**UDC**

中华人民共和国国家标准 **GB**

**P GB 5××××—20××**

**石油化工工厂信息系统设计规范**

**Code for design of plant information system**

**in petrochemical engineering**

**局部修订条文征求意见稿**

20XX－XX－XX 发布 20XX－XX－XX 实施

|  |
| --- |
| 中华人民共和国住房和城乡建设部  联合发布 |
| 国家市场监督管理总局 |

中华人民共和国国家标准

**石油化工工厂信息系统设计规范**

**Code for design of plant information system**

**in petrochemical engineering**

**GB/T** ×××××**－×**×××

主编部门：中国石油化工集团公司

批准部门：中华人民共和国住房和城乡建设部

施行日期：20XX年XX月XX日

中国计划出版社

2010 北京

前 言

本标准修订采用GB/T 50609-2010《石油化工工厂信息系统设计规范》。

本标准与GB/T 50609-2010的主要差异如下：

——新增了部分章节。在2.1节增加了2.1.5 智能服务平台 Intelligent service platform；在2.2节新增加2.2.1.A AAS 先进报警管理系统、2.2.7.A DMZ 隔离缓冲区 、2.2.12.A IDM 智能设备管理系统、2.2.17.A PCN 过程控制网、2.2.17.B SIL 安全完整性等级、2.2.17.C VLAN 虚拟局域网、2.2.32 JSA 安全作业分析；在3.1节新增加3.1.6及3.1.7条；在5.2节新增加5.2.13 水资源管理系统、5.2.14 碳资产管理系统、5.2.15 应急指挥系统、5.2.16 施工作业管控、5.2.17 危化品管理系统及5.2.18 环保管理子系统；在6.2节新增加6.2.13 合同管理系统；在7.2节新增加7.2.6 档案管理系统；在8.1节新增加8.1.4　智能服务平台、8.1.5 融合通讯系统、8.1.6工业无线网；在第8章新增加8.9节智能服务平台设计要素、8.10节融合通讯设计要素、8.11节工厂无线网设计要素。新增加第9章网络与信息安全，将原8.9 节信息安全内容调整并增加工控网隔离与防护的内容。

——删除了部分章节。删除8.9节信息安全。

本标准替代GB/T 50609-2010《石油化工工厂信息系统设计规范》,增加了部分新系统。

本规范由住房和城乡建设部提出并归口管理，由中国石油化工集团公司负责日常管理，由中国石化工程建设有限公司负责具体技术内容的解释。

本标准起草单位：中国石化工程建设有限公司、中国石化集团洛阳石油化工工程有限公司、中国石化集团上海工程有限公司、中国石化集团宁波工程有限公司、石化盈科信息技术有限责任公司

