ICS 75.180.01
CCS P71

团　　体　　标　　准

T/ZISIA 0001-2025

油田工业资产信息化运维管理平台技术要求

Oilfield industrial assets information operation and maintenance management platformTechnical requirements

（发布稿）

2025-04-01 发布　　2025-04-01 实施

中关村网络安全与信息化产业联盟发布　　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。

本文件由中关村网络安全与信息化产业联盟提出并归口。

本文件起草单位：中关村网络安全与信息化产业联盟、大庆油田有限责任公司数智技术公司、大庆油田有限责任公司第四采油厂、国家工业信息安全发展研究中心、长庆油田分公司、机械工业仪器仪表综合技术经济研究所、哈尔滨工业大学（深圳）、烽台科技（北京）有限公司、海洋石油工程股份有限公司特种设备分公司。

本文件主要起草人：王庆伟、徐帅、陈烁文、刘其飞、张哲宇、庄建斌、王晗、赵伟、杨为旭、汝佳、岳志鹏、宋小茜、薛浩、宋养齐、兰鹏博、邹冬、邵小洋、杨丹红、常莘东、王兆国、訾立强、张大强、王伟、王晶、李墨林。

引　言

随着油田企业数字化转型的不断推动，工业资产信息化运维管理技术已成为油田企业数字化转型升级不可或缺的力量。为确保工业资产能够安全、稳定、高效地服务于生产业务，构建一套科学、系统、可操作的信息化运维管理平台显得尤为重要。通过《油田工业资产信息化运维管理平台技术》团体标准的制定，引领并规范油田工业资产信息化运维管理技术的实践。

本标准旨在构建工业资产信息化运维的全方位透明监控体系，实现集中化、可视化与便捷化的信息化运维管理平台。同时通过本团体标准的实施，推动工业资产信息化运维管理技术的规范化发展，提升油田工业资产信息化运维管理水平，助力油田实现自动化运维管理，有效降低安全风险并减少运维人力成本支出。

油田工业资产信息化运维管理平台技术要求

1. 范围

本文件给出了油田工业资产信息化运维管理平台技术框架，规定了该框架中核心组件的技术要求。

本文件适用于油田工业资产信息化运维管理产品、系统或平台等的规划、设计、开发、建设和测评。

2. 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修改版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不标注日期的引用文件，其最新版本适用于本标准。

GB/T 42453-2023　信息安全技术 网络安全态势感知通用技术要求

GB/T 43709-2024　资产管理信息化 数据质量管理要求

GB/T 36626-2018　信息安全技术 信息系统安全运维管理指南

GB/T 22239-2019　信息安全技术 网络安全等级保护基本要求

GB/T 39204-2022　信息安全技术 关键信息基础设施安全保护要求

3. 术语和定义

GB/T 42453-2023、GB/T 43709-2024、GB/T 36626-2018、GB/T 22239-2019、GB/T 39204-2022 界定的以及下列术语和定义适用于本文件。以下术语和定义为本文件补充说明。

3.1 油田工业资产 Industrial assets

指在油田生产中，所运用的工业主机、控制设备、网络设备、数据库、仪器仪表、视频监控设备、防护设备以及油气井及相关设施、辅助设备等。

3.2 组件 Subassembly

指的是构成平台的基本单元或元素。这些组件可以是硬件、软件或软硬件结合体，它们共同协作以实现平台的各项功能。

3.3 模块 Module

指的是具有特定功能或职责的软件组成部分。这些模块共同协作，以实现平台的整体功能。

3.4 资产脆弱性 Asset vulnerability

指一个组织的资产（如设备、系统、软件或数据）在面临外部或内部威胁时所表现出的脆弱程度。

3.5 部署探针 Deploy probes

在网络或系统中安装特定的软件，以监控和分析网络流量或系统状态。

3.6 信息安全运维 Information security operation and maintenance

工业资产在网络中经过授权投入运行之后,确保信息系统免受各种安全威胁所采取的一系列预先定义的活动。

3.7 生产安全运维 Production safety operation and maintenance

在工业生产环境中，对生产环境中工业资产的安全配置进行检查和验证的过程,以确保生产过程的连续性、稳定性和安全性。

3.8 健康度监控 Health Degree Monitoring

主要指通过对资产和设备在网络环境下进行集中式数据采集与监控管理的控制系统进行全面持续监测与评估的过程，旨在确保系统稳定安全并满足业务需求，从而保证其在最佳工作条件下运行。

