石油石化行业信息系统安全
管理规范建设的思考



第四届中国石油石化网络安全应用研讨会暨北斗导航能源安全应用技术交流会

前言

石油石化行业当前处于数字化转型与智能化发展的关键阶段，信息化平台正在重塑油气行业的技术范式与产业生态。信息技术标准在油气行业信息系统平台化建设中发挥着基础性、战略性的引领性作用。

以SY/T 5231—2024 《石油工业信息系统安全管理规范》为主线，对石油石化行业信息系统安全管理标准体系建设现状和当前所面临的主要补强需求深入分析。以今后一段时期行业急需建设的20项信息系统安全管理相关的技术规范为目标，提出石油石化行业信息系统安全管理标准体系的规划与建设思路。增强信息系统部署环境安全，规范业务数据分类分级模式，深化人工智能融合应用，夯实关键信息基础设施安全防护基线。

汇报提纲

一、安全管理规范建设目标

二、安全管理规范基本现状

三、安全管理规范增强需求

四、安全管理规范建设展望

一、安全管理规范建设目标

1.总体目标：依据石油石化行业信息系统特点和国家合规要求，从物理安全、技术要求和管理规范等三个维度构建体系化的信息系统安全方案，增强来自国内外网络安全攻击的抵御能力，确保石油石化行业信息系统安全平稳运行。

- 统一安全基线：明确对云、物联网、工业控制、人工智能、大数据等平台应用的安全防护基本要求。
- 责任体系构建：界定从管理层到现场操作员的安全职责。
- 全生命周期管理：覆盖平台系统的设计、建设、部署、运维到退役各阶段。

一、安全管理规范建设目标

- **网络安全政策体系**

1. 《中华人民共和国网络安全法》2017年6月执行
2. 《中华人民共和国密码法》2020年1 月执行
3. 《中华人民共和国数据安全法》2021年9 月执行
4. 《中华人民共和国个人信息保护法》2021年11 月执行
5. 《关键信息基础设施安全保护条例》国务院 2021年9月发布施行
6. 《商用密码管理条例》国务院 2023年修订
7. 《网络安全等级保护条例》公安部 2018年，等保2.0

- **密码应用安全标准**

1. 《信息系统密码应用基本要求》GM/T 0054-2018 （国家密码局，行标）
2. 《信息安全技术 信息系统密码应用基本要求》 GB/T 39786-2021
3. 《信息安全技术 密码模块安全要求》GB/T 37092-2018
4. 《信息安全技术 信息系统密码应用测评要求》GB/T 43206-2023
5. 《信息安全技术 信息系统密码应用设计指南》GB/T 43207-2023

- **等级保护2.0标准**

1. 《计算机信息系统 安全保护登记划分准则》GB 17859-1999
2. 《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019
3. 《信息安全技术 网络安全等级保护实施指南》GB/T 25058-2019
4. 《信息安全技术 网络安全等级保护定级指南》GB/T 22240-2020
5. 《信息安全技术 网络安全等级保护安全设计要求》GB/T 25070-2019
6. 《信息安全技术 网络安全等级保护测评要求》GB/T 28448-2019
7. 《信息安全技术 网络安全等级保护测评过程指南》GB/T 28449-2018
8. 《信息安全技术 信息安全风险评估规范》GB/T 20984-2007
9. 《信息安全技术 个人信息安全规范》GB/T 35273-2020

- **关键信息基础设施保护标准**

1. 《信息安全技术 关键信息基础设施安全保护要求》GB/T 39204-2022
2. 《信息安全技术 关键信息基础设施安全控制措施》（国标制定中）
3. 《信息安全技术 关键信息基础设施安全测评要求》（国标制定中）
4. 《信息安全技术 关键信息基础设施安全检查评估指南》（国标制定中）

汇报提纲

一、安全管理规范建设目标

二、安全管理规范基本现状

三、安全管理规范建设需求

四、安全管理规范建设方案

二、安全管理规范基本现状

1.面向物联网系统和工控系统的安全管理规范相对完备。现行有效的信息系统及安全管理相关的国家标准，有6项由石油石化企业第一起草单位组织制定完成，体现了石油石化行业物联网建设管理特色需求。