本规范主要起草人员：

本标准所替代标准的历次版本发布情况为：

——GB/T 50609-2010

**《石油化工工厂信息系统设计规范》GB50516—2010**

**修订对照表**

**（方框部分为删除内容，下划线部分为增加内容）**

| 现行《规范》条文 | 修订征求意见稿 |
| --- | --- |
| **1 总 则** | **1 总 则** |
| **条文说明** | **条文说明** |
| 1.0.1 依据企业规模、运营管理模式、投资，建设国际水准、国内一流、具有石化行业特色的石油化工工厂。 | 1.0.1 依据企业规模、运营管理模式、投资，建设国际水准、国内一流、具有石化行业特色的石油化工工厂。工厂信息系统是为石油化工企业经营管理及生产管控服务的一体化网络信息集成平台。智能工厂、智慧工厂、数字工厂等亦泛指工厂信息系统。 |
| **2 术 语 和 缩 略 语** | **2 术 语 和 缩 略 语** |
| **2.1 术 语** | **2.1 术 语** |
| **2.1.1** 物资 Material  物质资料的简称，包括生产资料和生活资料。企业生产过程中所需要的物资主要指原材料、辅助材料、燃料、动力、配件、工具等。 | **2.1.1** 物资 Makings  物质资料的简称，包括生产资料和生活资料。企业生产过程中所需要的物资主要指原材料、辅助材料、燃料、动力、配件、工具等。 |
|  | 2.1.5 智能服务平台 Intelligent Service Platform  指基于石油石化行业数字化、网络化、智能化需求,构建工厂海量数据采集、汇聚、分析的服务体系，支撑工业资源泛在连接、弹性供给、高效配置，提供对象模型建模、大数据分析、智能APP组态开发、智慧决策和分析服务的工业云平台。 |
| **2.2　缩略语** | **2.2　缩略语** |
|  | 2.2.1.A AAS 先进报警管理系统 Advanced Alarm management System |
| 2.2.2 CCR 中央控制室 Central Control Room | 2.2.2 CCR 中心控制室 Central Control Room |
| 2.2.3 CCS 压缩机组控制系统 Compressor Control System | 2.2.3 CCS 压缩机控制系统 Compressor Control System |
| 2.2.4 CCTV 电视监视系统 Central Control Television | 2.2.4 CCTV 电视监视系统 Closed Circuit Television |
| 2.2.7 DCS 分散型控制系统 Distributed Control System | 2.2.7 DCS 分散控制系统 Distributed Control System |
|  | 2.2.7.A DMZ 隔离缓冲区 Demilitarized Zone |
| 2.2.12 FGS 火灾及气体检测系统 Fire and Gas Detection System | 2.2.12 GDS 可燃和有毒气体检测系统 Combustible Gas and Toxic Gas Detection System |
|  | 2.2.12.A IDM 智能设备管理系统 Intelligent Device Management |
| 2.2.17 MMS 机组监控系统 Machinery Monitoring System | 2.2.17 MMS 机组监测系统 Machinery Monitoring System |
|  | 2.2.17.A PCN 过程控制网 Process Control Network |
|  | 2.2.17.B SIL 安全完整性等级 Safety Integrity Level |
|  | 2.2.17.C VLAN 虚拟局域网 Virtual Local Area Network |
|  | **2.2.32** JSA 安全作业分析 Job Safety Analysis |
| **3 系统设计** | **3 系统设计** |
| **3.1 一般规定** | **3.1 一般规定** |
| **3.1.5**工厂信息系统的基础设施、PCS、MES和ERP的主要子系统应与工厂工程同步建设。 | **3.1.5**　工厂信息系统的基础设施、网络安全、PCS、MES和ERP的主要子系统应与工厂工程同步建设。 |
|  | **3.1.6**工厂信息系统建设可从数字化交付获取工程建设阶段产生的数据、文档和三维模型等数字化静态信息。 |
|  | **3.1.7** 移动应用应根据业务需求进行设计。 |
|  |  |
| **3.2 系统架构** | **3.2 系统架构** |
| 3.2.1 工厂信息系统总体架构应符合图3.2.1的要求。 |  |
|  |  |
| **3.3**　设计要素 | **3.3　设计要素** |
| 3.3.2 过程控制系统的设计应满足全厂生产装置、公用工程和储运系统等控制、操作、监视和管理的需要，并应满足执行层与计划层对数据采集的需要。 | 3.3.2 过程控制系统的设计应满足全厂生产装置、储运系统、公用工程和储运系统及辅助设施等控制、操作、监视和管理的需要，并应满足执行层与计划层对数据采集的需要。 |
| 3.3.8 设备管理子系统可在生产执行系统和经营管理系统中分别设计，功能上应有所侧重、互为补充。也可只在其中一个系统中设计，应包括本规范第5.2.9和6.2.5条的全部功能。 |  |
|  |  |
| **4　过程控制系统**  **4.1　一般规定** | **4　过程控制系统**  **4.1　一般规定** |
| 4.1.1　PCS应设计为用于全厂生产装置、公用工程及辅助设施的集成的自动控制及信息系统。 | 4.1.1　PCS应设计为用于全厂生产装置、储运系统、公用工程及辅助设施的集成的自动控制及仪表系统。 |
| 4.1.2　PCS应包括分散型控制系统（DCS）和/或现场总线控制系统（FCS）、安全仪表系统（SIS）、火灾及气体检测系统（FGS）、压缩机组控制系统（CCS）、机组监控系统（MMS）、可编程序控制器系统（PLC）、数据采集和监控系统（SCADA）、储运自动化系统（MAS）、仪表设备管理系统（AMS - Asset Management System）、在线分析仪系统（PAS）、操作数据管理系统（ODMS - Operational Data Management System）和先进过程控制（APC）等部分。 | 4.1.2　PCS应宜包括分散型控制系统（DCS）和/或现场总线控制系统（FCS）、安全仪表系统（SIS）、可燃和有毒气体检测系统（GDS）、压缩机控制系统（CCS）、机组监测系统（MMS）、可编程序控制器系统（PLC）、数据采集与监控系统（SCADA）、储运自动化系统（MAS）、智能设备管理系统（IDM）、在线分析仪系统（PAS）、先进报警管理系统（AAS）和先进过程控制（APC）等部分。 |
| 4.1.3　全厂的石油炼制及石油化工生产装置、公用工程及辅助设施宜采用统一品牌的分散型控制系统(DCS)和/或现场总线控制系统（FCS）作为主控制系统，并应在中央控制室（CCR）进行集中操作、维护和管理。特殊情况下，也可在现场控制室（LCR - Local Control Room）进行操作。 | 4.1.3　全厂的石油炼制及石油化工生产装置、储运系统、公用工程及辅助设施宜采用统一品牌的分散控制系统(DCS)和/或现场总线控制系统（FCS）作为主控制系统，并应在中心控制室（CCR）对生产过程进行集中控制、操作、监视和管理。特殊情况下，也可在现场控制室（LCR - Local Control Room）进行操作。 |
| 4.1.4　过程控制系统中的DCS/FCS、CCS、PLC等控制系统应采用性能可靠、技术先进、功能完备、互操作性和易维护性均良好的商业化系统及产品。 | 4.1.4　过程控制系统中的DCS/FCS、CCS、PLC等控制系统应采用性能可靠、技术先进、功能完备、互操作性和易维护性均良好的工业级控制系统及产品。 |
| 4.1.5　过程控制系统中的SIS、FGS、MMS等安全及保护系统应采用独立性、安全性和可用性均良好的商业化系统及产品，并应取得国际权威安全认证机构的安全认证，FGS还应取得国家消防电子产品强制性产品质量认证。 | 4.1.5　过程控制系统中的SIS、GDS、MMS等安全及保护系统应采用独立性、安全性和可用性均良好的工业级控制系统及产品，SIS应取得国家授权安全认证机构的安全完整性等级（SIL）认证。 |
| 4.1.6　过程控制系统应采用可靠的网络构架和安全措施，宜采用开放型系统结构，主控制系统网络应采用冗余、容错的工业级以太网，并应支持TCP/IP协议。主控制系统宜支持Modbus、Profibus、Foundation Fieldbus、HART及、OPC等通信协议。传递控制及安全联锁信号的通信接口应采用冗余方式。 | 4.1.6　过程控制系统应采用可靠的网络构架和安全措施，宜采用纵向分层、横向分域型系统结构，主控制系统网络宜采用冗余、容错的工业级以太网，并宜支持TCP/IP协议。主控制系统宜支持Modbus RTU、Modbus TCP、Profibus DP、Profibus PA、Foundation Fieldbus H1、HART、OPC DA/AE及OPC UA等通信协议。传递控制及安全联锁信号的通信接口应采用冗余方式。 |
| 4.1.9　过程控制系统宜安装在中央控制室（CCR）和多个现场机柜室（FAR）内。PCS的操作站应设置在相应的CCR内，PCS的控制站及输入/输出单元应设置在相应的FAR内。 | 4.1.9　过程控制系统宜安装在中心控制室（CCR）和多个现场机柜室（FAR）内。PCS的操作站应设置在相应的CCR内，PCS的控制站及输入/输出单元应设置在相应的FAR内。 |
| **4.2　设计要素** | **4.2　设计要素** |
| 4.2.1 DCS系统宜由操作站、工程师站、辅助操作台、打印机、大屏幕显示器、PC机、控制站、I/O机柜、安全栅柜或/及端子柜、配电柜及网络设备柜等组成。FCS系统宜由主控制系统、通信接口、现场总线设备、现场总线辅助设备及现场总线电缆等组成。CCR设置公共的工程师站宜用于组态、维护故障诊断及开车。先进过程控制(APC)和实时优化(RTO)的设备也宜安装在CCR内。CCR设公共的硬件平台、数采工作站及网络接口宜用于连接信息系统。各控制站应配置冗余的串行通信接口连接SIS、FGS、CCS、MMS、MAS、PLC、PAS等子系统。 | 4.2.1 分散控制系统（DCS）宜由操作站、工程师站、服务器、辅助操作台、打印机、大屏幕显示器、应用工作站、过程控制站、I/O机柜、安全栅柜、过渡端子柜、继电器/隔离器柜、配电柜及网络设备柜等组成。FCS系统宜由主控制系统、通信接口、现场总线设备、现场总线辅助设备及现场总线电缆等组成。CCR宜设置公共的工程师站用于组态、维护、故障诊断及开车。先进过程控制(APC)和实时优化(RTO)的服务器和应用工作站宜安装在CCR内。CCR应设公共的硬件平台、数据服务器、数采工作站及网络接口用于连接工厂信息系统。各控制站应配置通信接口连接SIS、GDS、CCS、MMS、MAS、PLC、PAS等子系统。 |
