ICS03.080

|  |
| --- |
| CCSA16 |

DB21

辽宁省地方标准

DB21/TXXXX—XXXX

|  |
| --- |
|  |

工业网络安全态势感知技术规范

Technical specifications for industrial network security situational awareness

（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

辽宁省市场监督管理局　发布

目　次

[1 范围 1](#_Toc20365)

[2 规范性引用文件 1](#_Toc28349)

[3 术语和定义 1](#_Toc14997)

[4 缩略语 2](#_Toc1351)

[5 整体架构 2](#_Toc13633)

[6 数据准备 3](#_Toc22977)

[6.1 数据采集 4](#_Toc16858)

[6.2 数据预处理 5](#_Toc29459)

[6.3 数据存储 5](#_Toc26878)

[6.4 数据传输 6](#_Toc25316)

[6.5 数据共享 6](#_Toc13934)

[7 态势评估与展示 6](#_Toc15250)

[7.1 总体要求 6](#_Toc8848)

7[.2 态势类别 7](#_Toc26949)

[7.3 公网侧态势类别 9](#_Toc26333)

[7.4 企业侧态势类别 9](#_Toc8841)

[8 态势告警与响应 10](#_Toc1014)

[8.1 安全态势告警要求 10](#_Toc7034)

[8.2 事件处置支持要求 10](#_Toc14364)

[9 态势感知系统安全要求 11](#_Toc4474)

[9.1 身份鉴别 11](#_Toc5962)

[9.2 访问控制 11](#_Toc12547)

[9.3 安全审计 11](#_Toc24715)

[9.4 数据安全性 11](#_Toc8524)

[9.5 系统安全防范 12](#_Toc24752)

[参考文献 13](#_Toc3708)

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：东北大学、沈阳华睿博信息技术有限公司、辽宁省先进装备制造业基地建设工程中心、沈阳鼓风机集团股份有限公司、国网辽宁省电力有限公司、中国电子信息产业集团有限公司、中国电子信息产业集团有限公司第六研究所、辽宁艾特斯智能交通技术有限公司、中国烟草总公司辽宁省公司、联通(辽宁)产业互联网有限公司、辽宁谛听信息科技有限公司、三六零安全科技股份有限公司、中国联合网络通信有限公司沈阳市分公司、沈阳绿盟网络安全技术有限公司、北京理工大学、北京圣博润高新技术股份有限公司、沈阳当先科技有限公司、南京估合信息科技有限公司、济南大学等。

本文件主要起草人：姚羽、邵华、郭剑峰、陈莹、郝玉明、胡博、周小明、张尼、吴云峰、黄书鹏、王宇飞、袁辉、吕生亮、杨道青、金阳、李士炜、梁艳、李冬妮、李小川、赵秀峰、李昊、杨巍、纪科、陈贞翔等。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通信地址：辽宁省沈阳市皇姑区北陵大街45-2号

归口管理部门联系电话：024-86913384

标准起草单位通信地址：辽宁省沈阳市和平区文化路三巷11号

标准起草单位联系电话：024-83687392

工业网络安全态势感知技术规范

1. 范围

本文件规定了工业网络安全态势感知系统的技术要求，包括数据准备、态势评估与展示、态势告警与响应、系统安全要求。

本文件适用于指导工业网络安全态势感知系统的设计、开发、建设、检测、部署和维护工作。

1. 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 20985.1 信息技术 安全技术 信息安全事件管理 第1部分:事件管理原理

GB/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 25069-2022 信息安全技术 术语

GB/T 30279 信息安全技术 网络安全漏洞分类分级指南

GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求

1. 术语和定义

以下术语和定义适用于本文件。



网络安全态势感知 network security situation awareness

通过采集网络流量、资产信息、日志、漏洞信息、告警信息、威胁信息等数据,分析和处理网络行为及用户行为等因素,掌握网络安全状态,预测网络安全趋势,并进行展示和监测预警的活动。

[来源：GB/T 42453-2023]

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。

[来源：GB/T 25069-2022,3.628]

预警 warning

针对即将或正在发生的网络安全事件或威胁，提前或及时发出的警示。

[来源：GB/T 25069-2022,3.739]

