S/N:1580242·026
9 158024 202601

统一书号：1580242·026
定　价：20.00元

油气田及管道工程计算机控制系统设计规范

中国计划出版社

UDC

中华人民共和国国家标准

P

GB/T 50823－2013

油气田及管道工程计算机控制系统设计规范

Code for computer control system design of oil/gas fields and pipelines

2012－12－25 发布　　2013－05－01 实施

中华人民共和国住房和城乡建设部
中华人民共和国国家质量监督检验检疫总局　联合发布

中华人民共和国国家标准

油气田及管道工程计算机控制系统设计规范

Code for computer control system design of oil/gas fields and pipelines

GB/T 50823 - 2013

主编部门：中国石油天然气集团公司
批准部门：中华人民共和国住房和城乡建设部
施行日期：2013年5月1日

中国计划出版社

2013 北京

中华人民共和国国家标准
油气田及管道工程计算机控制系统
设 计 规 范
GB/T 50823-2013
☆
中国计划出版社出版
网址：www.jhpress.com
地址：北京市西城区木樨地北里甲11号国宏大厦C座3层
邮政编码：100038　电话：(010) 63906433（发行部）
新华书店北京发行所发行
北京世知印务有限公司印刷

850mm×1168mm　1/32　3.125印张　78千字
2013年5月第1版　2013年5月第1次印刷
☆
统一书号：1580242·026
定价：20.00元

中华人民共和国住房和城乡建设部公告

第1600号

住房城乡建设部关于发布国家标准《油气田及管道工程计算机控制系统设计规范》的公告

现批准《油气田及管道工程计算机控制系统设计规范》为国家标准，编号为GB/T 50823—2013，自2013年5月1日起实施。

本规范由我部标准定额研究所组织中国计划出版社出版发行。

中华人民共和国住房和城乡建设部
2012年12月25日

前　言

本规范是根据住房和城乡建设部《关于印发〈2010年工程建设标准规范制订、修订计划〉的通知》(建标〔2010〕43号)的要求，由胜利油田胜利勘察设计研究院有限公司会同有关单位编制而成。

本规范编制过程中，编制组进行了广泛调查研究，认真总结实践经验，参考国内外有关标准，并在广泛征求意见的基础上，经审查定稿。

本规范共分9章和2个附录，主要内容包括：总则、术语和缩略语、系统结构和适用范围、基本过程控制系统(BPCS)、安全仪表系统(SIS)和火气系统(FGS)、系统软件及功能、控制盘和机柜、电气设计、控制室等。

本规范由住房和城乡建设部负责管理，由石油工程建设专业标准化委员会负责日常管理，由胜利油田胜利勘察设计研究院有限公司负责具体技术内容的解释。执行过程中如有意见或建议，请寄送胜利油田胜利勘察设计研究院有限公司(地址：山东省东营市济南路49号，邮政编码：257026)，以供今后修订时参考。

本规范主编单位、参编单位、主要起草人和主要审查人：

主编单位：胜利油田胜利勘察设计研究院有限公司

参编单位：大庆油田工程有限公司

中国石油天然气管道工程有限公司

主要起草人：田京山　程云海　王怀义　刘　强

徐　晶　梅　斌　梅　刚　张德发

高　原　冯立法　刘晓刚　聂中文

邢建芬　刘少宇　王志强　纪志军

王　静　王　愔　闫　辉　李　瑾
宋衍茹　杨立萍　李　敬

主要审查人：朱瑞苗　王小林　于建林　谷汉军
聂　华　王　新　高　湘　于清澄
陈月兰　张贵林　雷艳丽　李昌岑
张　涛　张正友

目　次

Contents

1 总 则

1.0.1 为指导和规范油气田及管道工程中计算机控制系统的设计工作，做到技术先进、经济合理、安全适用、节能环保，制定本规范。

1.0.2 本规范适用于陆上油气田及管道工程中新建、改建和扩建工程的计算机控制系统设计。

1.0.3 油气田和管道工程计算机控制系统的设计除应符合本规范外，尚应符合国家现行有关标准的规定。

2 术语和缩略语

2.1 术　语

2.1.1 计算机控制系统　computer control system

由一台或多台计算机、控制器、相关硬件、软件和通信网络组成对生产过程进行监视、控制及管理的控制系统。

2.1.2 基本过程控制系统　basic process control system

不执行任何安全完整性等级大于或等于1级的安全仪表功能，响应过程测量以及其他相关设备、其他仪表、控制系统或操作员的输入信号，按过程控制规律、算法、方式，产生输出信号实现过程控制及其相关设备运行的系统。

2.1.3 安全仪表系统　safety instrumented system

实现一个或多个安全仪表功能的系统。

2.1.4 火气系统　fire gas and smoke detection and protection system

用于监控火灾和可燃气、有毒气泄漏并具备报警和消防、保护功能的安全控制系统。

2.1.5 集成控制系统　integrated control system

将各自独立运行的基本过程控制系统、仪表安全系统和/或火气系统，通过通信网络链接在一起、共享操作显示的控制系统。

2.1.6 分散控制系统　distributed control system

控制功能分散、操作显示集中、采用分级结构的计算机控制系统，也称为分布式控制系统，或集散控制系统。

2.1.7 监控和数据采集系统　supervisory control and data acquisition system

以多个远程终端监控单元通过有线或无线网络连接起来，具有远程监测控制功能的分布式计算机控制系统。

2.1.8 可编程序控制器　programmable logic controller

是一种数字运算操作的电子系统，专为在工业环境下应用而设计。它采用了可编程序的存储器，用于在其内部存储执行逻辑运算、顺序控制、定时、计数和算术运算等操作指令，并通过数字或模拟式的输入和输出操作，控制各种类型的机械或生产过程。

2.1.9 远程终端单元　remote terminal unit

针对通信距离较长和工业现场恶劣环境而设计的具有模块化结构的特殊的计算机控制系统，它将末端检测仪表和执行机构与远程主控制系统连接起来，具有数据采集、控制和通信功能，它能接收主控制系统的操作指令，控制末端的执行机构动作。

2.1.10 安全完整性等级　safety integrity level

为安全功能的等级。安全完整性等级由低到高为SIL1～SIL4。

2.1.11 安全仪表功能　safety instrumented function

为了防止、减少危险事件发生或保持过程安全状态，用一个或多个测量仪表、逻辑控制器、最终元件及相关软件等实现的安全保护功能或安全控制功能。

2.1.12 维护超驰　maintenance override

在设备或线路维护期间，以预设值代替实际输入值，使安全仪表系统或火气系统连续工作的一种功能。

2.1.13 操作超驰　operational override

工艺过程启动期间，在预定的启动时间内以预设值代替实际输入值，用以满足启动条件的一种功能。

2.1.14 硬手操盘　hardwired panel

是由一系列按钮、开关、信号报警器及信号灯等组成，与控制器硬线连接，应独立于基本过程控制系统，完成最基本的紧急停车、火气消防操作与报警指示。

2.2 缩 略 语

CCR(central control room) 中央控制室或中控室
BPCS(basic process control system) 基本过程控制系统
DCS(distributed control system) 分散控制系统
DDE(dynamic data exchange) 动态数据交换
DMZ(demilitarized zone) 隔离区
ERP(enterprise resource planning) 企业资源管理系统
ESD(emergency shutdown) 紧急停车
FGS(fire gas and smoke detection and protection System) 火气系统
HMI(human machine interface) 人机接口
ICS(integrated control system) 集成控制系统
I/O(input/output) 输入/输出
KVM(keyboard、video、mouse) 键盘、显示器和鼠标
MIS(management information system) 管理信息系统
MOS(maintenance override switch) 维护超驰开关
MTBF(mean time between failures) 平均故障间隔时间
MTTR(mean time to repair) 平均修复时间
MTTF(mean time to failures) 平均无故障时间
OOS(operational override switch) 操作超驰开关
OPC[object linking and embedding(OLE) for process control] 用于过程控制的对象链接与嵌入
PLC(programmable logic controller) 可编程序控制器
RTU(remote terminal unit) 远程终端单元
SCADA(supervisory control and data acquisition) 监控和数据采集
SIF(safety instrumented function) 安全仪表功能
SIL(safety integrity level) 安全完整性等级

SIS(safety instrumented system) 安全仪表系统
SOE(sequence of event) 事件顺序记录系统
SPD(surge protective device) 电涌保护器
SQL(structured query language) 结构化查询语言

3 系统结构和适用范围

3.1 一 般 规 定

3.1.1 计算机控制系统硬件和软件应符合国家现行有关标准或相关国际标准的规定。

3.1.2 所选用的计算机控制系统硬件和软件应是经过类似工况和环境条件现场考验并良好运行的系统和设备。

3.1.3 系统的硬件和软件配置及其功能应与工艺过程的规模和控制要求相适应，并应易于扩展和维护。

3.1.4 系统设计应以系统生命周期成本最少为基本原则。

3.1.5 油气田工程计算机控制系统的设计要求应符合本规范附录A的规定，管道工程SCADA系统的设计要求应符合本规范附录B的规定。

3.2 系 统 结 构

3.2.1 典型的计算机控制系统结构宜由BPCS、SIS和FGS等子系统组成(图3.2.1)。

3.2.2 BPCS应通过通信接口与站场内外的第三方设备和/或系统连接。

3.2.3 通过必要的DMZ隔离措施，计算机控制系统和设备管理系统可向连接在信息网络上的其他系统提供数据。

3.3 系统适用范围

3.3.1 根据测控对象的不同，计算机控制系统可分为BPCS、ICS和SCADA三类。

3.3.2 采用计算机控制系统的站(库)应至少含BPCS。

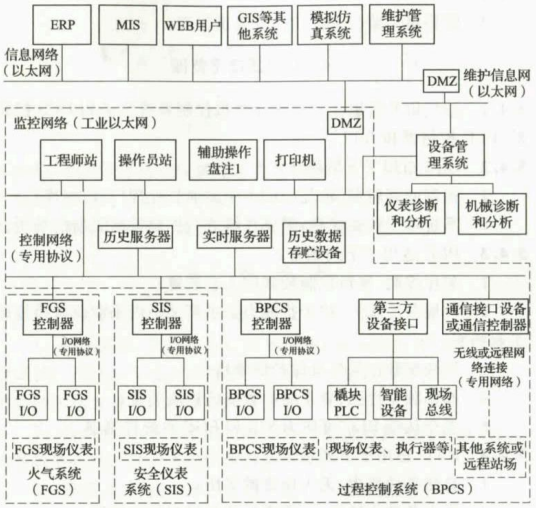

图3.2.1 典型计算机控制系统结构示意图

注：辅助操作盘应通过硬线与BPCS、SIS或FGS I/O模板连接。

3.3.3 ICS适用于下列场合：

1 由BPCS、SIS和FGS三个子系统组成的站(库)控制系统；

2 由BPCS和SIS两个子系统组成的站(库)控制系统；

3 由BPCS和FGS两个子系统组成的站(库)控制系统。

3.3.4 SCADA适用于下列场合：

1 测控点相对分散、距离较远，站场较多且分布较广，需用多个ICS、BPCS通过有线(或无线)通信方式集中到控制中心的

工程；

2 需要集中监控的油气田及管道工程。

3.4 控制器适用范围

3.4.1 油气田及管道工程领域计算机控制系统宜采用 DCS 控制器、PLC 控制器和 RTU。

3.4.2 DCS 适用于下列场合：

1 控制回路较多、较复杂的大中型油气处理厂及站(库)；

2 系统可用性要求高，需要在线进行控制策略更新的场所。

3.4.3 PLC 适用于下列场合：

1 顺序控制、逻辑控制较多的工艺装置；

2 环境条件恶劣、抗干扰能力要求高又不需采取改善措施的工业场所；

3 需快速数据采集及保护的场所；

4 操作独立性强、要求结构紧凑的橇块装置；

5 安全认证 PLC 可作为 SIS 和 FGS 系统控制器。

3.4.4 RTU 适用于下列场合：

1 自然条件恶劣、无人值守的场所；

2 供电条件比较恶劣，需要低功耗控制器的场所；

3 功能简单、监控点数少的场所。

4 基本过程控制系统(BPCS)

4.1 一 般 规 定

4.1.1 系统的可用性应满足工艺过程要求。

4.1.2 系统应具有良好的安全性。

4.1.3 系统应选用开放式结构，软硬件应模块化。

4.2 服 务 器

4.2.1 服务器应具有下列主要功能：

1 数据采集：负责与 I/O 采集设备(控制器或其他外围智能设备)进行通信，完成实时数据采集、控制、整定和工程值转换，可对数据采集方式和轮询时间进行设定。

2 数据服务：对采集的实时 I/O 数据进行数据库存储，并应为系统的各种数据请求提供数据源服务。

3 报警：根据报警组态自动产生并记录报警。

4 事件：记录系统、操作及各类动作触发的事件。

5 报表及打印：根据组态自动或人工触发报表并输出。

6 历史数据记录：根据组态按一种或几种速率将实时数据保存在历史数据库中。

7 历史归档：系统自动或手动将数据归档备份，需要时能从外部存储中恢复数据。

8 网络通信管理：向下对控制网进行管理，调度服务器与各控制器和智能设备间的通信，处理各种接口及通信协议转换；可管理与操作员站、工程师站、远程工作站、外部服务器等的通信。