| 4.2.2 安全仪表系统(SIS)，应根据生产装置、公用工程及辅助单元的安全完整性等级来设计，对重要的安全联锁保护、紧急停车系统及关键设备联锁保护宜设置安全仪表系统回路。SIS应实现与DCS的实时数据通信，SIS应设工程师站及顺序事件（SOE）工作站，相应的报警及操作宜通过辅助操作台上的开关和按钮、以及DCS的操作站来完成。 | 4.2.2 安全仪表系统(SIS)，应根据生产装置、储运系统、公用工程及辅助设施的安全完整性等级（SIL）来设计，对重要的安全联锁保护、紧急停车系统及关键设备联锁保护应设置安全仪表系统回路。SIS应实现与DCS的实时数据通信，SIS应设工程师站及顺序事件（SOE）工作站，相应的报警及操作宜通过辅助操作台上的开关和按钮、以及DCS的操作站来完成。 |
| 4.2.3 压缩机组控制系统(CCS)及机组监控系统（MMS）设计应符合下列要求：  1 应按装置或工艺单元分别设置压缩机组控制系统(CCS)。  4 大型电动机、汽轮机、压缩机和泵等转动设备机组应设置监控机械变量、运行状态，并具备在线分析和诊断功能的监控系统（MMS）。  5 机组监控系统的管理站应设置在中央心控制室。  6 机组控制系统CCS的控制站应设置在现场机柜室，机组控制系统CCS的操作站应设置在中央控制室。 | 4.2.3 压缩机组控制系统(CCS)及机组监控系统（MMS）设计应符合下列要求：  1 应按装置或工艺单元分别设置压缩机控制系统(CCS)。  4 大型电动机、汽轮机、压缩机和泵等转动设备机组应设置监控机械变量、运行状态，并具备在线分析和诊断功能的MMS。  5 机组监测系统的管理站应设置在中心控制室。  6 CCS的控制站应设置在现场机柜室，CCS的操作站应设置在中心控制室。 |
| 4.2.4 火灾及气体检测系统（FGS）应以现场机柜室（FAR）或生产装置为单位设置，并应符合下列规定：  1 各系统应设两路各自冗余的通信网络，一路宜连接到全厂的火灾及气体检测监视主系统（FGS），连接自动灭火系统，并连接到消防站。另一路宜连接到相关装置的DCS系统，在中央控制室内设置专用的DCS操作站用于FGS系统的显示、报警。  2 生产装置内可能泄漏或聚集可燃、有毒气体的地方，应分别设置可燃、有毒气体检测器，并应将信号接至到装置的火灾及气体检测系统或接到装置的DCS系统 | 4.2.4 可燃和有毒气体检测系统（GDS）应以现场机柜室（FAR）或生产装置为单位设置，并应符合下列规定：  1 在生产装置、储运系统、公用工程及辅助设施内可能泄漏或聚集可燃气体、有毒气体的场所，应分别设置可燃气体、有毒气体探测器，并应将信号接至对应的各个FAR内的GDS机柜中，在中心控制室内宜设置专用的GDS操作站用于全厂可燃和有毒气体泄漏的显示和报警，GDS应与DCS冗余通信。  2 GDS的报警信息和故障信息应通信到位于工厂消防监控中心或消防控制室内的图形显示终端上显示和报警。 |
| 4.2.8 数据采集与监控系统（SCADA）应对分布区域较广的设备和水、电、汽、风等公用工程消耗进行监视和控制，实现数据采集、参数记录报警、设备监控等功能。 | 4.2.8 数据采集与监控系统（SCADA）应对分布区域较广的管网、设备和水、电、汽、风等公用工程消耗进行监视和控制，实现数据采集、参数记录报警、设备监控等功能。 |
| **5 生产执行系统** | **5 生产执行系统** |
| **5.2　设计要素** | **5.2　设计要素** |
| **5.2.9** 设备管理子系统应实现设备运行状态的监控以及负荷核算与状态评估等，并应具有下列功能：  **2** 提供设备负荷核算与设备状态评估功能。 | **5.2.9** 设备健康管理子系统应实现设备运行状态的监控以及负荷核算与状态评估等，并应具有下列功能：  **2** 提供设备负荷核算、效能评估和分析功能。  **2.A** 提供设备故障判断和预警分析功能。 |
| **5.2.10** 能量管理子系统应依据装置对能量的需求，对全厂的水、电、汽、风等公用工程资源的生产和消耗数据进行收集、平衡和统计管理，并应具有下列功能： | **5.2.10** 能源管理子系统应依据装置对能量的需求，对全厂的水、电、汽、风等公用工程资源的生产和消耗数据进行收集、平衡和统计管理，并应具有下列功能： |
|  | **5.2.13** 工业水管理子系统应实现工业水药剂计划、运行参数监控分析和与工艺参数的相关性分析，并应具有下列功能：  1 药剂管理计划、用量的管理和跟踪分析。  2 工业水运行参数和用量的监控。  3 提供工业水用量的统计报表。  4 提供工业水运行指标与生产装置收率相关性分析功能。  5 提供与其它系统集成的接口。 |
|  | **5.2.14** 碳资产管理系统应实现碳资产计划、碳排放量计算和统计、碳盘查及核查文档管理，并应具有下列功能：  1 碳排放计划编制、发布和跟踪。  2 碳水平活动数据、排放因子及排放量的计算、统计和对比分析。  3 碳排放月度、年度统计报表在线编制、发布。  4 提供在线生成年度盘碳查清册和报告功能。  5 提供企业碳核查文档、凭证在线归档管理功能。  6 提供与其它系统集成的接口。 |
|  | **5.2.15**  应急指挥子系统对接处警、应急资源、应急处置过程和事故模拟进行管理，并应具有下列功能：  **1** 报警信息自动记录，警情定级和信息自动转发。  **2** 提供二维或三维的可视化应急地图。  **3**  集成工业视频、应急资源、应急队伍、应急车辆等数据。  **4**  提供应急处置功能，自动关联现场视频、人员、车辆和以及预案。  **5** 提供泄露、火灾等典型应急场景的模拟和演练。  **6**  提供与其它系统集成的接口。 |
|  | **5.2.16**  施工作业管控子系统对现场施工作业人员、设备和作业过程进行管理，并应具有下列功能：  **1** 提供作业风险库、施工机具风险库和作业环境风险库。  **2** 提供作业票据的申请、审批、会签和作业许可证的开具。  **3** 入厂\场人员器具检查和结果记录。  **4**  现场气体检测结果校验和记录。  **5** 安全措施清单与风险辨识措施匹配性检查。  **6** 现场作业人员资质查验和作业票证签发、记录和审批。  **7** 作业状态、视频监控、过程气体检测结果记录。  **8**  作业许可验收归档管理。  **9**  提供与其它系统集成的接口。 |
|  | **5.2.17** 危化品管理子系统对危化品的运输过程、存储过程进行监控、报警，并应具有下列功能：  **1**  提供二维或三维的危化品存储库和运输管网可视化模型。  **2**  集成危化品存储仓库相关工业视频、温度、湿度、烟感、红外传感器数据。  **3**  危化品运输车辆资质核查、车辆运输过程监控和异常报警。  **4** 危化品管输参数监控、异常报警。  **5**  提供与其它系统集成的接口。 |
|  | **5.2.18** 环保管理子系统提供污染源数据采集、监测和三废排放、治理设施监控、可视化环保地图，并应具有下列功能：  **1** 外排口、内排口在线监测和异常报警。  **2** 提供人工状态监测计划编制、发布、执行和跟踪统计。  **3** 环保治理设施状态监控和异常报警。  **4** 废水、废气、固废排放量计算、监控和统计。  **5** 基于二维或三维可视化的环保地图。  **6** 提供反映工厂环保管理状况数据的统计报告。  **7** 提供与其它系统集成的接口。 |
| **条文说明** | **条文说明** |
| **5.2.9**  设备管理子系统是对设备的运行、维护、保养和状态跟踪等进行管理，为设备预防性维护、缺陷发现等提供及时、准确的信息，减少设备非计划停车，确保设备的长周期运行。  **2** 主要对设备的生产能力、有效作业率等进行核算和评估。  **3** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与实时数据库和ERP的集成接口。 | **5.2.9** 设备健康管理子系统是对设备的运行、故障处置和状态跟踪等进行管理，为设备预防性维护、缺陷发现等提供及时、准确的信息，减少设备非计划停车，确保设备的长周期运行。  **2** 主要对设备的生产能力、性能等进行核算和评估。  **3** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与MES系统中的实时数据库、实验室信息管理、操作管理以及PCS系统中的机组监控和ERP等系统集成接口。 |
| **5.2.10** 能量管理子系统，对水、电、汽、风等公用工程产耗进行综合平衡，优化公用工程的生产运行，合理利用资源、节约能源，降低生产成本，实现对公用工程需求预测、计划、操作、采购、交易、价格评估等的管理与优化。 | **5.2.10** 能源管理子系统，对水、电、汽、风等公用工程产耗进行综合平衡，优化公用工程的生产运行，合理利用资源、节约能源，降低生产成本，实现对公用工程需求预测、计划、操作、采购、交易、价格评估等的管理与优化。 |
|  | **5.2.1**3 工业水管理子系统应对取水单元、输送单元、处理单元、用水单元、排放单元、回收单元的重点参数实现监控和优化，优化工业水生产运行，合理利用水资源，实现对药剂用量和工艺装置的分析优化。  **1** 监控工业水装置运行过程中的关键工艺参数、质量参数，并对异常指标进行报警和趋势分析，辅助水务工艺和操作优化调整。  **2** 采集工业水消耗实物量数据、工艺数据和质量数据并经管网平衡计算后形成统计矫正数据，基于矫正数据，实现药剂、用水量的统计结算和分析。  **3** 应建立与生产装置的产品收率预测相关性模型，对循环水、化学水参数及指标与产品收率影响因素进行相关性数据分析，分析产品收率与工业水直接的相关性，实现优化控制。  **4** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与MES系统中实时数据库、能源管理和ERP的集成接口。 |
