ICS 25.040
P 72
备案号：

SH

中华人民共和国石油化工行业标准

SH/T 3092—202X

代替 SH/T 3092—2013

石油化工分散控制系统设计规范

Design specification for distributed control system in petrochemical industry

（报批稿）

202X-XX-XX 发布　　202X-XX-XX 实施

中华人民共和国工业和信息化部　发布

工业和信息化部标准报批公示

工业和信息化部标准报批/
工业和信息化部标准报批公示
工业和信息化部标准报批公示
工业和信息化部标准报批公示
工业和信息化部标准报批公示
工业和信息化部标准报批公示

目　　次

前　　言 V
1 范围 1
2 规范性引用文件 1
3 术语和缩略语 2
3.1 术语和定义 2
3.2 缩略语 6
4 设计原则 7
4.1 一般规定 7
4.2 系统性能 7
4.3 系统功能 8
4.4 报警和事件记录 9
5 系统结构 10
5.1 功能结构 10
5.2 网络结构 11
6 系统安全 11
6.1 信息安全 11
6.2 网络安全 12
6.3 安全管理措施 13
6.4 安全管理系统 13
7 系统技术要求 14
7.1 过程控制站 14
7.2 过程接口单元 14
7.3 操作站 16
7.4 工程师站 17
7.5 历史服务器 17
7.6 网络管理服务器 18
7.7 安装条件 18
7.8 供电及接地要求 18
7.9 备品备件 19
8 网络系统 19
8.1 网络特性 19
8.2 网络设备 19
8.3 网络负荷 20
8.4 与第三方设备通信 20
9 辅助设备 21
9.1 辅助操作台 21

9.2 机柜 21
9.3 打印机 21
9.4 其他辅助仪表 21
10 高级应用 22
10.1 智能设备管理系统 22
10.2 实时数据服务 22
10.3 过程数据服务 22
10.4 先进控制 22
10.5 储运管理 22
10.6 网页浏览服务 23
10.7 报警管理系统 23
10.8 其他高级应用 23
11 软件配置 23
11.1 控制和操作软件 23
11.2 工程组态软件 23
11.3 软件版本 23
11.4 软件授权 23
12 工程实施 24
12.1 系统开工会 24
12.2 功能设计 24
12.3 组态 24
12.4 系统集成 25
13 工厂验收及集成测试 25
13.1 工厂验收测试 25
13.2 工厂集成测试 26
13.3 现场验收测试 27
14 工程服务 27
14.1 技术服务 27
14.2 现场服务 28
附录 A（资料性） 分散控制系统网络结构示意图 29
附录 B（资料性） 分散控制系统网络分区 33
附录 C（资料性） 分散控制系统网络安全结构示意图 35
本规范用词说明 39
附：条文说明 41

工业和信息化部标准报批公示

Contents

Foreword V
1 Scope 1
2 Normative references 1
3 Terms and Abbreviations 2
3.1 Terms and definitions 2
3.2 Abbreviations 6
4 Design Principles 7
4.1 General requirements 7
4.2 System performance 7
4.3 System function 8
4.4 Alarm and events 9
5 System architecture 10
5.1 Function architecture 10
5.2 Network architecture 11
6 System security 11
6.1 Information security 11
6.2 Network security 12
6.3 Security management requirements 13
6.4 Security management system 13
7 System technical requirements 14
7.1 Process control stations 14
7.2 Process interface units 14
7.3 Operator workstations 16
7.4 Engineer workstations 17
7.5 Historical servers 17
7.6 Network management servers 18
7.7 Installation conditions 18
7.8 Power supply and grounding requirements 18
7.9 Spare parts 19
8 Network System 19
8.1 Network Characteristics 19
8.2 Network Equipments 19
8.3 Network Load 20
8.4 Communication With Third-Party Devices 20
9 Auxiliary equipment 21
9.1 Auxiliary consoles 21
9.2 Cabinets 21
9.3 Printers 21
9.4 Other auxiliary instruments 21
10 Advanced application 22

10.1 Intelligent device management 22
10.2 Real-time data services 22
10.3 Process data services 22
10.4 Advanced process control 22
10.5 Storage and transportation management 22
10.6 Web servers 23
10.7 Alarm management system 23
10.8 Other application services 23
11 Software requirements 23
11.1 Process control and operating software 23
11.2 Engineering configuration software 23
11.3 Software version 23
11.4 Software license 23
12 Project implementation 24
12.1 Kickoff meeting 24
12.2 Function design 24
12.3 Configuration 24
12.4 Systems integration 25
13 Factory acceptance and integration testing 25
13.1 Factory acceptance 25
13.2 Factory integration acceptance 26
13.3 Site acceptance 27
14 Project services 27
14.1 Technical services 27
14.2 On-site services 28
Annex A (Informative) DCS network architechture diagram 29
Annex B (Informative) DCS network subarea 33
Annex C (Informative) DCS network safety architechture diagram 35
Explanation of wording in this specification 39
Add：Explanation of article 41

