ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团 体 标 准

T/CAMS XXXX—XXXX

流程工业网络安全防护体系

Network Security Protection System for Process Industry

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国机械工业标准化技术协会　　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。

本文件由中国机械工业标准化技术协会提出。

本文件由中国机械工业标准化技术协会仪器仪表及自动化专业委员会归口。

本文件起草单位：

本文件主要起草人：

流程工业网络安全防护体系

1 范围

本文件规定流程工业的网络安全风险识别、防护设施部署、网络威胁监测、安全措施验证、安全事件响应与处置的通用网络安全要求。

本文件适用于流程工业网络安全防护体系设计、实施与评估。

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—2022 信息安全技术 术语

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 36324-2018 信息安全技术 工业控制系统信息安全分级规范

GB/T 36323-2018 信息安全技术 工业控制系统安全管理基本要求

GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 37962-2019 信息安全技术 工业控制系统产品信息安全通用评估准则

GB/T 37980-2019 信息安全技术 工业控制系统安全检查指南

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 33009.1-2016 工业自动化和控制系统网络安全 集散控制系统（DCS） 第1部分：防护要求

GB/T 33008.1-2016 工业自动化和控制系统网络安全 可编程序控制器（PLC） 第1部分：系统要求

GB/T 26333—2010 信息安全技术 工业控制网络安全风险评估规范

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 术语和定义

下列术语和定义适用于本文件。

3.1 信息安全 information security

对信息的保密性、完整性和可用性的保持。

注：另外，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他性质。

3.2 网络安全 network security

对网络环境下存储、传输和处理的信息的保密性和可用性的保持。

3.3 安全策略 security policy

用于治理某一组织及其系统内管理、保护并分发影响安全及有关元素的资产（包括敏感信息）的一组规则、指导、和实践。

3.4 安全功能 security function

为实现安全要素的要求，并正确实施相应安全策略所提供的功能。

3.5 工业控制系统 industrial control system

在工业部门和关键基础设施中应用于各种工业生产的控制系统。

注：工业控制系统包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，例如可编程逻辑控制器（PLC）。

3.6 攻击 attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

3.7 威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

3.8 流程工业 process industry

指连续生产工业，被加工对象不间断地通过生产设备，经过一系列加工装置使原材料进行规定的化学反应或物理变化，得到最终的产品。

3.9 功能安全 functional safety

指避免由系统功能性故障导致的不可接受的风险。功能安全关注系统故障后的行为,而不是系统的原有功能或性能。

3.10 本体安全 ontological security

指工业控制系统中组成部分的安全，包括工控设备、监控软件等。

3.11 可信机制 trusted mechanism

采用已通过数学证明或彻底测试等方式证实的技术，实现对实体身份和行为的可预期，支持系统安全策略。

3.12 数字孪生 Digital twin

指现实世界物理系统的数字化映射系统，贯穿于物理系统的生命周期过程，并随物理系统同步动态演化。

3.13 高级持续威胁 Advanced Persistent Threat

指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定的目标。

3.14 完整性 Integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

3.15 可用性 Availability

数据或资源能被授权实体按要求访问和使用的特性。

3.16 安全事件 Security incident

系统、服务或网络的一种可识别状态的发生，它可能是对安全策略的违反或防护措施的失效，或未预知的不安全状况。

3.17 流程工业网络 process industrial networks

流程工业网络是指安装在流程工业生产环境中的一种全数字化、双向、多站的通信系统，可能覆盖IT侧和OT侧，，安全涉及多个范畴。

3.18 脆弱性 vulnerability

工控安全的脆弱性是指工控系统在防护措施中和在缺少防护措施时系统所具有的弱点。

4 防护体系概述

本标准针对流程工业网络安全面临的高级持续威胁（APT）风险和信息物理跨域破坏风险，通过全生命周期双安一体化防护保障工业控制系统和生产装置和工艺的安全，落实网络安全等级保护和关基保护制度。

