ICS 25.040
UNSPSC 32.15.20
CCS N 10

团 体 标 准

T/UNP 267—2024

DCS 工控网络安全审计分析系统技术要求

Technical requirement for DCS industrial control network security audit analysis system

2024－11－14 发布 2024－11－14 实施

中国联合国采购促进会 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。

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。

本文件由中国联合国采购促进会提出并归口。

本文件起草单位：东方电气中能工控网络安全技术（成都）有限责任公司、中科企服（深圳）科技有限公司、中科信泰（深圳）信息技术限公司、辽宁省友策网络技术有限公司。

本文件主要起草人：张宇、梁海、李秋宏、李斌、缪远银、赵东、程钰、林姿邑、冯鹏飞、杨刚、杨凯宇、郑祥、史媛媛、谭艺玲、刘芮歌。

引　言

为助力中国企业参与国际贸易，推动企业高质量发展，中国联合国采购促进会依托联合国采购体系，制定服务于国际贸易的系列标准，这些标准在国际贸易过程中发挥了越来越重要的作用，对促进贸易效率提升，减少交易成本和不确定性，确保产品质量与安全，增强消费者信心具有重要的意义。

联合国标准产品与服务分类代码（UNSPSC，United Nations Standard Products and Services Code）是联合国制定的标准，用于高效、准确地对产品和服务进行分类。在全球国际化采购中发挥着至关重要的作用，它为采购商和供应商提供了一个共同的语言和平台，促进了全球贸易的高效、有序发展。

围绕UNSPSC进行相关产品、技术和服务团体标准的制定，对助力企业融入国际采购，提升国际竞争力具有十分重要的作用和意义。

本文件采用UNSPSC分类代码由6位组成，对应原分类中的大类、中类和小类并用小数点分割。

本文件UNSPSC代码为“32.15.20”，由3段组成。其中：第1段“32”为大类，表示“电子元件及用品”，第2段为中类，“15”表示“自动化控制装置及组件及附件”，第3段为小类，“20”表示“过程控制或成套自动化系统”。

DCS 工控网络安全审计分析系统技术要求

1 范围

本文件规定了DCS工控网络安全审计分析系统的系统架构、功能要求、性能要求、接口要求、数据要求、安全要求、运维要求及评价改进。

本文件适用于DCS工控网络安全审计分析系统的设计、开发、应用和维护。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 系统架构

DCS工控网络安全审计分析系统设计遵循分层架构原则，系统架构见图1，应包括以下内容：

a) 应用层：负责实现主要业务功能，包括九元组解析、DCS协议解析、IT白名单、OT白名单、报文存储、流量转换、轮询读取、工艺点表、边缘计算、实时预警输出等模块；