序号	标准号	标准名称	牵头制定企业	备注
1	GB/T 50609-2010	石油化工工厂信息系统设计规范	中国石化	住建部归口
2	GB/T 42028-2022	面向陆上油气生产的物联网系统技术要求	中国石油	TC28归口
3	GB/T 41816-2022	物联网 面向智能燃气表应用的物联网系统技术规范	中国石油	TC28归口
4	GB/T 42588-2023	系统与软件工程 功能规模测量 NESMA方法	中国石油	TC28归口
5	GB/T 44249.1-2024	面向海上油气生产的物联网系统 第1部分：通用要求	中国海油	TC28归口
6	GB/T 44250.1-2024	面向油气长输管道的物联网系统 第1部分：总体要求	国家管网	TC28归口

二、安全管理规范基本现状

2.石油工业信息系统安全管理基本规范初步建成。SY/T 5231规定了石油工业信息系统安全管理的总体要求，涵盖了信息系统的技术、管理、建设、运维的各环节管理的基本要求和对于云计算、工控系统、物联网的增强管理要求，还包括关键信息基础设施的安全保护。描述了检测控制的证实方法。

序号	标准号	标准名称	备注
1	SY/T 7670—2022	油气田北斗应用技术规范	现行有效
2	SY/T 7696—2023	石油工业北斗综合监管技术应用规范	现行有效
3	SY/T 6227—2005	石油工业数据库设计规范	现行有效
4	SY/T 7797—2024	油气行业工业互联网平台架构与集成规范	现行有效
5	**SY/T 5231—2024**	**石油工业信息系统安全管理规范**	**现行有效**
6	SY/T 6783—2017	石油工业计算机病毒防范管理规范	现行有效
7	SY/T 7796—2024	海洋石油支持船物联网建设规范	现行有效
8	SY/T 7468—2020	油气生产物联网系统技术规范	现行有效
9	SY/T 7697—2023	石油化工行业视频监控管理平台接口技术规范	现行有效
10	SY/T 7672—2022	油气勘探开发专业软件接口规范	现行有效
11	SY/T 7671—2022	加油加气站信息系统建设技术规范	现行有效

二、安全管理规范基本现状

SY/T 5231基本要求

等保制度：第三级及以上系统应采用**密码技术**进行安全防护，并使用符合相关要求的密码产品和服务，在网络安全等级测评中同步开展**密码应用安全性评估**。第三级信息系统应每年至少进行一次等级测评，第四级信息系统应每半年至少进行一次等级测评。

物理环境：应重点加强对**资源集中的物理环境**，如云技术基础设施、重要网络节点、重要数据节点的物理环境安全防护。

通信网络：应依据不同的信息系统安全等级，**划分网络安全域**，对不同的安全域制定不同的安全策略。

区域边界：依据访问控制策略应采用合适的**访问控制技术**，实现不同信任级别的主体对不同安全域的访问控制。

计算环境：应建立信息系统的**身份鉴别机制**，并满足安全等级对应的技术要求。严格控制信息系统访问权限，对每个系统用户仅提供满足业务或管理需要的**最小权限**。

建设运维：开发阶段应将开发环境和运行**环境隔离**，软件使用前应完成**源代码检测**。分析运行中所面临的威胁与风险，建立对应的**安全管理制度**，应制定安全事件**应急预案**。

二、安全管理规范基本现状

数据安全

分级分类策略

应在信息系统的设计阶段，建立基于**数据分类分级的数据安全保护策略**，明确重要数据的保护措施。应制定数据备份和恢复策略，依据GB/T 22239的要求，安全保护等级第二级及以上系统应提供**异地数据备份**，第三级以上系统应提供**异地实时数据备份**。

安全保护措施

应严格控制重要数据的收集、存储、使用、加工、传输、提供和公开等关键环节，采取**加密、脱敏等技术手段**保护敏感数据安全。信息系统存在重要**数据跨境传输**，按照法律法规要求采取数据安全保护措施。应建立数据安全**监测和分析机制**，对威胁数据安全恶意行为具备发现和阻断能力。

