

# 中华人民共和国国家标准

GB/T 41262—2022

## 工业控制系统的信息物理融合异常 检测系统技术要求

Technical requirements for cyber-physical fusion anomaly detection  
specification of industrial control system

2022-03-09 发布

2022-10-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会

目次

前言 ..... I

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 3

5 系统概述 ..... 3

    5.1 系统架构 ..... 3

    5.2 功能模块 ..... 4

6 功能要求 ..... 5

    6.1 数据采集 ..... 5

    6.2 异常检测 ..... 6

    6.3 响应与告警 ..... 8

    6.4 检测结果处理 ..... 9

    6.5 管理控制 ..... 10

    6.6 安全管理 ..... 10

    6.7 日志管理 ..... 11

7 性能要求 ..... 11

    7.1 误报率 ..... 11

    7.2 漏报率 ..... 12

    7.3 流量监控能力 ..... 12

    7.4 并发连接数监控能力 ..... 12

    7.5 新建 TCP 连接速率监控能力 ..... 12

    7.6 检测时间 ..... 12

附录 A（资料性） 工业控制系统信息物理融合中的威胁 ..... 13

附录 B（资料性） 工业控制系统信息物理融合安全防护措施 ..... 14

参考文献 ..... 15

## 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。

本文件由中国机械工业联合会提出。

本文件由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本文件起草单位：中国科学院信息工程研究所、北京机械工业自动化研究所有限公司、浙江大学、杭州优稳自动化系统有限公司、北京工业大学、上海电力大学、中国科学院声学研究所、奇安信科技集团股份有限公司、中国信息通信研究院、中国科学院沈阳自动化研究所、浙江中控技术股份有限公司、北京东方通科技股份有限公司。

本文件主要起草人：孙利民、石志强、朱红松、闫兆腾、吕世超、陈新、刘俊矫、张雪嫣、孙洁香、王文海、张稳稳、赵璐、赖英旭、孙墨童、谷浩然、王勇、杨军、王勋、陈君、王弢、崔君荣、梁炜、张思超、蒋皓、李艺、倪平、陆卫军、章维、李志、孙玉砚、李红、文辉、路晓、崔婷婷。

# 工业控制系统的信息物理融合异常 检测系统技术要求

## 1 范围

本文件规定了融合信息空间和物理空间的工业控制系统异常检测技术架构、功能模块、功能要求及性能要求。

本文件适用于工业控制安全厂商、设备生产厂商研制高效的信息物理融合异常检测设备。

## 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 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
- GB/T 20275—2013 信息安全技术 网络入侵检测系统技术要求和测试评价方法
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- GB/T 36323 信息安全技术 工业控制系统安全管理基本要求
- GB/T 36324—2018 信息安全技术 工业控制系统信息安全分级规范

## 3 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

**工业控制系统 industrial control system; ICS**

一类用于工业生产的控制系统的统称。

注：它包含 SCADA、DCS 和其他一些常见于工业部门与关键基础设施的小型控制系统（如 PLC）等。

### 3.2

**信息物理融合 cyber-physical fusion**

将 ICS 中的指令、状态信息和真实物理系统相结合的过程。

注：具体体现为将 ICS 中生产控制设备中的物料流、信息流、能量流相结合。

### 3.3

**信息物理系统 cyber-physical system; CPS**

一个综合计算、网络 and 物理环境的多维复杂系统。

注：通过通信技术、计算机技术和控制技术的有机融合与深度协作，实现大型工程系统的实时感知、动态控制和信息服务。

### 3.4

**异常 abnormal**

故障、意外或攻击行为导致的系统出现异于正常或已有基线的情况。

注：包括恶意代码感染、网络攻击、固件篡改、控制逻辑篡改等信息安全事件，以及设备故障、误操作、能耗超出正常阈值、时序超出正常范围、状态统计数据超出正常范围等功能安全事件。

3.5

**异常检测    anomaly detection**

对 ICS 发生的异常进行检测的过程。

3.6

**误用检测    misuse detection**

一种能检测模式库中已涵盖的入侵行为或不可接受的行为的方式。

注：在误用检测中首先定义异常系统行为，然后将所有其他行为定义为正常，主要假设是具有能够被精确地按某种方式编码的攻击。通过捕获攻击及重新整理，可确认入侵活动是基于同一弱点进行攻击的入侵方法的变种。