9 安全管理：根据设置和设定的安全策略校核数据及服务请

求，允许合法用户的访问，禁止非法用户的请求。

4.2.2 服务器应根据系统规模、I/O 吞吐量、数据响应设置。服务器应根据系统的可用性和实际需要采取单机、冗余或按集群方式配置。

4.2.3 服务器硬件应选用商用产品，操作系统软件应采用商用开放平台。

4.2.4 满负荷应用条件下服务器应符合下列规定：

1 CPU 使用率除系统或程序启动外不应大于 40%；

2 内存使用率不应大于 50%；

3 网络占用率不应大于 60%。

4.2.5 服务器应采用冗余热拔插硬盘和电源。

4.2.6 小型系统服务器可与操作员工作站合二为一。

4.3 操作员工作站

4.3.1 操作员工作站应能与服务器通信，并应具有显示、操作、报警和打印功能，可作为 BPCS、SIS 和 FGS 等子系统的统一人机界面。

4.3.2 操作员工作站配置应符合下列规定：

1 操作员工作站可按权限和操作区域配置；

2 重要单元宜配置专用操作员工作站；

3 多台操作员站间应互为备用；

4 无人值守站场不宜设操作员工作站。

4.3.3 可根据需要设置无线或移动操作员站，此类操作员站应以监视和信息传送为主，不应具有操作和控制功能。

4.4 工程师工作站

4.4.1 工程师工作站应执行系统及设备的组态/编程（离线、在线）、调试、修改、测试、装载等功能，可进行系统管理。

4.4.2 工程师工作站与控制器连接宜通过控制网。

4.4.3 工程师工作站的配置应符合下列规定：

1 工程师工作站应根据系统的需要配置；

2 中央控制室/调度控制中心应配置工程师工作站；

3 数量多、分布地域广的站场宜配置便携式工程师工作站。

4.5 过程控制单元

4.5.1 控制器应能满足过程控制的要求，并应具有下列功能：

1 扫描和更新 I/O 数据；

2 连续控制；

3 批量及顺序控制；

4 逻辑和运算；

5 延时、计数和定时；

6 报警和系统诊断；

7 时钟同步；

8 接口通信。

4.5.2 控制器可为事件、报警和数据附加时间标签。

4.5.3 控制器负荷不应大于 70%。

4.5.4 重要站场（厂）的控制器、通信接口及电源应 1∶1 冗余配置。应根据系统的可用性和实际需要确定 I/O 模板的冗余配置。

4.5.5 各类 I/O 模板的技术规格应与现场信号源和负载匹配。

4.5.6 I/O 模板通道数量应符合下列规定：

1 模拟量输入模板不应多于 16 通道；

2 模拟量输出模板不应多于 8 通道；

3 热电阻、热电偶和脉冲量输入模板不应多于 8 通道；

4 数字量输入、数字量输出模板不应多于 32 通道。

4.5.7 信号应根据 I/O 信号类型、电源、电压等级、干扰和接地情况进行隔离，并应符合下列规定：

1 模拟输入模板通道与系统间应隔离；

2 有源模拟量输入信号应采用差分/双端输入和通道隔离；

3 接地不良的模拟量输入信号应采用差分/双端输入和通道隔离；

4 由强电磁干扰场合来的模拟量输入信号宜采用差分/双端输入和通道隔离；

5 模拟输出模板通道间、通道与系统间应隔离；

6 数字量输入模板应优先采用光电隔离，数字量输出模板应采用光电隔离或继电器隔离；

7 电压超过 36V 的数字量输入/输出信号宜采用继电器隔离；

8 由强电磁干扰场合来的数字量输入/输出信号宜采用继电器隔离。

4.5.8 I/O 点的备用量应符合下列规定：

1 各类 I/O 点的备用量应为实际 I/O 点数的 10%～30%；

2 I/O 卡件槽(位)的备用空间应为实际使用卡件槽(位)的 10%～30%。

4.5.9 所有 I/O 模板可远程组态，组态信息应记录。

4.5.10 I/O 模板宜能在线热拔插。

4.5.11 I/O 模板关联设备的配置应符合下列规定：

1 转换器或隔离器应根据信号源与 I/O 模板连接的需要设置；

2 本质安全回路应设置安全栅或采用具有本质安全认证的隔离 I/O 模板；

3 SPD 的设置应符合本规范第 8.3 节的要求。

4.5.12 距控制室较远的检测点，宜采用远程 I/O 单元或远程控制站。

4.6 网络与通信

4.6.1 计算机控制系统应支持标准的通信协议，且宜支持多种控

制器。

4.6.2 系统的通信接口应根据需要配置串行和并行通信接口、远程 I/O 通信接口、以太网(Ethernet)、DCS/PLC/RTU 接口、视频接口等。

4.6.3 通信网络的负荷不应超过 60%。

4.6.4 根据当地气候特点和供电情况，通信网络应采取必要的防雷及防电涌保护措施。

4.6.5 现场网络接口宜采用串行或以太网接口。

4.6.6 I/O 网络配置应符合下列规定：

1 I/O 网络宜冗余或环路配置；

2 远程 I/O 网络应冗余或环路配置；

3 远程 I/O 网络通信介质宜采用光纤。

4.6.7 控制网络宜采用工业以太网。控制网络应符合下列规定：

1 控制网络宜冗余或环路配置；

2 远程控制网络通信介质宜采用光纤，可采用公网、无线、卫星等。

4.6.8 监控网络宜采用工业以太网。大型或安全性要求高的系统，监控网络和控制网络宜分开设置。监控网络应符合下列规定：

1 中型系统监控网络宜冗余或环路配置；

2 大型系统或安全性要求高的系统，监控网络应冗余或环路配置；

3 远程监控网络应冗余或环路配置；

4 对移动操作员站应采取防止误操作、病毒、非法入侵等安全措施。

4.6.9 信息网络与计算机控制系统网络之间的连接应设置必要的隔离设备。

4.7 辅助操作设备

4.7.1 操作需要时可设置辅助操作台(盘)。

4.7.2 现场控制盘可设置触摸屏或操作面板。

4.8 外围设备

4.8.1 BPCS宜配置报警打印机和报表打印机，并可配置屏幕拷贝打印机。

4.8.2 操作员工作站和工程师工作站可配置专用键盘。

4.8.3 除键盘外，所有外围设备及接口应采用通用产品。

4.8.4 机架安装的冗余服务器宜通过KVM切换器共享键盘、鼠标和显示器。

5 安全仪表系统(SIS)和火气系统(FGS)

5.1 一般规定

5.1.1 安全仪表系统的具体要求应符合现行国家标准《石油化工安全仪表系统设计规范》GB/T 50770的有关规定。

5.1.2 安全仪表系统和火气系统设计应满足可靠性、可用性、可维护性、可追溯性和经济性要求。

5.1.3 安全仪表系统和火气系统的构成应使中间环节最少。

5.1.4 安全仪表系统和火气系统应通过硬线与现场仪表和设备连接。

5.1.5 安全仪表系统和火气系统应具有系统硬件和软件自诊断功能。

5.1.6 最终执行元件应由安全逻辑控制，不应手动干预安全逻辑的运行。

5.1.7 安全仪表系统和火气系统应设置SOE。

5.1.8 超驰期间应符合下列操作防护规定：

1 超驰不应屏蔽信号的报警功能；

2 超驰状态应报警，报警宜每隔2h重复一次；

3 超驰时间应限定，不宜超过8h；

4 传感器被超驰期间，应有备用手段或措施触发该传感器对应的最终执行元件；

5 BPCS故障不应影响超驰功能；

6 应设置“超驰允许”开关，转到“正常”状态可解除所有超驰。

5.2 安全仪表系统(SIS)

5.2.1 应根据确定的安全仪表完整性等级进行安全仪表系统配置。

5.2.2 安全仪表系统可实现一个或多个安全仪表功能，多个安全仪表功能可使用同一个安全仪表系统。当多个安全仪表功能在同一个安全仪表系统内实现时，系统内的共用部分应符合各功能中最高安全完整性等级要求。

5.2.3 SIL1 级 SIS 系统控制器宜独立，SIL2 级、SIL3 级 SIS 系统控制器应独立。

5.2.4 安全仪表系统的控制器、通信网络及供电电源宜冗余。

5.2.5 安全仪表系统的控制器、I/O 模板、电源及内部通信网络应具有相应的 SIL 认证。

5.2.6 安全仪表逻辑重启前应先复位。

5.2.7 安全仪表功能宜局限在本地，不宜使用远程停车控制。

5.2.8 在过程测控点较少且安全完整性等级小于或等于 SIL2 级的场合，可使用一套 SIS 控制器完成 BPCS 和 SIS 系统功能。

5.3 紧急停车(ESD)功能

5.3.1 ESD 功能回路应为故障安全型。

5.3.2 ESD 应根据故障的性质和工艺要求分级，高级别应自动触发低级别停车。

5.3.3 ESD 不应采用串级停车逻辑。

5.3.4 关断执行后，相关联的非 SIS 设备宜联锁动作到安全位置。

5.3.5 除紧急停车按钮输入外，所有可触发停车的输入信号应设置维护超驰开关，输出信号不应设置。

5.3.6 影响工艺过程启动的输入信号应设置操作超驰开关，应根据工艺要求设置操作超驰延时时间，工艺过程正常或延时结束后，应自动解除操作超驰。

5.4 火气系统(FGS)