应急处置机制

建立数据安全应急处置机制。发生数据安全事件，**启动应急预案，**防止危害扩大，消除安全隐患。应对**数据操作保存审计记录**，至少包括日期时间、主体身份、操作内容、操作结果等。

二、安全管理规范基本现状

云计算平台

◆ 满足计算资源、数据存储、虚拟网络等隔离控制的基础功能，不应承载高于自身安全等级信息系统，保证租户数据、虚拟机镜像在运行、备份、迁移等过程中保密性。提供边界防护、入侵防范、加密传输等安全功能。

◆ 能为租户提供对资源滥用、攻击行为、运行状态等监测功能。

◆ 供应链安全事件或威胁信息及时传达到租户，并采取措施降低风险。

◆ 平台与租户应划分安全责任，并签订相关保密协议及承诺书。应选择安全合规的云平台供应商，明确权限和责任。

◆ 云计算平台应加强其应用程序编程接口（API）的安全管控，建立授权隔离措施，防止滥用。

二、安全管理规范基本现状

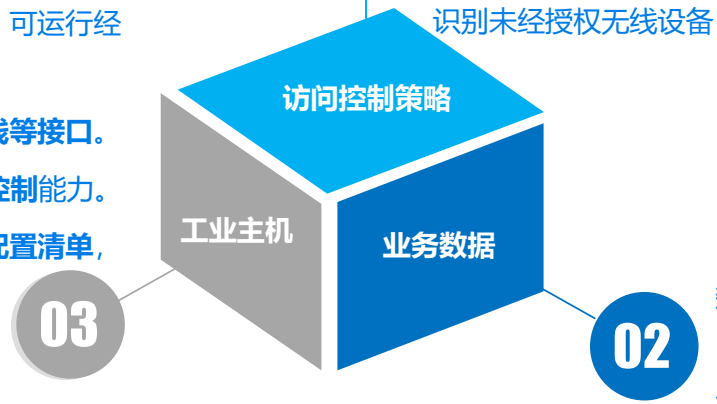
工业控制系统

◆ 工业主机应执行**最小化系统安装**，部署白名单控制策略，可运行经过授权和安全评估的软件。

◆ 应封禁或拆除工业主机上不必要的**移动存储、光驱、无线等接口**。

◆ 应具备对关键上位机HMI的外部物理**接口启用、禁用的控制**能力。

◆ 应建立工业控制网络、工业主机和工业控制设备的**安全配置清单**，并定期审计。



◆ 工业控制系统内应**划分不同安全区域**，区域间部署安全访问控制策略，通过检查数据包的源地址、目的地址、传输协议、所请求的服务等，及时制止不符合安全控制策略的数据包传输。