b) 运维层：负责系统的日常监控、故障处理与性能优化，确保系统的高效稳定运行；

c) 支撑层：为系统提供操作系统、数据库及中间件等基础服务，支持应用层的正常运行；

d) 网络层：保障系统各模块之间的高效通信和数据的安全传输；

e) 硬件层：提供服务器和存储设备等硬件资源，确保系统的计算能力和数据存储需求；

f) 安全层：通过权限管理、数据加密及安全审计等措施，确保系统和数据的安全；

g) 接口层：提供标准化接口，支持与外部系统的数据交互与协同工作。

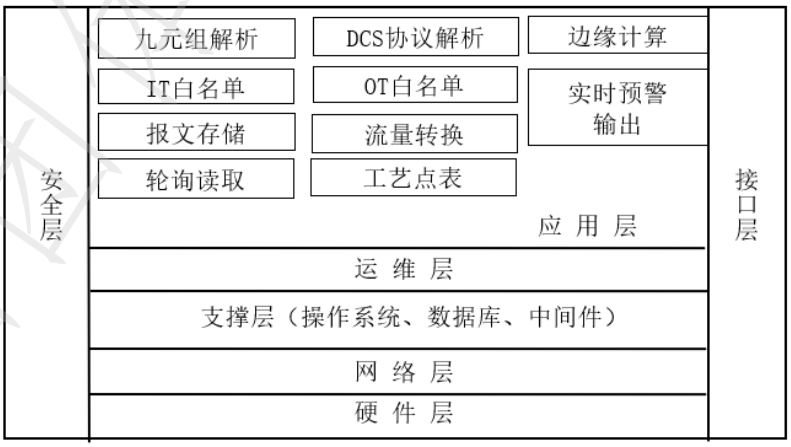

图 1 DCS 工控网络安全审计分析系统架构

5 功能要求

5.1 九元组解析模块

解析网络流量中的九元组特征信息。解析的九元组特征信息应包括：

a) 源 MAC 地址；

b） 目的 MAC 地址；
c） 源 IP 地址；
d） 目的 IP 地址；
e） 源目的端口；
f） 协议号；
g） 服务类型；
h） 接口索引。

5.2 DCS 协议解析模块

解析以太网数据包中的DCS工控协议信息。

5.3 IT 白名单模块

管理工控网络中的合法资产及合法资产产生的IT层通信行为，并实时验证九元组解析模块解析的九元组特征信息，若验证成功，则不进行处理，若验证失败，则存储该条九元组特征信息所对应的原始通信报文。

5.4 OT 白名单模块

管理工控网络在工业生产中各工程师站、操作员站的合法操作，并实时验证DCS工控协议信息中工程师站、操作员站的操作信息，若验证成功，则不进行处理，若验证失败，则存储该DCS工控协议信息所对应的原始通信报文。

5.5 报文存储模块

存储IT白名单模块和OT白名单模块验证失败时的原始通信报文。

5.6 流量转换模块

将九元组特征信息和DCS工控协议信息映射成边缘计算模块能识别的点表信息。

5.7 轮询读取模块

与DCS控制器通信，轮询读取DCS控制器中的工艺参数并映射成边缘计算模块能识别的点表信息。

5.8 工艺点表模块

根据能源装备运行机理、网络安全脆弱性、工艺过程变量建立网络安全保护策略。

5.9 边缘计算模块

根据工艺点表模块建立的网络安全保护策略对流量转换模块和轮询读取模块的点表信息进行审计分析，并判断是否有网络入侵，若有入侵，则输出预警信息。

5.10 实时预警输出模块

根据预警信息触发报警指令、能源装备紧急停机指令或超驰指令。

6 性能要求

6.1 接入速率

事件入库速率不应小于13000 EPS。

6.2 处理能力

系统每秒审计数量不应少于80000条。

6.3 无故障时间

系统平均无故障时间不应少于100000 h。

7 接口要求

7.1 设计原则

接口设计的基本原则包括但不限于：

a) 安全性原则：提供多种安全可靠的技术手段，保证接口数据的安全；
b) 开放性原则：采用通用的接口设计标准，保证与其他系统的互联互通；
c) 灵活性原则：根据业务变化，灵活调整接口容量与性能；
d) 松耦合原则：减少提供方的业务系统对接口服务实现的依赖性。

7.2 接口开发

接口开发要求包括但不限于：

a) 接口名称：接口的中文名称宜包含提供方名称、共享信息名称和接口分类等信息；
b) 接口方式：一般包括 WebService 和 REST 两种方式，若为 REST 方式，应标明 REST 操作；
c) 接口方法：命名应采用大小写混合的形式，以小写字母开头，名称中其他单词的首字母以大写字母开头，不宜使用下划线分割单词；
d) 接口测试：接口应对信息共享协同平台开放测试权限，并提供测试用例；
e) 接口授权：提供方授权的接口应管控参数 ApiKey；
f) 接口参数：
    1) REST 类型的服务接口，应在 Header 里传入授权验证相关的参数，不应使用信息共享协同平台保留的参数名 AppKey、AppSecret、ApiKey、ApiSecret，POST 方式的接口支持在 Body 中传递 Application/JSON 格式的参数；
    2) WebService 类型的服务接口，不应在 Header 传递参数，应在 Body 中进行传递；
    3) 传递参数为中文字符时，应采用 Utf-8 编码。
g) 返回数据：
    1) 接口注册时应标明接口的返回格式；
    2) 返回数据应采用固定的格式封装，通常为 xml、JSON 等。

7.3 接口发布

接口发布时，应准确填写接口描述信息。接口描述信息包括但不限于接口概述、接口名称、接口分类、接口方式、接口地址、接口授权、接口方法、输入输出参数及接口实例等。接口主要描述信息填写要求包括但不限于：

a) 接口概述：应描述出接口的提供方和功能；
b) 接口授权：应确定服务授权方，服务授权方包括信息共享协同平台和提供方；
c) 输入参数：针对每个接口方法，应给出参数名、参数说明、类型、约束等输入信息；
d) 输出参数：针对每个接口方法，应给出返回值格式等输出信息；
e) 接口实例：提供方应提供服务接口实例，并标注返回参数含义等信息。