|  | **5.2.14**本条规定了碳资产管理子系统的主要功能。  **1** 应执行ISO14064标准中规定的碳排放源分类、水平数据的计算方法，6大碳排放源包括固定排放、制程排放、逸散排放、移动排放、回收利用和间接排放。  **2** 应支持碳排放量的多维度分析、对比和统计，包括但不限于同类设施、同类排放源和历史数据的分析。  **3** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与能源管理、实验室信息管理、物料管理的集成。 |
|  | **5.2.15** 本条规定了应急指挥子系统的主要功能。  **1** 应建立警情模型，实现警情分级管理，支持警情信息通过短信、广播、电话等多路的群发通知。  **2** 基于二三维地理信息地图以可视化的模式集成事故、重大危险源、危化品、物资存放点、消防设施、应急队伍、应急车辆和人员等的位置和相关业务数据。  **3** 应急处置时应根据事故地点，自动关联现场视频监控、移动视频、应急资源分布、救援车辆人员分布、气体探测和气象等信息，自动匹配应急预案。  **4** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与实时数据库、环保管理、火灾及气体检测系统、安保系统、电视监控系统CCTV及ERP的集成。 |
|  | **5.2.16** 本条规定了施工作业管控子系统的主要功能。  **1** JSA建立包括但不限于以下7类作业，包括用火作业、受限空间作业、高处作业、临时用电、起重作业、盲板抽堵、动土作业。  **2** 应提供现场施工作业过程风险库与措施控制数据库功能，在风险识别时，风险与安全防范措施实现自动匹配。  **3** 入厂/场管理应对承包商和监护人员资质信息实现集成，包括对上岗证、监护资格证、特种作业证、签批资格。  **4** 安全防范措施确认、作业票签发宜与物联网定位、二三维地理信息地图进行集成，实现现场“四定”可视化管理，包括定位作业位置、确定作业单位、确定作业票和签发和确定作业时间。  **5** 应利用视频监控以及可燃气体监测系统，对直接作业过程、监护情况进行监测和记录，相关信息集成在系统中，实现事中监测和事后的追溯。  **6** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与火灾及气体检测系统、安保系统、电视监控系统CCTV、应急指挥系统的集成。 |
|  | **5.2.17** 本条规定了危化品管理系统的主要功能  **1** 建立基于二三维地理信息危化品存储库可视化存储模型，集成视频、温度、湿度、烟感、门禁等多种传感器，并与应急指挥进行联动报警。  **2** 危化品运输车辆应配备卫星定位系统和智能视频终端，实现车辆超速、路径偏移报警、人员驾驶异常行为的识别和报警。  **3** 建立危化品输送管道二维矢量可视化流程图，采集危险化学品运输运输环节温度、压力、流量等实时数据，对装置与装置之间的输送管道流通的状态信息进行实时监测。  **4** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与实时数据库、应急指挥以及火灾及气体检测系统、安保系统、电视监控系统CCTV实现集成。 |
|  | **5.2.18**本条规定了环保管理系统的主要功能  **1** 依据《HJ853-2017》，废气管理应建立类别法、实测法、产排污系数法、物料衡算法模型，对废气污染物的排放进行监控，实现从源头、处理过程、排放全过程运行参数的监控。  **2** 依据《中华人民共和国固废污染防治法》的规定，固废管理应以五联单为依据，实现固废申报、入厂、处置、出厂等全过程管理。  **3** 自动采集设施运行参数，实现对环保设施运行状况实现实时监控和异常报警。  **4** 基于人工监测、在线监测和人工录入数据，可按照废水、废气、固废、VOCs等排放物，实现外排口、装置及基于组织机构层级的环保核算统计。  **5** 应建立基于二三维的地理信息可视化地图，集成在线监测、人工监测、治理设施、检查督办等数据。  **6** 应支持标准数据库接口，满足MES其它应用系统对数据接口和数据结构的要求。应重点提供与实验室信息管理、实时数据库的集成。 |
| **6 经营管理系统** | **6 经营管理系统** |
| 6.1 一般规定 | 6.1 一般规定 |
| **6.1.1**经营管理系统应由ERP、CRM和SCM组成。 | **6.1.1**经营管理系统应由ERP、CRM和SCM为核心的一系列功能应用组成。 |
| **6.1.2**系统设计宜采用图6.1.2所示的逻辑结构。 | **6.1.2**系统设计宜采用图6.1.1所示的逻辑结构。 |
|  | **6.1.4**经营管理系统各子系统可从数字化交付获取数据和文档建立设备档案、资产台帐等。 |
| 6.2 设计要素 | 6.1 设计要素 |
| **6.2.1**  ERP应包括财务管理、物资管理、销售管理、生产计划管理、设备管理、质量管理、项目管理、人力资源管理、健康、安全与环保管理等子系统。 | **6.2.1** ERP应包括财务管理、物资管理、销售管理、生产计划管理、设备资产管理、质量管理、项目管理、人力资源管理、健康、安全与环保管理等子系统。 |
| **6.2.2** 财务管理子系统应包括财务会计、管理会计和资金管理等，并应具有下列功能：  **1** 财务会计：主要记录、核算、反映和分析资金在企业经济活动中的变动过程及其结果。包括总账、应收账、应付账、固定资产管理、现金管理及多币制、工资管理等。  4 能与物资管理、销售、生产计划、项目管理等子系统集成。 | **6.2.2**  财务管理子系统应包括财务会计、管理会计和资金管理等，并应具有下列功能：  **1** 财务会计：主要记录、核算、反映和分析资金在企业经济活动中的变动过程及其结果。包括总账、应收账、应付账、现金管理及多币制、工资管理等。  **4** 资产管理：对资产发生的成本费用进行核算和控制，对资产由采购至报废的整个生命周期提供完全支持。资产包括固定资产、在建工程、无形资产、长期待摊费用、使用权资产等。  **5** 能与物资管理、销售管理、生产计划、项目管理等子系统集成。 |
| **6.2.3** 物资管理子系统应对物资的流入、流经以及流出活动进行管理，应包括采购管理和库存管理等，并应具有下列功能：  3 采购管理：是对采购计划与请购、供应商选择、询价、报价、评标、订单、催交、检验、运输及材料接收等采购全过程的管理。  4 库存管理：对库存进行动态的管理、控制、跟踪和计划，管理物资入库、出库、转库、盘点等业务活动，与财务会计集成，进行成本评估。  5 仓库管理；定义仓库结构与货物存放策略，管理库存位置。  6 付款管理。  7 应能与销售、财务管理、生产计划等子系统集成。 | **6.2.3** 物资管理子系统应对物资的流入、流经以及流出活动进行管理，应包括采购管理和库存管理等，并应具有下列功能：  **3** 计划管理：对需求计划提报、变更进行规范管理，通过物料综合平衡生成采购计划。  **4** 采购管理：按照采购计划对采购寻源、采购竞价、采购订单、采购合同等采购过程进行在线管理，包括询价、报价、招标、评标、供应商选择等采购过程活动。  **5** 库存管理：对库存进行动态的管理、控制、跟踪和计划，管理物资入库、出库、转库、盘点等业务活动，与财务会计集成，进行成本评估。  **6** 过程控制：按照采购合同对采购执行过程中的物资质量和交货进度进行有效控制，包括生产制造、物资监造、供应商交货、质量检验、物流运输等功能。  **7** 能与销售管理、财务管理、生产计划、设备资产管理、项目管理等子系统集成。 |
| **6.2.4** 销售管理子系统应对企业内外部资源进行组织和规划，并应对产品销售与分销过程进行业务管理和跟踪监控，同时应具有下列功能：  **4** 发货管理：发货管理根据订单的交货日期对货物装运过程及到期日进行管理。主要功能包括更新订单发货状态及库存记录、生成交运文件及装箱单、生成“过期销售订单交运报告”。 | **6.2.4** 销售管理子系统应对企业内外部资源进行组织和规划，并应对产品销售与分销过程进行业务管理和跟踪监控，同时应具有下列功能：  **4** 发货管理：根据订单的交货日期对货物装运过程及到期日进行管理。主要功能包括更新订单发货状态及库存记录、生成交运文件及装箱单、生成“过期销售订单交运报告”。 |
| **6.2.5** 生产计划管理子系统应制定各种企业资源计划并跟踪执行，并应具有下列功能：  **6** 能与物资管理、销售、财务管理等子系统集成。 | **6.2.5**  生产计划管理子系统应制定各种企业资源计划并跟踪执行，并应具有下列功能：  **6** 能与物资管理、销售管理、财务管理等子系统集成。 |
| **6.2.6** 设备管理子系统应对设备维护计划及维护任务有关的活动进行管理，并应具有下列功能：  **3** 检维修管理：包括检修、故障管理、缺陷管理和费用管理等。 | **6.2.6**  设备资产管理子系统应对设备维护计划及维护任务有关的活动进行管理，并应具有下列功能：  **3** 检维修管理：包括检修、故障管理、缺陷管理和维修费用管理等。 |
| **6.2.7** 质量管理子系统应对质量计划、检验和控制的有关活动和信息进行管理，并应提供各类质量信息的查询、监控、分析与决策，同时应具有下列功能：  **8** 能与物资管理、销售等子系统集成。 | **6.2.7**  质量管理子系统应对质量计划、检验和控制的有关活动和信息进行管理，并应提供各类质量信息的查询、监控、分析与决策，同时应具有下列功能：  **8** 能与物资管理、销售管理等子系统集成。 |
| **6.2.9** 人力资源管理子系统应分析、监控组织结构、人员、薪酬等相关信息和人力资源关键绩效指标，并应具有下列功能：  1 组织结构管理：提供多种预定义组织模式，建立并管理适合企业实际的组织结构。  2 人事管理：实现人员招聘、员工培训与发展、人事成本计划等业务的管理，提供预定义工作流程的功能。  3 薪酬管理：实现员工工时统计、薪资计算、福利和差旅等的管理。  4 统计分析与报表管理：提供数据统计和报表功能，评估和分析人力资源绩效，模拟编制人力资源规划方案，支持辅助决策。  5 能与财务管理、生产计划管理等子系统集成。 | **6.2.9**  人力资源管理子系统应分析、监控组织结构、人员、薪酬等相关信息和人力资源关键绩效指标，并应具有下列功能：  **1** 组织结构管理： 提供多层管理架构，支持组织机构、岗位新增、变更、合并、撤销等管理；灵活设置组织机构属性、基本信息等；灵活查询分析，可回溯查询历史组织机构以及当时的人员情况，生成导出组织结构相关信息。  **2**  员工日常管理：支持员工入职、职业发展、退出的职业生涯周期的全流程体系，包括员工入职管理、试用期管理，内部人力资源调配，员工职业生涯规划与职业发展管理，员工离职、退休、工伤管理等功能。  **3** 时间管理：提供时间及员工出缺勤管理的功能，包括时间数据的收集、分析、为工资计算及休假管理提供数据支持等。自动计算加班费用，休假管理、轮班计划、计算生产奖励，以及劳动成本分配等。  **4** 薪酬和福利管理：支持薪酬核算、发放、过账到财务、银行转账的全过程闭环管理。支持根据人员分类不同，满足多种薪酬结构，提供灵活生成各类工资统计报表。  **5** 绩效管理：支持建立详细的目标和方案，进行绩效反馈审查（考核），薪酬调整，员工绩效可根据设定目标进行评测并作为薪酬发放的基础。  **6** 统计分析与报表管理：提供数据统计和报表功能，支持固定格式导出相关信息数据，可实现各级单位查询的权限控制。  **7** 能与财务管理、生产计划等子系统集成。 |