5.4.1 安全仪表系统与火气系统宜分开设置。

5.4.2 在安全仪表系统和火气系统点数较少时，两个系统可合用一套控制器，I/O 模板应分开，FGS 逻辑和 ESD 逻辑应分开。

5.4.3 当火气系统与安全仪表系统完全独立时，两者之间的信号应通过硬线连接。

5.4.4 探测器报警和火气逻辑重启前应先手动复位。

5.4.5 除手动报警按钮输入外，所有输入信号宜设置维护超驰开关，输出信号不应设置。

5.5 通 信 接 口

5.5.1 安全仪表系统、火气系统与基本过程控制系统间通信接口和网络应冗余。

5.5.2 安全仪表系统和火气系统的通信负荷不应超过 50%。

5.6 辅助操作设备

5.6.1 辅助操作设备应包括硬手操盘和(或)模拟显示盘(屏)，安全仪表系统应配置硬手操盘；火气系统宜设置硬手操盘，可设置模拟显示盘(屏)。

5.6.2 硬手操盘和模拟显示盘(屏)可独立设置，或与 BPCS 辅助操作台(盘)合并设置。

5.6.3 硬手操盘和模拟显示盘(屏)应通过硬接线与 SIS 和(或) FGS 连接。

5.6.4 硬手操盘应符合下列规定：

1 按钮应有防误触发保护；

2 ESD 和火灾、气体触发按钮应为红色带锁定按钮，相应指示灯应为红色；

3 复位按钮应为黑色；

4 维护超驰和操作超驰允许钥匙开关应为黄色，对应指示灯为黄色；

5 运行和正常指示灯为绿色，故障指示灯为红色；

6 硬手操盘应设置指示灯测试按钮，按钮为白色。

5.6.5 模拟显示盘(屏)应符合下列规定：

1 火灾、ESD公共报警指示灯为红色；

2 气体泄漏公共报警指示灯为黄色；

3 消防释放阀释放和工厂健康状态指示灯为绿色；

4 测试按钮为白色。

6 系统软件及功能

6.1 基本配置和功能

6.1.1 计算机控制系统应配置操作系统软件、监视控制软件、组态和编程软件、诊断和管理软件，根据需要可配置高级应用软件。

6.1.2 操作系统软件应符合下列规定：

1 系统应支持分布式网络，宜支持冗余结构；

2 应支持多种计算机硬件和网络接口；

3 应支持实时多任务。

6.1.3 监视控制软件应具有下列功能：

1 实时数据采集和处理；

2 过程控制；

3 人机界面(HMI)；

4 多种常规控制器的通信协议和OPC、DDE等通用通信协议；

5 诊断；

6 多种编程语言；

7 历史数据记录、管理及报表。

6.1.4 组态和编程软件应具有下列功能：

1 监视控制软件组态、编程；

2 控制器组态、编程；

3 在线或离线调试、修改、测试、装载；

4 显示画面组态；

5 报表组态；

6 通信和外部接口组态；

7 系统管理；

8 软件版本管理。

6.1.5 诊断和管理软件应具有下列功能：

1 监视和诊断系统通信链路的工作状态，统计通信成功及失败次数，通信失败报警；

2 监视和诊断控制器、输入/输出(I/O)模板及输入/输出(I/O)网络的运行状态和故障报警、输入/输出(I/O)诊断到具体板卡和通道；

3 冗余设备在线自诊断、故障报警、无差错切换；

4 计算机硬件、软件故障自诊断及报警。

6.1.6 应用软件的配置宜符合下列规定：

1 可配置批量跟踪、计量管理、泄漏监测、模拟培训等工程应用软件；

2 可配置压缩机、机泵等大型设备的应用管理软件；

3 可配置智能仪表设备管理系统。

6.2 人机界面

6.2.1 人机界面软件(HMI)应具有图形显示、操作功能，支持简体中文，支持多窗口及多屏显示。

6.2.2 生产运行操作画面宜包括菜单、动态流程图、测控点详细画面、数据总貌、组显示、趋势图、报警画面、记录显示、通信统计画面等。

6.2.3 SIS和FGS系统应设独立画面。

6.2.4 系统维护画面可进行整个系统的诊断和维护。

6.3 数据管理

6.3.1 数据库管理应具有下列功能：

1 在线和离线编辑、维护、查找、修改、链接；

2 数据库离线管理；

3 支持标准高级语言编写的程序访问数据库；

4 记录数据库修改。

6.3.2 实时数据及历史数据应符合下列规定：

1 实时采集数据应包括瞬时值、平均值、报警和事件；

2 实时数据应根据“先进先出”的原则在实时数据库中存储，存储时间应根据数据类型确定，超出部分应存入历史数据库；

3 历史数据的在线存储时间应根据用户要求确定；

4 实时数据和历史数据不同步时，应有相应的数据重建和修复手段。

6.4 报警和事件

6.4.1 系统应存储所有报警、报警确认、事件和信息。

6.4.2 系统宜对报警分级、分区、分组，自动记录报警信息和时间顺序，不同级别报警的颜色和行为应有区别。

6.4.3 报警信息应能以多种方式发布。

6.4.4 报警应具备确认功能。确认和未确认报警应有颜色或行为区别。对长时间已确认但未恢复正常的报警应定时重复报警。

6.4.5 系统宜设置报警频率统计功能。

6.4.6 报警宜包括下列类型：

1 模拟信号超出高、低限值；

2 模拟输入信号变化率超出限定值；

3 无理值报警；

4 数字信号报警；

5 信号短路、开路、接地故障等诊断报警；

6 超驰报警；

7 输入/输出强制报警；

8 硬件、通信及系统故障报警。

6.4.7 SOE应根据报警发生的先后顺序进行排序。首出报警应显示在报警汇总的最前面，以不同的颜色或行为突出显示。

6.5 报告和报表

6.5.1 系统应提供生产运行报表、事件报表、报警报表、安全系统相关报告、自定义报告。

6.5.2 报表宜使用通用电子表格软件。

6.5.3 报告和报表应能在线预览，历史报告和报表应能在线、离线存储和索引。

6.6 系 统 安 全

6.6.1 控制系统安全应采取下列措施：

1 控制系统应采用身份认证；

2 与管理网络间接口应采取安全措施；

3 无线数据传输宜加密；

4 通过公网传输的内容宜加密；

5 系统未使用的输入输出端口应禁止或封闭。

6.6.2 操作安全应采取下列措施：

1 操作员应定义不同的级别和权限；

2 登录宜有“空闲自动退出”机制；

3 操作宜增加确认环节；

4 操作应有记录。

6.6.3 控制安全及容错应采取下列措施：

1 控制模块的输出宜预设安全输出位置；

2 系统宜设置命令未完成报警和保护；

3 调节回路输出应自动跟踪、无扰切换；

4 无理值应钳位。

7 控制盘和机柜

7.0.1 盘、柜的材质宜为金属。

7.0.2 盘、柜尺寸不宜大于 1000mm×800mm×2000mm(宽×深×高)。

7.0.3 颜色应按照标准色标选择。盘和柜内、外宜喷漆。

7.0.4 盘、柜内配线应采用铜芯软导线，信号线线径不应小于 0.5mm^2，电源线线径不应小于 2.5mm^2。盘、柜内配线颜色宜按表 7.0.4 选择。

表 7.0.4 配线颜色

电缆类型		+ve /相		-ve /中	
电源	(AC)	褐色	(BR)	蓝色	(BL)
电源	(DC)	红色	(RE)	黑色	(BK)
模拟信号	(IS)	蓝色	(BL)	蓝色	(BL)
模拟信号	(Non-IS)	白色	(WH)	黑色	(BK)
数字信号	(IS)	蓝色	(BL)	蓝色	(BL)
数字信号	(Non-IS)	白色	(WH)	黑色	(BK)
保护地		绿/黄	(GN/YL)	—	
工作地		绿色	(GN)	—	
本安地		蓝色	(BL)	—	

注：AC 表示交流，DC 表示直流，IS 表示本安仪表信号，Non-IS 表示非本安仪表信号。

7.0.5 对于每一台单体设备供电应设一个电源回路，对于 24V 直流和 220V 交流的电源回路均要设断路器或熔断器，应符合下

列规定：

1 对于220V交流的电源回路，应选择双极断路器；

2 对于24V直流的电源回路，应选择双极断路器或者熔断器。

7.0.6 设有SPD时，外部信号、通信、电源电缆进出机、柜宜先接到SPD端子上。

7.0.7 电缆芯端头和盘内每根导线两端均应有标记。

7.0.8 36V以上的端子应有可拆卸的透明绝缘保护盖板，并贴有带电压等级的高压标识。

7.0.9 本安端子要有标识，电缆、接线和汇线槽应为蓝色。

7.0.10 汇线槽填充系数不宜大于60%。

7.0.11 柜内空间、端子数量应有20%的余量。

7.0.12 标牌应标注位号、制造商、尺寸、重量、防爆、防护、制造日期等。

7.0.13 前面板和盘内安装的设备下部均应有标志框。

7.0.14 排气扇应设置过滤网，顶装或后开门上安装。

7.0.15 照明灯照度不应低于300 lx，应配置门控开关。

7.0.16 盘、柜接地应符合本规范第8.3节的规定。

7.0.17 就地控制盘应符合下列规定：

1 应满足所在区域的防爆要求；

2 应满足所在区域的防护等级要求；

3 应满足所在区域的工作温度、湿度要求；

4 控制盘尺寸应根据进线和现场空间确定。盘内空间、端子数量应留有10%的余量。

8 电气设计

8.1 供 电

8.1.1 计算机控制系统应由专用的配电回路供电。交流供电电压宜为220V，直流供电电压宜为24V。

8.1.2 RTU可采用多种供电方式。

8.1.3 控制系统供电宜选用在线式不间断电源装置(UPS)。

8.2 电缆敷设

8.2.1 电缆桥架架空进线时应下坡向室外。

8.2.2 电缆沟进线时，室内沟底标高应高出室外沟底至少0.3m。

8.2.3 电缆进入控制室穿墙处应密封处理。

8.2.4 信号电缆与电力电源电缆应分开敷设，不可避免时应采取隔离措施。

8.2.5 电缆在桥架、电缆沟或室内敷设时，应按信号类型或电缆种类捆扎，成束敷设。

8.3 防雷及接地

8.3.1 计算机控制系统的防雷措施应符合现行国家标准《建筑物防雷设计规范》GB 50057、《建筑物电子信息系统防雷技术规范》GB 50343的有关规定，控制室和机柜间的防静电措施应符合《电子工程防静电设计规范》GB 50611的有关规定。

8.3.2 计算机控制系统的防雷措施应与供配电系统的防雷措施配合。

8.3.3 电涌保护器的选择应符合下列规定：

1 交流电源的SPD宜采用组合型SPD，电压保护水平不应

大于 1.5kV；同一线路上的 SPD 应进行能量配合。

2 仪表信号选用的 SPD 应有较小电压保护水平值，其标称放电电流不应小于 5kA(8/20μs)。

3 SPD 应设置在被保护设备端，宜采用接地连接线最短的接线方式。

4 SPD 接地端应接入保护接地。

8.3.4 计算机控制系统的工作接地、保护接地、防雷接地、防静电接地宜共用接地系统。接地电阻不宜大于 4Ω，接地连接线电阻不应大于 1Ω。

8.3.5 信号回路接地和本安系统接地应接入工作接地。

8.3.6 齐纳式安全栅应接入工作接地，隔离式安全栅可不接地。

8.3.7 屏蔽层应保证可靠的电气连接。单层屏蔽电缆的屏蔽层或双层屏蔽电缆的内屏蔽层或铠装双层屏蔽电缆的内、外屏蔽层应单点接入工作地，宜在控制室的一侧接地。非铠装双层屏蔽电缆的外屏蔽层、电缆铠装金属层应至少在两端接入保护地。

8.3.8 无屏蔽层的多芯电缆，其备用线芯应接入工作接地；对屏蔽层已接地电缆、穿钢管保护电缆、在金属电缆槽中敷设的电缆，其备用线芯可不接地。

8.3.9 设备金属外壳、金属构架、仪表电缆槽体、电缆保护管等均应可靠接地。

8.3.10 控制室和机柜间内活动地板、工作台的防静电接地应接入保护接地。

8.3.11 工作接地、保护接地应分别接入共用接地系统，不应串联或混接后接地。

8.3.12 保护接地与共用接地系统的连接不应少于 2 处，接地连接线应为不同路径走向。

9 控 制 室

9.1 布 局

9.1.1 控制室的设置应根据计算机控制系统的规模而定。规模较小的系统可设置一个控制室，规模较大的系统控制室宜包括操作室、机柜室、工程师室、不间断电源(UPS)室等。

9.1.2 房间的位置应符合下列规定：

1 操作室、机柜室和工程师室宜相邻布置；

2 操作室、机柜室和工程师室不宜与空调机室相邻，不可避免时应采取减振和隔声措施；

3 机柜室宜与 UPS 室相邻。

9.1.3 操作室和机柜室面积宜符合下列规定：

1 操作室内设备外缘距墙/柱不宜小于 1.2m，进深不宜小于 6m；

2 操作室有大屏幕时，操作台背面距大屏幕不宜小于 3m；

3 多排操作台之间净距离不宜小于 2.5m；

4 操作台可按直线、折线或弧线布置；

5 机柜室内成排机柜间距不宜小于 1.5m；

6 机柜正面净空不宜小于 1.2m，侧面净空不宜小于 0.8m；后开门机柜柜后净空不宜小于 1.0m；如柜后(侧)无辅助操作设备，且不需要后开门的机柜可直接靠墙安装。

9.1.4 工程师室的面积应按设备尺寸及维修的需要确定。

9.2 建 筑 要 求

9.2.1 控制室建筑设计应符合现行国家标准《建筑设计防火规范》GB 50016 的有关规定。

9.2.2 控制室宜吊顶。

9.2.3 操作室吊顶距地面净高不宜小于3.0m，机柜室吊顶距地面净高不宜小于2.8m。

9.2.4 控制室地面应符合下列规定：

1 控制室地面宜采用不易起灰尘的防滑防静电建筑材料，也可采用防静电活动地板。

2 大、中型机柜室宜采用防静电活动地板，活动地板下方的基础地面宜为水泥或水磨石地面。活动地板平均负荷不应小于5000N/m^2，水平度应为±2mm。

3 控制室基础地面应高出室外地面0.3m，当控制室位于有毒气体场所和/或爆炸危险场所(可燃气体或可燃蒸气相对密度大于0.75时)，室内基础地面应高出室外地面0.6m。

9.2.5 控制室墙面应符合下列规定：

1 控制室墙面应平整、光滑、不起灰；

2 使用的涂料、油漆不应反光，色调以浅色为宜；

3 必要时墙面应有吸声措施。

9.2.6 控制室门应符合下列规定：

1 大、中型控制室宜采用非燃烧型双向弹簧门，门宽应保证设备进出；

2 操作室与机柜室、工程师室之间应有方便的通道，与休息室、办公室相邻时，中间不宜开门；

3 长度大于12m或面积大于100m^2的控制室应设置两个或两个以上的门。

9.2.7 控制室窗应符合下列规定：

1 采用空调或正压通风的控制室，宜装密闭固定窗或双层密封窗；

2 操作室、机柜室朝向爆炸危险装置的一侧不应开窗，沙漠地区的控制室宜装密闭固定窗或双层密封窗。

9.3 采光与照明

9.3.1 控制室宜照明采光。自然采光时应有遮阳措施，避免出现眩光。

9.3.2 人工照明的照度标准，距地面0.75m平面上的照度应符合下列规定：

1 一般控制室应为300 lx；

2 中央控制室应为500 lx；

3 机柜室应为500 lx；

4 一般区域应为300 lx；

5 室外通道及设备检查等不经常到的区域应为50 lx～100 lx，照度相差不应超过3倍。

9.3.3 控制室应设事故照明系统，照度应为30 lx～50 lx。

9.3.4 灯具配置除满足照度要求外，还应光线柔和、无眩光。

9.4 暖　通

9.4.1 控制室的环境条件应符合下列规定：

1 控制室功能性房间温度宜控制在冬季20℃±2℃，夏季26℃±2℃，温度变化率宜小于5℃/h；

2 相对湿度宜保持在30%～60%，且不应结露；

3 空气净化度应控制在尘埃少于0.2mg/m^3(粒径小于10μm)，H_2S小于0.01mg/m^3，SO_2小于0.1mg/m^3，Cl_2小于0.01mg/m^3。

9.4.2 控制室功能性房间与辅助房间的通风空调应分开设置。

9.4.3 中央控制室空调气流组织应符合下列规定：

1 操作区气流组织宜上送下回；

2 机柜区气流组织宜下送上回；

3 气流组织采用其他形式时，应避免短路和循环不良。

9.4.4 空调系统主要设备宜设置备用主机。

9.4.5 控制室可设壁挂式或柜式空调器。

9.4.6 供暖宜采用空气调节装置。当采用水暖或蒸汽供热时，管道应采用焊接连接。在机柜和操作台 1m 范围内不应设置采暖设施。

9.5 安全措施

9.5.1 可燃(有毒)气体和液体的引压、取源管路不应引入控制室内。

9.5.2 控制室内可能出现可燃(有毒)气体时，应设置可燃气体检测报警器、有毒气体检测报警器。

9.5.3 控制室火灾自动报警系统的设置应符合现行国家标准《火灾自动报警系统设计规范》GB 50116 和《石油天然气工程设计防火规范》GB 50183 的有关规定。

