工业互联网产业联盟
Alliance of Industrial Internet

工 业 互 联 网 产 业 联 盟 标 准

AII/006-2021

工业互联网 网络安全数据采集装置技术要求

Industrial internet - Technical requirements for network security data acquisition device

工业互联网产业联盟

（2021 年 8 月 31 日发布）

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目　　次

前　言

本文件由工业互联网产业联盟提出并归口。

标准牵头单位：长扬科技（北京）有限公司、中国信息通信研究院

标准起草单位和主要起草人：

长扬科技（北京）有限公司：汪义舟、赵华、张亚京

中国信息通信研究院：李艺、田慧蓉

公安部第三研究所：邹春明、孙天宁

北京交通大学：陶耀东

中国石油天然气股份有限公司规划总院：郑正发、许涛

上海观安信息技术股份有限公司：谢江

北京微智信业科技有限公司：崔婷婷、刘如君

北京双湃智安科技有限公司：李鸿彬

深圳融安网络科技有限公司：汪敦全

南京中新赛克科技有限责任公司：汤永田、糜靖峰

北京华电众信技术股份有限公司：田海涛

江苏亨通工控安全研究院有限公司：郭立龙、陈夏裕

北京赋乐科技有限公司：任荣、王翔

航天新长征大道科技有限公司：陆和平

奇安信科技集团股份有限公司：崔君荣、王弢

北京东方国信科技股份有限公司：孙广明

东软集团股份有限公司：谷久宏

杉树岭网络科技有限公司：刘畅、井柯

北京万维物联科技发展有限公司：张森

杭州安恒信息技术股份有限公司：李显松、王晓翔

中国电子科技网络信息安全有限公司：李立

工业互联网创新中心（上海）有限公司：王潇潇、梁军、刘畅

北京安帝科技有限公司：谢斌、饶志波

引　言

我国工业互联网发展形势下 IT 技术与 OT 技术深度融合，面对互联网的攻击手段对工业互联网和工业生产带来的网络安全隐患，面向工业互联网场景的网络安全监测、分析、溯源、防护等需求激增，而工业互联网网络安全的监测、分析、溯源均离不开对工业互联网网络安全的原始数据进行采集。

工业互联网网络安全数据采集存在应用场景的不同，导致产品种类多、功能差异较大，接口兼容性差和产品带来的自身安全等问题；工业互联网网络安全数据采集方面缺乏统一标准，亟需制定。

本文件旨在指导各重点领域及相关单位进行网络安全数据采集装置设计、开发、生产和检测，推动网络安全数据采集装置标准化、提高兼容性，对加强工业互联网安全防护具有重要意义。

工业互联网 网络安全数据采集装置技术要求

1 范围

本文件规定了工业互联网网络安全数据采集装置的功能要求、自身安全要求、安全保障要求、硬件要求。

本文件适用于工业互联网网络安全数据采集装置的设计、开发、生产和检测。也适用于涉及到工业互联网网络安全数据采集装置的工程项目的设计、实施和验收。

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 信息安全技术 术语

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1.1

工业互联网 industrial internet

满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

[来源：YD/T 3804—2020，3.1.1]

3.1.2

网络安全数据 network security data

与网络安全直接或间接相关、可用于分析网络安全状况的数据的总称。包括采集装置采集获取的安全原始数据和基于原始数据分析加工得出的数据。安全原始数据包括设备基础数据、设备运行状态数据、网络状态数据、网络流量数据、应用数据。

3.2 缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

ICMP：网际控制报文协议（Internet Control Message Protocol）
IP：网际互连协议（Internet Protocol）
MQTT：消息队列遥测传输协议（Message Queuing Telemetry Transport）
OPC：流程控制的对象连接与嵌入技术（Object Linking and Embedding for Process Control）
OPC UA：OPC统一架构（OPC Unified Architecture）
PING：因特网包探索器（Packet Internet Groper）
POP3：邮局协议版本3（Post Office Protocol - Version 3）
SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
SNMP：简单网络管理协议（Simple Network Management Protocol）
SSH：安全外壳协议（Secure Shell）
TCP：传输控制协议（Transmission Control Protocol）
VPN：虚拟专用网络（Virtual Private Networks）
WMI：Windows管理工具的通信协议（Windows Management Instrumentation）