4. 缩略语

下列缩略语适用于本文件：

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

IP：互联网协议（Internet protocol）

FTP：文件传输协议（File Transfer Protocol）

SMB：服务器信息块（Server Message Block）

5. 油田工业资产信息化运维管理平台技术框架

油田工业资产信息化运维管理平台技术框架，其核心目标在于实现油田信息化运维

管理的全面化与智能化。该平台主要包含以下核心组件：资产识别与发现、工业资产台账、资产台账监控、数据采集与处理、监控告警、运维管理、态势展示界面以及系统安全和应急响应与灾备联动要求。

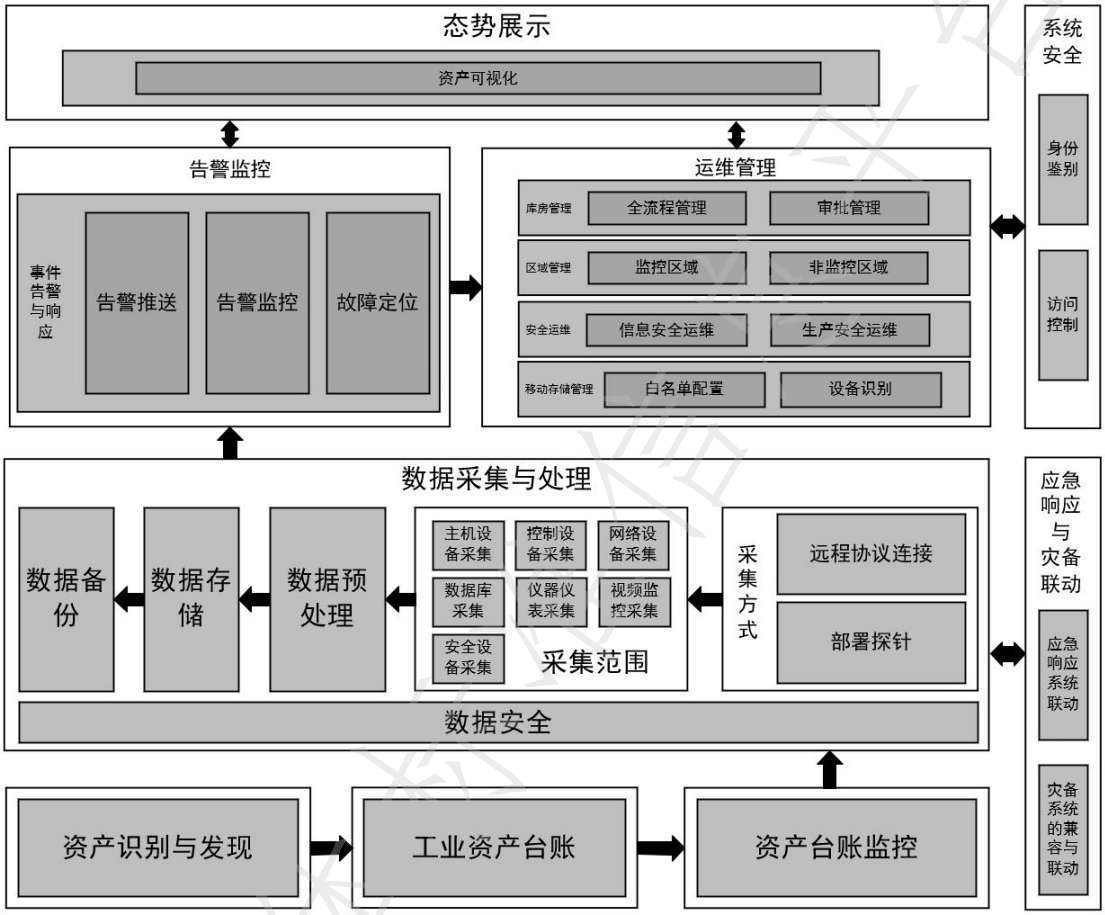

图 1　油田工业资产信息化运维管理平台技术框架

资产识别与发现组件会自动发现并识别油田内的各类工业资产并形成工业资产台账，工业资产台账组件会记录资产的基本信息、位置、状态等，方便资产台账监控组件进行实时监控资产的变化，确保资产信息的准确性和完整性。数据采集与处理组件通过部署在油田现场的采集设备，经由资产识别与发现组件形成的工业资产台账，实时收集油田工业资产其他设备的运行数据、环境数据等，对采集到的数据进行清洗、整理、转换等操作，以满足后续分析和应用的需求；监控告警组件则通过对油田工业资产的运行状态及所采集处理后的数据进行实时监控，及时发现异常情况，当监测到异常情况时，系统自动触发告警，并通过推送消息至相关人员进行处理，随后会对告警数据进行深入分析，找出问题的根源，为后续的运维工作提供指导。运维管理组件通过监控告警分析后的相关数据，进行库房管理模块、区域管理模块、安全运维模块等业务应用的开展；