◆ 工业控制系统与其他信息系统宜采用物理隔离，存在信息交换需求的，**应采用单向技术隔离手段**，不应采用FTP、HTTP、TelNet等高风险网络服务。

◆ 应对参与**无线通信的设备进行授权**以及执行使用进行限制。应识别未经授权无线设备，并报告未授权接入或干扰控制系统的行为。

◆ 应确保控制指令和工业数据的**加密存储和传输**。

◆ 应对关键业务数据，如工艺参数、配置文件、设备运行数据、生产数据、控制指令等进行**定期备份**。

◆ 应保留工业控制系统的相关**访问日志**，并对操作过程进行**安全审计**。

◆ 应在网络边界和重要网络节点进行安全审计，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**。

二、安全管理规范基本现状

物联网系统

◆ 感知终端设备应具有长时间工作的电力供应，**物理环境**应确保不被破坏和干扰。

◆ 感知终端设备应具备对其连接的感知终端设备进行**身份标识和鉴别的能力**。

◆ 感知层网关设备**主要部件**应设置明显的不易去除的标记。

◆ 感知层网关设备应具备对连接设备进行**标识和鉴别**的能力、控制外部连接数量的能力以及对**过滤非法和伪造连接**的能力。

◆ **关键感知层网关设备**应具有持续稳定的电力供应，其物理环境应确保良好的信号收发能力。

◆ 数据采集应采用**标准化时间戳**等技术确保数据可用性。

◆ 数据传输应能**鉴别数据的时效性**，避免历史数据的重放攻击。

◆ 数据传输应采用国家法律法规允许的**加密算法**确保数据传输的保密性，且具备数据**校验功能**，确保数据传输的完整性。

二、安全管理规范基本现状

关键信息基础设施

第一条~第三条

◆ 关键信息基础设施**运营者应保障**专门安全管理机构运行经费和关键信息基础设施安全防护经费。

◆ 关键信息基础设施**所属企业应配合**主管部门完成关键信息基础设施认定和变更。

◆ 应对**安全管理机构**的负责人和关键岗位的人员进行安全背景审查和安全技能考核，关键岗位应配备专人，并配备2人以上共同管理。

第四条~第六条

◆ 应采购通过国家检测**认证的设备和产品**，并建立和维护合格供应方目录。

◆ 应确保**重要数据和个人信息在境内存储**，因业务需要确需向境外提供数据的，应按照国家相关规定和标准评估。

◆ 应建立网络安全通报**预警制度和威胁情报共享机制**，及时掌握所在行业和领域的安全态势。

第七条~第八条

◆ 应关键信息基础设施每年至少进行一次网络**安全检测和风险评估**，并及时整改安全问题。

◆ 应建立**应急预案**，定期组织应急演练。

汇报提纲

一、安全管理规范建设目标

二、安全管理规范基本现状

三、安全管理规范增强需求

四、安全管理规范建设展望

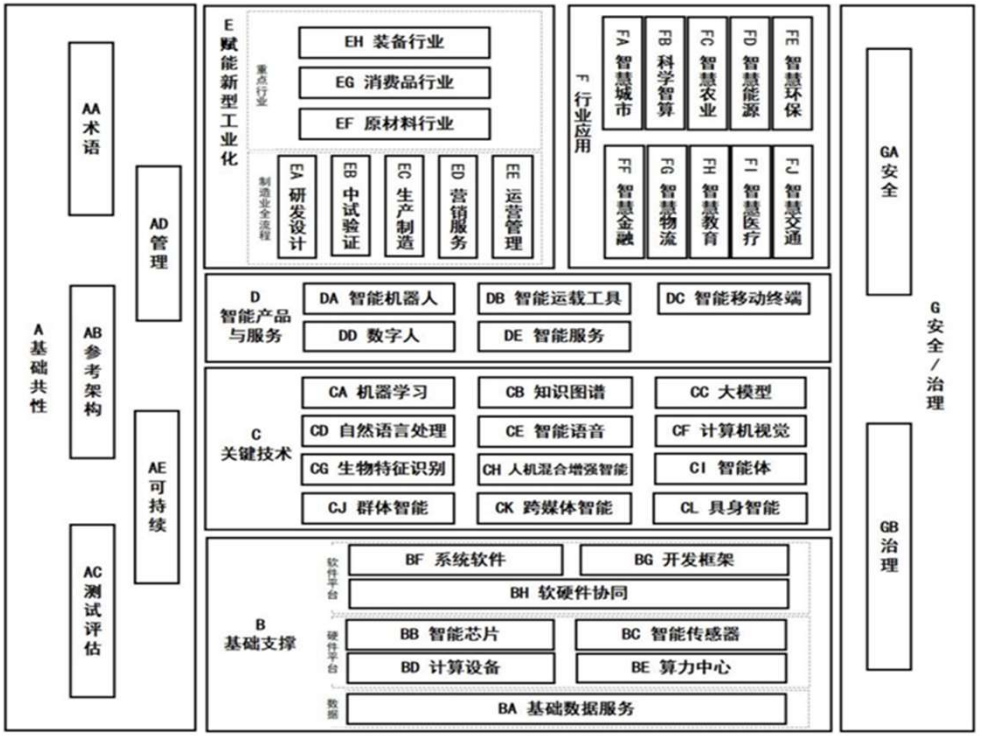
三、安全管理规范增强需求

1.行业业务共享驱动数据安全管理规范需要加强。油气行业数据采集、传输、存储、应用以及保密的管理，规范数据管理组织、安全技术、管控流程以及安全工具，确保数据行业内安全、高效、准确、完整共享。