4 产品描述

工业互联网网络安全数据采集装置（以下简称“采集装置”），通过监听、轮询和流量嗅探等方式，实现工业互联网网络安全数据的采集，并能对数据进行分析处理，将分析结果数据发送到网络安全数据中心或其他关联系统。采集装置可以作为服务端，通过监听采集数据，也可以作为客户端，通过轮询采集数据；采集装置通过流量嗅探方式采集流量数据。

采集装置可以通过硬件或软件形式实现。

采集装置的典型部署参见图1。

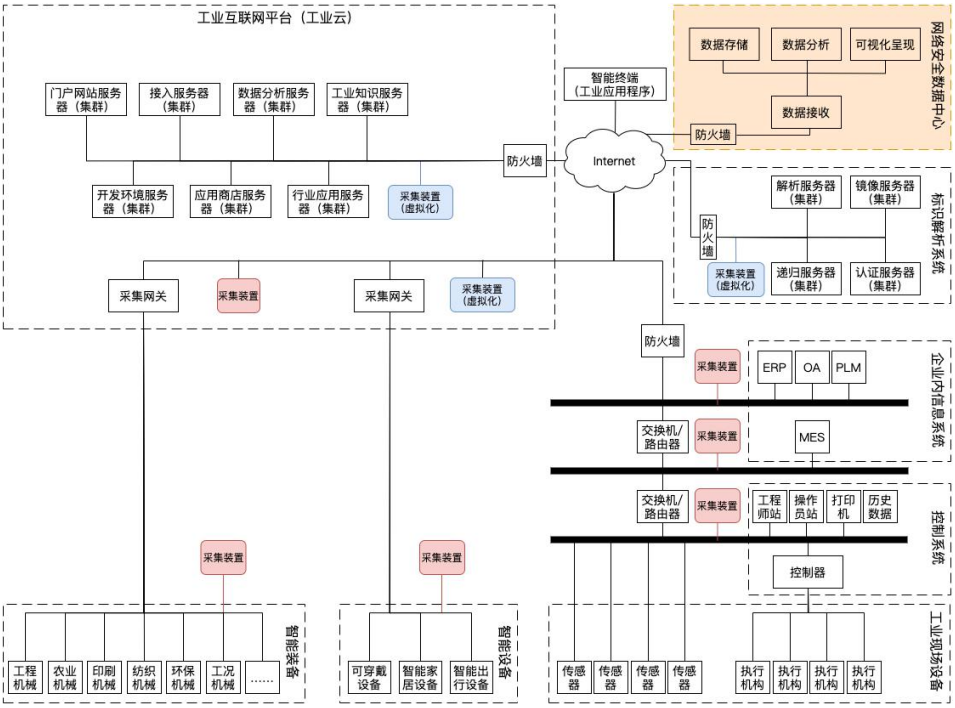

图 1 采集装置典型部署示意图

本文件将采集装置技术要求分为功能要求、自身安全要求、安全保障要求、硬件要求四个大类。其中，功能要求对采集装置应具备的安全功能提出具体要求，包括网络安全数据采集、网络安全分析、数据上报；自身安全要求针对采集装置的自身安全提出要求，包括安全管理、安全审计、安全支撑系统；安全保障要求针对采集装置的生命周期过程提出具体要求，包括开发、指导性文档、生命周期支持、测试；硬件要求包括硬件规格、电源要求、可靠性要求、环境适应性要求，采用软件化形式部署的采集装置不需要满足“硬件要求”。