工业和信息化部标准报批公示

前　言

根据中华人民共和国工业和信息化部《2022 年第一批行业标准制修订和外文版项目计划》（工信厅科函〔2022〕94 号）的要求，规范编制组经广泛调查研究，认真总结实践经验，参考有关国际标准和国外先进标准，并在广泛征求意见的基础上，修订本规范。

本规范经中华人民共和国工业和信息化部 202×年××月××日以第××号公告批准发布。

本规范共分为 15 章和 3 个附录。

本规范主要技术内容包括：分散控制系统设计原则、系统结构、系统安全、系统技术要求、网络系统、辅助设备、高级应用、软件配置、工程实施、验收测试、工程服务等。

本规范是在 SH/T 3092－2013《石油化工分散控制系统设计规范》的基础上修订而成，修订的主要技术内容是：

——修改了系统和网络结构；

——修改了设计原则；

——修改了系统安全；

——修改了报警功能；

——增加了远程 I/O 设备；

——修改了网络系统；

——取消了分散控制系统规格书模板、分散控制系统数据表模板、分散控制系统技术评价文件模板、操作站及辅助操作系统构成示意图等资料性附录。

请注意本规范的某些内容可能直接或间接涉及专利，本规范的发布和管理机构不承担识别这些专利的责任。

本规范由中国石油化工集团有限公司负责管理，由中国石化集团公司自动控制设计中心站负责日常管理，由中国石化工程建设有限公司负责具体技术内容的解释。执行过程中如有意见和建议，请寄送日常管理单位和主编单位。

本规范日常管理单位：中国石化集团公司自动控制设计技术中心站

通信地址：浙江省宁波市高新区院士路 660 号

邮政编码：315103

电　　话：0574-87974979

邮　　箱：cacd.snec@sinopec.com

本规范主编单位：中国石化工程建设有限公司

通讯地址：北京市朝阳区安慧北里安园 21 号

邮政编码：100101

本规范参编单位：中控技术股份有限公司

杭州和利时自动化有限公司

杭州康吉森自动化科技有限公司

本规范主要起草人员：杨　刚　冯　欣　叶向东　邱添爽　李志勉　刘奋民　许　韦　周新辉

本规范主要审查人员：裴炳安　胡红页　庄晓峰　魏剑萍　于宝全　范咏峰　田京山　林　融

范宗海　贺文敏　俞旭波　施建设　邵　瑜　刘　冰　陈　鹏　曾裕玲

刘建兵　宋志远　张同科　葛春玉　阎　洁　任　泓　孙　旭　刘洪兵

任　义　曹　斌　王　冰　胡海涛　解　伟

本规范1999年首次发布，2013年第1次修订，本次为第2次修订。

工业和信息化部标准报批公示

石油化工分散控制系统设计规范

1 范围

本规范规定了石油化工分散控制系统（DCS）工程设计的原则和要求。

本规范适用于石油化工及以煤为原料制取燃油和化工产品的企业新建、扩建和改建工程分散控制系统的工程设计。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本规范必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本规范；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

GB 42250	信息安全技术 网络安全专用产品安全技术要求
GB/T 4208	外壳防护等级(IP 代码)
GB/T 9771.1	通信用单模光纤 第 1 部分：非色散位移单模光纤特性
GB/T 9771.7	通信用单模光纤 第 7 部分：弯曲损耗不敏感单模光纤特性
GB/T 16839.1	热电偶 第 1 部分:电动势规范和允差
GB/T 16895.21-2020	低压电气装置 第 4-41 部分：安全防护 电击防护
GB/T 17626.2-2018	电磁兼容 试验和测量技术 静电放电抗扰度试验
GB/T 17626.3-2023	电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验
GB/T 17626.4-2018	电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验
GB/T 30094	工业以太网交换机技术规范
GB/T 30121	工业铂热电阻及铂感温元件
GB/T 37933	信息安全技术 工业控制系统专用防火墙技术要求
GB/T 37934	信息安全技术 隔离与信息交换系统安全技术要求
JB/T 8623	工业铜热电阻技术条件及分度表
SH/T 3006	石油化工控制室设计规范
SH/T 3081	石油化工仪表接地设计规范
SH/T 3082	石油化工仪表供电设计规范
SH/T 3164-2021	石油化工仪表系统防雷设计规范
IEC 61156-5	数字通信用对绞/星绞多芯和对称电缆 第 5 部分：传输特性低于 1000 MHz 的对绞或星绞对称电缆 - 水平层布线 - 分规范 (Multicore and symmetrical pair/quad cables for digital communications-Part 5: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz- Horizontal floor wiring-Sectional specification)
IEC 61000-4-8	电磁兼容性(EMC).第 4-8 部分:试验和测量技术 工频磁场抗扰度试验

(Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test)

ISA 71.04 过程测量和控制系统的环境条件：大气污染物 (Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants)

3 术语和缩略语

3.1 术语和定义

下列术语和定义适用于本规范。

3.1.1

分散控制系统 distributed control system

控制功能分散，操作和管理集中，以计算机和微处理器为设备核心的，采用分级网络结构为系统结构的控制系统。

3.1.2

同步 synchronization

在特定时间段内，从属变量或备用变量的数值与原变量数值，或冗余设备信息与工作设备信息之间跟随并保持一致。

3.1.3

冗余 redundancy

采用多于一个部件或设备实现相同功能。

注：根据冗余部件不同的工作方式，冗余形式可分为热备冗余、同步冗余、冷备冗余。

3.1.4

热备冗余 hot standby redundancy

工作部件和冗余部件同时运行，输出结果采用工作部件的输出。当工作部件出现故障时，系统自动切换至冗余部件运行。

3.1.5

同步冗余 synchronization redundancy

工作部件和冗余部件同时运行，输出结果保持同步。系统自动选择正常运行的部件，并实现无扰动切换输出。

3.1.6

冷备冗余 cold standby redundancy

工作部件正常运行，冗余部件处于准备启动状态。工作部件出现故障时，系统自动或手动启动冗余部件替代工作部件运行。

3.1.7

容错 tolerance

工作单元在内部出现硬件故障或软件错误时，不受硬件故障或软件错误的影响继续执行原定功能的能力。

注：容错形式分为硬件容错和软件容错两种。

3.1.8

硬件容错 hardware tolerance

工作单元在部分元件或部件出现硬件故障时，不受故障影响，继续执行原定功能的能力。

注：硬件容错是通过特定的容错技术实现的，如分支电路、多重电路、故障旁路、降低指标、负荷分散等，使工作单元在部分硬件故障发生时保持性能，并正常运行。

3.1.9

软件容错 software tolerance

软件在检测到可识别的错误时，能够持续执行预定功能的能力。

注：软件容错机制的工作原理是在检测到软件运行错误或数据错误时，跳过错误数据或程序段，或调整条件重新计算，继续运行。

3.1.10

失效 failure

元件、部件、系统或设备失去或降低原定的功能。

3.1.11

故障 fault

元件、部件或设备出现的损坏或非正常状态，会导致其原定的功能失效。

3.1.12

平均失效前时间 mean time to failure

工作单元失效前正常工作的平均时间。

3.1.13

失效率 failure rate

正常工作的产品在单位时间内失效的概率。

3.1.14

组态 configuration

根据控制系统的软件功能和数据格式，配置控制系统各级结构，并将控制过程相关的数据以及控制方案输入到系统中，使控制系统具有完成工艺过程等控制任务的功能。

3.1.15

过程控制站 process control station

DCS完成检测、控制、运算和诊断等功能的设备。

注：过程控制站主要由控制单元、过程接口单元、供电单元和通信单元等部分组成。

3.1.16

控制单元 control unit

也称控制器，是过程控制站的主要处理单元，承担过程控制站的数据处理、控制运算等任务。

3.1.17

输入/输出模件 input/output module(I/O)

控制系统与外部设备的信号接口模件。也称为卡件或模块。

注：输入/输出模件是过程控制站中的过程接口单元，用于将外部设备的标准信号转换成控制单元的数字信号，或将控制单元的数字信号转换为标准信号输出到外部设备。

3.1.18

电磁干扰 electromagnetic interference

电磁作用对电子设备工作的非正常影响。

3.1.19

电磁兼容性 electromagnetic compatibility

电子设备具有一定的抗电磁干扰能力，同时在正常运行中产生的电磁干扰不超过规定的限制值。

3.1.20

抗电磁干扰能力 immunity

电子设备或系统受到电磁干扰时维持正常工作的能力。简称抗干扰能力。

3.1.21

中心控制室 central control room

位于石油化工工厂内，用于全厂或生产区内安装仪表、控制系统及其他设备，具有生产操作、过程控制、安全保护、报警监控及应急响应、先进控制与优化、信息存储及读取、现场监视、仪表维护、仿真培训等功能的辅助生产建筑物。

3.1.22

现场控制室 field control room

位于石油化工工厂内，用于对装置、专用单元或联合装置安装仪表、控制系统及其他设备，具有生产操作、过程控制、安全保护等功能的辅助生产建筑物。现场控制室可分为装置控制室和联合装置控制室，也适用于公用工程、储运系统、成套设备的现场控制室。