本标准主要包括防护体系总体要求、安全风险识别、防护设施部署、网络威胁监测、安全措施验证、安全事件响应/处置等。本标准在通用工业控制系统网络安全要求基础上进一步明确增强流程工业网络安全的技术要求。

4.1 防护体系架构

流程工业网络安全防护体系应可覆盖典型流程工业全生命周期、集信息安全与功能安全于一体，防护体系架构应采用图1所示架构：安全风险识别、防护设施部署、网络威胁监测、安全措施验证、安全事件响应/处置等5个部分，具体内容如图1所示。

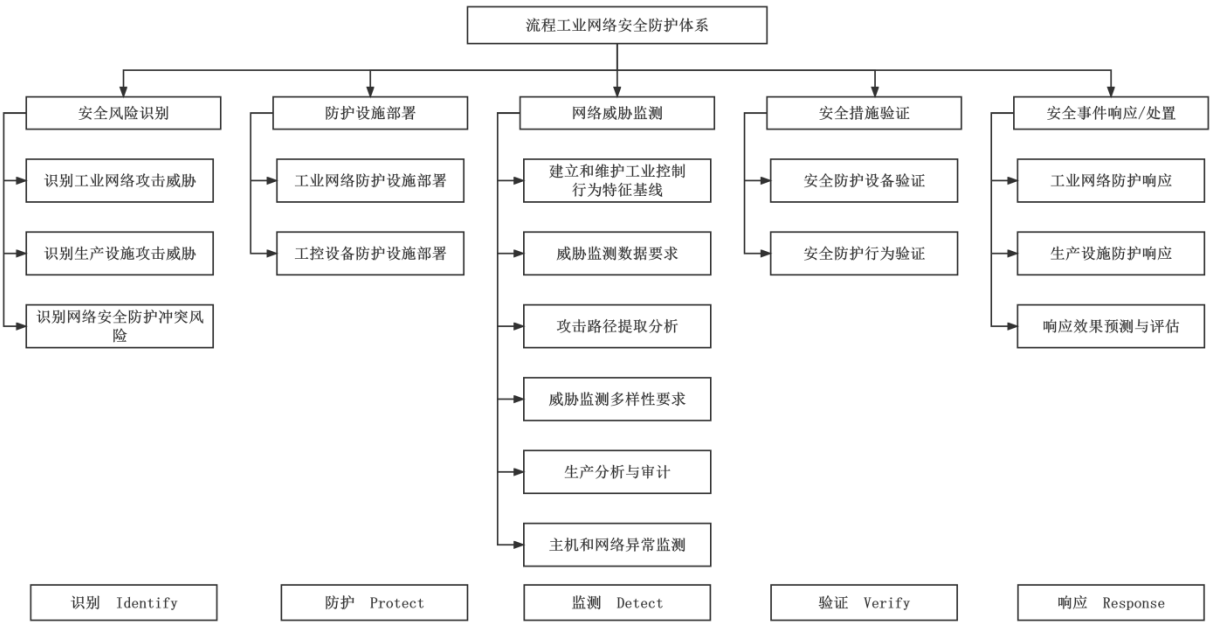

图1 基于IPDvR的网络安全防护体系架构

4.2 防护体系总体防护原则

流程工业网络安全防护体系应遵循如下防护原则：

--将信息安全与功能安全进行有机融合，规避、消除和缓解相互间的冲突，发挥相互间的补充、促进作用；

--识别、阻止、监测针对流程工业装置和工艺的脆弱性利用，对安全事件和处置措施进行联合响应和谨慎验证，防范通过网络形成跨域物理损伤的网络攻击形式。

5 安全风险识别

应将网络攻击脆弱性机理和网络攻击威胁识别纳入企业风险隐患排查。

5.1 识别工业网络攻击威胁

5.1.1 分析对象定义

分析内容应覆盖流程行业生产系统中工业控制网络常见的安全威胁和需要进行识别的网络威胁形式。针对生产系统中工业控制网络的破坏过程及方式，识别工业网络攻击威胁要求主要包括：