5 技术要求

5.1 功能要求

5.1.1 数据采集

5.1.1.1 采集对象

采集装置应不干扰采集对象的运行，采集对象应至少包括以下一种：

a）设备类

1）智能装备和智能设备；

2）工业现场设备；

3）网络通信设备，如交换机、路由器、采集网关等；

4）网络安全设备，如防火墙、VPN、安全网关等。

b）系统类

1）控制系统；

2）企业信息系统；

3）标识解析系统。

c）工业互联网平台。

5.1.1.2 采集方式

采集装置的采集方式要求如下：

a） 应支持采集装置作为服务端，以监听的方式进行数据采集；

b） 应支持流量嗅探；

c） 应支持常见通信协议，包括但不限于 ICMP、ARP 、SNMP、SYSLOG 等；

d） 支持采集装置作为客户端，以轮询的方式进行数据采集；

e） 支持宿主客户端程序采集；

f） 支持其它通信协议，包括但不限于 WMI、MQTT 等。

注：宿主客户端程序指安装和运行在实体或者虚拟主机中的软件，用于搜集主机侧安全相关的数据并发送至网络安全数据采集装置。

5.1.1.3 采集内容

5.1.1.3.1 设备基础数据

采集装置应支持采集对象的基础数据，包括但不限于：

a） 采集对象的基本信息，如设备名称、设备型号、制造商名称及品牌等；

b） 采集对象的操作系统或固件信息，包括操作系统或固件名称、版本标识等；

c） 设备的物理接口信息，包括物理接口数量、各物理接口的名称、类型和相关的配置参数等数据。

5.1.1.3.2 设备运行状态数据

采集装置应支持采集设备的运行状态数据，包括但不限于：

a）CPU运行状态数据，如CPU利用率、CPU温度；

b）内存运行状态数据，包括内存使用率；

c）磁盘运行状态数据，包括磁盘空间使用率；

d）设备运行的系统日志和告警数据。

5.1.1.3.3 网络状态数据

采集装置应支持采集设备的网络状态数据，包括但不限于：

a）物理接口的链路状态，包括在线状态、离线状态；

b）网络配置数据，包括网络接口名称、网络接口IP地址、子网掩码；

c）网络配置数据，包括DNS、路由、隧道等；

d）接口的ARP地址映射表。

5.1.1.3.4 网络流量数据

采集装置应支持采集网络流量数据：

a） 应支持原始网络流量数据留存；

b） 应支持常见 IT 应用协议的深度包解析，支持提取网络元数据如源 IP、目的 IP、源端口、目的端口、应用协议名称、应用协议特征、数据包大小等，包括但不限于 HTTP、FTP、Telnet、POP3、SMTP 等常见 IT 应用协议；

c） 应支持常见工控应用协议的深度包解析，支持提取网络元数据如源 IP、目的 IP、源端口、目的端口、应用协议名称、应用协议特征、数据包大小等，包括但不限于 Modbus TCP、S7Comm、OPC UA、MQTT 等常见工业互联网应用协议；