9.5.4 控制室内应设置相应的消防设施。

9.5.5 控制室的通信可按需要配备生产、行政、调度、消防电话、控制系统和生产管理系统所需的网络接口设备、全站广播系统等。

9.5.6 控制室的室内装修应采用非燃烧材料或难燃烧材料。

附录 A 油气田计算机控制系统设计要求

A.1 一般规定

A.1.1 油气田计算机控制系统应实现井场、站(厂)、集输管道等基本生产单元的生产过程数据采集和监控。

A.1.2 油气田工艺装置位置相对集中的站(厂)，宜采用 DCS 或 PLC 系统。

A.1.3 油气田井场、计量间、注配间、集油阀组间，阀室、单井集气站等工艺流程简单的站场，生产数据采集控制宜采用 RTU。

A.1.4 油气田站场 BPCS 与第三方控制设备、智能仪表通信时，应采用标准通信协议。

A.1.5 油气田站场监控系统应预留上传数据的以太网通信接口。

A.1.6 油气田计算机控制系统防雷及接地应符合本规范 8.3 节的规定。

A.1.7 沙漠油田计算机控制系统应适应环境特点和工艺生产处理规模的要求，实现井场、计量站(集油阀组间)、集气站等工艺过程相对简单的站场无人值守，定期巡检。

A.2 油气田 SCADA 系统

A.2.1 油气田 SCADA 系统应符合下列规定：

1 油气田 SCADA 系统应对油气田站场工艺生产过程和管道进行统一调度及优化管理，为生产决策、地下开发优化提供基础数据。

2 油气田 SCADA 系统宜由中心监控系统、站(厂)监控系统、远程数据采集单元、网络传输设备等构成。

A.2.2 系统配置及功能应符合下列规定：

1 系统硬件配置应符合下列规定：

1)宜配置实时服务器、历史服务器、Web 服务器、操作员工作站、工程师工作站、外部存贮设备、网络设备和打印机；

2)应设置实时数据服务器、历史数据服务器，宜采用客户机/服务器(C/S 或 B/S)结构，可根据需要配置 Web 服务器；

3)实时数据服务器和历史数据服务器宜合并设置，根据可利用率需要可冗余配置，电源、网络应冗余配置；

4)工程师工作站宜独立配置，操作员工作站数量应根据生产管理需要进行配置；

5)报表打印机、报警打印机可分开设置。

2 系统软件配置应符合下列规定：

1)应配置操作系统软件、SCADA 系统软件、数据库管理软件和高级应用软件；

2)操作系统宜采用 Windows 平台，应支持中文显示和输入；

3)高级应用软件应以生产管理、安全管理、优化分析为主。

3 SCADA 系统宜具有下列主要功能：

1)采集和处理各井场、站(厂)的主要工艺生产数据；

2)监视各井场、站(厂)的可燃(有毒)气体、火灾报警；

3)监视各站(厂)的关键设备和配电系统状态；

4)工艺流程的动态显示；

5)报警显示、管理及事件的查询、打印；

6)实时数据和历史数据的采集、归档、管理以及趋势图显示；

7)储库的储量预测和计划；

8)管道泄漏监测；

9)系统诊断和网络监视及管理；

10)时钟同步；

11)为油田其他信息管理系统提供基础数据。

A.3 油气田站场监控系统

A.3.1 油气田站场监控系统应符合下列规定：

1 油气田集中处理站、天然气净化厂(处理厂)等工艺过程较复杂的站(厂)，宜设置相对独立的 BPCS、SIS 和 FGS；BPCS 软硬件宜采用 DCS。

2 油气田工艺过程相对简单，调节回路较少，对安全可靠性没有特殊要求的站(厂)宜设置 BPCS，BPCS 控制器宜采用 PLC。

3 气田集气站工艺生产过程控制宜采用 PLC，紧急停车系统如果点数较少时，宜采用由继电器等元件组成的逻辑控制回路，并辅以手动硬操作按钮实现。

4 工艺处理功能单一的油气田站场应设置 RTU，根据生产管理需要可就地设置触摸屏或操作面板。

5 SIS 和 FGS 的设计应符合本规范第 5 章的规定。

6 油气田火灾及可燃(有毒)气体报警系统设计应符合下列规定：

1)油气田火灾探测报警系统和消防联动控制系统的设置应符合现行国家标准《石油天然气工程设计防火规范》GB 50183及《石油化工企业设计防火规范》GB 50160 的有关规定；

2)气体检测点数较少时，可采用盘装模拟仪表，报警输出应上传到 BPCS 系统；

3)气体检测点数较多时，可采用独立的数据采集装置或与 BPCS 系统合并设置，但 I/O 卡件应独立设置，并配备便携式可燃(毒性)气体报警器；

4)气体检测系统和火灾检测报警系统可合并设置，构成相对独立的火气系统；

5)应设置与站(厂)BPCS 系统的通信接口；

6)应采用经过公安部消防产品合格评定中心(CCCF)认证的火灾报警设备。

A.3.2 系统软、硬件配置应符合下列规定：

1 软件配置见本规范第 6 章。

2 BPCS 硬件配置应符合下列规定：

1)工艺生产过程相对简单，对计算机控制系统可利用率要求不高的独立站(厂)宜设置 1 台操作站(兼工程师工作站)，并宜设置 1 台报表兼报警打印机；

2)工艺过程复杂或含有多个工艺处理单元的站(厂)宜设置 1 台工程师工作站，根据操作管理需求可设置多台操作员工作站，报表打印机和报警打印机宜分开设置；

3)集中处理站、天然气净化厂(处理厂)或对安全可靠性要求较高的站(厂)，BPCS 的控制单元、电源、网络应冗余配置；重要控制回路的 I/O 宜冗余配置。其他站(厂)BPCS 硬件的冗余设置应简单优化；

4)集中处理站、天然气净化厂(处理厂)等站(厂)应根据操作管理需求，设置实时数据服务器和历史数据服务器；

5)BPCS 的设计应符合本规范第 4 章的规定。

A.3.3 站场控制系统功能宜符合下列规定：

1 站(厂)控制系统宜具有下列基本功能：

1)采集和处理站(厂)及所辖井场的工艺生产数据；

2)实时监控工艺生产过程和关键设备运行状态；

3)可燃(有毒)气体、火灾报警和安全状况监视；

4)工艺流程参数实时显示、报警、管理及事件的查询、打印；

5)实时和历史数据的采集、存储、管理以及趋势图显示；

6)PID 控制、批量控制、顺序逻辑控制；

7)ESD 功能；

8)第三方设备监控和运行管理；

9)预留通信接口，实现数据共享和数据集成；

10)向上一级控制系统上传数据、报警信息并接收和执行其下达的指令。

2 采用远程终端单元(RTU)的站场可具有下列功能：

1)采集站场工艺生产数据；

2)自动选井控制，单井产量计量；

3)机采油井远程启停控制；

4)计量间恒温掺水控制，注配间恒压恒流控制；

5)为上一级站场计算机控制系统提供有关数据并接受其下达的指令。

A.4 油气田站场控制室

A.4.1 油气田新建站(厂)控制室的设计，应预留机柜和操作台的位置；工艺处理功能单一没有扩建可能的站场可不预留位置。

A.4.2 采用分岗控制的站场可设功能合一的控制室，不宜单独设机柜室和操作室。控制室可隔断为机柜室和操作室。

A.4.3 当控制室设置多套自控系统或电视监控系统时，操作台宜统一布置，规格、颜色应统一。

A.4.4 控制室的设计应符合本规范第 9 章的规定。

附录B　输油气管道SCADA系统设计要求

B.1　一般规定

B.1.1　管道SCADA系统应对管道进行统一监控、调度和管理。

B.1.2　管道SCADA系统宜由主调度控制中心、备用调度控制中心的控制系统和沿线站场的控制系统、监控(监视)阀室RTU及通信系统组成。

B.1.3　主调度控制中心、备用调度控制中心应具有切换功能。主调度控制中心应具备下达允许和终止备用调度控制中心操作的权限。

B.1.4　调度控制中心与站场控制系统应具有操作权限的切换功能。

B.1.5　管道SCADA系统应保持时钟同步。

B.2　调度控制中心

B.2.1　硬件配置应符合下列规定：

1　调度控制中心的计算机控制系统应配置实时服务器、历史服务器、路由器、交换机、操作员工作站、工程师工作站、外部存储设备和网络打印机，应通过以太网相互连接。

2　调度控制中心的计算机控制系统可设置应用服务器、设备管理服务器、地理信息服务器、Web服务器、培训工作站、背投影系统等附属功能设备。

3　服务器应采用客户机/服务器(C/S)结构，实时和历史服务器宜采用冗余配置和UNIX或Windows实时多任务操作系统。

4　服务器负荷应满足本规范第4.2.4条的规定。

5　SCADA系统的局域网、路由器、交换机及网络连接应冗余配置。

6　SCADA系统应配备工作站，工作站宜采用工业级计算机。

7　宜冗余配置外存储设备。

8　SCADA系统局域网络与外部应用网络间应具有安全防护措施。

B.2.2　软件配置应符合下列规定：

1　计算机系统应配置操作系统软件，服务器宜采用UNIX操作系统，可采用Windows操作系统；其他计算机应采用Windows操作系统。

2　监控软件宜配置SCADA系统软件。

3　SCADA系统宜配置数据库管理软件。

4　应根据需要配置管道高级应用软件。

B.2.3　主要功能应符合下列规定：

1　SCADA系统调度控制中心应符合下列规定：

1)根据不同功能配备不同的服务器，分担不同的任务；

2)操作员工作站具备不同级别、不同区域或不同数据集合的操作权限。

2　SCADA系统调度控制中心宜具有下列主要功能：

1)监视各工艺站场及阀室工艺设备运行状态；

2)工艺流程动态显示；

3)报警显示、报警管理以及事件的查询、打印；

4)管道全线的工艺过程控制；

5)实时、历史数据的采集、归档、管理以及趋势图显示；

6)报表的生成和打印；

7)输量计划、批输计划、混油量计算、混油跟踪及处理；

8)管道全线过程优化；

9)管道全线安全保护；

10)贸易结算和管理；

11)管道泄漏检测和定位；

12)罐区管理；
13)清管器跟踪；
14)SCADA 系统的故障诊断和远程维护；
15)网络和通信通道的监视及管理；
16)系统时钟同步；
17)在线培训、测试和维护；
18)数据共享和数据集成。

3 局域网络应符合下列规定：
1)调度控制中心的局域网(LAN)应满足实时、多任务、多参数的要求。应采用标准的、开放型局域网络结构。
2)非授权的工作站不应接入，在网络设备上未投入使用的网络接口应进行“非使能”设置。
3)局域网络应有防电涌功能。

4 SCADA 系统软件宜符合下列规定：
1)模块化结构设计；
2)支持客户机/服务器(C/S)结构，支持分布式服务器；
3)支持冗余服务器和网络；
4)支持离线组态和在线组态；
5)具有直观、用户友好的操作界面；
6)具有图形编辑功能；
7)具有丰富的图形库；
8)具有完善的安全措施；
9)历史数据库采用标准数据库；
10)数据库管理；
11)报警和事件管理；
12)报告生成及管理；
13)根据需要编制中文操作员在线帮助；
14)通信管理；
15)支持标准编程语言；

16)在操作模式下，应能调用外部或内部程序；
17)支持世界大多数知名 PLC 和 RTU 的通信协议。

B.3 站场控制系统

B.3.1 系统配置应符合下列规定：

1 工艺过程较复杂的站场，宜设置相对独立的基本过程控制系统、安全仪表系统、火灾及可燃(有毒)气体报警系统。

2 工艺过程简单，安全仪表系统点数较少时，可按照本规范第 5.2.8 条设置站场控制系统。

3 基本过程控制系统宜由过程控制单元、操作员工作站、网络设备和辅助设备组成。

4 安全仪表系统应包括紧急停车系统、安全保护系统。

5 火灾及可燃气体报警系统宜包括可燃(有毒)气体检测系统、火灾自动报警系统和自动消防控制系统。

6 安全仪表系统、火灾及可燃气体报警系统可与基本过程控制系统共用操作员工作站等外围设备。

B.3.2 系统功能应符合下列规定：

1 站场控制系统宜具有下列主要功能：
1)接受和执行调度控制中心的控制命令，进行站场控制和设定值调整，并能独立工作；
2)过程变量的采集和数据处理；
3)向调度控制中心传送必要的工艺过程数据和报警信息；
4)工艺流程、动态数据显示；
5)设备的运行状态检测；
6)工艺参数的报警、存储、记录、打印；
7)主要工艺过程参数的控制；
8)故障自诊断；
9)通信信道故障监测。

2 基本过程控制系统配置应符合下列规定：

1)过程控制单元的控制器、I/O 网络、局域网、通信接口、电源宜按冗余配置。

2)基本过程控制系统与第三方智能仪表系统或设备之间宜采用通信接口连接。

3)站场控制系统的电涌防护设计应满足雷电防护分区、分级确定的防雷等级要求。

3 安全仪表系统配置应符合下列规定：

1)站场控制系统宜独立设置紧急停车系统；

2)全线应设置安全保护系统；

3)安全仪表系统的控制器、I/O 网络、局域网、通信接口、电源宜按冗余配置。

4)安全仪表系统的设置应满足本规范第 5.2 节的要求。

4 火灾及可燃气体报警系统配置应符合下列规定：

1)可燃(有毒)气体检测系统宜设置独立的盘、柜；

2)火灾自动报警系统可与可燃(有毒)气体检测系统合用盘、柜；

3)自动消防控制系统宜独立设置。

5 过程控制单元硬件设置应符合下列规定：

1)控制器应符合下列规定：

宜采用 32 位及以上的中央处理器(CPU)；

内存不宜小于 4M；

处理能力应有 40%以上的余量；

应与时钟同步；

输入和输出的模拟量和数字量均宜附加时间标签；

I/O 模板应有故障自诊断功能；

模板应能带电插拔。

2)I/O 模板应是多通道的，通道数量和技术要求应符合下列规定：

模拟输入模板不应多于 16 通道，模拟/数字转换器

不应少于 12 位，有源输入或无源输入可任选；

当模拟输出模板为 8 通道时，模拟/数字转换器不应少于 12 位，输出信号应为 4mA～20mA 直流或 1V～5V 直流，并应具有输出隔离、短路保护和断路报警功能，带负载能力不应小于 500Ω；