1. 缩略语

下列缩略语适用于本文件：

IM:即时通讯(Instant Messaging）

IP:互联网协议(Internet Protocol)

OPC:用于过程控制的OLE(OLE for Process Control)

OPC DA:OPC实时数据访问(OLE for Process Control Data Access)

OPC UA:OPC统一体系架构(OLE for Process Control Unified Architecture)

1. 整体架构

工业网络安全态势感知系统框架主要包括数据汇聚、态势评估与展示、态势告警与响应和系统安全要求。其中，数据准备包括数据采集、数据预处理、数据存储、数据传输、数据共享；态势评估与展示包括资产态势、脆弱性态势、安全事件态势、行为态势；态势告警与响应包括安全态势告警、事件处置支持系统安全要求包括身份鉴别、访问控制、安全审计、数据安全性、系统安全防范。工业网络安全态势感知系统框架如图1。

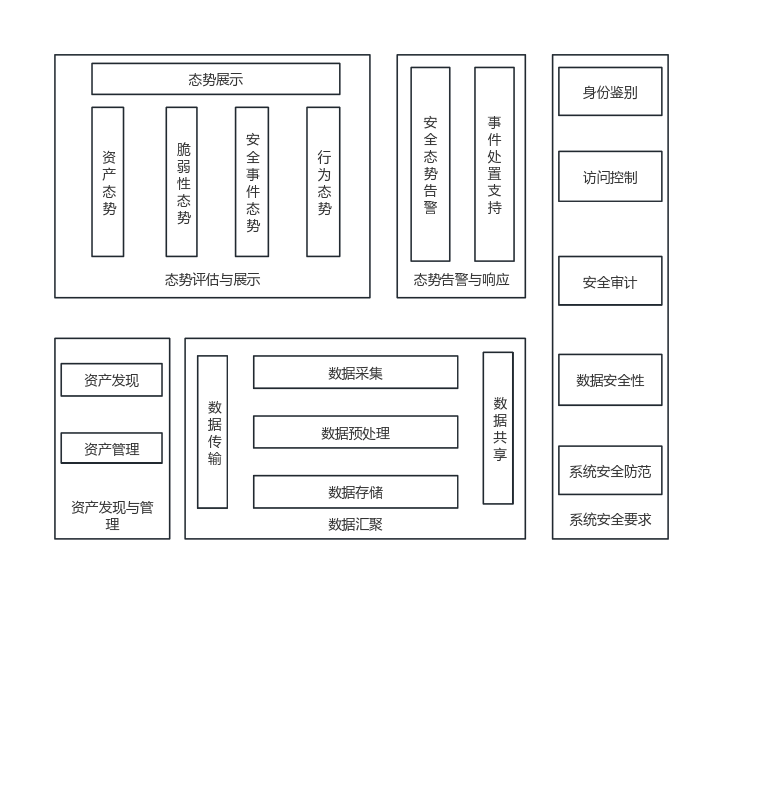


图1 工业网络安全态势感知系统框架

1. 资产发现与管理
   1. 资产发现

本项要求包括：

1. 应能够识别的资产种类包括但不限于工业互联网平台、联网设备及系统、工业APP、工业数据等；
2. 应支持IP自动发现、指纹自动识别和数据同步的方式在系统数据库中录入资产信息，实现对资产流量监视、端口状态统计、协议状态统计、资产活跃状态监视、资产访问行为监视等管理方式；
3. 应能够随时对资产可能出现的变更或退网方式及时响应。
   1. 资产管理

本项要求包括：

1. 应建立资产台账，对资产清单、资产统计信息进行维护管理；
2. 应对所有资产建立资产画像，包括但不限于基本信息、硬件信息、操作系统信息、变更记录、运行信息、端口和服务、资产会话、漏洞、告警、不合规配置项、资产风险值等信息；
3. 应能够自动梳理资产，自动生成资产台账，基于资产基线、网络会话，记录资产变更，监测未知资产接入。
4. 数据汇聚
   1. 数据采集
      1. 总体要求
         1. 数据来源