d） **支持私有工控应用协议的深度包解析，支持导入私有工控协议的解析脚本，根据私有工控协议的解析脚本提取网络元数据。**

5.1.1.3.5 应用数据

采集装置应支持采集采集对象的应用数据：

a） 采集对象上的应用配置数据，如应用名称、应用版本标识、服务名称、服务端口、服务所采用的通信协议等；

b） 采集对象上的告警数据；

c） 采集对象的应用运行日志数据，如数据库运行日志、关键中间件运行日志等。

5.1.2 网络安全分析

5.1.2.1 数据预处理

采集装置应支持对采集到的数据进行预处理，包括但不限于：

a）将采集到的重复的数据进行清洗；

b）将采集的数据进行数据格式转换，且转换时不能造成关键数据项丢失；

c）将采集的数据进行标签化描述，标签化包括采集对象的基础数据、设备运行状态、网络运行状态；

d）具备复杂数据的关联预处理，包括用户行为关联、网络攻击数据关联、应用行为关联预处理。

5.1.2.2 采集对象基础数据分析

采集装置应支持从采集数据中分析采集对象的基础数据，包括但不限于：

a） 形成工业互联网中的设备资产清单，并分析设备资产清单的变更，包括增加、减少设备；

b） 形成设备的网络接口与物理接口的对应绑定，并分析设备的物理接口变更，包括增加、减少物理接口，分析设备的网络接口变更，包括增加、减少网络接口、网络配置变更；

c） 分析设备硬件模块变化，包括增加硬件模块、拆除硬件模块等；

d） 分析设备操作系统或固件的版本变化，包括版本的升级、降级等变更；

e） 分析采集对象应用软件、操作系统或固件存在的漏洞。

5.1.2.3 设备运行状态分析

采集装置应支持从采到的数据中分析设备的运行状态，包括：

a） 设备的启动、停止、重启；

b） 分析设备的运行状态，包括 CPU 利用率超阈值、CPU 温度超阈值、内存利用率超阈值、硬盘利用率超阈值等；

c） 分析设备接入外设的行为，包括接入的外设名称、外设类型、外设型号、接入的接口、接入时间、拔出时间、停留时长等；

d） 分析设备连接网络的行为，包括连接的网络类型、连接网络的接口、连接时间、断开时间、联网时长等；

e） 分析设备的不安全配置，包括弱口令、风险端口开放情况等。

5.1.2.4 网络运行状态分析

采集装置应支持从采到的数据中分析网络运行状态，包括：

a） 形成网络拓扑；

b） 分析网络拓扑变化；

c） 分析网络运行健康状态，如网络带宽占用阈值、网络可达、网络延迟等；

d） 分析异常连接，包括工业互联网内部对象之间的异常连接、从工业互联网内网至互联网外网的异常外联、从工业互联网外网到工业互联网内部的异常接入分析。

5.1.2.5 用户行为分析

采集装置应支持从采集到的数据中分析用户行为，包括：

a） 用户访问来源地区；

b） 用户操作行为，如变更口令、变更配置、操作时间段等；

c） 用户行为轨迹；

d） 用户行为频次。

5.1.2.6 网络攻击分析

采集装置应支持从采到的数据中分析网络的安全性，包括：

a） 网络中发生的网络扫描行为，包括扫描时间、扫描来源、扫描频次等；

b） 网络中发生的 DoS、DDoS、APT 攻击、勒索蠕虫攻击、木马攻击行为，包括攻击时间、攻击目标、攻击来源、攻击类型、攻击频次、攻击结果、僵尸网络的主机数量、IP 地址等，统计攻击流量；

c） 网络中发生的漏洞利用的攻击行为，包括利用时间、攻击来源、存在漏洞的设备、利用的漏洞、

漏洞类型、漏洞利用频次等。

5.1.2.7 应用分析

采集装置应支持从采集到的数据中分析:

a） 应用的异常状态，如备机应用心跳丢失、应用错误等；

b） 应用存在的已知漏洞；

c） 应用的不安全配置，如弱口令、风险端口开放情况等；

d） 应用通信关系（包括主体和客体之间一对一、多对多的应用协议通信），包括通信方向、协议名称、通信频次、流量等。

5.1.3 数据上报

采集装置应支持对网络安全数据中心或其它关联系统上报数据，具体要求如下：

a） 采集装置支持设置网络安全数据中心或其它关联系统的通信参数；

b） 采集装置与关联系统通信应采用加密协议，加密应符合相关要求；

c） 采集装置本地监听固定服务端口，固定端口号可配置；

d） 采集装置支持在线和离线上报数据；

e） 上报数据可独立设置上报数据权限，如分开设置采集数据和安全分析数据；

f） 采集装置应支持设置上报速率限制、上报系统缓存容量和数据上报优先级；

g） 采集装置应按数据优先级上报，数据上报积压时，应支持丢弃低优先级的数据并产生告警。

5.2 自身安全要求

5.2.1 安全管理

5.2.1.1 管理方式

采集装置的管理方式要求如下：

a） 管理界面应简洁直观，引导提示明确；

b） 采集装置应支持通过网络接口进行管理；

c） 管理接口与数据采集接口物理分离；

d） 采集装置应支持授权用户通过本地连接进行管理;