3.7

**信息流    information flow**

ICS 控制设备中的系统控制指令和设备状态等数据。

3.8

**物料流    material flow**

物质流

在 ICS 中原材料或半成品加工、检验、装配、试验、存储等过程数据。

3.9

**能量流    energy flow**

能耗流

ICS 中的原材料或半成品在整个生产过程中所产生的能量数据。

3.10

**脆弱性    vulnerability**

可能被一个或多个威胁利用的资产或控制的弱点。

[来源：GB/T 29246—2017, 2.89]

3.11

**高级持续性威胁攻击    advanced persistent threat; APT**

利用各种先进的攻击手段，对高价值目标进行的有组织、长期持续性网络攻击行为。

注：此种攻击需要长期经营与策划，因此具有极强的隐蔽性和针对性。在 ICS 中，此种攻击会带来更严重的财产损失和威胁。

3.12

**虚假数据攻击    false data injection attack**

利用状态估计器中不良数据辨识方法的局限性，恶意篡改元件的量测值，使控制中心误判当前状态，继而造成工控系统安稳控制措施误动或拒动，从而影响工控系统安全稳定运行的攻击行为。

注：通过恶意篡改设备中的数据而实施的攻击，都可视为虚假数据攻击。

3.13

**ARP 毒药攻击    ARP poisoning**

对 ARP 缓存表进行篡改，导致发送给正确主机的数据包被发送给另外一台由攻击者控制的主机的攻击行为，也称 ARP 欺骗(ARP spoofing)。

3.14

**内部威胁    insider threat**

内部人利用获得的信任或授权做出损害授信组织合法利益的行为。

注：内部威胁不仅仅是内部成员的有意或无意导致的损失，还包括一些外部伪装成内部成员的攻击。

3.15

**告警 alert**

当异常发生时,异常检测系统向授权管理员发出的紧急通知。

3.16

**误报 falsepositive**

异常检测系统在未发生异常时告警,或者发出错误的告警信息。

3.17

**漏报 falsenegative**

当攻击发生时异常检测系统未告警。

4 缩略语

下列缩略语适用于本文件。

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

CIP:通用工业协议(Common Industrial Protocol)

CPU:中央处理器(Central Processing Unit)

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

MAC:媒体存取控制(Media Access Control Address)

OPC:面向对象链接与嵌入的过程控制协议[Object Linking and Embedding(OLE) for Process Control]

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

SCADA:监视控制与数据采集系统(Supervisory Control and Data Acquisition)

SIS:安全仪表系统(Safety Instrumented System)

VPN:虚拟专用网络(Virtual Private Network)

WIA-FA:工业自动化无线网络(Wireless Networks for Industrial Automation-Factory Automation)

5 系统概述

5.1 系统架构

工业控制系统信息物理融合异常检测系统基本结构如图 1 所示,主要分为 3 个部分:感知层、网络层和控制层。感知层主要是由传感器、执行器等 ICS 现场设备组成,如阀门、开关等。感知层中的传感器作为 CPS 中的末端设备,主要采集物理环境中具体信息和状态信息形成流数据,通过网络层发送传输到控制层,同时接受来自控制层返回的相应的信息,感知层设备在感知执行物料流的同时完成生产的过程中会产生相应的能耗变化形成能量流。网络层是连接信息世界和物理世界的桥梁,主要实现信息流的实时传输。控制层主要是由具有逻辑控制的工控设备和上位机组成,如 SCADA、DCS、PLC 等,根据接收的感知层信息流进行相应的分析,将控制指令下发给感知层设备控制生产工艺,并形成物料流数据。感知层和控制层设备同时对应 CPS 框架的物理层,网络层对应 CPS 框架的网络层。

针对 CPS 框架下“物料流、信息流、能量流”之间的消耗关系,异常检测系统中的数据采集模块对现场的流量、故障、网络等数据进行采集。异常检测模块通过生成受保护 ICS 的物料流、信息流、能量流实时关系基线和正常情况,构建异常检测匹配模型,当不匹配时即出现异常,如产生设备故障或遭受外部攻击等。响应和告警模块根据检测出的异常不同类型生成相应的响应结果,传递给检测结果处理模块进行最终的异常处置。异常检测过程中所有的运行过程都应完成日志记录、管理控制 and 安全管理,保