2. 人工智能深度应用推动安全管理规范升级。目前领域仅有中国石油发布的1项企业标准《勘探开发知识图谱与人工智能平台技术规范》，尚无行业层面的人工智能油气标准，推动行业产业智能化生态建设。

三、安全管理规范增强需求

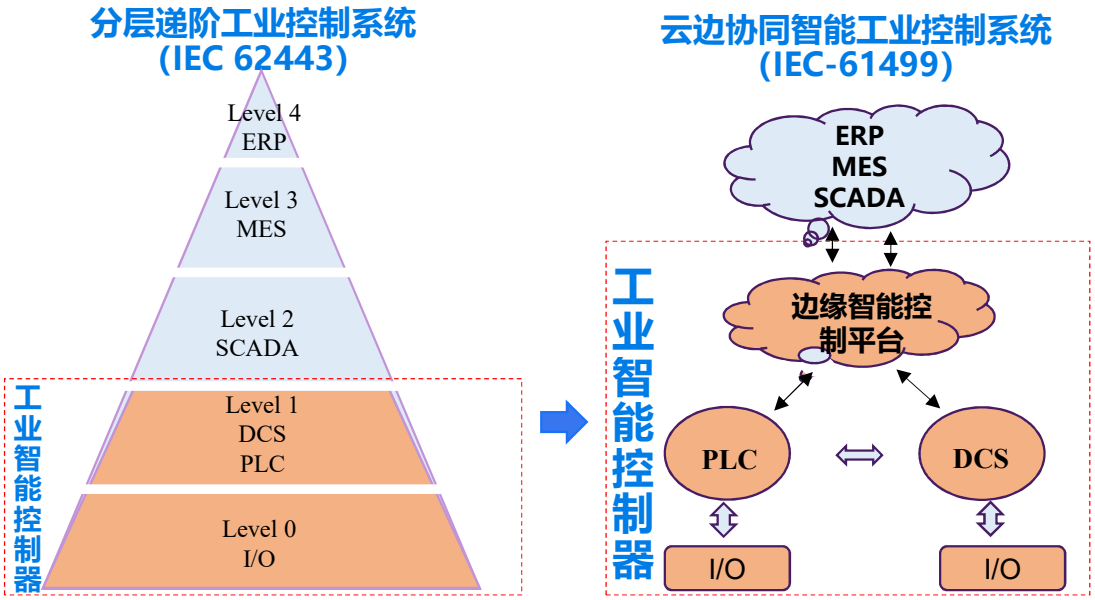
人工智能标准	2024年6月底
发布的国际标准	28项
在研的国际标准	29项
发布的国家标准	10项
制定中的国家标准	25项
发布的行业标准	16项
发布的团体标准	上百项



三、安全管理规范增强需求

3. 工业控制系统的新型架构牵引安全管理规范迭代。

云边协同的智能工业控制系统安全是工业互联网与数字化转型核心挑战之一，现有的云计算安全技术规范和边缘计算安全技术规范为云边协同的智能工业控制系统提供了基础框架，但未完全覆盖云边跨层协同联动的安全特性安全管理需求。对供应链安全、边缘侧设备漏洞治理和云端数据防泄露等方面的安全亟须通过技术与管理结合的方式，构建多层次、全生命周期的“边缘免疫、云端智控、跨层联动”安全防护体系。



三、安全管理规范增强需求

4.国家战略部署引领行业安全管理规范体系完备进程。国家对信创、IPV6、自主工业软件、北斗应用和关键信息基础设施等明确提出的最新战略部署和政策要求，对石油石化行业信息系统的应用管理和安全防护提供了方向指引。

序号	标准号	标准名称	主要技术内容	备注
1	能源20240670	在役油气长输管道数字化规范	在役油气长输管道数字化恢复的基础规定、数据恢复范围、数字化恢复技术要求、信息恢复要求、数字化成果移交及移交流程。	2026
2	能源20240671	石油石化数字化转型技术指南	石油石化行业数字化转型建设的总体架构、业务架构、数据架构、应用架构及网络安全架构。	2026
3	能源20240688	液化天然气接收站数字化导则	液化天然气接收站工程的数字化：职责和分工、交付基础、交付信息的 内容与形式、交付流程、交付平台。	2026
4	能源20240697	储气库数字化设计导则	储气库数字化设计过程中各参建单位的职责分工、工作内容和深度，数字化移交、交付物标准。	2025
5	能源20240822	石油行业管道数据字典	油气管道工程结构化数据内容和定义，对工程项目全生命周期数据库及数据模型设计提出约束。	2026
6	能源20240823	石油工业应用软件工程规范	软件需求、设计、开发、测试、安装运行、验收，运维，还包括开发技术、开发模式和开发方法的选择等。	2026