热电阻输入模板不应多于 8 通道，应能接收三线制或四线制热电阻信号输入；

数字量输入模板不应多于 16 通道，应采用光电隔离，并应能承受 380V 的峰值电压，且输入应与地隔离；

数字量输出模板不应多于 16 通道，输出应与地隔离，且应有短路保护；

通信模板的每个通信口宜接入 1 个通信设备或总线，应能完成不同通信协议间的转换。

3)CPU 机架与 I/O 机架之间宜采用网络连接。

4)24V 直流电源应冗余设置。

5)应配带用于安装过程控制单元所有设备的安装附件。

B.3.3 系统网络及设备应符合下列规定：

1 站场控制系统的网络设备应符合下列规定：

1)应由网络交换机、路由器及连接电缆和附件组成；

2)通过网络设备的连接，应组成冗余工业以太网；

3)交换机应采用工业级以太网交换机，不宜少于 24 端口，应采用模块化设计，并应支持单/多模光纤接口(SC/LC)或 RJ45 接口；

4)路由器、交换机应支持标准的 TCP/IP 协议；

5)路由器、交换机应满足站场控制系统的配置要求。

2 站场控制系统的操作员站应符合下列规定：

1)关闭操作员站不应对过程控制单元的信号传输、运行有任何影响；

2)操作员站的具体配置可根据具体工程确定。

3 站场控制系统的软件配置应符合下列规定：

1)应配备完整的过程控制和检测软件、生产运行操作和数据处理软件；

2)应配置操作员站操作系统软件、控制程序编程软件、HMI组态软件，可在需要时配置高级语言编程软件；

3)应支持多种编程语言。

4 控制程序编程软件宜符合下列规定：

1)编程软件应支持国际标准的语言，应具有多个PID运算模块和其他常用的功能模块，具有批量及顺序控制功能模块。

2)编程软件可在标准中文Windows平台上运行。

B.4 阀室系统

B.4.1 监视阀室、监控阀室宜具有下列基本功能：

1 监视阀室宜设置数据信号远传设备，并宜具有下列主要功能：

1)监视线路截断阀运行状态；

2)为调度控制中心提供有关数据。

2 监控阀室应设置RTU，宜具有下列主要功能：

1)过程变量的检测、控制和数据存储及处理；

2)监控线路紧急截断阀的运行状态；

3)逻辑控制；

4)执行关阀命令；

5)供电系统的监控；

6)采集可燃气体检测信号；

7)采集阴极保护站的相关变量(需要时)；

8)为调度控制中心提供有关数据；

9)接受并执行调度控制中心下达的命令。

B.4.2 监控阀室RTU的配置应符合下列规定：

1 应采用以太网接口与调度控制中心通信，应能适应现场环境条件；

2 应配置通信接口，可与第三方智能设备连接；

3 应配置与计算机连接的标准接口。

B.4.3 RTU的软件宜符合下列规定：

1 编程软件应选用开放式结构，应功能强大、灵活方便、界面友好；

2 编程软件应具备在现场通过笔记本计算机读写RTU中的相关数据、组态等功能。

本规范用词说明

1 为便于在执行本规范条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的：

正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况下均应这样做的：

正面词采用“应”，反面词采用“不应”或“不得”；

3）表示允许稍有选择，在条件许可时首先应这样做的：

正面词采用“宜”，反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的，采用“可”。

2 条文中指明应按其他有关标准执行的写法为：“应符合……的规定”或“应按……执行”。

引用标准名录

《建筑设计防火规范》GB 50016

《建筑物防雷设计规范》GB 50057

《火灾自动报警系统设计规范》GB 50116

《石油化工企业设计防火规范》GB 50160

《石油天然气工程设计防火规范》GB 50183

《建筑物电子信息系统防雷技术规范》GB 50343

《电子工程防静电设计规范》GB 50611

《石油化工安全仪表系统设计规范》GB/T 50770

中华人民共和国国家标准

油气田及管道工程计算机控制系统设计规范

GB/T 50823 - 2013

条文说明

制 订 说 明

《油气田及管道工程计算机控制系统设计规范》GB/T 50823—2013，经住房和城乡建设部2012年12月25日以第1600号公告批准发布。

本规范制订过程中，编制组进行了广泛调查研究，总结了我国油气田及管道工程中采用计算机控制系统的实践经验，参考了国外先进的技术法规、技术标准，广泛征求了油气田及管道工程计算机控制系统设计、制造、操作维护等方面技术人员的意见，在此基础上编制本规范。

为了便于广大设计、施工、科研、学校等单位有关人员在使用本规范时能正确理解和执行条文规定，《油气田及管道工程计算机控制系统设计规范》编制组按章、节、条顺序编制了本规范的条文说明，对条文规定的目的、依据以及执行中需注意的有关事项进行了说明。但是本条文说明不具备与规范正文同等的法律效力，仅供使用者参考。

目　次

1 总 则

1.0.2 “陆上油气田及管道工程”包括两大类工程，其一是陆上油气田为满足原油/天然气生产而建设的油气收集、净化处理、计量、储运设施及相关辅助设施，其二是原油、石油产品、天然气、液化石油气等输送管道中的各种站场、线路及相关辅助设施。

现场仪表、执行机构、自控阀等现场设备和闪光报警器、单回路调节仪等盘装仪表不在本规范范围内，应符合现行国家标准《油气田及管道工程仪表控制系统设计规范》GB/T 50892 的有关规定。

“计算机控制系统”类型较多，本规范主要是针对在油气田及管道工程已得到广泛应用的控制系统（ICS、BPCS、SIS、FGS、SCADA 等）进行编制的，未包括现场总线控制系统（FCS）、嵌入式系统等，也不包括管理信息系统（MIS）、地理信息系统（GIS）等。

油气田及管道工程中系统规模大小不一，推荐根据站场类型进行分类。本规范中出现的大、中、小系统，其应用场合如下：

调控中心、天然气净化厂、大型联合站、大型油库应采用大型控制系统，计量间、井场、阀室采用 RTU 或小型的 PLC 控制系统，其他一般采用中型控制系统。

1.0.3 由于本规范是专业技术标准，其内容涉及范围较广，涉及其他有关标准规范要求的，就应执行有关标准、规范，不能与之相抵触，特别是强制性条款应严格执行。本条所涉及标准、规范请见引用标准名录。

2 术语和缩略语

本章所列术语及缩略语，其定义及范围仅适用于本规范。

2.1 术　　语

2.1.1 计算机控制系统的广义理解一般也包括现场仪表、控制阀等，本条界定本规范所指计算机控制系统不包括仪表、执行机构、自控阀等现场设备和闪光报警器、单回路调节仪等盘装仪表。

2.1.2 基本过程控制系统也常被称为过程控制系统(process control system，PCS)。

2.1.3 广义的安全仪表系统包括过程工业中的紧急停车系统(ESD)、燃烧管理系统(BMS)、压缩机控制系统(CCS)、火气系统(FGS)、高完整性压力保护系统(HIPPS)等以安全保护和抑制减轻灾害为目的的自动化安全保护系统。本规范不包括燃烧管理系统(BMS)和压缩机控制系统(CCS)，根据现场应用惯例将火气系统单列。

2.1.5 集成控制系统英语翻译也称作 integrated control and safety system(ICSS)。

2.1.9 “远程终端单元”也可由 PLC 配套通信设备组成。

2.1.13 操作超驰也称为启动超驰(start-up override)或工艺超驰(process override)。

2.2 缩　略　语

DMZ 是英文“demilitarized zone”的缩写，中文名称为“隔离区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立的一个非安全网络与安全网络之间的缓冲区，

这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。这种网络部署比起一般的防火墙方案，对攻击者来说又多了一道关卡，可更加有效地保护内部网络。

3 系统结构和适用范围

3.1 一 般 规 定

3.1.3 计算机控制系统硬件和软件选型时需根据测控对象规模及特点、可靠性要求、安全需求、自然地理环境、社会因素、用户当前生产管理水平、操作维护能力、发展规划要求、经济效益及资金情况，统筹考虑，合理安排。兼顾用户现有运行系统维修维护工作方便，新建系统宜选用相同种类的计算机控制系统，减少维护成本。

3.1.4 设计时应考虑全系统生命周期成本，除系统购买成本，还应考虑系统的安装、调试、维护、使用和退出成本。如图1所示，系统生命周期是设计、安装调试、运行和退出的循环。应根据工程规模、被控过程对象的危险和风险大小、工艺的成熟和复杂程度等因素，实施生命周期内必要的管理活动。自控系统生命周期主要活动见表1。

图1 计算机控制系统生命周期循环

表1 计算机控制系统生命周期各阶段活动

阶段	活动	目标	主要的输入	主要的输出
设计	评估/概念性设计	确定项目的经济目标和基础要求	经济目标 工艺设计 工艺物料平衡图(PFD)图 主设备清单 现有系统及基础设施总图 控制系统选用标准	计算机控制系统概念设计

续表1

阶段	活动	目标	主要的输入	主要的输出
设计	选择/前期设计	确定项目范围、功能和总体指标	设计基础 P&ID图 设备清单 危险与可操作性(HAZOP)分析 控制系统初步设计	控制系统规格书
	确定/详细设计	准备报价、发布并选择供应商，硬件设计、I/O表和通信接口设计，中控室、现场仪表、电缆敷设设计，仪器供电、接地设计，控制系统与其他系统和硬件的接口设计	控制系统规格书 设计标准和惯例 设计文件深度要求	硬件和软件选择，详细技术要求，安装/建造图纸
安装调试	执行/项目实施和管理	按设计进行项目实施，满足预算、计划和技术三要素	项目目标，预算和计划	设计图纸和规格书升版，设备和材料采购，硬件组态和调试，软件功能开发和测试
	建造、安装和调试	仪表及控制系统的安装、调校和回路测试	设计图纸和规格书 组态和编程 自控设备和系统手册	控制系统完工
	试运行	控制系统运行准备	性能指标 监控要求	控制系统运转前所有故障的识别及纠正

续表 1

阶段	活动	目标	主要的输入	主要的输出
运行	运行/操作	调整控制系统达到最优的运行效率	性能指标 监控要求	收益/成本比最大化
	运行/维护	维护、预防性维护和维修	竣工文件和培训资料	性能最优、可用性最高，维护、维修记录
退出	退出、再利用和延寿	保障安全，减少非计划停产	设计文件 维护、维修记录 延寿评估报告	退出计划，再利用设计

系统概念设计阶段应对系统的实施成本、计划、生命周期成本、可操作性和维护性进行综合考虑。

自控设备管理系统可为自控设备性能评估、更换和延寿提供一手资料，是现场系统生命周期管理的主要工具之一。在大型炼化企业已经有较广泛应用，在油气田及管道领域的应用刚刚起步。该系统可对自控设备进行组态、标定、回路检查以及状态监测，设备出现故障时，还可提供诊断参考。大型站(库)可配置自控设备管理系统。

3.2 系统结构

3.2.1 计算机控制系统各子系统可配置独立的控制器和 I/O 模板，控制器与 I/O 模板间通过专用的 I/O 网络连接，完成数据采集和控制。控制器通过控制网络与 BPCS 服务器连接，以 BPCS 上位软件作为统一的人机接口平台。BPCS 服务器与监控网络连接，为监控层设备提供数据服务并响应其指令。

油气田及管道领域涉及的测控对象多，测控规模大小不一，应用的计算机控制系统也多种多样。图 3.2.1 仅是给出了一套计算

机控制系统可能包括的各个部分，规范各章围绕该结构对各部分进行规范。

3.3 系统适用范围

3.3.2 BPCS 是最基本的计算机控制系统，其构成多种多样，较常用的有两种：DCS 系统和上位监控软件加 PLC。

3.4 控制器适用范围

3.4.2 DCS 与 PLC 在各自保留自身原有特点的基础上，又相互补充、相互靠拢、相互渗透。目前的 DCS 已有很强的顺序控制功能，而 PLC 处理复杂控制的功能也很强，且两者都能组成大型网络。DCS 与 PLC 的适用范围已有很大交叉，并都可以作为 SCADA 系统的组成部分。

4 基本过程控制系统(BPCS)

4.1 一 般 规 定

4.1.1 系统的可用性(Availability),也称作可用率,计算公式如下:

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \times 100\% \qquad (1)$$

式中:MTBF——系统的平均无故障间隔时间;

MTTR——平均故障修复时间。

系统的可用性宜不低于99.9%,即每年整个系统的累计故障修复时间不得超过8h。

保证系统可用性的手段及措施一般有:冗余、容错、故障自诊断、隔离等。

4.2 服 务 器

4.2.2 服务器按功能可分为实时服务器、历史服务器、I/O服务器、通信服务器等,这几类服务器可单独设置或功能合并。如负荷较轻时,实时服务器、历史服务器和I/O服务器、通信服务器通常合并为1台服务器;如历史存储及相关任务较重时,可单独设置历史服务器;对I/O采集的实时性要求高时,可单独设置I/O服务器;需要多协议转换时,可采用通信服务器。

4.2.6 服务器可与操作员工作站合二为一,也常被简称为操作员工作站或HMI,操作员工作站本身具备系统服务器的功能,可进行数据采集、存储,同时又可作为人机界面,供操作人员使用,完成系统监控与操作。在小型控制系统或控制室空间有限时,常采用此模式。

4.3 操作员工作站

4.3.2 现行行业标准《可编程控制器系统设计规定》HG/T

20700—2000中对操作员工作站配置数量提出了一个经验性的粗略估算方法,是按数字量I/O点数[模拟量I/O点数折算成数字量I/O点数来估算,即1个AI(AO)=15个DI(DO)]的数量来配置,具体数量应符合如下要求:

1000～1500数字量I/O点:可配置2台;

1500～3000数字量I/O点:可配置2～3台;

3000～5000数字量I/O点:可配置3～4台;

5000～8000数字量I/O点:可配置4～6台;

8000数字量I/O点以上:可根据实际需要配置。

本条不适用于控制中心。

4.5 过程控制单元

4.5.2 可在I/O模板、控制器或服务器处为事件、报警和数据附加时间标签,目前常用的是在服务器处附加,但随着计算机控制系统网络化趋势的发展,控制器作为站场一个节点,则越来越多地连接到SCADA系统中。为保证数据,特别是报警和事件的实时性,推荐在控制器上附加时间标签。

4.5.4 重要站场(厂)常见的有:大型联合站、油气处理厂、大型油库、有毒天然气站场、高压天然气站场、长输管线站场等。

4.5.7 本条第3款:计算机控制系统接地电阻一般要求不大于4Ω,但在沙漠和山区,这一指标较难实现,一般接地电阻超过10Ω认为是接地不良。从无接地或接地不良的现场仪表输出的模拟量信号易受干扰,需在I/O模板处采用"差分/双端输入和通道隔离"以减小对系统和其他通道的干扰。

4.6 网络与通信

4.6.1 计算机控制系统通信常用的国际标准有:

(1)IEEE 802系列是IEEE(电气和电子工程师协会)标准中关于局域网和广域网的一系列标准。计算机控制系统中的信息

网络层和监控网络层多采用符合《CSMA/CD 访问控制方法与物理层规范》IEEE 802.3 中的 TCP/IP 协议。随着工业以太网的发展，越来越多的控制层网络也中是以 TCP/IP 协议为基础构建的。

(2)IEC 61158(现场总线标准)系列是经过长期技术争论而逐步走向合作的产物，标准采纳了经过市场考验的主要类型的现场总线、工业以太网和实时以太网。IEC 61784 系列标准是 IEC 61158的配套规范，其对应关系见表 2。

