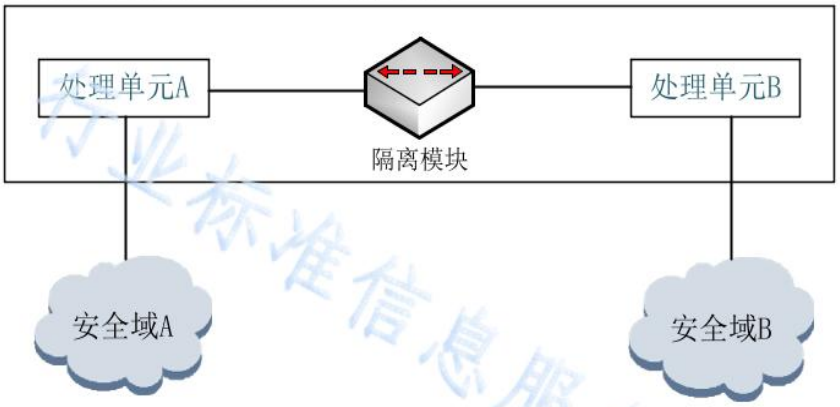

图1 工业互联网安全隔离与信息交换系统功能模块示意图

6 功能要求

6.1 协议要求

6.1.1 工业通信协议支持

6.1.1.1 OPC UA 协议

应支持统一框架协议OPC UA通讯协议中命令方法的深度解析，如：枚举主机，通道浏览，点位查询，协议读写方向控制等。

6.1.1.2 工业数据采集协议支持

工业数据采集协议支持要求包括：

a) 应支持常见工控协议实时数据的点位级采集；
b) 应支持通过代理组件采集OPC DA数据源；
c) 应支持通过专用采集驱动采集常见PLC内外部寄存器数据实时数据；
d) 应支持采集Modbus TCP协议常见功能码数据的实时数据；
e) 应支持三种及以上数据采集协议，包括但不限于OPC UA、S7COMM、Ethernet/IP、IEC104、Modbus TCP等。

6.1.1.3 工业数据转发协议支持

应支持多种转发协议与监控平台互联互通，如：Modbus TCP、OPC UA、MQTT、HTTP将采集到的数据和状态（可进行数据量批次设置）对外发送到监控平台的功能。

6.1.2 通用数据传输协议支持

通用数据传输协议支持要求包括：

a) 应支持超文本传输协议HTTP协议深度解析与控制，如：信息获取，传输文件，传输实体文件，搜索，获取报文头部等操作；
b) 应支持文件传输协议FTP协议深度解析与控制，如：认证安全机制，目录调整，主被动传输模式，创建目录，删除目录，收集文件信息详细目录，上传文件，文件重命名等操作；
c) 应支持SMB/CIFS、FTP、FTPS、NFS等多种通信协议进行文件交换，支持文件内容、类型过滤，支持重名处理机制，支持目录内子目录同步；
d) 应支持邮件传输协议SMTP、邮件接受协议POP3的深度解析与控制，如：身份认证，发送者地址，邮件附件，获取邮件，删除某一邮件等操作，测试连接是否成功等；
e) 应支持数据库协议在操作过程中深度解析与控制，如：查询，插入，删除，更新，创库，删库，数据库级别设置等应用动作深度控制；
f) 应支持国内外常用的各种类型数据库的同步，支持同构、异构数据库之间的同步，同步数据可具体设置到字段级别。

6.1.3 协议隔离

不同安全域之间传输的信息流应执行网络层协议剥离，以非TCP/IP的私有协议格式传输。

6.2 断网续传

应具有在网络离线时缓存数据的功能，并在恢复网络后能够将缓存数据上传到监控平台的功能。同时支持历史数据可用存储空间控制和历史数据发布周期设置，支持续传模式选择：全部或变化。