汇报提纲

一、安全管理规范建设目标

二、安全管理规范基本现状

三、安全管理规范增强需求

四、安全管理规范建设展望

四、安全管理规范建设展望

新兴技术在行业深度应用趋势

人工智能技术应用：初至波拾取、层位识别、抽油机井工况诊断、生产参数优化、钻井事故预防、油藏参数推荐。

物联网融合应用：井口设备监控、场站监控、物流监控、管道监控、炼厂环境监控。

云计算深化应用：各业务板块的专业云、通用技术基础平台等。

01

基础数据分级分类：数据标准工作导则、数据技术规范类包括架构资源目录、业务数据规范、数据标注规范等。

智能技术应用类：机器学习模型评价规范类、知识图谱技术要求及评估规范类、智能应用使用及管理标准等。

02

物联网平台技术规范类：包括勘探开发、炼油与化工、销售等。

03

云计算应用类：PaaS平台技术规范类、云计算运营与维护规范类、异构计算资源池建设与运维规范类、微服务拆分指南等。

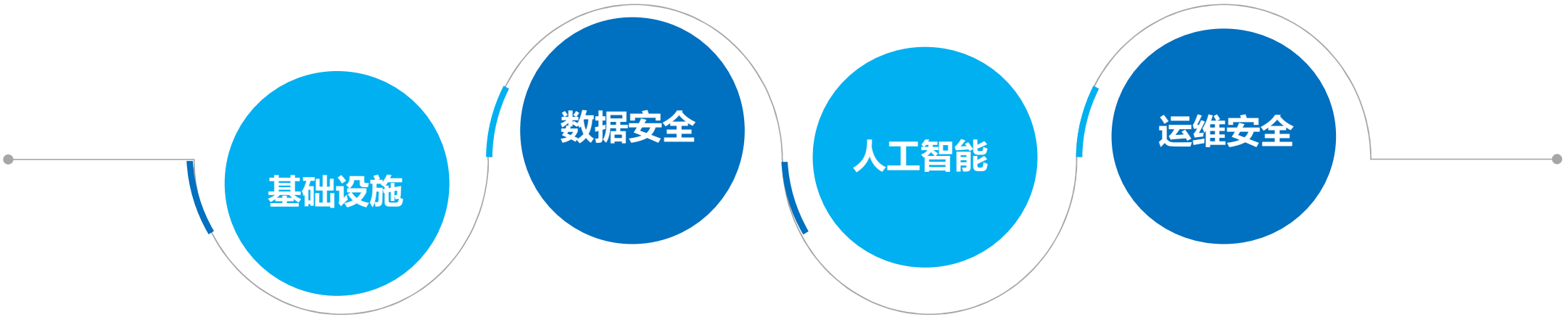
新技术标准引领与支撑

四、安全管理规范建设展望

石油石化行业信息系统安全管理标准体系建设规划思路

数据分类分级安全管理。规范石油天然气行业数据安全管理与共享应用，全面提升数据安全能力。

安全运维和应急管理。重点加强关键信息基础设施的安全防护，实现安全与业务的良性互动循环。



夯实安全管理底座。构建“自主可控、安全可信”的行业信息化软硬件基础实施防护规范。

智能化技术规范。知识管理、图像分析、算法模型、大模型评测、安全规范及数字孪生全链条技术。

四、安全管理规范建设展望

1. 夯实信息系统安全管理底座。构建“自主可控、安全可信”的行业信息化软硬件基础实施防护规范。加速实现**软件自主化、云网协同化、物联智能化、边缘实时化**， 为国家能源安全与数字化转型战略部署在行业的落地实施提供有力的统一技术保障。