表 2　IEC 61158 与 IEC 61784 定义的现场工业通信网络

IEC 61784 通信行规族(CPF)		IEC 61784 行规(CP)及对应于 IEC 61158 中的现场工业通信网络类型(Type)	
CP#	技术名称	CP#	Type#
1	Foundation Fieldbus	CP 1/1 FF H1	1,9
		CP 1/2 FF HSE	5
		CP 1/3 FF H2	1,9
2	CIP	CP 2/1 ControlNet	2
		CP 2/2 Ethernet/IP	2
		CP 2/3 DeviceNet	2
3	PROFIBUS & PROFINET	CP 3/1 PROFIBUS DP	3
		CP 3/2 PROFIBUS PA	3
		CP 3/3 PROFINET CBA	10
		CP 3/4 PROFINET IO CC-A	10
		CP 3/5 PROFINET IO CC-B	10
		CP 3/6 PROFINET IO CC-C	10
4	P-NET	CP 4/1 P-NET RS485	4
		CP 4/2 P-NET RS232	4
		CP 4/3 P-NET on IP	4
5	WorldFIP	CP 5/1 WorldFIP	7

续表 2

IEC 61784 通信行规族(CPF)		IEC 61784 行规(CP)及对应于 IEC 61158 中的现场工业通信网络类型(Type)	
CP#	技术名称	CP#	Type#
5	WorldFIP	CP 5/2 WorldFIP with sub MMS	7
		CP 5/3 WorldFIP minimal for TCP/IP	7
6	INTERBUS	CP 6/1 INTERBUS	8
		CP 6/2 INTERBUS TCP/IP	8
		CP 6/3 INTERBUS mini subset of CP 6/1	8
		CP 6/4	8
		CP 6/5	8
		CP 6/6	8
7	SWIFTNET	已撤销	6
8	CC－Link	CP 8/1 CC-Link/V1	18
		CP 8/2 CC-Link/V2	18
		CP 8/3 CC-Link/LT	18
9	HART	CP 9/1 HART	20
10	VNET/IP	CP 10/1 VNET/IP	17
11	TCnet	CP 11/1 TCnet-star	11
		CP 11/2 TCnet-loop	11
12	EtherCAT	CP 12/1	12
		CP 12/2	12
13	ETHERNET Powerlink	CP 11/1 EPL	13
14	EPA	CP 14/1 NRT	14
		CP 14/2 RT	14
		CP 14/2 FRT	14

续表 2

IEC 61784 通信行规族(CPF)		IEC 61784 行规(CP)及对应于 IEC 61158 中的现场工业通信网络类型(Type)	
CP#	技术名称	CP#	Type#
15	MODBUS－RTPS	CP 15/1 MODBUS TCP	15
		CP 15/2 RTPS	15
16	SERCOS	CP 16/1 SERCOS Ⅰ	16
		CP 16/2 SERCOS Ⅱ	16
		CP 16/3 SERCOS Ⅲ	19
17	RAPIEnet	CP 17/1 RAPIEnet	21
18	SafetyNet p	CP 18/1 RTFL	22
		CP 18/2 RTFN	22

(3)工业以太网与实时以太网的关系。

一般将用于工业控制系统的以太网统称为工业以太网，但是按照国际电工委员会 SC 65C(Industrial networks)的定义，工业以太网是用于工业自动化环境，符合《CSMA/CD 访问控制方法与物理层规范》IEEE 802.3 标准，按照《媒体访问控制(MAC)网桥》IEEE 802.1D 和《局域网虚拟网桥》IEEE 802.1Q，对其没有进行任何实时扩展(Extension)而实现的以太网。通过采用减轻以太网负荷，提高网络速度，采用交换式以太网和全双工通信，采用信息级、流量控制以及虚拟局域网等技术提高了以太网的实时性，到目前为止可以将工业以太网的实时响应时间做到 5ms～10ms，相当于现有的现场总线。工业以太网在技术上与商用以太网是兼容的。

对于响应时间小于 5ms 的应用，工业以太网已不能胜任。为了满足高实时性能应用的需要，各大公司和标准组织纷纷提出各种提升工业以太网实时性的技术解决方案。这些方案建立在 IEEE 802.3 标准的基础上，通过对其和相关标准的实时扩展，提

高实时性，并且做到与标准以太网的无缝连接，这就是实时以太网(Real Time Ethernet，简称 RTE)。

4.6.5 现场网络是 BPCS 与现场智能设备的通信链接，主要通信接口有：

(1)串行数据接口。串行通信接口是最常用的通信接口，现场大多数智能仪表，如分析仪、流量计、变送器、机械保护系统、PLC、小型控制器等，都支持与控制系统间的串行数据通信。常用物理接口和通信协议如下：

RS-232，一种半双工短距离单设备串行通信接口，通信距离不超过 15m。当需要远距离传输时，需要增加协议转换器。通信协议宜采用 Modbus RTU。

RS-422，一种全双工远距离单设备串行通信接口。通信协议宜采用 Modbus RTU。

RS-485，一种半双工远距离单设备或者多设备串行通信接口，该接口是现场应用最广泛的通信接口；多个 RS-485/422 设备可以通过菊花链的方式组成一点对多点的通信网络，由于一般相同厂商的设备才相互兼容，除非经过验证，否则不同厂商的 RS-485/422设备不宜组网。通信协议宜采用 Modbus RTU。

另外，通过串口转以太网模块，大量 RS-232/422/485 设备可借此接入以太网。

HART，是一种两线制连接的智能仪表通信协议，它是加载在 4mA～20mA 模拟量信号上的数字调制信号，支持多点通信。

(2)现场总线。现场智能仪表和设备可通过现场总线连接在一起，与过程控制系统通信，不但可以进行常规的监视和控制，还能传输丰富的诊断信息，可进行远程设定，同时节省电缆与施工敷设工作量。常见的现场总线有：

FF 现场总线：连接现场智能仪表和控制阀，可就地组网进行连续控制和测量。

Profibus 总线：常用于连接开关阀、智能电气设备等数字量设

备和智能变送器。

Devicenet 总线：常用于有大量简单设备的防爆场合，如机械控制、开关阀控制、智能电气设备控制等。

4.6.7 I/O 网络连接控制器和 I/O 模板，其协议是厂商专有的。

4.6.9 信息管理系统间主要通过信息网络连接，信息管理系统主要有“企业资源管理系统(ERP)”、“地理信息系统(GIS)”、“工厂信息管理系统(MES)”、“管理信息系统(MIS)”等。计算机控制系统与这些信息管理系统之间连接时，应采取相应的网络安全措施，如采用硬件防火墙、安全隔离网闸、Web 服务器、FTP 服务器等设备做物理隔离，并在两端配置防病毒软件和软件防火墙等以保护计算机免受病毒或网络攻击。

4.7 辅助操作设备

4.7.1 辅助操作台(盘)用于安装特殊需要的记录仪、信号报警器/灯、后备手操器，以及联锁、紧急关断、机泵等的控制开关、按钮或转换开关等。

4.8 外 围 设 备

4.8.1 报警打印机宜为针式打印机，便于报警实时打印。

4.8.2 专用键盘常见的是 DCS 键盘，具有特制的功能键和用户定义键及比普通键盘更好的防水和防尘性能。

4.8.4 KVM 切换器的正式名称为多计算机切换器，可让系统管理员通过一组键盘、显示器和鼠标，控制多台服务器或电脑主机的计算机外围设备。目前 KVM 的功能不仅限于键盘、鼠标和显示器的切换，已经扩展到串口设备，如利用串口完成集线器、路由器、储存设备及 UPS 等的切换控制。

5 安全仪表系统(SIS)和火气系统(FGS)

5.1 一 般 规 定

5.1.1 完整的安全仪表系统和火气系统应包括现场的传感器、探测器件和最终执行元件以及逻辑控制单元，本规范仅重点讨论逻辑控制单元(包括控制器、I/O 卡件、通信网络)及辅助操作设备，对仪表安全系统在油气田及管道工程中的应用原则作出规范，有关安全仪表系统的具体要求应符合现行国家标准《石油化工安全仪表系统设计规范》GB/T 50770 的有关规定。

5.1.5 通过回路诊断和系统自诊断，可检测线路的开路和短路故障、仪表故障或 I/O 模板通道故障，检测到这些故障后系统应立即报警提醒操作员处理；同时可执行自动 MOS 操作，短时间隔离故障，减少不必要的停车。执行自动 MOS 操作应注意：

(1)应是有人值守站场；

(2)应在 BPCS 上报警；

(3)自动 MOS 操作应有时间限制，延时时间一般不超过 1h，超出设定延时时间后，如故障不恢复或未检测到手动 MOS，应自动撤销 MOS，此时可能导致系统停车。

5.1.6 SIS 系统和 FGS 系统的最终执行元件，如紧急切断阀、紧急泄放阀、雨淋阀等的开关控制，应由 SIS/FGS PLC 根据因果表逻辑判断完成，不应在 BPCS 画面上设置最终执行元件的手动操作开关/按钮。

另外，如果确实需手动操作只有两个途径：一是在工程师站上强制；二是通过对输入参数维护超驰，断开逻辑。采取这些措施会使系统处于维护(不安全)状态，工程师应尽快处理问题，尽早取消强制或超驰，使系统返回安全状态。

5.1.7 油气田及管道工程的工艺参数变化都较缓慢，由停车引起的次级停车时间间隔也较长，因此除压缩机防喘振等特殊应用外，SOE 的分辨率不要求太高，但不应大于 100ms。

5.2 安全仪表系统(SIS)

5.2.2 安全仪表系统按照 SIL 等级的要求分为 1、2、3、4 级。SIL 等级越高，安全仪表系统实现安全功能越强。油气田及管道工程不高于 SIL3。

5.2.4 不少厂家的 SIS 系统部件不冗余也具有一定的 SIL 等级认证，冗余虽不能提高 SIS 系统的 SIL 等级，但可以大大增加系统的可用性。考虑到油气田及管道工程的重要性及连续不间断的运行需求，SIS 系统控制器、通信网络及供电电源等宜按冗余设计。

5.2.5 安全仪表系统的内部通信网络是指以下两类：SIS 控制器和 I/O 模板之间的通信网络，SIS 控制器与 SIS 控制器间的通信网络。

5.2.6 安全仪表逻辑动作，如停车执行后，不应自动重启，应先复位，复位方式有如下三种：

(1)自动逻辑复位：非主流程上的单元级停车，如容器液位低低停车，在液位恢复后，可自动逻辑复位。

(2)手动逻辑复位：除自动逻辑复位外，必须先在 HMI 和或硬手操盘上手动复位，安全逻辑才能重启。

(3)就地手动复位：紧急泄放阀、重要流程上的切断阀、转动设备、现场锁定手动按钮(如 ESD 按钮)应就地手动复位。

5.2.7 本条规定适用于多个站场组成的 SCADA 系统中(各站场设置 SIS 系统)，这些站场一般是上下游管线，工艺过程相互关联，在一个站场出现重大事故时，为预防次生灾害，一般需要计划关停其他站场。设计人员经常会混淆紧急停车和按计划关停的区别，如在一个长输管道 SCADA 系统中，某一中间站场发生管线破裂，站场内压力变送器会检测到压力低低，自动触发安全逻辑关断相

应紧急切断阀；这时在远端的调控中心也会收到该站场压力低低的报警，操作员可通过 SCADA 系统远程关停上下游站场，以避免次生灾害的发生。在这个例子里，站场内压力低低是停车原因，导致站场内相关的切断阀关闭是停车结果，原因直接导致结果是个完整的紧急停车过程；而上下游站场的远程关停是个按计划关停的过程，在这些站场里并没有发生足以导致停车的事故，它们都是安全的，此时的关停是有计划的，可最少关闭甚至不关闭紧急切断阀，仅动作必需的工艺阀门即可，转动设备也可以缓慢关停，甚至是不关，比如对压缩机等旋转设备，可以通过关闭出口阀，打开回流阀，使压缩机处于低负荷或无负荷状态下运行。这样有利于流程的再启动，减少停车时间和损失。

5.2.8 采用这种混合应用前必须认真论证，且必须满足如下条件：

(1)BPCS 和 SIS 规模都较小；

(2)BPCS 功能简单，没有复杂的调节回路；

(3)BPCS 操作和逻辑不影响 SIS 逻辑的执行；

(4)除与上位系统软件通信外，BPCS 宜无其他通信口；

(5)如选用的控制器厂商有混合应用的推荐方案，SIS 系统的搭建和模板选型必须严格按厂商的推荐方案执行。

5.3 紧急停车(ESD)功能

5.3.2 ESD 停车级别一般分为 4 级，见表 3。

表 3 ESD 停车级别

停车级别	名称	触发原因	停车结果
ESD-0	弃厂	火灾、爆炸等无法挽回的事故	关断所有紧急切断阀，打开所有紧急泄放阀，断开现场供电，延时断开 UPS 供电
ESD-1	泄压停车	火灾、可燃气体泄漏、爆管等重大事故	关断所有紧急切断阀，打开所有紧急泄放阀，断开现场供电

续表 3

停车级别	名称	触发原因	停车结果
PSD	过程停车	影响主工艺生产的故障	工艺过程停车，关断所有紧急切断阀和转动设备
USD	单元停车	单台设备或不影响主工艺流程的单列设备故障	关断事故区域单台设备或单系列设备，关断相关紧急切断阀和转动设备

5.3.3 串级停车逻辑指由一个停车结果触发另一停车，如由一个紧急切断阀的关闭到位作为停车原因，去触发上游紧急切断阀的关断。

5.3.4 相关的非 SIS 设备一般指与被关断设备流程上有关联的调节阀、开关阀、转动设备等，这些设备一般由 BPCS 控制。如在一座油罐出口设置一台紧急切断阀和一台调节阀，分别由 SIS 和 BPCS 控制。在紧急切断阀关断时，调节阀也应联锁关闭；在故障解除、复位后，紧急切断阀会迅速全开，由于调节阀此时还是关闭状态，可在 BPCS 控制下慢慢开启，避免停车复位后对下游流程产生较大的冲击。

要实现该功能，推荐做法是紧急切断阀的开关状态直接由 BPCS 采集，在 BPCS 中完成联锁控制。

5.3.5 除停产检修外，紧急停车按钮和最终执行元件，如紧急关断/泄放阀等，不应被超驰或旁路。

5.4 火气系统(FGS)