7.4 接口更新

提供方若因业务变更，需对交换数据进行变更时，应在不影响使用的原则下对已发布的服务接口更新，接口更新时应保留原版本。服务接口更新要求包括但不限于：

a) 应提前在信息共享协同平台进行更新备案，说明服务更新的计划停止时间、重新启动时间、变更内容等；
b) 不应在工作时间内进行服务接口更新；
c) 不应变更输入、输出参数。

7.5 授权验证

应通过信息共享协同平台分配的接口密钥、访问令牌等方式对调用服务申请进行授权验证。

8 数据要求

8.1 数据采集

8.1.1 全面性

应采集DCS工控网络中的各种数据，包括网络流量数据、设备状态数据、系统日志数据、用户操作日志等，实现对工控网络活动的全方位监测。支持对不同类型工控协议进行解析，并提取关键信息用于审计。

8.1.2 实时性

应具备实时采集数据的能力。对关键设备和重要操作的监测，应达到毫秒级的数据采集响应。

8.1.3 准确性

保证采集数据准确无误。采用可靠的数据采集技术和校验机制，并对采集数据进行格式标准化处理便于后续分析和处理。

8.2 数据传输

8.2.1 安全性

采用加密传输技术，保障数据在传输过程中的保密性和完整性，防止被窃取、篡改或破坏。建立安全的传输通道，如VPN或专用网络，限制数据传输的访问权限，仅授权设备和用户可访问传输中的数据。

8.2.2 稳定性

确保数据传输稳定，不应因网络故障或传输中断导致数据丢失。采用可靠传输协议和数据缓存机制，在网络出现问题时应自动恢复传输。对数据传输进行实时监测，及时发现并解决传输中的问题。

8.2.3 高效性

优化数据传输效率，减少传输时间和带宽占用。采用数据压缩技术和并行传输方式，提高数据传输速度。根据数据重要性和紧急程度，设置不同传输优先级，确保关键数据及时传输。

8.3 数据存储

8.3.1 大容量

具备足够存储容量，能存储大量工控网络安全审计数据。根据工控网络长期运行和数据积累情况，存储系统应具备可扩展性。采用分布式存储技术，提高存储可靠性和性能。

8.3.2 安全性

对存储数据进行加密处理，保护数据保密性。采用访问控制技术，限制对存储数据的访问权限，仅授权用户可查看和使用数据。定期对存储数据进行备份，防止数据丢失，备份数据应存储在安全位置，确保发生灾难时可恢复数据。

8.3.3 索引和查询

建立高效索引机制，便于用户快速查询和检索审计数据。支持多种查询方式，如关键字查询、时间范围查询、设备查询等。提供数据可视化功能，将存储数据以直观图表形式展示，便于用户分析和理解。

8.4 数据备份

8.4.1 定期备份

制定合理数据备份计划，定期对存储数据进行备份。备份频率应根据数据重要性和变化频率确定，确保数据安全性和可恢复性。备份数据应存储在不同物理位置，防止因单一存储设备故障导致数据丢失。

8.4.2 完整性验证

进行数据备份时，应进行完整性验证，确保备份数据准确和完整。采用校验和哈希值等技术对备份数据进行验证。定期对备份数据进行恢复测试，确保需要时能成功恢复数据。

8.4.3 自动化备份

实现数据备份自动化，减少人工干预和错误。采用专业备份软件和工具，设置备份策略和任务，自动执行备份操作。

8.5 数据管理

8.5.1 权限管理

建立数据管理权限体系，划分不同用户对数据的访问权限和操作权限。仅经过授权的用户可进行数据查询、分析、修改和删除等操作。对用户操作进行审计和记录，确保数据安全性和合规性。

8.5.2 数据清理

定期对存储数据进行清理，删除过期和无用数据，释放存储空间。制定数据清理策略，确保清理过程不影响数据完整性和可用性。对清理数据进行备份，便于需要时恢复。

8.5.3 数据分析

提供强大数据分析功能，对采集的工控网络安全审计数据进行深入分析。通过数据分析，发现潜在安全威胁和异常行为，为安全决策提供依据。支持多种数据分析方法和工具，如统计分析、关联分析、机器学习等。

8.5.4 数据报告

生成详细数据报告，向用户展示工控网络安全状况和审计结果。报告应包括数据采集情况、安全事件分析、风险评估等内容。支持定制化报告，用户可根据需求选择报告内容和格式。

9 安全要求

9.1 网络安全

9.1.1 采用防火墙、入侵检测系统等网络安全设备，保护数据采集系统与外部网络的连接安全。
9.1.2 对网络通信进行加密，确保数据在传输过程中的保密性和完整性。
9.1.3 限制网络访问权限，被授权的用户和设备才能访问数据采集系统。