态势展示组件则根据运维场景，调用数据进行多维度展示。

6. 技术要求

6.1. 资产识别与发现

本项要求包括：

a) 应支持厂商类型等供应链识别；

b) 对资产设置唯一标识编码；

c) 应建立工业资产指纹库；

d) 应支持主动与被动相结合的方法，来发现并确认资产信息；

e) 应支持配置资产识别与发现的范围。

6.2. 工业资产台账

本项要求包括：

a) 应建立油田工业资产台账列表；

b) 应支持资产数量、在离线状态和网络安全威胁的实时数量统计；

c) 应支持列出资产库存清单；

d) 应支持资产监控状态手动启停；

e) 应支持资产台账导入导出等；

f) 应支持对导入导出的操作进行权限管理，授权人员具备编辑修改、导入导出等操作权限，保障台账的精准性。

6.3. 资产台账监控

本项要求包括：

a) 应对每个工业资产设备的型号、版本、运行状态等进行识别校验；

b) 应支持资产台账的变更监控，包括资产的增删改查等属性变更操作；

c) 应支持监控变更类型，如位置变更、权属变更等；

d) 应支持台账信息变更记录，并保存记录日志；

e) 应支持对油田工业资产的健康度监控进行分析，能够预测资产的潜在威胁和故障趋势，并提供相应的维护建议和优化方案。

6.4. 数据采集与处理

6.4.1. 数据采集策略

6.4.1.1. 采集方式

对于不同的数据源，数据采集应支持以下一种或多种采集方式：

a）应支持远程协议连接、部署探针程序等方式主动获取数据源；

b）应支持第三方设备获取数据源；

c）应支持手动导入数据源的数据；

d）应支持对数据采集频率进行设置。

6.4.1.2. 采集范围

6.4.1.2.1. 主机设备采集范围

本项要求包括：

a）应支持采集主机基础配置信息，包括但不限于：IP 地址、MAC 地址、主机型号、运行时间、当前在线状态、操作系统等；

b）应支持采集主机资源配置信息，包括但不限于：CPU、内存、磁盘使用率采集等；

c）应支持采集应用服务信息；

d）应支持采集的已安装应用信息；

e）应支持采集当前设备网卡进出速率；

f）应支持采集主机告警监测。

6.4.1.2.2. 控制设备采集范围

本项要求包括：

a) 应支持采集基础配置信息，包括但不限于：IP 地址、MAC 地址、设备型号、运行时间、当前在线状态以及内存使用情况等；

b) 应支持采集设备运行信息；

c) 应支持采集设备自身故障日志。

6.4.1.2.3. 网络设备采集范围

本项要求包括：

a) 应支持展示设备基础配置信息；

b) 应支持采集设备网口配置信息，包括实时上下行速率等；

c) 应支持采集交换机端口网络接口封禁或启用的状态；

d) 应支持采集交换机光口收发功率监控。

6.4.1.2.4. 数据库采集范围

本项要求包括：

a) 应支持采集基础配置信息，包括但不限于：数据库类型、运行时间、在线状态、版本等；

b) 应支持采集表空间信息；

c) 应支持采集用户名、默认表空间、临时表空间、创建时间、系统权限、对象权限；

d) 应支持采集数据库会话进程信息；

e) 应支持采集连接信息；

f) 应支持操作日志、死锁和锁定用户。

6.4.1.2.5. 仪器仪表采集范围

本项要求包括：

a) 应支持采集仪器仪表类型；

b) 应支持采集传统仪器仪表通信状态、故障状态及故障类型；

c) 应支持采集 wia-pa 智能仪器仪表通信状态、故障状态及故障类型。

6.4.1.2.6. 视频监控设备采集范围

本项要求包括：

a) 应支持采集主流的视频监控设备；

b) 应支持采集网络通信数据、设备状态、设备故障信息等；

c) 应支持基于设备日志生成告警信息、报警类型、报警等级等。

6.4.1.2.7. 安全设备采集范围

本项要求包括：