工业网络安全态势感知系统应能采集以下两种以上不同来源的数据：

1. 资产数据；
2. 网络流量数据；
3. 安全漏洞数据；
4. 安全事件数据；
5. 日志数据；
6. 第三方提供的数据。
   * + 1. 采集能力

工业网络安全态势感知系统应具有以下采集能力：

1. 应具有实时采集工业网络数据包的能力；
2. 应同时支持被动采集(如代理、探针、共享)和主动采集(如扫描)两种方式；
3. 应支持通过接口或人工导入等方式采集第三方数据；
4. 应支持配置过滤规则对采集数据内容进行筛选；
5. 采集协议应满足GB/T 42453-2023中的要求，并支持SYSLOG、SNMP Trap、FTP、SFTP、JDBC、ODBC、Net flow等多种日志采集方式；
6. 采集内容应满足GB/T 42453-2023中的要求。
   * 1. 公网侧数据采集
        1. 数据来源

公网侧数据来源应包括：

1. 工业网络平台的数据；
2. 工业网络企业数据。
   * + 1. 采集能力

应具有实时采集暴露在互联网侧的工业网络资产(工控系统、物联网、应用站点)数据的能力。

* + 1. 企业侧数据采集
       1. 数据来源

企业侧数据来源应包括：

1. 网络设备、终端设备和安全设备产生的日志数据；
2. 网络设备、终端设备和安全设备产生的告警数据。
   * + 1. 采集能力

企业侧数据采集应具有以下采集能力：

1. 应具有实时采集企业侧工业资产(网络设备、终端设备、安全设备)数据的能力；
2. 应具有定期采集工业设备及终端日志的能力；
3. 应支持深度解析常用工控协议（例如Modbus TCP、Siemens S7、OPC DA、OPCUA、DNP3、Profinet、Ethernet/IP、IEC104等），将原始的通信数据转化为可读性强、易于理解和处理的格式，能够对每个用户命令做出详细分析，如果出现IP碎片，可以对数据包进行重装还原，然后再进行分析，协议分析大大降低了入侵检测中常见的误报现象。
   1. 数据预处理

数据预处理应满足以下要求：

1. 应能根按照GB/T 42453-2023中的要求对收集的数据进行筛选、变换、补全、标记；
2. 应能对数据进行分类分级：安全漏洞分类遵守GB/T 30279的规定，安全事件分类分级参照GB/Z 20986；
3. 应能根据需要对数据进行实时处理和离线处理。
   1. 数据存储

数据存储应满足以下要求：

1. 应能存储结构化数据、半结构化数据和非结构化数据；
2. 存储内容应满足GB/T 42453-2023中的要求；
3. 应能存储原始数据、预处理后的数据和威胁情报库、地理信息库等第三方数据；
4. 应能自动存储处理安全事件所产生的相关业务数据；
5. 数据存储时间应满足GB/T 42453-2023中的要求，其中日志数据应至少保存6个月；
6. 应能保证存储数据的可用性、完整性和保密性；
7. 应能检索所存储数据，并提供检索接口；
8. 应能存储工业设备（例如，各品牌PLC、RTU、IED等）指纹库、工业恶意行为指纹库（例如，Siemens S7、Modbus、Bacnet、Ethernet/IP等协议）、工业恶意组织指纹库、工业网络漏洞库等专业知识库。
   1. 数据分析

应根据GB/T 42453-2023中的要求对网络攻击、资产风险、安全事件进行分析。

* 1. 数据传输

数据传输应满足以下要求：

1. 应能对数据传输状态进行监控，能对传输任务进行启动、停止操作；
2. 应具备数据传输缓存功能，确保网络中断或阻塞时数据不丢失；
3. 应能保证传输数据的完整性和保密性，保证重要数据的实时性。
   1. 数据共享

数据共享应满足以下要求：

1. 应能将工业网络重大安全事件、重大漏洞等数据上报给上级监管系统；
2. 应能将工业网络重大安全事件、重大漏洞、处置办法等数据发送给其它态势感知系统；
3. 应能接收其它系统共享的工业网络重大安全事件、重大漏洞、处置办法等数据；
4. 应能对共享数据进行脱敏；
5. 应能增、删、改数据共享用户信息，能设置数据共享用户的权限；
6. 数据共享过程应可跟踪、可追溯、可审计。
7. 态势评估与展示
   1. 总体要求