9.2 数据安全

9.2.1 在数据传输过程中，应保证数据的安全性，包括数据传输加密、身份认证、完整性保护和可追溯性等方面。
9.2.2 对采集到的数据进行加密存储，防止数据泄露。
9.2.3 对数据进行访问控制，被授权的用户才能访问特定的数据。

9.3 安全审计

9.3.1 应记录以下内容：

a) 访问控制；
b) 请求错误；
c) 操作系统事件；
d) 控制系统事件；
e) 备份；
f) 存储事件；
g) 配置更改；
h) 潜在侦查活动；

i） 审计日志事件等。

9.3.2 单个审计记录应包括：

a） 时间标识；
b） 源；
c） 分类；
d） 事件 ID；
e） 事件结果。

9.3.3 应从系统的多个组件中记录审计信息，集中管理审计事件。

9.3.4 应根据日志管理和系统配置来合理分配审计存储容量，审计记录到达存储容量时，应发出报警信息。

9.3.5 审计处理失败时，应提供报警功能，防止基本服务和功能的丢失。

9.4 用户身份验证和授权

9.4.1 采用强身份验证机制，如用户名和密码、数字证书等，确保用户的身份真实可靠。

9.4.2 对用户进行授权管理，根据用户的角色和权限分配相应的操作权限。

9.4.3 定期更新用户密码，防止密码被破解。

9.5 安全管理

9.5.1 建立安全管理制度，确定安全责任和流程。

9.5.2 对系统进行定期安全审计，发现和修复安全漏洞。

9.5.3 应定期检查和更新系统安全配置，确保系统的安全性，防止系统漏洞被利用。

9.5.4 建立数据备份和恢复验证机制，实施容灾备份和存储介质安全管理，保障存储数据的可用性和完整性。

10 运维要求

10.1 运行

10.1.1 人员培训

应定期对系统管理员和用户进行安全培训，培训内容包括最新的安全威胁、防护措施、安全策略等。通过内部宣传、安全演练等方式，提升员工的安全意识。鼓励员工积极参与安全管理工作，共同维护系统的安全。

10.1.2 自检

10.1.2.1 应定期检查系统的运行状态，包括 CPU 使用率、内存占用率、磁盘空间等。

10.1.2.2 应通过冗余配置、负载均衡等技术手段提高系统的可靠性和稳定性，确保 DCS 工控网络安全审计分析系统持续稳定运行，无频繁故障或异常中断。

10.1.2.3 应定期对系统进行数据校验和比对，确保数据的完整性和一致性。保证系统采集、分析和报告的数据准确无误，防止数据丢失、篡改或错误解读。

10.1.3 存档

应对系统运行维护的时间记录进行存档、留存，每年宜进行1次。

10.2 维护

10.2.1 变更管理

10.2.1.1 应建立 DCS 变更管理策略与规程并实施 DCS 变更管理系统，至少包括：

a） 授权跟踪；
b） 备份与存储；
c） 补丁管理；
d） 防恶意代码升级等。

10.2.1.2 应详细说明变更的内容与位置，并符合变更申请要求。
10.2.1.3 变更的批准与实施应分别交付不同的职能部门或个人进行。
10.2.1.4 应定期对变更管理的安全策略与规程进行评审。

10.2.2 补丁管理

10.2.2.1 应建立并实施补丁管理和反病毒管理程序。
10.2.2.2 应评估并确定补丁安装对系统安全的影响，确保补丁安装后系统满足目标安全等级。
10.2.2.3 系统升级与维护应满足所在网络分区或环境的安全防护要求。

11 评价改进

11.1 评价

11.1.1 建立科学合理的评价指标体系，对系统的性能、功能、用户体验等方面进行评价。
11.1.2 评价指标包括响应时间、准确性、可扩展性、用户满意度等。
11.1.3 定期对系统进行评价，收集用户反馈意见，及时发现问题并改进。

11.2 改进

11.2.1 根据评价结果，制定改进计划，对系统进行优化和升级。
11.2.2 持续关注用户需求和技术发展动态，及时引入新的功能和技术，提高系统的竞争力。
11.2.3 建立用户反馈渠道，及时处理用户的问题和建议，不断改进系统的用户体验。