|  | 6.2.13 合同管理系统应对企业合同的全生命周期进行管理，为企业的业务决策支撑提供依据。并应具有下列功能：  **1** 合同准备：包括对合同基本要素、合同项目信息、合同签约依据等合同准备信息的管理。  **2** 合同订立：包括合同订立、审查审批、打印、签署、内部合同电子签名盖章、外部合同盖章备案等。  **3** 合同履行：主要包括合同变更管理、转让管理、中止管理、发案管理、终止管理、收付款管理等。  **4** 合同终结：主要包括对合同终结、电子归档、纸质归档、临时归档的管理等。  **5** 合同相对人管理：主要包括对合同相对人的资质证照、相对人申请、编辑、复核等进行管理，保证合同相对人的合法性。  **6** 合同文本管理：主要包括对合同文本的申请、审批、启用、版本，编号、引用次数等进行管理。  **7** 查询统计：主要包括合同查询及合同报表等功能，为企业的合同数据查询提供便利。 |
| **条文说明** | **条文说明** |
| **6 经营管理系统** | **6 经营管理系统** |
| **6.2.2** 本条规定了财务管理系统的主要功能。  **1** 财务会计通过与管理会计、销售分销、物流管理、采购等功能的集成，实现企业经济活动中财务会计的记录和管理。  **2** 通过与销售分销、物流管理、采购、设备维护等功能的集成，获取实时的生产经营成本数据，根据企业定义的各组织层面，跟踪企业的成本构成及影响成本的各种因素，基于会计核算的数据，分析比较生产经营中的各种信息，进行相应的预测、管理和控制活动，提供企业内部管理控制及内部考核评价所需的各种信息。 | **6.2.2** 本条规定了财务管理系统的主要功能。  **1** 财务会计通过与管理会计、销售管理、物资管理、采购等功能的集成，实现企业经济活动中财务会计的记录和管理。  **2** 通过与销售管理、物资管理、采购、设备资产管理等功能的集成，获取实时的生产经营成本数据，根据企业定义的各组织层面，跟踪企业的成本构成及影响成本的各种因素，基于会计核算的数据，分析比较生产经营中的各种信息，进行相应的预测、管理和控制活动，提供企业内部管理控制及内部考核评价所需的各种信息。  **4** 资产管理应通过资产的购置、废弃、转移和折旧等业务的输入、计算和处置，有效管理企业实体资产的整个生命周期。 |
| **6.2.3** 物资管理子系统建立供应商档案，确定合理的订货量和供应商，用最新的成本信息来调整库存成本，保证最佳的安全储备，提供订购、验收信息，跟踪催交采购或外委加工的物资，保证货物及时到达。  1 物资指原料、辅料、成品、半成品、生产资源等。物资基础数据指要管理的物资的基础信息，是物资采购、销售业务、库存管理、生产计划以及财务会计管理中最基本、最基础的数据来源，包括描述物资的物理（自然）属性和管理（控制功能）属性，物理属性如规格、名称、密度、描述等，管理属性如编码、类型等。  **3** 采购计划应根据物资需求计划、库存量及设备维护计划确定。采购管理应按工厂管理要求对采购各环节设置相应的审批权限和流程。  5 仓库管理根据工厂实际情况定义仓库结构，将仓库分为不同的物理或逻辑存储区，利用已定义的策略分配货物存放的位置，缩短运输途径，节省时间，减小错误率，提高仓库利用率。仓库管理应与库存管理、销售子系统紧密集成。  6 核对采购订单与采购发票，当两者不一致时，可进行人工干预。发票校验通过后，进行付款确认，并自动将采购数据传递到财务管理子系统中。 | **6.2.3** 物资管理子系统应建立供应商档案，确定合理的订货量，保证最佳的安全储备，提供采购、库存信息，跟踪物资交货进度，保证货物及时到达。  **1** 物资基础数据是物资采购、销售业务、库存管理、生产计划以及财务会计管理中最基本、最基础的数据来源，包括描述物资的物理（自然）属性和管理（控制功能）属性，物理属性如规格、名称、密度、描述等，管理属性如物料类型、采购组等。  **2** 供应商档案信息包括供应商基础数据和采购控制数据，如供应商编码、供应商类型、供应商名称、通讯方式、开户银行等。  **3** 采购计划应根据物资需求计划、库存量及在途资源确定。采购管理应按工厂管理要求对采购各环节设置相应的审批权限和流程。  **5** 加强过程控制，根据采购订单安排质量检查、跟踪交货进度，保证采购质量和货物及时到达。  **6** 采购发票与采购订单、入库单集成，发票校验通过后，进行付款确认，并自动将采购数据传递到财务管理子系统中。 |
| **6.2.4**  销售管理子系统提供实时动态的销售信息资源，为营销业务、内控管理、绩效考评和决策分析提供有效保障。  6 销售统计分析提供销售统计、销售分析和客户分析等。销售统计可根据多种订单属性生成统计结果，销售分析可对目标、渠道、时间、数量、金额、利润及绩效等生成分析结果，客户分析可对客户投诉、原因等生成分析结果。销售分析可采用销售帐目分析、销售功能成本分析、市场单位销售成本分析。 | **6.2.4**  销售管理子系统提供实时动态的销售信息资源，为营销业务、内控管理、绩效考评和决策分析提供有效保障。  **5** 销售统计分析提供销售统计、销售分析和客户分析等。销售统计可根据多种订单属性生成统计结果，销售分析可对目标、渠道、时间、数量、金额、利润及绩效等生成分析结果，客户分析可对客户投诉、原因等生成分析结果。销售分析可采用销售账目分析、销售功能成本分析、市场单位销售成本分析。 |
| **6.2.5**  生产计划管理子系统是以计划为导向的先进的生产和管理方法。  5 生产订单指定加工的物料、时间、地点、作业方式、所需资源及成本结算等。 | **6.2.5**  生产计划管理子系统是以计划为导向的先进的生产和管理方法。  **4** 生产订单指定加工的物料、时间、地点、作业方式、所需资源及成本结算等。 |
| **6.2.6** 设备管理子系统用于生产设备、厂房及其它固定资产的维修保养管理，实现对设备维护维修的进度安排及成本分析等。MES中设备管理子系统，重点实现设备运行状态的监控以及负荷核算与状态评估等。  1 设备物资清单指设备的零部件清单和设备与其零部件的关联关系，便于维修计划过程中设备结构的展示和物资计划的制定。  2 系统基于定义好的维修周期，自动按时产生预防性维修工单，执行有规律的维修任务，优化维护工作，避免生产因为设备故障而停止。工单管理用于规范设备维修流程，缩短维修时间，合理安排维修计划及相关资源与活动，控制维修成本和优化备品备件库存。  3 检维修管理包括检修通知、资源分配及成本分析。资源分配主要指人数、工时、所需材料及工具等的分配。可根据预防性维护计划和检修通知，自动或人工产生维修工单。故障管理包括历史维修记录的管理。 | **6.2.6** 设备资产管理子系统用于生产设备、厂房及其它固定资产的维修保养管理，实现对设备维护维修的进度安排及成本分析等。MES中设备健康管理子系统，重点实现设备运行状态的监控以及负荷核算与状态评估等。  **1** 设备物资清单指构成设备的零部件清单及零部件在设备的具体位置，详细的设备物资清单有利于设备结构的展示及在编制维修计划过程中快速选择维修用物资。  **2**  预防性性维护是针对有规律的周期性维修任务，通过定义预防性维护计划并调用，自动按时生成预防性维修工单。  **3** 检维修管理包括检修通知、检维修工单计划、资源分配及成本分析。资源分配主要指人数、工时、所需材料及工具等的分配。可根据预防性维护计划和检修通知，自动或人工生成维修工单。  **4** 故障管理包括故障提报、故障处理、故障消除、故障原因分析等的过程管理。 |
| **6.2.7** 质量管理子系统贯穿采购、生产、销售与分销全过程，实现原辅料的采购、产成品生产与销售、客户投诉处理等核心业务质量信息的管理及集成，规范并优化质量管理方面的主要业务，完善与固化工作流程。  5 质量通知单提供了处理有关缺陷问题的有效方法。通过质量通知的记录与跟踪执行，可对客户投诉进行记录和处理，帮助企业提高产品质量和客户满意度。 | **6.2.7** 质量管理子系统贯穿采购、生产、销售全过程，实现原辅料的采购、产成品生产与销售、客户投诉处理等核心业务质量信息的管理及集成，规范并优化质量管理方面的主要业务，完善与固化工作流程。  **4** 质量通知单提供了处理有关缺陷问题的有效方法。通过质量通知的记录与跟踪执行，可对客户投诉进行记录和处理，帮助企业提高产品质量和客户满意度。 |
| **6.2.9** 本条规定了人力资源管理子系统的主要功能。  **1** 组织结构主要包括组织单元、职位、工作和任务等。  2 招聘管理应基于互联网发布、收集招聘信息，实现招聘的流程化管理，帮助企业挖掘人力资源。员工培训与发展管理提供查询、判断和评价员工能力和其它有关员工潜力的信息，为员工职业发展制定培训计划，并对培训效果进行评估，管理和查询培训信息。人力成本计划管理按照组织机构计算和管理人事成本，对人事计划做出成本模拟分析和备选方案。  3 工时统计可安排企业的运作时间以及劳动力的工作时间表，记录员工出勤情况。薪资计算可综合各种因素，自动计算薪酬。福利管理可制定福利方案，监督和管理福利项目。差旅管理可制定出差计划，实现出差申请、审批、报销的自动化。  4 在统计分析的基础上，对企业组织结构、人员编制和职务模型的多种方案进行模拟比较和评估，根据组织结构变化，提供人力安排的建议，分析、预测人力成本，辅助管理者做出最终决策。 | **6.2.9** 本条规定了人力资源管理子系统的主要功能。  **1** 组织结构主要包括组织单元、职位、工作和任务等。  **2** 员工日常管理主要包括员工从招聘、入职、内部人力资源调配、职业发展、退出职业生涯的全生命周期管理。  **3** 时间管理主要包括记录员工出勤情况，为工资计算和休假管理提供数据支持。能自动计算加班费用，进行休假管理、轮班计划、计算生产奖励、以及劳动成本分配等。  **4** 薪酬和福利管理包括薪酬核算、发放、过账到财务、银行转账的全过程闭环管理。  **5** 绩效管理包括制定绩效方案和目标、执行绩效评价反馈审查等。  **6**在统计分析的基础上，对企业组织结构、人员编制和职务模型的多种方案进行模拟比较和评估，根据组织结构变化，提供人力安排的建议，分析、预测人力成本，辅助管理者做出最终决策。 |