e） 支持授权用户通过远程连接进行管理,远程管理应采用加密的协议进行通信并支持通信端口设置；

f） 支持集中管理。

5.2.1.2 身份标识与鉴别

采集装置的身份标识与鉴别安全要求包括但不限于：

a） 对用户身份进行标识，身份标识具有唯一性；

b） 用户执行安全动作前需对其身份进行鉴别；

c） 对用户身份鉴别信息进行安全保护，保障鉴别信息存储和传输过程中的保密性；

d） 具有登录失败处理功能，如限制连续的非法登录尝试次数等相关措施；

e） 具有无操作超时处理功能，当用户登录后，无操作时长超过阈值时强制退出；

f） 身份鉴别口令应满足一定复杂度。设置鉴别口令时，应进行复杂度检查。应支持定期提醒更换口令；

g） 支持删除默认账号或修改默认账号名称；

h） 用户首次登录时，要求强制修改默认口令；

i） 对授权用户选择两种或两种以上组合的鉴别技术进行身份鉴别，其中一种需采用密码技术。

5.2.1.3 用户角色管理

采集装置的用户角色和权限管理应满足以下要求：

a） 对用户角色进行标识，用户角色标识具有唯一性；

b） 按用户角色划分功能权限，角色应相互制约；

c） 支持授权用户添加、删除角色，修改角色名称、权限。

5.2.1.4 时间和时钟源管理

采集装置的时间和时钟源的管理应满足以下要求：

a） 支持与外部时间服务器保持时钟同步；

b） 支持所有用户查看采集装置的当前时间；

c） 支持授权用户查看当前设置的时钟源、修改时钟源。

5.2.1.5 物理接口和网络参数管理

采集装置的物理接口和网络参数管理应满足以下要求：

a） 支持授权用户查看物理接口和网络参数，包括：物理接口名称、物理接口类型、物理接口地址、接口 IP 地址、子网掩码、路由目标网段、路由下一跳地址、串口波特率、串口数据位数、串口停止位数、串口校验方式、DNS 服务器通信参数、时间服务器通信参数、集中管理服务器通信参数、相关关联系统接口服务器通信参数等；

b） 支持授权用户设置或修改接口和网络参数，包括：接口 IP 地址、子网掩码、路由目标网段、路由下一跳地址、串口波特率、串口数据位数、串口停止位数、串口校验方式、DNS 服务器通信参数、时间服务器通信参数、集中管理服务器通信参数、相关关联系统接口服务器通信参数等。

5.2.1.6 网络诊断

采集装置应提供网络诊断工具，包括 PING、Traceroute、SSH 等。

5.2.1.7 安全配置管理

采集装置应支持授权用户查看、设置采集装置的安全配置信息，包括：

a） 访问安全设置，包括限制管理端 IP 地址和 MAC 地址、密码错误尝试次数、连续输入密码错误锁定时长等；

b） 存储安全设置，包括存储时长、存储容量等；

c） 状态告警阈值设置，包括 CPU 利用率阈值、CPU 温度阈值、内存使用率阈值、磁盘使用率阈值等。

5.2.1.8 数据采集配置管理

采集装置应支持授权用户查看、设置数据采集配置信息，包括但不限于：

a） 基本信息，如部署地点、采集目标系统名称等；

b） 采集设备信息，如设备名称、设备型号、通信参数等；

c） 采集方式；

d） 采集内容；

e） 采集频率。

5.2.1.9 自身状态监测

采集装置应支持监测自身的状态，包括但不限于：CPU 利用率、CPU 温度、内存使用率、磁盘使用率等。

5.2.1.10 数据存储

数据存储要求包括但不限于：

a） 应将配置数据、自身日志、网络安全数据存储在掉电非易失性存储介质中；

b） 应将配置数据、自身日志、网络安全数据加密存储，防止未经授权的查看和修改；

c） 应具有存储空间耗尽处理功能，当剩余存储空间达到预定义的阈值时进行告警。

5.2.1.11 数据查询

应支持授权用户查询配置数据、自身日志、网络安全数据。

5.2.1.12 数据备份与恢复

应支持授权用户对数据进行备份与恢复，要求包括但不限于：

a）备份、恢复配置数据、自身日志、网络安全数据；

b）支持全量方式；

c）支持增量方式。

5.2.1.13 升级

应支持授权用户对采集装置进行本地或远程升级，要求包括但不限于：

a） 支持全量方式；

b） 支持增量方式；

c）支持软件升级包校验，确保升级包完整；

d）支持数据保护，升级过程确保配置数据、自身日志、网络安全数据完整；

e）升级后支持业务自动恢复。

5.2.2 安全审计

采集装置的安全审计要求包括但不限于：

a） 对用户的登录和退出、增加/删除/修改用户、增加/删除/修改/备份/恢复配置数据、删除/备份/恢复网络安全数据、删除自身日志、采集装置开启/重启/关机、时间同步等行为生成日志；

b） 对采集装置的异常状态进行告警，并生成日志，异常状态包括但不限于：CPU 利用率、CPU 温度、内存使用率、磁盘使用率超过阈值，功能模块或组件停止运行等；

c） 日志应包括如下内容：行为发生的日期和时间、类型、主体、客体、结果、事件描述；

d） 向授权用户提供查看、删除、备份和恢复日志的功能；

5.2.3 安全支撑系统

采集装置的支撑系统安全要求包括但不限于：

a） 进行必要的裁剪，不提供多余的组件或服务，或者可关闭非必要的服务；

b） 不存在已知的中、高风险安全漏洞；

c） 应具备检测并抵御各种常见网络攻击的能力及抵御渗透攻击的能力；

d） 应具备抵抗对采集装置暴力破解的能力，支持系统加固，包括但不限于可执行程序资源压缩等保护技术；
e） 采集装置应确保在正确存放和使用过程中，配置数据、自身日志、网络安全数据等不出错、不丢失；
f） 支持采用商用密码算法对数据存储、上报进行安全防护。