6.3 多通道采集与转发

多通道采集与转发要求包括：

a) 数据采集应支持多通道，通道可挂载多种设备的采集模式；
b) 数据转发服务应提供同时将数据上传到多个监控平台的能力。

6.4 在线监测

应支持监测设备在线情况功能，同时支持在线检测时对采集通道和转发通道报文的监控功能，支持在线监控时观察采集数据的变化情况，设备授权情况等功能。

6.5 访问控制

6.5.1 基于白名单的访问控制

应配置和应用基于白名单的访问控制策略，默认禁止白名单之外的网络访问。

6.5.2 网络层访问控制

网络层访问控制要求包括：

a) 应基于源IP地址、目的IP地址、源端口号、目的端口号、传输协议等要求，进行访问控制；

b) 应支持开启STP协议、MSTP生成树协议，防止网络形成环路。

6.5.3 IP 地址/MAC 地址绑定

应支持自动或手工绑定通信接口对端设备的接口IP地址和MAC地址，当通信接口对端设备的IP地址和MAC地址与绑定列表不符时阻止通信。

6.5.4 应用层访问控制

应用层访问控制要求包括：

a) 应识别和控制HTTP、FTP、TELNET等应用层协议的访问；

b) 应至少支持两种工业应用协议的访问控制。

6.6 信息摆渡

两个处理单元之间应采用专用的隔离部件，并确保两个处理单元不能同时与专用隔离部件物理连通。

6.7 残余信息保护

应保证分配的资源中不包含之前连接活动中所产生的任何信息内容。

6.8 不可旁路

在与安全有关的操作被允许执行之前，应确保通过安全功能策略的检查。

6.9 抗拒绝服务攻击

应具备一定的抗拒绝服务攻击能力，如：SYN Flood攻击、UDP Flood攻击、ICMP Flood攻击、TearDrop攻击、Land攻击等。

6.10 双机热备

应具备双机热备的能力。

7 系统管理要求

7.1 标识和鉴别

7.1.1 唯一性标识

应保证所有用户、设备、系统都具有唯一的标识。

7.1.2 管理员属性定义

应为每个管理员规定与之相关的安全属性，如管理员标识、鉴别信息、隶属组、权限等，并提供使用默认值对创建的每个管理员的属性进行初始化的功能。

7.1.3 管理员角色

应区分管理员角色，能划分为系统管理员、安全操作员和安全审计员，且三类管理员角色权限相互制约。

7.1.4 基本鉴别

应保证任何用户在执行安全功能前都要进行身份鉴别。若其采用网络远程方式管理，还应对可管理的IP、MAC地址进行限制。

7.1.5 多鉴别

应能向管理角色提供除口令身份鉴别机制以外的其他身份鉴别机制（如证书、智能IC卡、指纹等鉴别机制）。

7.1.6 超时锁定或注销

当已通过身份鉴别的管理角色空闲操作的时间超过规定值，在该管理角色需要执行管理功能前，应对该管理角色的身份重新进行鉴别。

7.1.7 鉴别失败处理

应为管理员登录设定一个授权管理员可修改的鉴别尝试阈值，当管理员的不成功登录尝试超过阈值，系统应通过技术手段阻止管理员的进一步鉴别请求。

7.2 安全管理

7.2.1 接口及管理安全

接口及管理安全要求包括：

a) 应支持业务接口和管理接口应采用不同的网络接口；

b) 管理接口及管理界面应不存在已知的中、高风险安全漏洞。

7.2.2 管理信息传输安全

当需要通过网络进行管理时，应能对管理信息进行保密传输。

7.2.3 安全状态监测

安全状态监测要求包括：

a) 对系统中的CPU、内存、存储空间等系统资源使用状态进行监测；

b) 对系统的主要功能模块运行状态进行监测。

7.3 数据完整性

应对储存于设备中的鉴别数据和信息传输策略等关键数据采取完整性保护措施，避免被篡改。

7.4 日志审计管理

日志审计管理要求包括：

a) 应生成访问控制策略匹配的访问请求，包括允许及禁止的访问请求；
b) 应识别及抵御的各类攻击行为。
c) 日志内容应包括日期、时间、源目的MAC地址、源目的IP地址、源目的端口号、协议类型；
d) 日志内容应包括工业协议的操作类型、操作对象、操作值等相关参数；
e) 日志内容应包括攻击事件的类型及描述。

7.4.1 系统日志生成

系统日志生成要求包括：

a) 身份鉴别，包括成功和失败；
b) 因鉴别失败次数超过阈值而采取的禁止进一步尝试的措施；
c) 访问控制策略的增加、删除、修改；
d) 管理员的增加、删除、修改；
e) 时间同步；
f) 超过保存时限的审计记录和自身审计日志的自动删除；
g) 审计日志和审计记录的备份与恢复；
h) 存储空间达到阈值报警；
i) 其他事件。

7.4.2 系统日志内容

系统日志内容至少应包括日期、时间、事件主体、事件客体、事件描述等。

7.4.3 审计日志管理

审计日志管理要求包括：

a) 应只允许授权管理员能够对审计日志进行读取、存档、导出、删除和清空等操作；
b) 应提供能查阅日志的工具，支持多条件对审计日志进行组合查询；
c) 审计事件应存储于掉电非易失性存储介质中，且在存储空间临近和达到阈值时，通知授权审计员；
d) 应支持以标准格式将审计日志外发到专用的日志服务器；
e) 日志留存时间应不少于6个月。

8 性能要求

8.1 百兆网络性能要求

百兆网络性能要求包括：

a) 网络吞吐量应不小于100Mbps；
b) 内部交换带宽应不小于100Mbps；
c) 数据时延应不超过1ms。

8.2 千兆网络性能要求

千兆网络性能要求包括：

a) 网络吞吐量应不小于1Gbps；

b) 内部交换带宽应不小于1Gbps；

c) 数据时延应不超过1ms。

参 考 文 献

[1] GB 40050-2021 网络关键设备安全通用要求
[2] GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求
[3] GB/T 20277-2015 信息安全技术 网络和终端隔离产品测试评价方法
[4] GB/T 20279-2015 信息安全技术 网络和终端隔离产品安全技术要求
[5] GB/T 37934-2019 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求