|  | **6.2.13** 合同管理系统是对合同全生命周期的管理。实现了合同准备、合同订立、合同履行、合同终结的全过程管理，实现了合同相对人、合同标准文本的管理，同时支持对合同数据查询统计。通过合同管理系统的应用，能全面提升了企业的合同管理水平，为企业的业务决策支撑提供依据。 |
|  |  |
| **7 综合信息管理系统** | **7 综合信息管理系统** |
| **7.1 一般规定** | **7.1 一般规定** |
| **7.1.1** 综合信息管理系统应包括OA、EIP，电子文档管理、工厂数据仓库、生产运营指挥等子系统。 | **7.1.1** 综合信息管理系统应包括办公自动化（OA）、企业信息门户（EIP）、电子文档管理、档案管理、工厂数据仓库、生产运营指挥等子系统。 |
| **7.2 设计要素** | **7.2 设计要素** |
| **7.2.1** OA应根据具体的办公业务流程和职能划分，选择下列功能： | **7.2.1** 办公自动化子系统（OA）应根据具体的办公业务流程和职能划分，选择下列功能： |
| **7.2.2** 企业信息门户（EIP）应提供统一的按角色展现的各种信息和业务系统的平台，并应具有下列功能： | **7.2.2** 企业信息门户（EIP）应提供统一的按角色展现的各种信息和业务系统的平台，并应具有下列功能：  6 企业信息门户宜分为内网、外网信息门户。 |
| **7.2.4** 工厂数据仓库子系统应对描述工厂组成元素的相关数据、文件和逻辑与物理模型进行组织和管理，并应基于工厂结构建立数字工厂模型、提供协同工作平台、支撑工厂建设与运维管理，同时应具有下列主要功能：  1 工厂数据仓库系统管理工厂建设期间和运营维护期间的各种工厂数据和文件，提供工厂各管理岗位综合信息查询平台。  2 数字模型实现工厂数据在更广泛业务基础上的紧密关联，将工厂当前状况以视图的形式全面实时地展现给各级决策/管理者。 | **7.2.4** 工厂数据仓库子系统应基于工厂对象的相关数据、文件和逻辑进行组织和管理，基于工厂结构建立数字工厂模型，具备协同工作能力，能够支撑工厂建设期与运维期数据管理，实现对数字工厂模型的管理，并应具有下列主要功能：  1 工厂数据仓库系统管理工厂建设期和运营维护期的各种工厂及工厂对象数据、文件、模型等信息，提供工厂建设期及运营维护期各类信息的综合查询。  2 数字工厂模型实现各类数据在更广泛业务基础上的紧密关联，将工厂当前状况以视图的形式全面实时地展现给各级决策/管理者。 |
| **7.2.5** 生产运营指挥子系统应对分散在不同系统中的离散数据源进行抽取、转换、分析关联和组织，并应将生产运营数据和业务流程进行实时的可视化展示，并应具有下列主要功能：  4 支持标准浏览器的信息展示，支持与EIP的集成。 | **7.2.5** 生产运营指挥子系统应对分散在不同系统中的离散数据源进行抽取、转换、分析关联和组织，并应将生产运营数据和业务流程进行实时的可视化展示，实现企业上下级之间、部门之间沟通的实时、一致与协同，实现对生产运营指挥的辅助决策，并应具有下列主要功能：  4 支持标准浏览器的信息展示，支持与企业信息门户（EIP）的集成。 |
|  | **7.2.6** 档案管理系统是建设涵盖档案全业务流程档案管理体系，实现企业档案的收、存、管、用的全生命周期管理，保证档案的安全规范管理，实现公文和合同档案的在线归档及利用。功能主要包含：  **1** 档案收集。  **2** 档案保管。  **3** 档案利用。  **4** 档案检索。  **5** 档案统计。  **6** 安全。  **7** 还应包括三维工厂的数字化交付、2D/3D设计图纸、工程档案、设计档案的全部电子档案移交和管理。 |
| **条文说明** | **条文说明** |
| **7.2.2** 本条规定了企业信息门户的主要功能。  **3** EIP重点集成经营管理、生产执行、办公自动化、电子文档管理、工厂数据仓库等系统。  **4** 信息展示平台主要应包括在线或离线的信息访问、搜索、内容发布、工作流管理、可视化等功能。  **5** EIP应提供安全的访问控制功能，宜支持单点登录。 | **7.2.2** 本条规定了企业信息门户的主要功能。  **3** EIP重点集成经营管理、生产执行、办公自动化、电子文档管理、工厂数据仓库等业务系统。  **4** 信息展示平台主要应包括在线或离线的信息访问、搜索、内容发布、工作流管理、可视化等功能。建设以企业多项业务为数据的内部门户，实现多业务系统的信息、待办、数据、消息、页面的全面整合。提供一个统一的信息服务功能入口，减少信息孤岛，实现信息共享。  **5** EIP应提供安全的访问控制功能，应支持单点登录。 |
|  | **7.2.6** 档案管理系统是建设涵盖档案全业务流程档案管理体系，实现企业档案的收、存、管、用的全生命周期管理，保证档案的安全规范管理，实现公文和合同档案的在线归档及利用。功能主要包含：  **1** 档案收集。包括档案整理、档案著录、预归档、档案移交清单、目录、脊背等的打印等。  **2** 日常档案管理（保管）。包括库房管理、档案移交功能、档案接收、档案移动、档案鉴定等。  **3** 提供分类检索、跨库检索、全文检索等多维度的检索。  **4** 档案利用。借阅管理、档案共享、专题推送。  **5** 档案统计。包括固定报表查看、用户自定义的统计报表查看。  **6** 档案安全。通过技术手段在档案系统安全模块中增加安全保护措施，如数字水印、离线保护、数字签章等，以保证文档在保管、利用过程中真实、完整、不被篡改，使档案安全管理体系的建设落到了实处。  **7** 具有包括三维工厂的数字化交付、2D/3D设计图纸、工程档案、设计档案的全部电子档案移交和管理功能。 |
| **8　信息系统基础设施** | **8　信息系统基础设施** |
| **8.1 一般规定** | **8.1 一般规定** |
| 8.1.1　信息系统基础设施应包括网络系统、计算机设备、基础软件、存储与备份系统、安保系统、综合布线系统及电子信息系统机房等主要内容。可按应用系统需求减少或扩充信息系统基础设施内容。网络系统应由管理信息网和过程控制网构成。管理信息网应由电信网、安保网和办公与生产管理网构成。 | 8.1.1　信息系统基础设施应包括网络系统、计算机设备、基础软件、存储与备份系统、安保系统、综合布线系统及电子信息系统机房、智能服务平台、融合通讯系统、工业无线网等主要内容。可按应用系统需求减少或扩充信息系统基础设施内容。网络系统应由管理信息网和过程控制网构成。管理信息网应由电信网、安保网和办公与生产管理网构成。 |
|  | 8.1.4 智能服务平台宜以服务形式提供工厂信息系统所需要的资源。应满足下列要求：  1 边缘端数据采集和控制。  2 物联套件设备接入、对象化模型组织、数据存储处理、可视化数据分析、工业APP开发环境、大数据分析和人工智能算法应用等；  3 工业APP及开放的生态环境。  4 支持公有云、私有云、混合云和独立部署。 |
|  | 8.1.5 融合通讯系统宜基于IP网络，采用软硬件配合的交换技术和分布式系统架构，支持将行政电话、调度电话、火灾报警电话、无线集群、CCTV、视频会议及智能终端统讯息统一。系统应具有上述信号源的切换、调度、存档和回放等功能。 |
|  | 8.1.6 工业无线网宜包括工业WiFi无线网、工业4G专网和工业5G等。主要应用的通讯协议和传输技术包括WIA-PA、WIFI、4G、5G等。 |
| **8.7 　安保系统设计要素** | **8.6 　安保系统设计要素** |
| **8.8　综合布线系统设计要素** | **8.7　综合布线系统设计要素** |
| **8.9　电子信息系统机房设计要素** | **8.8　电子信息系统机房设计要素** |
|  | **8.9　智能服务平台设计要素** |
|  | 8.9.1 工业物联网接入服务(IIOT)应实现海量物联数据的采集、接收、集成、转换、标准化以及智能推送，为智能服务平台提供基础的物联接入能力及泛在感知服务。  8.9.2 实时计算环境服务应建立统一的实时计算环境，提供实时计算框架等。  8.9.3 通用PssS服务应包括平台技术服务组件、业务服务组件以及平台的运维监控部件。  技术服务组件宜包括消息总线服务、分布式缓存服务、内容存储服务、日志服务和应用安全服务。  业务服务组件应包括标准化服务，工厂模型服务，生产监测服务，班次日历服务，预测预警服务和物料平衡服务。  8.9.4 企业服务总线宜采用服务总线框架加集成适配器的模式，基于企业业务对象和业务活动建设企业服务库。  8.9.5 宜提供地理信息平台服务，将多种地理信息数据及功能发布成服务地理信息服务包括数据服务、目录服务和功能服务。可供二维地理信息展示，也可实现实时定位。  8.9.6 三维数字化平台服务宜包含工程级、仿真级的工厂三维模型，集成工程建设和运营期的各类数据，为企业提供可视化应用服务。  8.9.7 应用门户和个人工作台是用户访问平台应用（含工业套件、工业App等）的统一入口，应基于应用安全服务并支持自定义用户操作环境和数据按需主动推送。  8.9.8 智能服务平台生态环境具有一定数量工业机理模型、微服务组件或工业APP。 |
|  | **8.10　融合通讯设计要素** |
|  | 8.10.1 融合通讯系统应采用基于网络的分布式层级接入和控制结构。  8.10.2 核心调度平台宜采用双机热备，应支持语音通信的录音和视频通信的录像、在线检索、编辑等。应能够支持PSTN固话、4G/5G手机、集群对讲的音频呼叫，以及对视频监控、移动单兵、视频会议的视频调度。  8.10.3 融合接入网关应支持将各种视频信号接入，办公电话、手机、座机等的互通，支持单呼、群呼、会议等模式。应实现对多种对讲网络的统一接入，应支持跨地域、跨频段的融合互通。录音采集应具备在不影响线路通话的情况下，实时监测线路的通话状态和录音等功能。 |
|  | **8.11　工厂无线网设计要素** |
|  | 8.11.1 工厂无线网应通过无线网核心设备与核心交换机互联，中间宜通过安全策略及安全设施隔离。  8.11.2 工厂无线网对接入的无线终端设备应进行准入身份认证及数据加密。  8.11.3 工厂无线网基站、无线终端设备应根据所在区域防爆安全要求采用相应的防爆防护措施。  8.11.4 基站应选用UPS等不间断供电措施。 |