5.3 安全保障要求

5.3.1 开发

5.3.1.1 安全架构

开发者应提供采集装置安全功能的安全架构描述，要求如下：
a） 与采集装置设计文档中对安全功能实施抽象描述的级别一致；
b） 描述与安全功能要求一致的采集装置安全功能的安全域；
c） 描述采集装置安全功能初始化过程为何是安全的；
d） 证实采集装置安全功能能够防止被破坏；
e） 证实采集装置安全功能能够防止安全特性被旁路。

5.3.1.2 功能规范

开发者应提供完备的功能规范说明，要求如下：
a） 完全描述采集装置的安全功能；
b） 描述所有安全功能接口的目的与使用方法；
c） 标识和描述每个安全功能接口相关的所有参数；
d） 描述安全功能接口相关的安全功能实施行为；
e） 描述由安全功能实施行为处理而引起的直接错误消息；
f） 证实安全功能要求到安全功能接口的追溯；
g） 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

5.3.1.3 实现表示

开发者应提供全部安全功能的实现表示，要求如下：
a） 提供采集装置设计描述与实现表示实例之间的映射，并证明其一致性；
b） 按详细级别定义采集装置安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c） 以开发人员使用的形式提供。

5.3.1.4 产品设计

开发者应提供采集装置设计文档，要求如下：
a） 根据子系统描述采集装置结构；
b） 标识和描述采集装置安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e） 根据模块描述安全功能；
f） 提供安全功能子系统到模块间的映射关系；
g） 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；

h） 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；

i） 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

5.3.2 指导性文档

5.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；

b） 描述如何以安全的方式使用采集装置提供的可用接口；

c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；

d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；

e） 标识采集装置运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；

f） 充分实现安全目的所必须执行的安全策略。

5.3.2.2 准备程序

开发者应提供采集装置及其准备程序，技术要求如下：

a） 描述与开发者交付程序相一致的安全接收所交付采集装置必需的所有步骤；

b） 描述安全安装采集装置及其运行环境必需的所有步骤。

5.3.3 生命周期支持

5.3.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a） 为采集装置的不同版本提供唯一的标识；

b） 使用配置管理系统对组成采集装置的所有配置项进行维护，并唯一标识配置项；

c） 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；

d） 配置管理系统提供一种自动方式来支持采集装置的生成，通过该方式确保只能对采集装置的实现表示进行已授权的改变；

e） 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发采集装置。实施的配置管理与配置管理计划相一致；

f） 配置管理计划描述用来接受修改过的或新建的作为采集装置组成部分的配置项的程序。

5.3.3.2 配置管理范围

开发者应提供采集装置配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a） 采集装置、安全保障要求的评估证据和采集装置的组成部分；

b） 实现表示、安全缺陷报告及其解决状态。

5.3.3.3 交付程序

开发者应使用一定的交付程序交付采集装置，并将交付过程文档化。在给用户方交付采集装置的各版本时，交付文档应描述为维护安全所必需的所有程序。

5.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在采集装置的开发环境中，为保护采集装置设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

5.3.3.5 生命周期定义

开发者应建立一个生命周期模型对采集装置的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护采集装置的模型。