5.4.1 工业领域的火气系统一般有三种组成方式：

(1)所有火气设备进火气报警控制器，火气报警控制器与 SIS 系统通过硬线连接，与 BPCS 系统通过通信接口连接。

(2)所有室外火气设备接入安全认证 PLC 组成的火气系统 PLC，室内火气探头进室内火气报警控制器。

(3)所有火气设备接入安全认证 PLC 组成的火气系统 PLC。

本规范所指的火气系统仅适用于后两种，火气报警控制器要求见相关规范。

5.4.2 有别于 ESD 逻辑的非励磁(失电)停车，FGS 是励磁(带电)输出，平时火气输出回路是非励磁(失电)状态，因此两个系统的模板和逻辑应分开。

5.4.4 宜在 HMI 和/或硬手操盘上分别设置手动复位按钮，并应注意如下事项：

(1)部分火气探测器，如感烟、感温探测器须回路断电才能恢复，在系统设计时应考虑；

(2)火气逻辑动作，如执行消防输出后，不应自动重启，应先复位。

5.4.5 除停产检修外，火灾和可燃气体手动报警按钮、最终执行元件(如消防释放阀)不应被超驰或旁路。

5.5 通信接口

5.5.1 安全仪表系统、火气系统和基本过程控制系统建议选择同一公司产品，有利于无缝连接。

5.6 辅助操作设备

5.6.4 硬手操盘可分为 ESD 部分和 FGS 部分，配置建议如下：

(1)ESD 部分：

按停车级别或区域设置 ESD 按钮，宜设置状态指示灯；

按停车级别设置复位按钮；

按停车级别设置 ESD 公共报警指示灯；

设置系统正常指示灯；

设置维护超驰允许钥匙开关和状态指示灯；

设置操作超驰允许钥匙开关和状态指示灯。

(2)FGS 部分：

按消防分区设置火灾手动报警按钮和状态指示灯；

按消防分区设置气体泄漏手动报警按钮和状态指示灯；
按消防分区设置公共火灾报警指示灯；
按消防分区设置公共气体泄漏报警指示灯；
按消防分区设置消防启动按钮和状态指示灯；
设置消防泵/泡沫泵手动启动按钮和泵状态、故障指示灯；
设置消防释放阀手动打开按钮和开关状态指示灯；
设置火灾报警复位按钮；
设置气体泄漏报警复位按钮；
设置报警确认按钮；
设置火气维护超驰允许钥匙开关和状态指示灯。

(3)硬手操盘设置指示灯测试按钮。

5.6.5 模拟显示盘(屏)建议包括如下指示：

(1)按消防分区设置火灾公共报警指示灯；

(2)按消防分区设置气体泄漏公共报警指示灯；

(3)按消防分区设置消防释放阀释放指示灯；

(4)按停车级别和区域设置 ESD 公共报警指示灯；

(5)设置系统正常状态指示灯；

(6)设置指示灯测试按钮。

6 系统软件及功能

6.1 基本配置和功能

6.1.3 监视控制软件图形显示和操作响应时间可参考表 4。

表 4 图形显示和操作的响应时间

功　能	推荐值	最大值
数据采集显示	1.0s	3.0s
报警事件分辨率	<0.2s	0.5s
SOE 事件分辨率	<50ms	100ms
显示画面调用(250 个动态参数)	<2.0s	4.0s
显示刷新	1.0s	4.0s
控制输出	<0.5s	2.0s
汇总信息	1.0s	2.0s
PID 回路控制	<0.25s	1.0s
8 参数趋势显示调用	<2.0s	3.0s
模拟输出显示	1s	2.0s
基于 NTP/SNTP 时钟同步精度	±50ms	±100ms
其他方式时钟同步精度	±0.1s	±1s
冗余服务器切换时间	<5s	15s

注：所有功能测试应在系统峰值负载下进行，如大量过程参数同时变化，多个点同时报警或在多个操作员工作站同时调用新画面和打印报告。

数据采集速率应根据系统性能和被控对象特性来确定，在有线通信连接下建议的服务器数据采集速率是：

(1)模拟信号：温度 10s、压力 1s、流量 2s、液位 2s、其他 5s；

(2)数字信号：1s。

6.1.6 智能仪表设备管理系统是针对智能仪表、智能阀门定位器

等进行在线组态、调试、校验管理、诊断及数据库记录的设备管理应用软件，目前主流DCS厂商都有自己的智能仪表设备管理系统，其应用已经有十多年历史，在炼化领域尤其广泛，在部分管道项目中也开始应用。建议在智能仪表、阀门数量较多的工程中配置。

6.2 人机界面

6.2.2 生产运行操作画面宜包括：

(1)菜单画面，列出可显示的全部画面的一个目录，可以在此画面上直接调用所需画面。

(2)动态流程图显示画面，用图形、颜色、数据等组合显示装置的运行状态和变量的实时值，生产运行和SIS参数可在同一幅画面中显示。流程图画面可分为总流程图、各工艺流程图和重要设备单体流程图三类。

(3)测控点详细画面，点击屏幕上的位号可激活与该位号相关联的测控点详细画面，可显示该点的全部信息，可进行与测控点相关的设置，如扫描、报警、设定值、死区等的设置。

(4)数据总貌画面，列表显示全部过程变量，应包括橇块部分数据总貌。

(5)组显示画面，在每一组显示画面上，同时显示几个(如8个)相关检测控制点的信息；

(6)趋势显示画面，每幅趋势显示画面应在同一坐标上，同时显示至少4个变量的变化趋势。每个变量的变化趋势应以不同颜色显示。应有2个～3个间隔时间供用户自由选择，如1h、8h、24h等。

(7)通信统计显示画面，显示各级通信状态。

(8)报警显示画面，应有多种可供选择的声响和颜色，报警级别用不同的声响区分，并能通过显示画面确定第一报警原因。过程存在的所有报警可同时显示。

(9)报警总汇和报警记录显示画面。

(10)报警组态画面。

(11)多值比较画面，在综合控制系统中，有些监测点可能设置多台变送器(如2台)，分别进入BPCS和SIS系统，如果有这种情况存在，应单独设置多值比较画面。多值比较画面是将同一监测点设置多块仪表的数据全部分列在一起，显示实时值、偏差值和偏差报警，仪表数据偏差超过报警限会触发报警。

6.2.3 SIS和FGS系统应设独立画面，建议包括停车层次图、SIS流程图、维护、火气总貌、火气分区及数据总貌等画面。

(1)停车层次图，可显示各级别停车的关系和停车因果联系，显示所有停车原因与结果的对应状态。

(2)SIS流程图，根据P&ID软件开发，仅显示SIS参数的动态流程图画面。

(3)SIS维护超驰画面，以列表及图标方式显示每个停车的因果关系，每一停车原因可单独设置维护超驰/正常状态。

(4)SIS操作超驰画面，以列表及图标方式显示每个需超驰回路的输入、输出关系，对每个回路可单独设置操作超驰开关、延时时间、剩余时间和剩余时间报警。

(5)SIS数据总貌画面，列表显示所有SIS相关参数值。

(6)火气总貌画面，显示所有报警分区的报警和消防状态。

(7)火气分区画面，显示火气分区的报警和消防状态，每个探头和输出设备都可以显示，并可以进行火气维护超驰操作。

(8)火气数据总貌画面，列表显示所有火气相关参数值。

6.2.4 工程师应能够在维护画面上方便地进行整个系统的诊断和维护，能准确地观察到系统发生故障的位置，指导维护人员对全系统进行维护，这些画面宜包括：

(1)系统诊断画面，在此画面上显示系统设备、通信及网络的诊断结果及发生故障设备的位置等。

(2)系统维护画面，根据自诊断结果，显示维护提示指导维修人员。

(3)系统资源使用情况画面，显示整个系统资源的使用情况及各设备负荷，便于系统管理和负荷调整。

(4)设备状态画面，显示设备状态，发生故障时可显示故障设备位置及相关故障信息。

6.3 数据管理

自控系统涉及的数据和文件如图2所示，文件记录应严格管理。

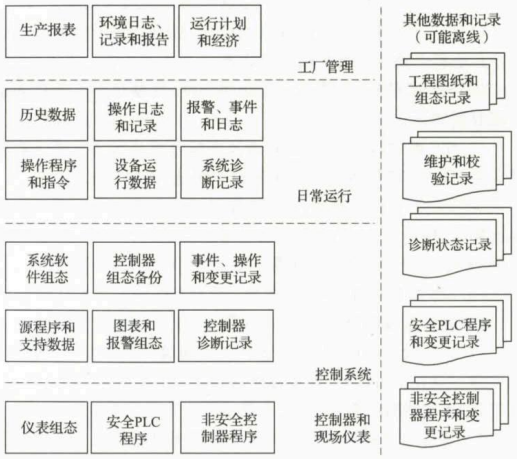

图2 计算机控制系统数据文件文档结构图

6.3.2 实时历史数据宜根据下列规定设置：

(1)实时数据采集宜按下列规定设置：

1)快速瞬时值：快速采集各参数的瞬时值，采样周期一般是1s～30s，每个点的采样周期独立可调；

2)慢速瞬时值：用较慢速度采集各参数的瞬时值，采样周期一般是1min、6min、1h、8h等，每个点的采样周期独立可调；

3)慢速平均值：用较慢速度采集各参数一段时间内的平均值，采样周期一般是1min、6min、1h、8h等，每个点的采样周期独立可调；

4)报警和事件：发生时记录。

(2)不同类型的实时数据在实时数据库中存储的时间不同，宜设置为：

1)快速瞬时值在实时数据库中存储时间较短，一般为12h～24h；

2)慢速瞬时值存储时间稍长，一般1min的存储30d，6min的存储90d；

3)慢速平均值存储时间稍长，一般1min的存储30d，6min的存储90d；

4)报警和事件一般记录90d。

(3)历史数据库的在线存储时间一般是3年。

6.4 报警和事件

6.4.2 报警宜至少分为高高(HH)、高(H)、低(L)和低低(LL)4个级别，不同级别报警的颜色和行为设置如表5所示。

表5 不同级别报警的颜色和行为设置

过程状态	报警未确认	报警已确认	正常未确认	正常已确认
首出报警	红色双倍闪烁	红色	正常色双倍闪烁	正常色
高高和低低报警	红色闪烁	红色	正常色闪烁	正常色
高和低报警	黄色闪烁	黄色	正常色闪烁	正常色

6.4.4 报警记录应能记录位号、描述、报警等级、报警限、报警值、报警发生和恢复时间、报警持续时间和报警确认时间，报警时间需精确到秒级。

6.4.6 本条第3款：系统内有量程限制的点，如超过正常范围一定

的阈值，认为是无理值。如一模拟量输入点，正常范围是 4mA ～20mA，设置的阈值是±10%，当信号输入小于 3.6mA 或大于 22mA 时，认为是无理值，应报警。

6.4.7 参见第 6.4.2 条的条文说明。

6.6 系统安全

6.6.2 本条第 2 款："空闲自动退出"是一种自动保护机制，指在系统登录后，如一定时间内无操作（键盘、鼠标无动作），系统会自动退出登录，防止操作人员不在情况下，非授权人员对系统误操作。

6.6.3 本条第 1 款：预设安全位置应根据工艺要求确定，一般有故障关（FC）、故障开（FO）、故障保位（FL）和故障到特定输出值。

本条第 2 款：未完成报警是指操作命令发出后，在一定时间内未接收到期望的反馈而产生的错误报警。如阀门开关动作，假设该阀最长开阀时间是 20s，开阀时间预设为 30s（一般预设值略长于最长开阀时间）；在开阀命令发出后，若在 30s 内接收到阀开到位信号，则认为开阀正常；否则认为是阀门卡堵，未完成开阀操作，应发出开阀故障报警。

本条第 4 款：无理值钳位：对系统内有量程限制的值可设置无理值钳位，即超出正常值后，数据库存储值就钳位在预设的数值上，不再增大或减小，以防止计算和存储错误。如某测量值量程为 0～100，钳位值设为量程的±10%，则钳位行为如表 6 所示：

表 6 无理值钳位表

实际测量值	数据库存储值	无理值报警
50	50	无
>110	110	报警
<−10	−10	报警

8 电气设计

8.1 供 电

8.1.3 UPS 宜符合下列规定：

(1)UPS 的容量按实际 UPS 供电负荷的 1.5 倍考虑。

(2)技术指标应符合下列规定：

1)输入参数：

输入电压：三相 380V±15%或单相 220V±15%；

输入频率：50Hz±2.5Hz。

2)输出参数：

交流电源：电压 220V±5%，频率 50Hz±0.5Hz，波形失真率小于 5%；

直流电源：电压 24V±0.3V，纹波电压小于 0.2%，交流分量（有效值）小于 40mV；

允许电源瞬断时间：小于或等于 4ms；

电压瞬间跌落：小于 10%；

三相交流供电的相间负荷不平衡度应小于 20%。

(3)UPS 的后备电池宜选用密封免维护电池。

(4)配置自启动应急发电机的站场，UPS 后备供电时间宜为 30min，配置手动启动发电机的站场，UPS 后备供电时间宜为 1h。

(5)UPS 应具有故障报警及保护功能，宜有报警输出接点。报警信息宜上传至计算机控制系统。

8.2 电缆敷设

8.2.3 穿墙密封可防止尘埃、雨水、可燃/有毒气体及小动物入室。

8.3 防雷及接地

8.3.2 防雷是一项系统工程，需要电力、自控、通信、阴极保护及建筑等多专业协调完成。在设计中需要分析雷击危害造成的影响，对于仪表和控制系统等重要设施，需要结合现场实际情况，综合雷击风险与投资预算，确定经济合理的技术方案。中国气象局第20号令《防雷减灾管理办法》(2011年9月1日)中第二十七条规定“大型建设工程、重点工程、爆炸和火灾危险环境、人员密集场所等项目应当进行雷电灾害风险评估，以确保公共安全。”因此，新建的油气生产设施均需要按照防雷安全管理要求进行风险评估，通常是由地方气象机构组织完成，建设单位按照评估意见进行设计施工后，依据中国气象局第21号令《防雷装置设计审核和竣工验收规定》对防雷工程进行审查及验收。