本项要求包括：

1. 应建立工业网络安全态势评估体系，描述工业网络的安全态势；
2. 应能建立工业网络数据分析模型，对采集的工业网络数据进行分析计算，识别网络脆弱性、安全事件、用户行为等；
3. 应支持包括但不限于网络设备（如上位机、工业安全网关、工控安全审计、主机安全卫士）的入侵检测，并进行日志关联和量化分析；
4. 应覆盖DCS网络、PLC网络、数控机床DNC网络等不同行业应用场景的工控系统；
5. 应采用流量镜像的方式对工控网络进行全流量数据监听，不主动发包，不对工业网络做任何修改；
6. 应能评估两种以上工业网络安全态势，包括但不限于资产态势、流量态势、运行态势、攻击态势、横向威胁态势、脆弱性态势、安全事件态势、行为态势等；
7. 具有关联关系的不同种类安全态势，应能够实现信息共享和联动展示。
   1. 专题态势评估与展示
      1. 资产态势评估

本项要求包括：

1. 应能实时获取当前工业网络资产总数，并按区域、类型、重要程度分布进行统计；
2. 应能对每个工业网络资产的型号、版本、运行状态等进行识别；
3. 应能对资产的IP的地址以及开放的端口等进行识别；
4. 应能对工业网络资产的安全状况进行分析，包括资产存在的威胁和脆弱性类型、数量等。
   * 1. 流量态势评估

应满足GB/T 42453-2023中的要求。

* + 1. 运行态势评估

应满足GB/T 42453-2023中的要求。

* + 1. 攻击态势评估

应满足GB/T 42453-2023中的要求。

* + 1. 横向威胁态势评估

应基于系统通信基线模型，对不同业务系统、不同区域之间的信息流动进行监测，对跨区通信、非法接入、非法外联行为进行统计分析，及时发现信息泄露、越权访问和违规操作行为。

* + 1. 脆弱性态势评估

本项要求包括：

1. 应具备工业网络安全漏洞库,漏洞库包含国家权威机构发布的工业网络安全漏洞，能够对工业网络资产进行漏洞发现和漏洞匹配；
2. 应能对各类工业设备的操作系统、应用和第三方组件存在的常见漏洞进行监测；
3. 应能展示漏洞总体分布、存在高危漏洞的资产、漏洞类型分布、漏洞危害等级等；
4. 应能对工业设备系统安全配置的脆弱性进行识别,分析和指出工业网络资产存在的安全配置的脆弱性。
   * 1. 安全事件态势评估

本项要求包括：

1. 应具有从采集的数据中分析出安全事件，对安全事件进行多维度(种类、地域、威胁类型、资产等)分类处理的能力；
2. 应具有对不同安全事件进行分类告警的能力，如特别重大事件、重大事件、较大事件、一般事件等；
3. 安全事件必须包含发生时间、IP地址、区域、域名、事件类型、数量和危害等级等信息；
4. 应支持对同类安全事件进行合并。
   * 1. 行为态势评估

本项要求包括：

1. 应能支持对异常行为规则的自定义；
2. 应能及时发现全网的异常行为(如访问频次超限、访问流量超限、权限异常提升、账户异常更改、日志异常变化、文件异常外发、非法外联、非法访问、非法文件下载等)，并进行统计分析。
   * 1. 态势展示

本项要求包括：

1. 应满足GB/T 42453-2023中的要求；
2. 应能实时展示安全态势，包括但不限于以下几种资产态势：脆弱性态势、安全事件态势、行为态势；
3. 应能同时展示多种安全态势；
4. 应能通过设置过滤条件选择展示特定类型的安全态势；
5. 应能对安全态势进行历史回溯与展示，回溯时间可以设置；
6. 应能展示跟安全态势相关的关键数据，如资产、脆弱性、安全事件、异常行为的列表与统计值。
   1. 公网侧态势评估与展示

本项要求包括：

1. 应具备工控系统、物联网、应用站点特征库，能够识别暴露在互联网侧的设备和站点；
2. 应能对工业互联网资产所对应的单位、行业进行统计。
   1. 企业侧态势评估与展示
      1. 资产态势