证异常检测系统自身的稳定性、可用性和安全性。

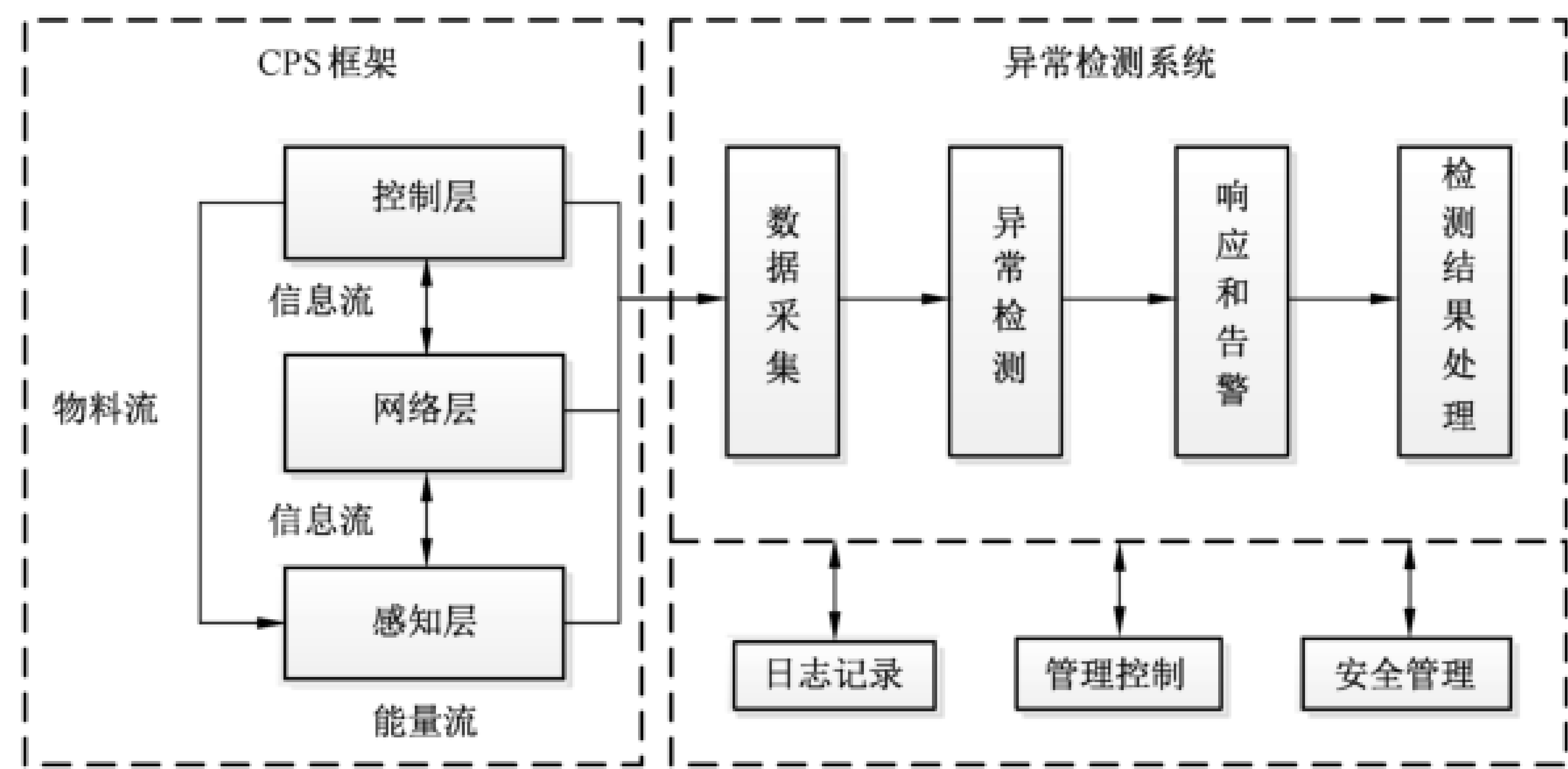


图 1 信息物理融合异常检测架构图

5.2 功能模块

本文件按照工业控制系统信息物理融合异常检测的安全功能要求的强度,将工业控制系统信息物理融合异常检测产品分为基本级和增强级,如表 1 所示。工业控制系统信息物理融合异常检测安全保障应符合 GB/T 18336.3—2015 的相关要求。安全功能强弱和安全保障要求高低是等级划分的具体依据。其中,基本级安全功能要求应具备 GB/T 22239—2019 中的第二级安全保护能力;增强级安全功能要求应具备 GB/T 22239—2019 中第三级安全保护能力。在增强级中新增的要求会通过加粗黑体标识。