|  |  |
| --- | --- |
| **条文说明** | **条文说明** |
|  | 8.1.4 智能服务平台是满足石油石化行业数字化、网络化、智能化需求,构建基于海量数据采集、汇聚、分析的服务体系，支撑工业资源泛在连接、弹性供给、高效配置的工业云平台。平台应提供对象模型建模、大数据分析、智能APP组态开发、智慧决策和分析服务。  智能服务平台一般分为三层：  第一层是工业物联服务(IIOT)层，主要负责边缘端数据采集和控制；  第二层是工业操作系统平台（PASS），主要负责物联套件设备接入、对象化模型组织、数据存储处理、可视化数据分析、工业APP开发环境、大数据分析和人工智能算法应用等；  第三层是智能工业APP及生态环境，与合作伙伴一起构建面向石油石化行业的智能工业APP行业全面解决方案。    8.1.5 融合通讯系统宜将语音调度、视频调度、移动单兵调度等多种关键业务功能整合在一个系统上，实现音视频业务的实时交互，满足用户扁平化可视化指挥调度的需求。系统应为基于IP网络、采用软硬件配合的交换技术和分布式系统架构，集行政电话、调度电话、火灾报警电话、无线集群、CCTV、视频会议及智能终端于一体的可视化通信系统。系统应满足各种信号源的切换、调度、存档和回放等功能，并能够实现多级联网融合调度。 |
| 8.2.6 无线网络技术有Wi-Fi、Mesh等技术，设计时采用必要的身份认证和加密技术，如802.1x、WPA加密等确保无线网络的安全性和稳定性。 | 8.2.6 无线网络技术有Wi-Fi、Mesh、4G、5G等技术，设计时采用必要的身份认证和加密技术，如802.1x、WPA加密等确保无线网络的安全性和稳定性。 |
|  | 8.9　智能服务平台设计要素  8.9.1 物联网接入服务(IIOT)实现海量物联数据的采集、接收、集成、转换、标准化以及智能推送，为智能制造平台提供基础的物联接入能力及泛在感知服务。  8.9.2 实时计算环境服务建立统一的实时计算环境，提供实时计算框架等。  8.9.3 通用PAAS服务包括平台核心基础部件、技术服务组件、业务服务组件以及平台的运维监控部件。  8.9.4 技术服务组件宜包括消息总线服务、分布式缓存服务、内容存储服务、日志服务和应用安全服务。  内容存储服务能提供基于分布式的非结构化数据存储和全文检索功能。  日志服务提供对各种日志数据的分布式存储，统一管理和全文检索。  应用安全服务应包括认证、鉴权、审计及单点登录功能。  8.9.5 业务服务组件应包括标准化主数据服务，工厂模型服务，生产监测服务，班次日历服务，预测预警服务和物料平衡服务。  标准化主数据服务对实物资产进行完备的标准化描述，范围覆盖全部系统、设备、零部件及连接部位，粒度粗到工厂级细到零部件级，支持行业级、领域级、企业级等多标准描述和管理能力，为资产数字化提供模型支撑。  工厂模型服务宜按照S95标准定义工厂对象数字化描述。  生产监测服务实时监测工厂状态。  班次日历服务通过配置班次日历的基础数据（包括班次、轮班域、班组、排班逻辑等），提供生产排班、统计排班、统计日历等服务。  利用工业数据湖实现统一数据标准、统一数据模型、统一业务视图、统一数据管控，实现“一次录入、全局使用、数出一家、量出一门”。  8.9.4 企业服务总线采用服务总线框架加集成适配器的模式，基于企业业务对象和业务活动建设企业服务库。  8.9.5 企业数据仓库基于统一的企业数据标准，建设企业全业务模型，集中采集、清洗、加工企业各种异构数据。应实现统一数据标准、统一数据模型、统一业务视图、统一数据管控，提供快速数据建模、数据采集、实时共享和数据分析的可视化管理产品，以及统一的作业调度和过程监控工具。  8.9.6 地理信息平台服务通过平台将多种地理信息数据及功能发布成服务，既可以为安全管控、环保管控提供二维地理信息展示。也可以通过对人员实时位置进行测定，为三维、巡检、应急等上层应用提供准确、稳定的的空间坐标等信息。地理信息服务划分包括为数据服务、目录服务和功能服务。  8.9.7 三维数字化平台是企业级数字工厂模型管理和共享的平台，搭建三维数字化平台，为设备、安环的可视化应用提供支撑环境。三维数字化平台一般包含工程级、仿真级的工厂三维模型，通过集成工程建设和运营期的各类数据，提供运行管理、检维修、技术改造等的可视化应用。  8.9.8 应用门户和个人工作台是用户访问平台应用（含工业套件、工业App等）的统一入口，基于应用安全服务提供菜单、应用操作、业务数据等权限控制，并支持自定义用户操作环境，实现应用访问导航。个人工作台支持将用户需要的数据主动推送。  8.9.9 企业云节点通过对服务器、存储、网络等资源整合和共享，实现云资源（计算、存储、网络和安全等）的可视化、自助化和自动化管理。  管理平台的自服务模块为企业提供全自动的资源支持，支持在线提交服务请求、远程管理和维护已申请的产品和服务。实现在统一的界面上管理与维护云计算节点上的所有资源。  云管理平台应提供应用、虚拟资源和物理资源的统一管理，用户可以根据应用部署需求灵活选择对应的服务。 |
|  | 8.10　融合通讯设计要素  8.10.1 融合通讯平台应提供各类接入网关接口，通过接入网关连接各专业系统，并能够进行协议IP化标准转换，解决协议差异造成的互通阻碍，实现各种通信手段协同。  8.10.2 核心调度平台，负责所有终端的注册和通信的交换，宜支持HA双机热备。语音通信的录音和视频通信的录像，支持录制文件的在线检索、编辑等。  控制终端应能够实现指挥调度人员对PSTN固话、3G/4G手机、集群对讲的音频呼叫，以及对视频监控、移动单兵、视频会议的视频调度。  8.10.3 融合接入网关应支持将各种视频信号接入，办公电话、手机、座机等的互通，支持单呼、群呼、会议等模式。应实现对多种对讲网络的统一接入，应支持跨地域、跨频段的融合互通。录音采集能够实现在完全不影响线路通话的情况下，实时监测线路的通话状态、录音、脱网录音等功能。  视频接入网关应能够将各种视频信号接入到融合调度指挥系统当中，将原有以监控为主的工作方式转变为以调度业务为主体的工作机制。与程控交换系统对接，应实现与办公电话、手机、座机等的互通，支持单呼、群呼、会议等。应实现对多种对讲网络如常规对讲、数字集群的统一接入，应实现跨地域、跨频段的融合互通。录音采集部分应建设为一套电话线路通话信息采集和录制系统，采用旁路连接方式，能够实现在完全不影响线路通话的情况下，实时监测线路的通话状态、录音、脱网录音等功能。  8.10.4 融合通讯传输网络应实现基于以下各种网络部署和通信：  IP网络 融合调度指挥系统的所有服务器设备、网关设备、IP终端、工业电视、视频会议等设备均应能够直接接入到用户的IP网络内。  Wi-Fi网络 在有基于Wi-Fi网络环境下的移动单兵需求时，移动单兵（应满足而不限于智能手机终端、工业防爆终端等）能够通过Wi-Fi网络注册到核心调度平台。  4G网络 在有基于4G公网网络环境下的移动单兵需求时，移动单兵（应满足而不限于智能手机终端、工业防爆终端等）能够通过4G公网网络注册到核心调度平台。 |