本项要求包括：

1. 应具备工业设备特征库，能够识别接入的各种类型的工业设备；
2. 应能实时呈现生产网内工业网络资产的拓扑结构。
   * 1. 安全事件态势

本项要求包括：

1. 应支持对工业设备所使用的各类通信协议网络数据流的解析,具备工业系统攻击代码特征库，并具备工业控制系统攻击代码特征库更新能力；
2. 应具备工业控制系统网络数据恶意攻击行为检测分析能力,能从采集的数据中分析出安全事件并及时告警；
3. 应能根据告警信息，综合工业控制系统的多方面约束和目标，制定最优安全策略及具体的实施方案。
   * 1. 行为态势

本项要求包括：

1. 应能通过网络流量分析工业企业用户行为和设备行为，包括用户行为、设备通信情况等；
2. 应能实时获取并展示当前企业内部的异常情况，包括异常告警时间、受害资产、关键操作、源IP、目的IP。
3. 态势告警与响应
   1. 安全态势告警要求
      1. 总体要求

本项要求包括：

1. 应全面监测系统内的违规操作、攻击入侵、异常行为；
2. 应支持对海量事件进行去重、归并、关联分析处理；
3. 应能支持短信、邮件或IM等告警方式；
4. 应能在安全事件、漏洞或异常行为发生时，及时发送告警信息；
5. 应建立告警分级机制，对不同级别的安全态势进行不同的告警；
6. 应结合其他安全设备事件、资产和网络基线模型、资产库和漏洞库信息进行分析减少误告警；
7. 应基于基线模型和会话数据，深入挖掘长时间历史数据，能够发现到单点设备忽视的潜在威胁，如跨区通信、未知设备接入行为、异常远程登录等。
   * 1. 企业侧态势告警

本项要求包括但不限于：

1. 应能结合威胁情报进行态势告警，包括但不限于：高危漏洞被利用、设备被攻击事件等；
2. 应能显示告警与厂区资产的对应关系；
3. 应提供对外预警接口，同步预警信息至各类工业网络安全监管系统。
   1. 事件处置支持要求
      1. 总体要求

本项要求包括：

1. 可按照GB/T 20985.1所确定的阶段开展网络安全事件处置工作；
2. 应参考GB/Z 20986对网络安全事件进行分类、分级；
3. 应能提供事件处置过程中需要的基础数据信息；
4. 应能通知网络安全事件发生单位执行处置工作；
5. 应能接受通知，协助处置网络安全事件；
6. 应能对网络安全事件的处置流程进行跟踪和记录；
7. 应将网络安全事件的处置过程信息和结果输入到工业网络安全态势感知系统中；
8. 应能对事件处置情况进行统计分析。
   * 1. 企业侧事件处置支持

应在处置时特别关注生产功能安全和生产连续性要求。

1. 态势感知系统安全要求
   1. 身份鉴别

本项要求包括：

1. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
2. 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
3. 应强制用户首次登录时修改初始口令；
4. 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。
   1. 访问控制

本项要求包括：

1. 应提供访问控制功能，对登录的用户分配账户和权限；
2. 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
3. 应授予不同账户为完成各自承担任务所需的最小权限,并在它们之间形成相互制约的关系。
   1. 安全审计

本项要求包括：

1. 应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
2. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
3. 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
4. 应确保审计记录的留存时间符合法律法规要求。
   1. 数据安全性

本项要求包括：

1. 应采用密码技术保证重要数据在传输过程和存储过程中的保密性和完整性,包括但不限于鉴别数据、重要业务数据等；
2. 应提供重要数据的数据备份与恢复功能；
3. 应保证存有重要数据的存储空间被释放或重新分配前得到完全清除。
   1. 系统安全防范

本项要求包括：

1. 应遵循最小安装的原则，仅安装需要的组件和应用程序；
2. 应关闭不需要的服务、端口，关闭默认共享和高危端口；
3. 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
4. 应保护态势感知系统免受恶意代码攻击,例如采用免受恶意代码攻击的技术措施或可信验证机制。

参　考　文　献

1. GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求
2. YD/T 4214-2023 工业互联网安全态势感知系统技术要求

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_