a) 应支持采集设备基本配置信息等，包括但不限于：IP 地址、MAC 地址、网络状态、产品信息、工作模式、设备日志、运行时间等；

b) 应支持第三方数据对接功能，对采集内容范式化，并上报 Syslog 日志功能等。

6.4.2. 数据预处理

本项要求包括：

a) 应支持基于数据预处理规则对采集的原始数据进行筛选处理；

b) 应验证数据的完整性和一致性，处理重复数据和冗余数据，提高数据的质量；

c) 应支持基于资源库对采集的原始数据进行补全；

d) 应支持根据应用场景判断对数据进行实时处理和离线处理。

6.4.3. 数据存储

本项要求包括：

a) 对敏感数据进行加密存储，确保数据在传输和存储过程中的安全性；

b) 应支持存储实时数据，满足快速查询和实时监控的需求；

c) 应支持存储原始数据、预处理后的数据、历史运行数据；

d) 应支持检索所存储数据，并提供检索接口，自动设置各类数据的存储时间；

e) 应支持存储管理数据，如操作日志、安全策略日志、第三方设备安全日志；

f) 日志数据应至少保存六个月。

6.4.4. 数据备份与恢复

本项要求包括：

a) 应支持定期对数据进行备份；

b) 应支持日志全量导出及备份，应支持通过 FTP、SMB 等方式进行数据备份；

c) 应支持根据日志存储空间和保存时长设定日志清除策略；

d) 应支持网络日志、系统日志的展示列表，并能够根据时间范围、关键字等进行日志搜索定位；

e) 在数据丢失或损坏时，通过备份文件进行数据恢复；

f) 应支持冗余机制，防止数据丢失。

6.5. 监控告警

6.5.1. 告警推送要求

本项要求包括但不限于：

a) 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；

b) 应支持邮件告警功能，提供邮件告警服务器配置及收件人管理功能；

c) 应支持在安全事件、漏洞或异常行为发生时，及时发送告警信息；

d) 应支持即时通讯方式告警；

e) 应支持冗余告警机制，确保在主告警通道失效时，能够通过备用通道（如短信、电话、备用邮件服务器等）及时推送告警信息，避免因单一告警通道故障导致告警信息丢失。

6.5.2. 故障定位要求

本项要求包括但不限于：

a) 应支持节点网络故障诊断；

b) 应支持生产业务系统数据链路故障诊断；

c) 应支持生产业务系统数据波动诊断；

d) 应支持网络攻击事件诊断；

e) 应支持网络攻击链路可视化。

6.5.3. 告警监控要求

本项要求包括但不限于：

a) 应支持告警信息实时刷新呈现，可根据告警等级、告警分类等多个维度进行展示、分类和排序；

b) 应支持告警事件的搜索功能；

c) 应支持 IT 和 OT 设备告警统计；

d) 应支持告警原因分析，可以根据综合监测内容初步分析告警原因；

e) 应支持告警事件闭环处理机制，及时反馈告警事件处理情况；

f) 应支持根据业务需求和设备性能变化，动态调整告警阈值；

g) 应引入工单管理程序，将告警事件自动转化为工单，并分配给相应的处理人员。

6.6. 运维管理

6.6.1. 库房管理

本项要求包括：

a) 应支持设备入库、出库、换新、维修、报废的全流程管理；

b) 应支持配置资产流程管理负责人审批策略；

c) 应支持与工单管理程序集成，通过程序进行审批操作与历史数据备份；

d) 应支持对备件使用情况进行统计分析，包括出入库的新件、备件、报废件变更数量及占比、审批结果进行动态同步。

6.6.2. 区域管理

本项要求包括：

a) 应支持配置监控区域和非监控区域，可根据应用场景区分资产监控区域；

b) 应支持监控区域列表及新增区域配置；

c) 应支持资产的区域配置转移，能够对资产所在区域进行灵活配置和修改。