表 1 安全功能要求等级划分

| 安全功能要求 |              | 基本级 | 增强级 |
|--------|--------------|-----|-----|
| 数据采集   | 感知层数据采集      | *   | * * |
|        | 网络层数据采集      | *   | * * |
|        | 控制层数据采集      | *   | * * |
|        | 协议解析         | *   | * * |
|        | 入侵诱捕         | —   | *   |
|        | 其他安全防护设备数据接入 | —   | *   |
|        | 事件辨别扩展接口     | —   | *   |
| 异常检测   | 感知层异常检测      | *   | * * |
|        | 网络层异常检测      | *   | * * |
|        | 上位机异常检测      | *   | * * |
|        | 控制器异常检测      | *   | * * |
|        | 工艺参数异常检测     | —   | *   |
|        | 行为异常检测       | *   | * * |
|        | 威胁事件监测       | *   | * * |
|        | 基于白名单规则分析    | —   | *   |
|        | 自学习          | *   | * * |

表 1 安全功能要求等级划分（续）

| 安全功能要求                               |             | 基本级 | 增强级 |
|--------------------------------------|-------------|-----|-----|
| 响应和告警                                | 事件响应        | *   | *   |
|                                      | 安全告警        | *   | *   |
|                                      | 告警方式        | *   | *   |
|                                      | 告警处置        | *   | * * |
|                                      | 与其他安全防护设备联动 | —   | *   |
|                                      | 全局预警        | *   | *   |
| 检测结果处理                               | 结果记录        | *   | *   |
|                                      | 结果可视化       | *   | *   |
|                                      | 统计分析        | *   | * * |
|                                      | 关联分析        | —   | *   |
|                                      | 可选查阅        | *   | *   |
|                                      | 报告输出        | *   | *   |
| 管理控制                                 | 唯一性标识       | *   | *   |
|                                      | 管理员角色定义     | *   | *   |
|                                      | 基本鉴别        | *   | *   |
|                                      | 鉴别失败处理      | *   | *   |
|                                      | 超时锁定或注销     | *   | *   |
|                                      | 升级管理        | *   | * * |
| 安全管理                                 | 接口安全管理      | *   | *   |
|                                      | 安全状态监测      | *   | *   |
|                                      | 存储安全        | *   | *   |
|                                      | 分布式部署       | —   | *   |
|                                      | 自身安全保障      | *   | *   |
| 日志管理                                 | 日志生成        | *   | *   |
|                                      | 日志内容        | *   | *   |
|                                      | 日志存储        | *   | * * |
| 注：“*”表示具有该要求，“* *”表示要求有所增强，“—”表示不适用。 |             |     |     |

6 功能要求

6.1 数据采集

6.1.1 感知层数据采集

系统应具有感知层中信息流、物料流和能量流的数据识别和采集能力，应识别和采集的数据包括：

- a) 固件版本等感知层设备的软件资产数据；



- b) 厂商名称、设备类型、设备型号等资产硬件设备指纹信息；
- c) 能耗、温度等能耗信息；
- d) 原料、材料、半成品进行加工或处理过程中的物料信息；
- e) 生产流程、参数工艺等工艺信息。

#### 6.1.2 网络层数据采集

系统应支持接入网络层数据，具体应支持以下功能：

- a) 异常流量采集，例如网络扫描、强力攻击、木马后门攻击、拒绝服务攻击、勒索病毒传播等；
- b) MAC 头、IP 头在内的全部网络流量分组的采集；
- c) 通过无线方式连接的网络数据接入，如 5G、Wi-Fi、工业无线 WIA-FA 等。

#### 6.1.3 控制层数据采集

系统应支持接入控制层数据的接入，具体应支持以下功能：

- a) 组态软件、web 组件、操作系统等资产软件信息的探测识别；
- b) 厂商名称、设备类型、设备型号等资产硬件设备信息的探测识别；
- c) 接入工业控制设备自身功能故障异常数据介入功能，如 PLC、DCS、SCADA、SIS 等；
- d) 数据批量导入导出。

#### 6.1.4 协议解析

系统应支持网络层通信协议和工业控制协议的解析，具体应支持以下功能：

- a) 网络通信协议解析，如 HTTP、FTP、SNMP、Telnet 等；
- b) 工业控制协议解析，如 OPC、S7、IEC61850、IEC60870-5-104、CIP、DNP3、Modbus 等；
- c) 现场总线数据无扰监听和解析；
- d) 自定义工控协议格式规约解析；
- e) 工控协议内容深度解析，包括工控协议的操作类型、操作对象、操作范围等参数。