--可识别的工业控制网络安全威胁；

--需要进行识别的网络威胁形式。

5.1.2 识别的工业控制网络安全威胁

识别工控网络脆弱性利用包括：

- 利用通信中的脆弱性；
- 利用网络边界脆弱性；
- 利用网络硬件脆弱性；
- 利用网络配置脆弱性；
- 利用无线连接脆弱性。

识别工控设备脆弱性利用包括：

- 利用工控硬件脆弱性；
- 利用工控软件脆弱性；
- 利用应用配置脆弱性。

识别利用防护系统发动网络攻击包括：

- 利用防护系统安全架构脆弱性；
- 利用防护系统安全访问脆弱性；
- 利用防护系统安全处理脆弱性；
- 利用防护系统安全运维脆弱性。

5.1.3 工业互联网攻击路径

识别工业互联网攻击路径包括：

--远程运维带来的远程攻击通道；

--工程师站移动介质带来的跨网攻击通道；

--监控层与制造执行层之间的信息交互通道；

--来自关联的其它（辅助）系统的横移通道；

--通过无线检测、巡检等辅助设施引入的攻击通道。

5.2 识别生产设施攻击威胁

5.2.1 分析对象

识别生产设施攻击威胁覆盖流程行业生产系统中的信息层和物理层的脆弱性（包括：工业控制系统脆弱性和工控网络脆弱性是信息层面的；装置及流程工艺脆弱性是物理层面的），在进行脆弱性分析时着重分析各部分脆弱性的关联性：工业控制系统脆弱性可被工控网络脆弱性攻击，进而利用装置及流程工艺脆弱性。

针对生产设施的攻击威胁旨在破坏生产过程，造成生产停止（或产能下降、产品质量降低）、设施损毁、环境污染、人身伤害或财产损失。识别生产设施攻击威胁包括：

--识别对工业控制系统的网络攻击威胁；

--识别利用工业控制系统对装置和工艺的跨域物理攻击威胁。

5.2.2 识别对装置和工艺的跨域物理攻击威胁

识别对装置和工艺的跨域物理攻击威胁包括：
--人工控制失效；
--监测信息无效；
--生产控制权；
--生产系统被操控；
--自动控制紊乱；
--保护系统被禁用。