5.3.3.6 工具和技术

开发者应明确定义用于开发采集装置的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

5.3.4 测试

5.3.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a） 表明测试文档中所标识的测试与功能规范中所描述的采集装置的安全功能间的对应性；

b） 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

5.3.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a） 证实测试文档中的测试与采集装置设计中的安全功能子系统和实现模块之间的一致性；

b） 证实采集装置设计中的所有安全功能子系统、实现模块都已经进行过测试。

5.3.4.3 功能测试

开发者应测试采集装置安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a） 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b） 预期的测试结果，表明测试成功后的预期输出；

c） 实际测试结果和预期的一致性。

5.3.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

5.3.4.5 脆弱性评定

基于已标识的潜在脆弱性，采集装置能够抵抗以下攻击行为：

a） 具有基本攻击潜力的攻击者的攻击；

b） 具有增强攻击潜力的攻击者的攻击。

5.4 硬件要求

5.4.1 硬件规格

采集装置硬件配置应满足以下要求：

a） 应具备单独的管理接口，接口类型为以太网接口，管理接口与通信接口要求分离；
b） 磁盘要求：系统盘和数据盘物理分开。

5.4.2 电源要求

采集装置内部电源模块应满足以下要求：
a）支持双路交流或直流电源独立供电，任一回路电源中断不造成装置故障或重启；
b）若采用直流电源模块，电压纹波系数小于 5%；
c）若采用交流电源模块，电压 220V，电压允许偏差 -20%～+15%，频率:50Hz，频率允许偏差±5%，波形为正弦波，谐波含量小于 5%；
d）电源模块失电信号有硬接点输出；
e）采集装置面板上有电源指示灯显示电源故障状态。

5.4.3 可靠性要求

采集装置的平均故障间隔时间应大于50,000小时。

5.4.4 环境适应性要求

采集装置的环境适应性应符合国家和相关行业的要求。

6 等级划分要求

6.1 等级划分说明

根据采集装置应提供的功能要求、自身安全要求和安全保障要求的强弱，将产品的要求分为基本级和增强级。基本级规定了产品应达到的基本的要求，增强级规定了产品除具备基本级要求以外，还应增强的要求。

6.2 功能要求等级划分

采集装置功能要求等级划分见表1。

表 1 采集装置功能要求等级划分

功能要求			基本级	增强级
网络安全数据采集	采集对象		5.1.1.1	5.1.1.1
	采集方式		5.1.1.2 a）b）c)	5.1.1.2
	采集内容	设备基础数据	5.1.1.3.1	5.1.1.3.1
		设备运行状态数据	5.1.1.3.2	5.1.1.3.2
		网络状态数据	5.1.1.3.3 a）b）	5.1.1.3.3
		网络流量数据	5.1.1.3.4 a）b）c)	5.1.1.3.4
		应用数据	5.1.1.3.5 a）b）	5.1.1.3.5
网络安全分析	数据预处理		5.1.2.1 a）b）	5.1.2.1
	采集对象基础数据分析		—	5.1.2.2
	设备运行状态分析		—	5.1.2.3
	网络运行状态分析		—	5.1.2.4

	用户行为分析	—	5.1.2.5
	网络攻击分析	5.1.2.6	5.1.2.6
	应用分析	5.1.2.7 a）	5.1.2.7
数据上报		5.1.3	5.1.3

6.3 自身安全要求等级划分

采集装置自身安全要求等级划分见表2。

表 2 采集装置自身安全要求等级划分

自身安全要求		基本级	增强级
安全管理	管理方式	5.2.1.1 a）～d）	5.2.1.1
	身份标识与鉴别	5.2.1.2 a）～h）	5.2.1.2
	用户角色管理	5.2.1.3	5.2.1.3
	时间和时钟源管理	5.2.1.4	5.2.1.4
	物理接口和网络参数管理	5.2.1.5	5.2.1.5
	网络诊断	5.2.1.6	5.2.1.6
	安全配置管理	5.2.1.7	5.2.1.7
	数据采集配置管理	5.2.1.8	5.2.1.8
	自身状态监测	5.2.1.9	5.2.1.9
	数据存储	5.2.1.10	5.2.1.10
	数据查询	5.2.1.11	5.2.1.11
	数据备份与恢复	5.2.1.12	5.2.1.12
	升级	5.2.1.13	5.2.1.13
安全审计		5.2.2	5.2.2
安全支撑系统		5.2.3 a）～e）	5.2.3

参考文献

[1] GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件
[2] GB/T 20945—2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法
[3] GB/T 37941—2019 信息安全技术 工业控制系统网络审计产品安全技术要求
[4] GB/T 37953—2019 信息安全技术 工业控制网络监测安全技术要求及测试评价方法
[5] GA/T 911—2010 信息安全技术 日志分析产品安全技术要求
[6] YD/T 3804-2020 工业互联网安全防护总体要求
[7] AII/003—2018 工业互联网 安全总体要求