#### 6.1.5 入侵诱捕

系统应支持接入蜜罐捕获的入侵源数据或相同功能产品获取到的威胁情报。

#### 6.1.6 其他安全防护设备的数据接入

系统应支持接入防火墙、安全审计设备、漏洞扫描、VPN 等受防护目标中部署的其他安全防护设备的数据。

#### 6.1.7 事件辨别扩展接口

系统应具备事件辨别扩展接口，具体应支持以下功能：

- a) 以云服务等方式接收安全应急通报机构共享的安全事件或威胁情报；
- b) 将发现的异常向安全应急通报机构上报。

### 6.2 异常检测

#### 6.2.1 感知层异常检测

系统应支持对感知层设备的异常检测，具体应支持以下功能：

- a) 对现场设备违规外联、违规接入等异常检测；

- b) 感知层设备断线、损坏等功能异常检测；
- c) 感知层设备遭受未授权访问、数据篡改等异常检测。

注：具体感知层威胁及对应防护措施见附录 A、附录 B。

### 6.2.2 网络层异常检测

系统应支持对网络层通信协议和工控协议的通信流量异常检测，具体应支持以下功能：

- a) 监测受保护网段内的地址、端口的报文流量和字节流量；
- b) 非正常报文流入工业控制网络的检测；
- c) 网络通信中存在的嗅探、非法监听等检测；
- d) 对无线通信的异常流量检测；
- e) IPv4/v6 双栈协议中的异常流量检测；
- f) 隐匿通信通道检测。

注：具体网络层威胁及对应防护措施见附录 A、附录 B。

### 6.2.3 上位机异常检测

系统应支持对控制层中工程师站、操作员站等上位机的异常检测，具体应支持以下功能：

- a) 对上位机下行的控制指令进行异常检测；
- b) 对上位机与其他业务管理的信息系统之间信息流的异常检测；
- c) 对上位机违规开启端口或服务、异常配置、异常组态变更的检测；
- d) 识别上位机上违规使用应用软件情况，如游戏、视频、社交应用、远程控制等；
- e) 对上位机中 USB 等外设违规接入检测；
- f) 发现误操作、恶意操作等违规操作行为；
- g) 对上位机中 CPU、内存等资源使用情况设置正常阈值，当出现异常使用情况时具备实时检测能力。

### 6.2.4 控制器异常检测

系统应支持控制层控制设备的异常检测，具体要求包括：

- a) 应支持对控制设备的数据内容和负载信息等异常检测；
- b) 应支持对控制设备自身故障、SIS 告警的异常检测；
- c) 应支持对控制设备感染恶意代码的异常检测；
- d) 应支持对控制设备的误用检测；
- e) 应具备控制器中控制点位、控制值、控制器状态信息等异常检测能力。

### 6.2.5 行为异常检测

系统应具备对受保护目标 ICS 中攻击入侵行为的检测能力，具体要求包括：

- a) 应支持网络扫描行为检测，如端口扫描、口令破解等；
- b) 应支持对网络攻击行为检测，如 IP 欺骗、IP 碎片攻击、ARP 毒药攻击、虚假数据攻击、序列攻击、中间人攻击、重放攻击等；
- c) 应支持对通信协议、软件、嵌入式设备等已知漏洞攻击行为检测；
- d) 应支持对 ICS 中误操作、工程师站组态变更、操控指令变更、PLC 下装、固件升级等关键行为异常的检测；
- e) 应支持对 ICS 存在的 APT 攻击检测；
- f) 应支持对通信协议、软件、嵌入式设备等未知漏洞攻击行为检测；

- g) 应具有攻击者、攻击方式、攻击链路的分析和刻画能力。

#### 6.2.6 工艺参数异常检测

系统应具备对受保护 ICS 中业务工艺生产状态异常检测能力,具体应支持以下功能:

- a) 对物料流异常、能耗异常的检测;
- b) 对工艺参数变更、重要工艺故障的检测;
- c) 对未按规定的造成加工件或成品严重影响的异常检测。

#### 6.2.7 威胁事件检测

系统应具备对实时检测受保护目标 ICS 威胁事件的能力,具体要求包括:

- a) 应支持网络安全威胁事件实时检测,例如:缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、敏感信息泄露等;
- b) 应支持受保护目标 ICS 安全管理中存在不合规的异常检测,具体要求应符合 GB/T 36323 的相关规定;
- c) 应支持内部威胁检测;
- d) 应具有威胁类型和危害程度的评估能力;
- e) 应支持潜在或隐藏的威胁事件检测;
- f) 应支持对接收到的共享威胁情报在受保护目标 ICS 中进行检测识别;
- g) 应具有威胁对象定位、影响范围评估的能力;
- h) 应具有威胁来源追溯的能力。

#### 6.2.8 基于白名单规则分析

系统应具有基于白名单规则分析能力,具体应支持以下功能:

- a) 对 PLC、SCADA、RTU 等控制器的白名单检测;
- b) 针对控制器的数据包进行快速有针对性的捕获与深度解析;
- c) 结合白名单对不符合规则的控制器的异常进行告警。

#### 6.2.9 自学习

系统应具有自学习能力,具体应支持以下功能:

- a) 基于自学习模式,对 ICS 中的协议和流量行为进行被动式的学习,从而自动生成相关策略;
- b) 自学习模式下的网络流量行为不产生告警;
- c) 自学习模式的功能包括资产识别、网络基线和工控协议白名单。

### 6.3 响应与告警

#### 6.3.1 异常分类

系统应具备对检测到的异常进行分类的能力,具体应支持以下功能:

- a) 对不同类型的信息安全类异常进行分级,分级方式见 GB/T 36324—2018 中 5.1;
- b) 对不同类型的功能安全类异常进行分级,分级方式见 GB/T 36324—2018 中 5.2.2;
- c) 对应的响应方式,包括告警、阻断和排除等。

#### 6.3.2 安全告警

系统应支持在检测到异常时产生告警,并向用户提供处理建议。

### 6.3.3 告警方式

系统应具备根据异常的风险类型向用户提供不同的告警方式,具体应支持以下功能:

- a) 通过管理界面告警;
- b) 向网络管理人员发送告警邮件或手机短信;
- c) 向网管中心发送 SNMP Trap 信息。

### 6.3.4 告警处置

系统应具备告警处置功能,具体要求包括:

- a) 在受保护目标 ICS 遭受到严重影响入侵事件或故障时,应具备对关键路径上的目标提供处置建议的能力,避免或限制对受保护目标 ICS 造成更严重的结果;
- b) 系统应在受保护目标 ICS 遭受到严重影响入侵事件时,具有阻断能力。

### 6.3.5 排除响应

系统应在失效告警或误报异常时,提供用户排除响应的操作选项。

### 6.3.6 全局预警

系统应具备对受保护目标 ICS 的自动化全局智能预警能力。

### 6.3.7 与其他安全防护设备联动

系统应具备在检测到异常时,与防火墙、网关、安全审计等其他安全防护设备联动响应能力。

## 6.4 检测结果处理

### 6.4.1 结果记录

系统应具备对异常检测的结果进行实时记录的能力,提供用户对结果可视化展示、可选查阅和结果报告输出。

### 6.4.2 统计分析

系统应具有统计分析能力,具体要求包括:

- a) 应支持包括通信流量、上位机、控制器、行为、威胁等异常的统计分析;
- b) 应支持工艺参数等异常的统计分析;
- c) 应具有挖掘受保护目标 ICS 中潜藏或未知异常的能力。

### 6.4.3 关联分析

系统应具备对物料流、信息流、能量流多维数据一致性异常关联分析的能力。

### 6.4.4 结果可视化

系统应具有异常检测结果可视化能力,具体应支持以下功能:

- a) 提供图形化展示模块和仪表盘功能;
- b) 提供全面实时的信息展示;
- c) 从资产、协议流量、网络威胁等多个视角展示;
- d) 结合实时曲线、动态占比、动态排行等显示模块。

#### 6.4.5 可选查阅

系统应具有异常检测结果可选查阅能力,具体应支持以下功能:

- a) 提供用户按照时间、类型、IP 地址等不同属性的单选项查询;
- b) 多属性联合查询。

#### 6.4.6 报告输出

系统应支持用户以 PDF、Word、HTML 等不同格式的输出检测结果报告。

### 6.5 管理控制

#### 6.5.1 唯一性标识

系统应保证用户具有唯一的标识,用于区分不同用户的身份和权限。

#### 6.5.2 管理员角色定义

系统应具有管理员角色定义功能,具体应支持以下功能:

- a) 针对管理员角色建立配置、授权、审计相互独立的账号机制;
- b) 将超级用户特权集进行划分,分别授予配置管理员、安全管理员和审计管理员;
- c) 实现配置管理、安全管理和审计管理功能的同时,也保证管理员权限的隔离。

#### 6.5.3 基本鉴别

系统应具有基本鉴别功能,具体应支持以下功能:

- a) 用户在登录、配置、修改口令或升级时具备要求身份鉴别的能力;
- b) 首次使用时,强制要求用户修改默认口令或设置口令;
- c) 支持对口令的强度进行检查的能力,避免用户使用弱口令或默认口令。