5.3 识别网络安全防护冲突风险

5.3.1 分析对象定义

应对流程工业典型安全事件的静态分析，从功能安全和信息安全2个方面，分别开展分析，包括：
--功能安全分析；
--信息安全分析。

6 防护设施部署

6.1 流程工业网络防护设施部署

流程工业网络防护设施部署中的安全设备应不少于图2所示，其中NGU指面向工业嵌入式系统的网络信息安全单元，可信PLC指具备内生安全防护能力的安全可信PLC控制器。

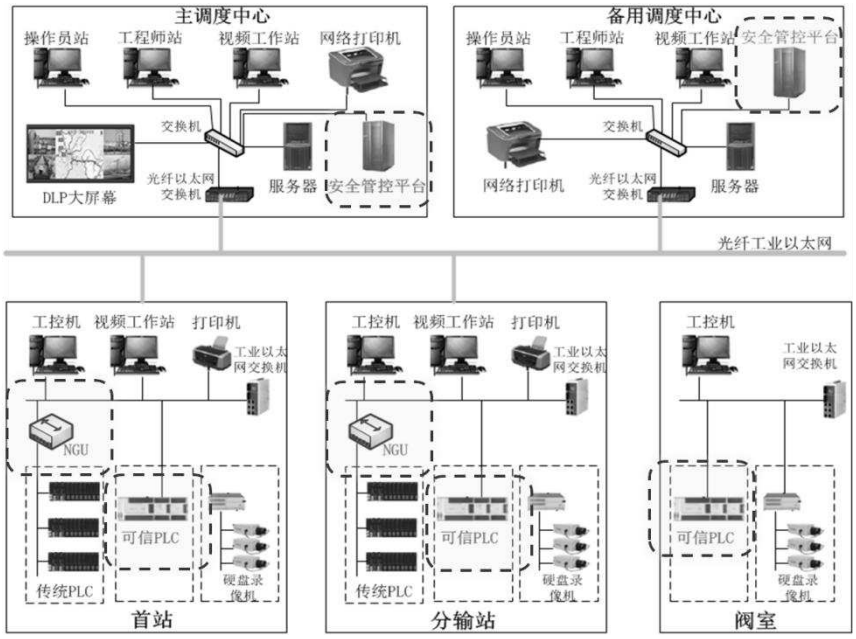

图2 流程工业网络防护设施部署架构图

6.1.1 安全防护内容

流程行业工业网络中网络安全防护设施部署，包括：

--网络分区与边界隔离；

--恶意代码防护技术；

--漏洞发掘和安全监测；

--协议仿真；

--控制装置仿真；

--威胁主动感知要求。

6.1.2 网络分区与边界隔离

安全区域内部的节点具有相同的安全等级和相互的信任关系。工控网可使用不同物理网络、VLAN和路由区将不同的安全区域的业务流进行安全隔离。

6.1.3 恶意代码防护技术

防恶意代码是保护工业网络安全的基本技术，部署的网络防护设备包括：

--白名单软件；

--杀毒软件。

6.1.4 漏洞发掘和安全监测

工业企业可部署所需的监测措施，针对典型网络攻击（病毒传播、DoS）、异常网络行为、设备非授权接入、APT 攻击、关键操作指令、关键工艺参数等进行分析，发现工业控制系统内部及外部存在的安全威胁。可与边界防护措施形成互补、联动，也可为安全事件分析提供证据支撑，进而有效提高整体网络安全防护水平。应对流程行业工业网络中开展漏洞发掘和安全监测等防护设施部署，包括：

--漏洞发掘软件；

--态势感知系统。

6.1.5 协议仿真

流程工业生产系统地外网网络环境中应部署完整的流程工业深度仿真欺骗诱捕系统，实现对APT威胁的主动感知。网络协议范围包括：工业控制系统实时监控协议、现场总线协议、工程师站下装协议、

工程师协同维护网络协议、集成和互联系统之间网络通信协议、系统外部传输网关通信协议。网络协议仿真中常见通用协议蜜罐的实现包括：FTP、Telnet、SNMP、SMTP、TFTP、MQTT、COAP、POP3、OPC、S7、通用计算机网络协议。工控协议仿真中常见通用协议的实现包括：Modbus TCP、DNP3、FINS、S7、Ethernet/IP，需实现指令级别的高交互过程。

6.1.6 控制装置仿真

控制装置仿真中典型工业控制设备包括：前置服务器、历史服务器、RTU、PLC、HMI、保护装置等工控设备蜜罐，其中PLC包括西门子、施耐德、ABB、和利时、欧姆龙、罗克韦尔等主流厂商，实现伪装工控设备与真实设备在协议交互、执行输出方面具备与真实设备同等的交互能力。

6.1.7 威胁主动感知要求

威胁主动感知需可防御不少于5类攻击过程。

6.2 工控设备防护设施部署

6.2.1 设施部署范围及要求

对流程行业工业网络中开展工控设备防护设施部署范围及要求，包括：

--设备安全；

--控制安全；

--数据保护；

--系统安全要求。

6.2.2 设备安全

工业企业需根据自身需求，使用采取措施对设备固件进行安全加固的设备，并建立设备、操作系统漏洞发现和补丁更新机制，确保及时发现相关安全漏洞、进行补丁升级。必要时，采用基于硬件的可信验证技术，为设备的安全启动以及数据传输机密性和完整性保护提供支持。