序号	标准名称	主要技术要求	备注
1	石油工业专业软件技术规范	信创适配要求、数据接口行业标准适配，代码安全管理和软件资质认证等。	2027
2	石油天然气云计算技术	混合云架构、容器化部署，跨云数据同步、数据加密与跨境传输管理要求。	2027
3	石油工业物联网 炼化	传感器接入要求，通信网络架构规范，数据的采集频度和边缘预处理要求。	2028
4	石油工业物联网 加油站和油库	加油机物联网的数据实时上传，油库安全监测，防入侵系统和数据脱敏等安全管理。	2028
5	油气生产现场边缘计算应用技术	硬件的设备选型算力要求和实时性能指标等要求，轻量化智能模型和本地自治算法执行要求。	2026
6	油气工业控制系统网络安全防护建设	防护架构设计，终端与数据安全防护，监测与响应能力建设，安全制度与流程及供应链安全。	2027

四、安全管理规范建设展望

2. 数据分类分级安全管理。通过精准化、差异化的防护策略，规范行业数据安全管理与共享应用，提升数据安全能力。避免因数据泄露导致生产事故，**安全合规前提下释放数据价值**，充分驱动行业智能化升级。

序号	标准名称	主要技术内容	备注
1	石油工业数据资源目录	按数据类型划分维度，以安全划分级别，建立行业生产数据资源目录树。	
2	勘探开发元数据规范	建立元数据分类与层级包括资源级、实体级、属性级，做好命名与编码规则，质量控制与维护。	2026
3	油气输送管道主体设施命名、编码及管理数据规范	管道主体设施命名原则，设施类型分类，采用层次化编码，数据安全管理技术。	
4	石油天然气数据安全管理指南	以数据资源目录为基础，对油气生产数据全生命周期安全技术管理和应用权限流程管理。	2025
5	油气管网大数据技术规范	统一数据格式，规范数据完整性、一致性阈值，制定行业数据安全共享应用。	2027
6	油气数据共享交易指南	数据确权与定价，划分数据权属，统一定价模型和数据交易平台与合规流程。	2028

四、安全管理规范建设展望

3.油气勘探开发安全智能化技术规范体系。为推进人工智能与数字技术在油气行业的深度应用，实现数据驱动决策，构建“**知识图谱-AI模型-数字孪生”闭环**的全链条技术标准体系。

序号	标准名称	主要技术要求	备注
1	油气勘探开发知识智能化技术规范	基于地质、工程、生产等多源数据，构建行业知识图谱，支持规则推理与机器学习融合推理。	2026
2	油气勘探开发图像智能分析技术规范	数据处理与标注要求，算法性能评测量化指标。	2026
3	油气人工智能算法和模型技术规范	算法选型与开发，模型验证指标与部署要求，对识别模型偏差、数据偏见等风险管控。	2026
4	油气工业大模型评测规范	从基础能力、识别准确度和内容合规性等维度评测，行业评测数据集的构建方法等。	2025
5	油气工业人工智能安全规范	对数据采集、传输、存储和销毁等数据周期的安全管理，模型对抗攻击的防御以及鲁棒性能。	2026
6	油气勘探开发数字孪生技术规范	多尺度建模方法与实时数据集成，油气智能场景的应用。	2027

四、安全管理规范建设展望

4.信息系统安全运维和应急管理。关键信息基础设施的安全防护是行业信息系统安全重点，信息系统评价是信息系统安全管理的杠杆。系统安全运维实现“安全赋能业务，业务驱动安全”的良性互动循环。

序号	标准号	主要技术要求	备注
1	石油工业关键信息基础设施保护实施规范	构建“物理安全+网络安全+数据安全+应急响应”的多层防护体系，对软硬件供应商进行安全审查，确保供应链安全，定期开展网络攻击模拟演练，建立“责任到人”的网络安全责任制、国产化替代方案和与国家级安全监测平台对接，实现威胁情报共享。	/
2	石油工业信息系统评价规范	从技术、安全、业务和成本等方面构建评价维度，采用定量指标、定性评估和动态调整的评价方法，对油气行业信息系统的可用性、可靠性、安全性、经济性 进行综合评估，确保系统符合业务需求和行业安全标准。	/

感谢聆听！