|  |  |
| --- | --- |
|  |  |
| **8.6　信息系统安全设计要素** | **9　网络与信息安全** |
|  | **9.1　一般规定** |
| 8.6.1 应依据国家信息系统安全等级保护相关标准，确定信息系统安全等级，设计工厂信息系统安全保障体系。信息系统安全保障体系由技术和管理体系构成。 | 9.1.1应在适度安全与等级保护的原则下，在保证物理安全，建立健全安全运行管理规定的基础上，从技术和管理两个层面着手，以安全技术为支撑，重在管理，构建完善的体系架构。在技术层面上包括架构安全、配置安全和安全技术三方面的内容；在管理层面上包括组织机构、流程管理等内容。 |
| 8.6.2技术体系应包括下列主要内容：  1 物理安全应包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等内容。  2 网络安全应包括结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等内容。  3 主机安全应包括身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制等内容。  4 应用安全应包括身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等内容。  5 数据安全及备份恢复应包括数据完整性、数据保密性、备份和恢复等内容。 | 9.1.2 为保证工控系统安全，对于过程控制系统网络设计应遵循“纵向分层、横向分域、操作分区、控制优先”的设计原则，并应实施安全隔离防护与完整性管理。 |
| 8.6.3 管理体系应包括下列主要内容：  1 安全管理制度应包括管理制度的制定和发布、评审和修订等内容。  2 安全管理机构应包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等内容。  3 人员安全管理应包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容。  4 系统建设管理应包括系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择等内容。  5 系统运维管理应包括环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。 | **9.2　基本安全设计要素** |
| 8.6.4 物理安全设计宜符合现行国家标准《信息安全技术 信息系统物理安全技术要求》GB/T 21052的有关规定。应对信息系统设备、设施、介质和信息免遭自然灾害、环境事故、人为以及各种以物理手段进行的违法犯罪行为导致的破坏和丢失进行重点保护，在系统设备的选择、放置等方面应符合有关防火、防爆、防雷、防腐、HSE等规定。 | 9.2.1 物理环境安全应包括物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、温湿度控制、电力供应、物理位置选择、防静电、电磁防护等内容：  1 机房场地应选择在具有防震、防风和防雨等能力的建筑内；应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。  2 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。  3 应将设备或主要部件进行固定，并设置明显的不易除去的标识；应将通讯线缆铺设在隐蔽安全处。  4 应将各类机柜、设施和设备等通过接地系统安全接地。  5 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。  6 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；应采取措施防止机房内水蒸气结雾和地下积水的转移与渗透。  7 应采用防静电地板或地面并采用必要的接地防静电措施。  8 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。  9 应在机房供电线路上配置稳压器和过电压防护设备；应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。  10 电源线和通信线缆应隔离铺设，避免互相干扰。 |
| 8.6.5 网络构架和软硬件配置应进行安全设计。 | 9.2.2 通信网络安全应包括网络架构、通信传输、可信验证等内容：  1 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。  2 应采用校验技术保证通信过程中数据的完整性。  3 宜基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 8.6.6 信息系统安全应设计有利于实现单点登录、自身安全性能良好的身份鉴别系统。身份鉴别系统应满足下列技术要求：  1 应具备账户、组织结构、身份认证、授权和审计等管理功能。  2 应遵循本地认证与集中认证相结合，静态口令、动态口令与PKI认证相结合，认证、授权与记账（3A）服务器冗余配置等原则。  3 应至少具备用户名/口令、令牌/智能卡、PKI、生物特征鉴别、IP地址和域名、硬件序列号等认证方式中的一种，并应根据系统安全等级选择。 | 9.2.3 区域边界安全应包括边界防护、访问控制、可信验证、入侵防范、恶意代码防范、安全审计等内容：  1 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。  2 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；应能根据会话状态信息为进出数据流提供明确的允许/拒绝访间的能力。  3 应在关键网络节点处监视网络攻击行为。  4 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。  5 应在网络边界、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；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；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。  6 宜基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 8.6.7 访问控制策略应在物理、网络、主机、应用的各个层面部署，并应满足下列技术要求：  1 机房应部署门禁系统，对出入人员进行控制、鉴别和记录。  2 应在网络边界部署访问控制设备，应启用访问控制功能。并应根据访问控制列表对数据包和系统资源实现允许或拒绝用户访问。  3 应启用访问控制功能，并应依据安全策略控制用户对资源的访问。  4 应提供访问控制功能控制用户组和用户对系统功能和用户数据的访问。 | 9.2.4 计算环境安全应包括身份鉴别、访问控制、入侵防范、恶意代码防范、可信验证、数据完整性、数据备份恢复、安全审计、剩余信息保护、个人信息保护等内容：  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，身份鉴别信息具有复杂度要求并定期更换；应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。  2 应对登录的用户分配账户和权限；应重命名或删除默认账户，修改默认账户的默认口令；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；应授予管理用户所需的最小权限，实现管理用户的权限分离。  3 应启用安全审计功能，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；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；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 应遵循最小安装的原则，仅安装需要的组件和应用程序；应关闭不需要的系统服务、默认共享和高危端口；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；应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。  5 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。  6 宜基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。  7 应采用校验技术保证重要数据在传输过程中的完整性。  8 应提供重要数据的本地数据备份与恢复功能；应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。  9 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。  10 应仅采集和保存业务必需的用户个人信息；应禁止未授权访间和非法使用用户个人信息。 |
| 8.6.8 网络系统应部署病毒防护、关键数据及文档加密等系统，对数据传输和存储进行保护。 | **9.3 等级保护设计要素** |
| 8.6.9 网络系统应部署入侵检测、漏洞扫描、安全审计等系统。 | 9.3.1 网络安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，应按照国家标准《网络安全等级保护基本要求》GB/T 22239、《网络安全等级保护定级指南》GB/T 22240开展工作。 |
| 8.6.10 网络系统应按信息系统安全等级规定进行冗余设计和配置，建立适当的冗余恢复机制。 | 9.3.2 信息系统根据其在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素，由低到高划分为五级。 |
| 8.6.11 企业应制定信息系统安全策略。 | 9.3.1 网络安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，应按照国家标准《网络安全等级保护基本要求》GB/T 22239、《网络安全等级保护定级指南》GB/T 22240开展工作。 |
| 8.6.12 企业应设置信息系统安全管理机构，并应制定相应的安全管理制度，同时应定期组织员工进行安全意识培训。 | 9.3.3 信息系统在规划、立项阶段应确定安全保护等级，并制定相应的安全设计方案。 |
| 8.6.13 企业应建立信息系统安全事件应急响应机制，重要信息系统应建立应急预案。 | 9.3.4 等安全保护等级初步确定为第二级及以上的等级保护对象，需进行专家评审、主管部门核准和备案审核，最终确定其安全保护等级。 |
|  | **9.4　工控系统隔离与防护设计要素** |
|  | **9.4.1 控制网络安全配置**  9.4.1.1　网络架构  a) 过程控制系统网络架构的配置应符合纵向分层、横向分域的设计原则。  b) 过程控制系统网络层级宜分为现场总线层（L0）、过程控制层（L1）、操作监控层（L2）、高级应用层（L3）和隔离缓冲区（DMZ，L3.5），各层之间应采用网络交换机连接。  c) 过程控制系统网络应根据工艺操作需要和数据交换最小原则进行横向分区，各分区网络及设备应能独立运行、独立开停车，数据应能独立存储。过程控制层和操作监控层宜按照物理子网方式设置独立分区，也可采用设备虚拟局域网（VLAN）方式分区。  d) 过程控制系统与工厂信息系统的生产执行系统网络之间应通过数据缓冲区隔离为不同区域，区域间应采用工业级网络隔离设备（如硬件防火墙、网闸等）隔离并采取访问控制措施。  e) 过程控制系统应通过OPC服务器和网络隔离设备向设置在数据缓冲区的数据缓冲服务器传输数据，数据缓冲服务器应能通过网络隔离设备向生产执行系统传输数据。  f) 过程控制系统应使用工业级网络设备单独组网，严禁与过程控制系统无关的第三方应用系统、计算机或网络设备接入过程控制网（PCN）。 |
|  | 9.4.1.2　通信传输  a) 过程控制系统的过程控制网（PCN）宜采用冗余、容错的工业以太网组成的局域网，并宜支持TCP/IP协议。  b) 当过程控制系统使用广域网进行控制指令或相关数据传输时，应采用加密认证技术措施实现身份认证、访问控制和数据加密传输。  c) SIS、GDS、CCS、PLC、SCADA等第三方控制系统宜采用Modbus RTU串行通信方式与DCS系统通信，当第三方控制系统采用Modbus TCP通信方式直接接入过程控制层交换机时，应加装工业防火墙隔离。  d) 当独立配置的AAS、OTS、APC、RTO等高级应用服务器与过程控制系统的OPC服务器通信时，应加装工业防火墙隔离。 |
|  | 9.4.1.3　网络设备  a) 过程控制系统应采用带网管功能的工业交换机，宜在高级应用层配置网管服务器，并安装具有对交换机的网络拓扑、流量监测、工作状态及运行负荷进行监控的管理软件。  b) 不同物理网络分区的网络交换机不得共用；不同网络层级的网络交换机不得共用。  c) 现场总线层的网关或通信模件、过程控制层和操作监控层的网络交换机应按1:1冗余配置，并应采用冗余供电方式；高级应用层和数据缓冲区的网络交换机宜按1:1冗余配置，并宜采用冗余供电方式。  d) 工业防火墙、网闸等网络隔离设备应具备检测结果报警及报警信息远传功能。报警日志应至少包括源MAC地址、源IP地址、协议类型、目的MAC地址、目的IP地址、发生时间、处理结果等信息，报警日志保留期限不应小于6个月。  e) 网络隔离设备应独立配置，不得采用带有防火墙功能的网络交换机替代，更不得采用软件隔离代替硬件隔离。网络隔离设备应通过工控系统的安全性和兼容性测试。  f) 网络隔离设备应具备工控系统通信协议内容识别和网络访问控制能力，并应启用网络访问安全策略以保障双向通信安全。  g) 过程控制系统应关闭或限制使用网络交换机、硬件防火墙或路由器上备用的物理端口，应关闭或限制使用服务器中不必要的协议和服务。 |
|  | **9.4.2 区域边界安全防护**  9.4.2.1　访问控制  a) 在过程控制系统中应禁止开通E-mail、Web、Telnet、HTTP及FTP等通用网络服务及拨号访问服务。  b) 应禁止从企业外部网络远程登录、访问、维护过程控制系统。  c) 应在过程控制系统内设置具有安全审计、流量分析、异常检测、入侵检测和报警功能的网络安全监控系统。  d) 应禁止未经国家授权的第三方机构对运行中的过程控制系统进行渗透测试和攻击测试。 |
|  | 9.4.2.2　无线使用控制  a) 过程控制系统确需采用无线网络时，应对无线连接进行授权、监控及隔离。  b) 应对所有参与无线通信的用户（人员 、软件、设备)提供唯一性标识和鉴别，并进行授权及使用范围限制。  c) 应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护。  d) 对采用无线通信技术的过程控制系统，应能识别在其控制区域内发射的未经授权的无线设备，并识别及报告未经授权试图接入或干扰控制系统的行为。 |
|  | 9.4.2.3　身份认证  a) 登录及访问过程控制系统的计算机时，应采用口令密码、USB密钥、IC卡授权、指纹识别或虹膜识别等手段进行身份认证管理。采用口令密码时，应设置强口令密码并定期更换。对于关键控制系统的访问宜采用多因素组合身份认证。  b) 应按最小特权原则合理分类设置用户权限，应定期审计用户权限并做好审计记录。  c) 应加强身份认证信息保护，禁止在不同系统和网络环境下共享。 |
|  | **9.4.3 安全控制环境**  9.4.3.1　控制设备安全  a) 过程控制系统自身应能实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制使得第三方控制系统无法实现上述要求时，应由其上位控制系统或管理系统实现同等功能；  b) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下，应使用专用设备和专用软件对过程控制系统进行补丁更新、软件升级、硬件和固件更新；  c) 应关闭或拆除过程控制系统上的软盘驱动器、光盘驱动器、USB接口、多余串行口或以太网口等，确需保留的应通过相关的技术措施实施严格的监控管理；  d) 应保证过程控制系统在运行前经过了安全性检测，避免控制设备固件中存在恶意代码程序。  e) 在过程控制系统的控制器与过程控制网相连接的控制器侧宜加装工业防火墙。 |
|  | 9.4.3.2　数据备份与恢复  a) 应对过程控制系统中的动态过程数据、动态诊断数据（系统报警、SOE等）、静态工程组态文件（包括数据库、控制程序、联锁逻辑、操作画面及报表等）、控制回路设定参数、报警及联锁设定值等重要数据进行备份和保护。  b) 宜在过程控制系统的高级应用层设置数据备份与恢复（B&R）服务器，对过程控制系统中的全部数据进行周期性自动差分备份，当数据服务器宕机或数据丢失时，应能自动进行数据恢复。  c) 应对过程控制系统中的全部数据和文件进行双份异地磁介质存储备份，每年应至少备份2次，备份数据应至少保留一个大检修周期。 |
|  | 9.4.3.3　时钟同步  a) 过程控制系统应采用一套内置高精度铷原子钟的NTP网络时钟同步服务器，外部时钟源应能同时接收北斗、GPS或其它卫星定位系统的授时信号。  b) 外部时钟源宜仅用于过程控制系统首次开车投用、装置大检修和改造后的再次投用前的系统时间校准。 |
|  | 9.4.3.4　软件补丁和病毒防护  a) 在过程控制系统的工程设计和系统采购阶段，应选定和采购防病毒软件；在硬件集成、软件组态和系统FAT阶段，应同步安装并测试防病毒软件。  b) 在过程控制系统中的操作站、工程师站、服务器等计算机中,应安装经过合法授权并通过厂家的安全性和兼容性测试的防病毒软件，并应采用具有进程和服务功能的应用程序白名单策略。  c) 宜在高级应用层（L3）安装专用的防病毒服务器，也可与网管服务器共用一台服务器，用于集中对过程控制系统中的防病毒软件和/或计算机软件进行离线安装、补丁更新、离线病毒库更新、版本升级和维护管理。  d) 严禁过程控制系统中的任何计算机接入公共网络对软件程序和病毒库进行升级和更新。  e) 防病毒软件应选用主动式病毒防护软件，以防止防病毒软件攻击正常操作软件导致事故发生。防病毒软件应为合法授权的正式版本，并且已通过控制系统厂家的安全性和兼容性测试。  f) 当发现过程控制系统疑似被病毒感染时，应按照应急预案及时采取紧急防护措施。 |
|  | 9.4.3.5　物理和环境安全防护  a) 对于过程控制系统的操作站、工程师站、服务器、控制器、I/O单元、网络设备等关键设备所安装的中心控制室、现场机柜室等区域应采取门禁和访问控制措施，并应安装视频监控系统、防侵入系统等物理安全防护措施。  b) 应拆除或关闭过程控制系统中计算机上不必要的USB口、光盘驱动器、无线接口等，应采取专盘、专用、专人管理等手段避免非法侵入，应严格限制和管理便携式计算机、移动操作终端、PDA等终端设备的使用。  c) 工业防火墙、网闸等网络隔离设备应具备对工控系统安装场所的工作温度、电磁兼容性、安装方式、供电方式、接地方式等物理环境的适用能力，其安全可靠性应符合过程控制系统的长周期运行要求。 |
| **引用标准名录** | **引用标准名录** |
|  | 信息安全技术 网络安全等级保护基本要求，GB/T 22239-2019  信息安全技术 工业控制系统安全控制应用指南，GB/T 32919-2016 |
| **条文说明** | **条文说明** |
| **8.6　信息系统安全设计要素** | **9 网络安全**  **9.1　一般规定** |
| 8.6.1 在建立工厂信息系统的同时应在适度安全、等级保护的原则下，依据国家信息系统安全等级保护相关标准，确定信息系统安全等级，建立有效的信息系统安全保障体系，满足信息的机密性、完整性、可用性、可控性、抗抵赖性等方面的安全需求。 | 9.1.1应在适度安全与等级保护的原则下，在保证物理安全，建立健全安全运行管理规定的基础上，从技术和管理两个层面着手，以安全技术为支撑，重在管理，构建完善的体系架构。在技术层面上包括架构安全、配置安全和安全技术三方面的内容；在管理层面上包括组织机构、流程管理等内容。 |
| 8.6.2 通过专用的安全技术，如身份鉴别、访问控制、内容安全、冗余恢复和审计跟踪等，实现信息系统的安全防护、检测和响应恢复。 | **9.2　基本安全设计要素** |
| 8.6.5 网络构架安全设计应重点考虑安全域的划分以及Internet、服务器、终端等接入安全。应对各种网络设备、计算机设备、应用软件和系统软件在功能可用性配置的基础上，重视安全配置设计。 | 9.2.2应在安全通信网络设置审计机制,由安全管理中心管理。  可采用由密码等技术支持的完整性校验机制,以实现通信网络数据传输完整性保护。  可采用由密码等技术支持的保密性保护机制,以实现通信网络数据传输保密性保护。  通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品,在设备连接网络时,对源和目标平台身份、执行程序进行可信验证,并将验证结果形成审计记录。 |
| 8.6.6 身份鉴别是对系统中的主客体进行鉴别，并且给这些主客体赋予恰当的标志、标签、证书等。 | 9.2.3应根据区域边界安全控制策略,通过检查数据包的源地址、目的地址、传输层协议和请求的服务等,确定是否允许该数据包通过该区域边界。  应在安全区域边界设置审计机制,并由安全管理中心统一管理。  可在安全区域边界设置防恶意代码网关,由安全管理中心管理。  应在区域边界设置探测器,探测非法外联等行为,并及时报告安全管理中心。  宜基于可信根对区域边界计算节点的BIOS、引导程序、操作系统内核、区域边界安全管控程序等进行可信验证,并在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录。 |
| 8.6.7 访问控制是控制和检查主体对客体的访问，实现权限管理和分级控制的技术。访问控制技术应融入到机房管理、网络设备、计算机设备、基础软件、应用软件等信息系统的各个环节。 | 9.2.4应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户表示的唯一性；在每次用户登录系统时，采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别，并使用密码技术对鉴别数据进行保密性和完整性保护。  应在安全策略控制范围内,使用户对其创建的客体具有相应的访问操作权限,并能将这些权限的部分或全部授予其他用户。访问控制主体的粒度为用户,客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。  应提供安全审计机制,记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。该机制应提供审计记录查询、分类和存储保护,并可由安全管理中心管理。  可采用常规校验机制,检验存储的用户数据的完整性，以发现其完整性是否被破坏。  可采用密码等技术支持的保密性保护机制,对在安全计算环境中存储和处理的用户数据进行保密性保护。  应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品,对用户使用的客体资源,在这些客体资源重新分配前,对其原使用者的信息进行清除,以确保信息不被泄露。  应安装防恶意代码软件或配置具有相应安全功能的操作系统,并定期进行升级和更新,以防范和清除恶意代码。  宜基于可信根对计算节点的BIOS、引导程序、操作系统内核、应用程序等进行可信验证,并在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录。 |
| 8.6.8 在网关、服务器、桌面系统、邮件系统等多个层次上构建集中管理的企业级病毒防护系统。关键数据及文档加密系统应具备一定强度的加密机制，提供内容级的加密和权限管理，支持集中管理、分散使用，具备动态加解密、实时权限回收、离线安全使用等机制，保证其机密性。 |  |
| 8.6.9 应部署基于网络的入侵检测系统（NIDS）及针对关键服务器的主机入侵检测系统（HIDS）。入侵检测系统的功能和技术指标宜符合国家标准《信息安全技术 入侵检测系统技术要求和测试评价方法》GB/T 20275的要求，并选用性能良好、特征库更新及时可靠的产品。  漏洞扫描系统的功能和技术指标宜符合国家标准《信息安全技术 网络脆弱性扫描产品技术要求》GB/T 20278、《信息安全技术 网络脆弱性扫描产品测试评价方法》GB/T 20280的要求，并选用性能良好、漏洞库更新及时可靠的产品。  安全审计内容包括重要用户行为、系统资源使用、重要系统命令使用等系统内重要的安全相关事件。审计记录应包括事件的日期、时间、类型、主客体标识和结果等。安全审计应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。 |  |
| 8.6.10 冗余恢复机制一般包括网络结构冗余、关键网络设备冗余、网络设备关键部件冗余、安全设备冗余及服务器冗余等。冗余恢复实现了对异常、故障、事故、入侵等安全事件发生后的有效响应。 |  |