针对设备本体安全，不可采用外置安全模块，应采取本体内置可信模块。

6.2.3 控制安全

对于控制安全与防护，主要应从控制协议、控制软件和控制功能入手。加强认证授权、协议加密、协议过滤和恶意篡改等方面技术，并在使用前确保开展控制协议健壮性测试、软件安全测试及加固等工作。在恶意代码防护、补丁升级和漏洞修复方面还应建立切实可行的防护机制，确保落实到位。

6.2.4 数据保护

对于工业互联网的数据安全防护，工业企业可采取数据加密、访问控制、身份认证、数据脱敏及业务数据隔离等多种防护措施协同联动的方式进行防护，覆盖包括数据收集、传输、存储、处理、脱敏和销毁等全生命周期。

6.2.5 系统安全要求

整体安全防护系统需通过信息安全等级SL2认证及功能安全完整性SIL2认证。

7 网络威胁监测

7.1 建立和维护工业控制行为特征基线

7.1.1 分析对象定义

应对流程工业生产过程建立和维护工业控制行为特征基线，利用流程工业连续性、周期性等特点，基于工艺过程和控制逻辑，结合工业控制网络环境下的数据流变化以及控制协议交互序列，对生产工艺控制过程、生产过程数据变化、控制协议交互序列进行关联分析，通过智能学习算法挖掘控制不变量组

合、事件依赖关系以及过程数据变化的时序特征，进一步通过多核学习、深度学习等智能技术对上述特征进行融合，形成工业特征知识图谱，将工业生产过程中的各种状态节点、状态间迁移关系、导致状态变化的组合条件以图的方式表示。工业生产过程控制行为特征提取所涉及环节包括：

--多维工控数据采集；
--工业特征预处理；
--多维工业特征提取；
--多维工业特征融合；
--控制行为知识图谱构建。

7.1.2 多维工控数据采集

多维工控数据采集涉及内容包括：生产工艺过程、工艺过程数据、工业控制逻辑、工业控制协议。

7.1.3 工业特征预处理

通过不同来源收集到的工控行为相关数据在数据类型、表述方法等各方面会存在差异，在做特征提取建模之前，对工业特征进行预处理，解决不一致性问题。

7.1.4 多维工业特征提取

多维工业特征提取涉及内容包括：工艺过程建模、控制逻辑建模、控制行为建模、控制协议建模、统计学算法和机器学习算法。

7.1.5 多维工业特征融合

多维工业特征融合所考虑方面涉及内容包括：控制不变量组合、时间依赖关系、工艺过程数据变化规律。

7.1.6 控制行为知识图谱构建

控制行为知识图谱构建涉及内容包括：工业生产过程中的各种状态节点、状态间迁移关系、导致状态变化的组合条件。

7.2 威胁监测数据要求

针对不同工艺过程开展安全事件历史数据分析，应充分考虑工艺设备、操作更新等原因带来的数据不一致性问题，选取合适的威胁检测数据采集分析周期。威胁监测数据要求包括：

--威胁监测既要基于实时数据，也要针对历史数据进行分析；
--要保障历史数据的完整性；
--历史数据的采样周期应不小于3个月且不大于12个月。

7.3 潜在攻击路径提取分析

7.3.1 分析对象定义

应对流程行业生产系统中潜在攻击路径提取分析，包括：

--攻击路径生成；
--攻击路径可视化。

7.3.2 攻击路径生成

实时提取现场信息，根据工业网络攻击威胁分析和生产设施攻击威胁分析结果，分析识别和评估攻击路经，攻击路径生成包括：

--攻击路径并行规划：使用多个规划器并行搜索子场景下的所有攻击路径；
--攻击路径合并：将所有攻击路径进行合并生成攻击图。

7.3.3 攻击路径可视化