6.6.3. 安全运维

6.6.3.1. 信息安全运维

本项要求包括：

a) 应支持基于采集内容自定义配置信息安全运维检查，如检查与业务无关用户、指令、进程、检查数据是否被篡改、检查内部应用是否被攻击或滥用、检查磁盘利用率过高、检查串网互联、外网互联、检查高危端口访问、开放脆弱性端口等自定义检查项；

b）应支持对油田工业资产进行信息安全运维，包括远程访问与共享安全访问、控制与身份验证、未启用密码最短留存期、最小长度及复杂性策略、入侵检测、流量监控与分析、故障响应和性能评估、检查日志文件大小异常、检查是否存在暴力破解、检查非业务 IP 访问登录数据库、数据库暴力破解等；

c）应支持对设备安全（硬件设备安全、软件设备安全）、数据安全（数据备份安全、数据传输安全、数据存储安全、数据使用安全）、网络安全（网络设备安全）、应用安全（应用数据安全、应用操作安全）等进行信息安全运维；

d）应支持对防护设备的日志分析包括：日志接收时间、设备 IP、日志分类、协议等；

e) 应支持定期进行安全风险评估，识别网络中存在的潜在安全威胁和漏洞；

f) 应支持安全事件响应，生成安全事件的报告、分析、处置和跟踪流程;

g) 应支持基于采集内容自定义配置信息安全运维检查项，包括检查与业务无关的用户、指令、进程，检查数据是否被篡改，检查内部应用是否被攻击或滥用，检查磁盘利用率过高，检查串网互联、外网互联，检查高危端口访问及开放脆弱性端口等。

6.6.3.2. 生产安全运维

本项要求包括：

a) 应支持对设备生产状态异常行为规则的自定义；

b) 应支持定期对油田工业资产进行配置核查，及时识别和纠正不符合安全标准的配置；

c) 应支持对异常行为，如生产数据缺失、生产数据中断、工作模式变更、运行状态、资源使用、权限异常提升、用户异常更改、文件异常下载、非法下载、日志异常变化等分析记录，并进行统计分析。

6.6.4. 移动存储设备管理

本项要求包括：

a) 应支持主动扫描工业资产是否接入未授权USB介质；

b) 应支持对使用的存储设备进行识别名称、类型、版本、厂商、硬件 ID；

c) 应支持对使用的存储介质进行白名单配置。

6.7. 态势展示

6.7.1. 资产可视化

本项要求包括：

a) 应支持展示资产的风险等级和威胁态势，通过颜色、图标等方式直观表示资产的安全状态；

b) 应支持所展示的非结构化数据满足数据的完整性、准确性；

c) 应支持展示资产名称、告警名称、告警重要性等工控安全警告；

d) 应支持展示在线资产详情、离线资产详情、资产类型详情、告警处理详情等资产详情；

e) 应支持探针数据、运维数据集中态势展示。

6.8. 系统安全要求

6.8.1. 身份鉴别

本项要求包括：

a) 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；

b) 应要求用户登录需进行验证码确认；

c) 用户身份鉴别信息丢失或失效，应采用技术措施确保鉴别信息重置过程的安全。

6.8.2. 访问控制

本项要求包括：

a) 应提供用户访问控制功能，对登录的用户分配账户和权限；

b) 应授予不同账户的权限不同，使其形成制约；

c) 应授予不同端（包括 PC 端和移动端）登录账户的权限不同，使其形成制约；

d) 应支持移动端访问时的用户与 PC 端访问用户具有统一性；

e) 应及时删除或停用多余的过期用户，避免共享用户的存在。

6.9. 应急响应与灾备联动要求

本项要求包括：

a) 应支持平台与灾备系统的兼容与联动，在发生重大安全事件或灾难时，能够自动或手动触发灾备系统，确保灾后数据的恢复与业务系统的重建；

b) 应支持平台与应急响应系统联动，联动过程进行日志记录和审计，包括事件触发时间、响应措施等，并生成详细的日志报告。