#### 6.5.4 鉴别失败处理

系统应具备用户鉴别尝试失败的阈值,确保用户身份鉴别失败超出阈值时,系统支持阻断进一步鉴别的请求。

#### 6.5.5 超时锁定或注销

系统应具备用户登录超过规定时间阈值时,对用户进行超时锁定或注销当前用户登录状态,确保用户重新进行身份鉴别。

#### 6.5.6 升级管理

系统应具有自身升级管理的能力,具体要求包括如下:

- a) 应支持离线和在线两种升级方式;
- b) 应支持系统版本或规则库版本老旧影响使用的情况下向用户发送告警信息;
- c) 应具备对升级来源进行校验的能力。

### 6.6 安全管理

#### 6.6.1 接口安全管理

系统应具有接口安全管理能力,具体应支持以下功能:

- a) 提供用户不同接口,如工业控制设备故障接入、检测数据或结果导入导出、其他安全防护设备数据接入、系统升级等;
- b) 遵循最小化原则,确保接口在使用时才被用户开启。

#### 6.6.2 安全状态监测

系统应支持对自身安全状态的实时监测能力,具体应支持以下功能:

- a) 发现系统存在的版本未升级、规则库老旧等问题时,提醒用户升级;
- b) 发现穷举攻击、未授权访问等安全验证绕过问题时,提醒用户更改口令。

#### 6.6.3 存储安全

系统应具备安全保护机制,具体要求包括:

- a) 应支持不同类型数据的防篡改功能;
- b) 应支持存储空间监测功能,保证系统中数据的存储安全。

#### 6.6.4 自身安全保障

系统自身其他安全保障应符合 GB/T 20275—2013 中 6.2.4 的要求。

#### 6.6.5 分布式部署

系统应具备分布式部署的受保护 ICS 同步关联的异常检测分析能力。

### 6.7 日志管理

#### 6.7.1 日志生成

系统应具备自动对数据采集、异常检测、响应与告警、检测结果处理和管理控制过程中产生的操作和数据进行自动化生成日志的能力。

#### 6.7.2 日志内容

系统保存的日志应包括检测到异常的具体日期、时间、用户标识、描述、告警信息和用户响应等内容,同时应包括系统的登录、升级、配置等操作内容。

#### 6.7.3 日志存储

系统日志存储应具备安全存储的功能,具体要求包括:

- a) 应在受限访问权限的情况下进行安全存储;
- b) 应具备安全加密、备份和恢复能力;
- c) 日志存储时间不应少于 6 个月。

## 7 性能要求

### 7.1 误报率

误报率要求如下:

- a) 系统应将误报率控制在应用许可的范围 10% 以内;
- b) 不应受保护的 ICS 产生影响;
- c) 支持 IPv6 网络环境下工作的系统误报率应满足上述指标。

## 7.2 漏报率

漏报率应符合 GB/T 20275—2013 中规定的相关指标。

## 7.3 流量监控能力

系统单口监控流量应符合 GB/T 20275—2013 中规定的相关指标。

## 7.4 并发连接数监控能力

系统单口监控并发连接数应符合 GB/T 20275—2013 中规定相关指标。

## 7.5 新建 TCP 连接速率监控能力

系统单口监控新建 TCP 连接速率应符合 GB/T 20275—2013 中规定的相关指标。

## 7.6 检测时间

系统的异常检测时间性能要求如下：

- a) 功能安全类异常检测时间应不高于 1 s；
- b) 信息安全类异常检测时间应不高于 3 s。

## 附录 A

(资料性)

## 工业控制系统信息物理融合中的威胁

## A.1 感知层安全威胁

感知层主要由各种物理传感器、执行器等组成,是整个物理信息系统中信息的来源。为了适应多变的环境,网络节点多布置在无人监管的环境中,因此易被攻击者攻击。常见的针对感知层的攻击方式有:

- a) 数据破坏:攻击者未经授权,对感知层获取的信息进行篡改、增删或破坏等;
- b) 信息窃听:攻击者通过搭线或利用传输过程中的非法监听,造成数据隐私泄露等问题;
- c) 节点捕获:攻击者对部分网络节点进行控制,可能导致密钥泄露,危及整个系统的通信安全。

## A.2 网络层安全威胁

网络层一般要接入网络,而接入网络本身就会给整个物理信息系统带来威胁。一方面,作为链接感知层和控制层的数据传输的通道,其中传输的信息易成为攻击者的目标;另一方面,由于接入网络,网络层易受到攻击。网络层的主要安全威胁如下:

- a) 拒绝服务攻击:攻击者通过先向服务器发送大量请求,使得服务器缓冲区爆满而被迫停止接受新的请求,使系统崩溃从而影响合法用户的使用;
- b) 选择性转发:恶意节点在接收到数据后,不全部转发所有信息,而是将部分或全部关键信息在转发过程中丢掉,破坏了数据的完整性;
- c) 方向误导攻击:恶意节点在接收到数据包后,对其源地址和目的地址进行修改,使得数据包沿错误路径发送出去,造成数据丢失或网络混乱。

## A.3 控制层安全威胁

控制层中数据库中存放着大量用户的隐私数据,因此在这一层中一旦发生攻击就会出现大量隐私泄漏的问题。针对应用层的主要威胁有。

- a) 用户隐私泄漏:用户的所有的数据都存储在控制层中的数据库中,其中包含用户的个人资料等隐私的数据都存放在数据库中,一旦数据库被攻陷,就会导致用户的隐私产生泄漏,造成很严重的影响。
- b) 恶意代码:恶意代码是指在运行过程中会对系统造成不良影响的代码库,攻击者一般会将这些代码嵌入到注释中,脚本一旦在系统中运行,就会对系统造成严重的后果。
- c) 非授权访问:对于一个系统,会有各种权限的管理者,比如超级管理员,对该系统有着最高的操作权限,一般管理员对该系统有部分的操作权限。非授权访问指的就是攻击者在未经授权的情况下不合理的访问本系统,攻击者欺骗系统,进入到本系统中对本系统执行一些恶意的操作就会对本系统产生严重的影响。
- d) 软件设计缺陷:工业控制软件的开发人员不同的编程能力、对功能的理解能力,以及软件供应链环节使用存在潜在隐患的开源程序、第三方组件等,导致软件开发存在设计缺陷。这些设计缺陷一旦被攻击者挖掘到漏洞,可被用于发起拒绝服务攻击、验证绕过、非授权访问或窃取敏感数据等。如勒索病毒事件、国际知名 SCADA 软件被曝光一系列远程命令执行高危漏洞等。



附 录 B  
(资料性)

工业控制系统信息物理融合安全防护措施

B.1 感知层防护措施

感知层主要由各种物理传感器等组成,因此感知层的安全主要涉及各个结点的物理安全。针对感知层可能出现的物理攻击,采取以下安全措施进行相应的保护。感知网络层的物理传感器一般放在无人的区域,缺少传统网络物理上的安全保障,节点容易受到攻击。因此,在这些基础结点上设计的初级阶段就要充分考虑到各种应用环境以及攻击者的攻击手段,建立有效的容错机制,降低出错率。对节点的身份进行一定的管理和保护,对结点增加认证和访问控制,只有授权的用户才能访问相应供应结点的数据,这样的设计能够使未被授权的用户访问无法访问结点的数据,有效地保障了感知网络层的数据安全。

B.2 网络层防护措施

在网络层中采取安全措施的目的就是保障 CPS 通信过程中的安全,主要包括数据的完整性、数据在传输过程中不被恶意篡改,以及用户隐私不被泄露等。具体措施可以结合加密机制、路由机制等方面进行阐述。点对点加密机制可以在数据跳转的过程中保证数据的安全性,由于在该过程中每个节点都是传感器设备,获取的数据都是没有经过处理的数据,也就是直接的数据,这些数据被攻击者捕获之后立即就能得到想要的结果,因此将每个节点上的数据进行加密,加密完成之后再传输可以降低被攻击者解析出来的概率。安全路由机制就是数据在互联网传输的过程中,路由器转发数据分组的时候如果遭遇攻击,路由器依旧能够正确地进行路由选择,能够在攻击者破坏路由表的情况下构建出新的路由表,做出正确的路由选择,CPS 针对传输过程中各种安全威胁,可设计出更安全算法,建设更完善的安全路由机制。

B.3 控制层防护措施

控制层是 CPS 决策的核心部分,所有的数据都是传到控制层处理的,因此要对控制层的数据的安全性和隐私性进行保护。针对控制层的安全措施有以下几种,主要是加强不同应用场景的身份认证,在控制层中,有系统管理员,高级管理员,对于系统,他们的管理权限不同,攻击者可以欺骗系统进而对系统采取不法的操作,因此加强不同应用场景的身份认证可以有效地保护系统使其不受攻击者侵害。

控制层软件部分要考虑供应链全链安全,设计者利用安全代码审计技术,提前对出厂产品进行安全测评;用户单位要引入主动脆弱性挖掘分析技术,提前对使用者的工业控制系统软件进行定期安全分析;第三方安全机构要关注软件新曝光漏洞,及时通报用户更新升级。

参 考 文 献

- [1] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇
-