8.3.3 本条对电涌保护器的选择进行了规定。

1 本款是根据现行国家标准《低压电涌保护器(SPD) 第1部分：低压配电系统的电涌保护器 性能要求和试验方法》GB 18802.1、《低压配电系统的电涌保护器(SPD) 第12部分：选择和使用导则》GB/T 18802.12进行编制。组合型SPD是由电压开关型元件和限压型元件组成，能量配合应根据SPD制造商提供资料进行，若缺少相关数据，可以按照Ⅱ级试验的SPD标称放电电流不应小于5kA、Ⅲ级试验的SPD标称放电电流不应小于3kA进行。

2 本款是根据现行国家标准《低压电涌保护器 第22部分：电信和信号网络的电涌保护器(SPD)选择和使用导则》GB/T 18802.22进行编制。仪表信号通常为24V直流，SPD的保护水平应与信号设备的冲击耐压水平一致；在防雷分区LPZ1/2区标称放电电流不应小于5kA，在防雷分区LPZ2/3区标称放电电流不应小于0.5kA。考虑到目前信号用SPD标称放电电流基本为5kA及以上，因而统一规定其标称电流不应小于5kA。

3 本款主要是考虑SPD与被保护的仪表或控制系统距离过

大时，回路振荡现象导致的过电压引起设备故障。

4 控制系统信号通常以电源负极作为参考点，控制系统内电源一般为24V直流。不同控制系统的参考点有接入工作接地的，也有浮空的情况，而参考点接入工作接地的电势变化对系统不会产生影响，不论是否接地，其信号正极与负极之间的额定电压维持在24V直流。采用共用接地系统时，保护接地系统通常为多点接地，其对地工频电阻较小，接地可靠，发生雷电电涌时，冲击放电电流能够快速泄放，因此规定电源SPD接地端接入保护接地。

8.3.7 一般情况下，单点接地的屏蔽层应在信号源接收端，即机柜端接地；当信号源接地时，单点接地的屏蔽层应在信号源端，即现场端接地。

8.3.11 计算机控制系统的工作接地和保护接地需要分别设置等电位连接(EB)，EB可以是端子板、端子箱或者沿机柜平行敷设的铜排等。接地系统的基本结构如图3所示，其中工作接地为一点接地，图3中的工作接地汇流排、工作接地EB与共用接地系统连接前，均应保证对地绝缘。

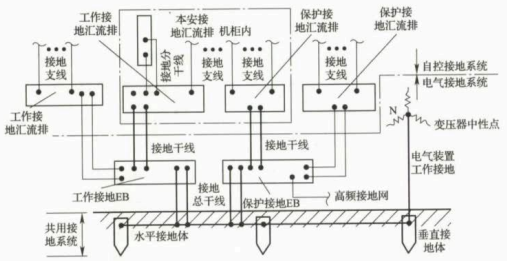

图3 控制室接地系统示意图

机柜内接地汇流铜排的截面积不宜小于25mm×6mm。接地线不小于1.5mm²，接地支线不小于4mm²，接地分干线不小于

6mm²，接地干线不小于 16mm²，接地总干线宜为 25mm² ～ 50mm²。

8.3.12 本条规定是保证接地的可靠性，对于数字信号，不同路径走向可以有效避免谐振造成接地阻抗无穷大的问题。

9 控 制 室

9.4 暖 通

9.4.1 计算机控制系统本身对温度、湿度的环境要求较宽。室内温度除应满足设备要求，还应兼顾室内工作人员长期工作健康和舒适方面的要求，本规范按现行国家标准《采暖通风与空气调节设计规范》GB 50019 中舒适性空气调节室内计算温度的指定范围，同时考虑我国人民不同季节着装习惯，按夏、冬两个季节分别确定。

计算机控制系统对环境温度剧烈变化要求严格，需防止温度在宽范围内波动引起短时间结露的可能性。温度指标在选择空调制冷机组时，考虑分步启动程序即可满足。

相对湿度根据人体生理学原理，考虑舒适性指标。另外，对于计算机的电子芯片和线路（密封型产品例外），如湿度太高，大气中含有一定浓度的腐蚀性气体 SO_2 等会使腐蚀加快；如湿度过低，由于空气中运动物体摩擦易发生静电，严重时放电会干扰硬、软件的正常工作，空气加湿 30% 以上是有效经济地防止静电干扰的措施，所以本条规定基于提高设备的工作可靠性、寿命和工作人员的舒适性而制定。

空气净化要求主要是对尘埃和 H_2S、SO_2、Cl_2 等有害气体浓度的限制。根据现行国家标准《电工电子产品应用环境条件 第1部分：贮存》GB/T 4798.1 对环境参数的严酷程度和适用条件以及对化学活性物质含量和机械活性物质含量的规定，尘埃一项稍放宽，氯气含量则按国际标准限制，其余与国家现行有关标准大致相当。

9.4.6 有别于通信和网络中心，油气田及管道工程控制系统采用

工业级设备，电缆及供配电也作了许多保护措施，控制室内设备除无法防水喷溅外，防静电地板下的电缆短时间浸泡不会发生故障。因此只要是做好防喷溅措施，如采用金属罩保护好暖气片，暖气管线室内不留阀门和放水口，管道连接全部采用焊接等，控制室内可以采用水暖或蒸气供热。

附录A　油气田计算机控制系统设计要求

A.1　一般规定

A.1.1　油气田计算机控制系统包括对一个区块或多个区块的生产调度管理系统和所辖站场的监控系统，生产调度管理系统对区块内站场生产过程进行监视和优化管理；站场监控系统对本站及所辖井、站工艺生产过程进行实时监控。

A.1.2　工艺装置相对集中的站(厂)，包括多个工艺处理装置或多个工艺单元。油气处理厂、天然气净化厂、原油稳定装置等工艺装置或单元较多，工艺过程相对复杂的站(厂)，经过调研统计，基本过程控制系统都采用了DCS(或大型PLC)系统。如塔里木油田的迪那油气处理厂、英买力油气处理厂，长庆油田苏里格第二油气处理厂、天然气第二净化厂，大庆油田的北Ⅰ-1和南压天然气处理厂的基本过程控制系统均采用不同品牌的DCS系统。而独立建设、工艺处理装置(单元)相对较少的场站，如原油脱水站、接转站、集气站、采出水处理站、注入站(注水站、注聚站)、配制站等工艺站场，经过调研表明，基本过程控制系统均采用了中小型PLC系统。

A.1.4　油气田站场如果第三方自带控制系统的设备或智能仪表较多，当与BPCS采用通信方式传输数据时，采用标准通信协议，可采用串口的通信协议如MODBUS，PROFIBUS等，也可采用工业以太网TCP/IP协议，便于BPCS的组态、调试和通信数据上传。如果站场控制系统需要急停这些设备时，不宜采用通信方式实现，而宜采用硬线连接方式实现。

A.3　油气田站场监控系统

A.3.1　本条规定了油气田站场监控系统的基本要求。

2 转油站、注水站、注聚站、配制站、采出水处理站等站场，工艺过程简单，调节回路较少，对安全可靠性没有特殊要求，基本过程控制系统宜采用 PLC 系统。

3 根据长庆榆林、靖边、苏里格等气田多年的运行管理经验，多井集气站工艺生产过程控制采用可编程序控制器 PLC，紧急停车系统由于 I/O 点较少，均没有设置独立的具有 SIL 认证的逻辑控制器，都是通过继电器和紧急停车按钮实现紧急停车控制。如果 I/O 点较多，经过风险评估，用继电器等元件组成的逻辑控制回路不能满足要求，应采用具有 SIL 认证的逻辑控制器。

6 本款对油气田火灾及可燃(有毒)气体报警系统设计进行了规定。

2)“气体检测”指可燃(毒性)气体检测；油气田需要设置可燃(毒性)气体报警系统的站场很多，中小型站场气体检测点数少于 30 点可直接采用盘装表方式进行监视报警或采用独立的数据采集系统。

3)根据现行国家标准《石油化工可燃气体和有毒气体检测报警设计规范》GB 50493—2009 第 5.3.2 条的规定编写，当与 BPCS 系统合并设计时，应考虑相应的安全措施，保证装置 BPCS 出现故障或停用时，可燃(毒性)气体检测报警系统仍能保持正常工作状态，采用独立的 I/O 卡件就是措施之一。也可以考虑采用其他的安全措施，如独立设置的控制器和操作站，配备足够的便携式可燃(有毒)气体检测报警仪。

4)油气田油气处理规模较大的站(厂)和库容较大的油库，如集中处理站、天然气净化厂(处理厂)、单罐容积大于 30000m^3 的油库，可燃(有毒)检测报警系统应优先考虑与火灾检测报警系统合并设置，构成火气系统。

5)FGS 与 BPCS 的通信接口可以是串口，也可以是以太网接口。

A.3.2 本条对系统软、硬件配置作出规定。

2 本款对 BPCS 硬件配置作出规定。

1)接转站(增压点、转油站)、放水站、原油脱水站，注入站(注聚站、注水站、注汽站)，水处理站(采出水、地下水)、供水站，集气站、增压站、输气站、锅炉房等油气田站场宜设置一台操作员工作站和一台打印机。如果需要监控的生产数据较多，可以设置一机双屏操作员工作站。

3)对安全可靠性要求较高的站(厂)是指中断生产会造成环境污染、人员伤亡和经济损失的站场；其他站(厂)是指中断生产不会造成人员伤亡和立即造成环境污染及经济损失不大的站场，一般只设控制器冗余。油气田除上述站(厂)外，BPCS 的控制单元、网络、电源不宜冗余配置。

4)集中处理站、天然气净化厂(处理厂)等大型重要的站场宜设置独立的数据服务器，中小型站场的数据服务器可与操作员工作站合并设置。

A.3.3 本条对站场控制系统功能作出规定。

“站场”包括油气田井场、站、库，而“站(厂)”是指除井场外的站、库。站(厂)控制系统指油气田站(厂)采用的控制系统总称，可能是 BPCS 或 BPCS、SIS 或 FGS 的组合。本条第 1 款中的站(厂)是指一般有人值守，设置操作员工作站，具有监视操作功能的站(厂)。本条第 2 款中的站场是指一般无人定岗值守，不设置操作员工作站的站场。

附录B　输油气管道SCADA系统设计要求

B.1　一般规定

B.1.2　主调度控制中心、备用调度控制中心的控制系统简称“调度控制中心”或“控制中心”；沿线站场的控制系统简称“站控制系统”；监控（监视）阀室的RTU控制系统简称“阀室RTU”或“阀室”。

B.1.3　当调度控制中心的主通信信道出现中断，系统应自动切换到备用信道；若备用信道也发生故障，经通信网络管理系统判断确认后，系统应切换到备用调度控制中心，并发出报警信号。

B.1.4　调度控制中心计算机控制系统或通信系统故障时，应由站场控制系统接管控制权来完成各工艺站场的控制。

B.2　调度控制中心

B.2.2　本条对软件配置作出规定。

4　根据管道运行需要及管网复杂程度，配置管道高级专用软件。包括管道泄漏检测及定位、管道效率、批量输送管理、混油量计算、清管器跟踪、过程预测、模拟培训、管道运行模拟等功能模块软件。

B.2.3　本条对主要功能作出规定。

1　本款对SCADA系统调度控制中心作出规定。

1）调度控制中心一般配置有实时服务器、历史服务器、模拟仿真服务器和Web服务器，这些服务器分担的任务如下：

实时服务器：负责处理、存储、管理从沿线各站的控制设备采集的实时数据，并为网络中的其他服务器和工作站提供实时数据。通常实时数据服务器中同时运行通信管理软件，完成与沿线各站

的通信链接、协议转换、网络管理等任务。

历史服务器：主要完成历史数据的存储、管理，并为网络中的其他服务器和工作站提供数据。

模拟仿真服务器：运行管道模拟仿真软件，完成在线模拟仿真、管道泄漏检测及定位、管道负荷预测、输油计划等功能，同时提供培训功能。

Web服务器：是SCADA系统与外部其他服务器（设备管理服务器、地理信息服务器、管理信息系统等）的接口。SCADA系统将有关信息写入Web服务器，并对其实时更新。

4）管道全线的工艺过程控制包括全线正常的启输/停输、全线的增输/减输、操作参数远程设定等。

9）管道全线安全保护包括水击保护、紧急停输。

11）管道连续（在线）泄漏检测方法大致可分为两类：内部（间接）检测和外部（直接）检测。内部检测方法主要有：体积（或质量）平衡法、统计分析法、实时瞬态模型法（RTTM）、压力分析法（负压波法）、音波法。外部检测方法主要有：光纤预警、智能防腐层预警等技术方法。

目前，上述检测方法基本上都存在可靠性不高、响应时间过长、灵敏度差、定位效果差等不足。因此，设计时应综合考虑各种检测方法的特点，审慎选择。目前较多采用不同的检测方法组合使用，结合各自不同的优缺点，功能上互补，以取得相应的功能要求。

12）指液体管道工艺站场设置的储罐，其过程参数与管道运行相关，可纳入站控制系统统一管理。

B.3　站场控制系统

B.3.1　本条对系统配置作出规定。

4　紧急停车系统是为工艺站场紧急切断和放空而设置的控制系统，安全保护系统是为管道全线水击事件、安全事件发生后，

采取相应的保护措施而设置的控制系统。

B. 3. 2 本条对系统功能作出规定。

2 本款对基本过程控制系统配置作出规定。

2)此处第三方智能仪表系统或设备一般意义上指相对独立于站场控制系统的成橇设备的控制系统或其他带有通信接口的复杂智能仪表,如加热炉系统的控制器、密度计橇的二次仪表、电力综合保护系统、计量系统的流量计算机、超声波流量计等。

S/N:1580242·026
9 158024 202601

中国计划出版社
电话:400-670-9365
网址:www.cn9365.org
刮涂层 输防码 查真伪

统一书号：1580242·026
定　　价：20.00元