3.1.23

现场机柜室 field auxiliary room

位于石油化工工厂内，用于装置或联合装置安装仪表、控制系统机柜及其他设备，具有过程控制、安全保护等功能的辅助生产建筑物。

注：现场机柜室正常情况下不设操作和监控岗位。

3.1.24

操作分区 operation subarea

以生产操作或管理职能划分的工艺装置、公用工程单元、储运单元等组成的操作运行区域。

3.1.25

防火墙 firewall

设置在网络中的专用设备或一系列集成的安全组件，用于监控和管理网络通信，使得只有符合安全策略规定并且经过授权的通信流能够通过。是网络安全借用词。

3.1.26

隔离网闸 gap

通过专用硬件使两个或者多个网络在不连通的情况下，实现数据安全传输和资源共享的网络安全设备。

3.1.27

安全网关 security gateway

根据预先定义的访问控制策略和安全防护策略，解析和过滤经过网关的数据流，向被保护的网络提供安全互联的网关。

3.1.28

恶意代码 malicious code

存在于软件或数据文件中的外来非正常运行代码，发生作用时可能对系统造成软件或硬件的错误运行、不良影响、数据破坏、安全危害或系统损坏等。

3.1.29

审计 audit

对网络和系统中的各类活动进行跟踪、记录和分析，并在发生安全事件时提供必要的证据和线索。审计活动包括审计策略的制定、审计数据的收集、审计记录的分析和处理，以及审计结果的报告等。是网络安全借用词。

3.1.30

审计（审查）日志 audit logging

以审视、分析和监督为目的的相关信息安全事态的数据记录。

3.1.31

入侵 intrusion

对于网络或设备的非经授权的访问、篡改、破坏或获取信息资源的行为。是网络安全借用词。

3.1.32

入侵检测 intrusion detection

对网络或计算机系统中的潜在入侵行为进行检测、监控和分析的过程，通过捕获、记录并分析网络或系统中的数据流及活动模式，识别异常行为、未授权访问或潜在的非正常活动。

3.1.33

服务器 server

网络中为客户端计算机或设备提供各类应用和数据服务的设备，常用于专用软件运行、数据存储、数据管理、网络服务、资源共享等。

3.1.34

抗干扰能力分级 performance criterion

电子设备抗电磁干扰能力的程度分级：

A级：在制造厂或委托方或用户规定的技术规范限值内性能正常；

B级：功能暂时丧失或性能暂时降低，但在干扰停止后受试设备能自行恢复，无须操作者干预；

C级：功能暂时丧失或性能暂时降低，但需操作者干预才能恢复正常；

D级：因硬件或软件损坏，或数据丢失而造成不能自行恢复至正常状态的功能丧失或性能降低。

3.1.35

报警抑制 alarm suppress

当报警被激活时，防止其向操作员发出报警警示。

注：报警抑制分为手动抑制和自动抑制。

3.1.36

报警停用 alarm disable

在长期维修或不使用期间，停用报警功能，并可在需要时手动启用。在报警停用期间，报警功能不起作用。

3.1.37

白名单 white list

预先定义的可信赖的实体（如电子邮件地址、IP地址、程序等）列表，只有列表中的实体才能访问或使用系统资源。

3.1.38

黑名单 black list

预先定义的禁止、限制使用权限的实体（如电子邮件地址、IP地址、程序等）列表，系统将按照预设的安全机制自动拒绝其访问请求或执行相关操作。

3.2 缩略语

下列缩略语适用于本规范：

AI	Analog Input	模拟量输入
AO	Analog Output	模拟量输出
APC	Advanced Process Control	先进控制
CCR	Central Control Room	中心控制室
CCS	Compressor Control System	压缩机控制系统
DCS	Distributed Control System	分散控制系统
DI	Digital Input	数字量输入
DO	Digital Output	数字量输出
EMC	Electromagnetic Compatibility	电磁兼容性
EMI	Electromagnetic Interference	电磁干扰
ERP	Enterprise Resource Planning	企业资源计划系统
FAR	Field Auxiliary Room	现场机柜室
FAT	Factory Acceptance Test	工厂验收
FCR	Field Control Room	现场控制室
GDS	Gas Detection System	可燃气体和有毒气体检测系统
HART	Highway Addressable Remote Transducer	可寻址远程传感器高速通信协议
HMI	Human Machine Interface	人机接口
IDM	Intelligent Device Management	智能设备管理系统
IFAT	Integration Factory Acceptance Test	工厂集成验收
I/O	Input/output module	输入/输出模件
MES	Manufacturing Execution System	生产管理系统
MTTF	Mean Time to Failure	平均失效前时间
NAT	Network Address Translation	网络地址转换
OPC	Object Linking and Embedding (OLE)for Process Control	用于过程控制的内部数据设备连接协议
OTS	Operator Training Simulation	操作人员仿真培训系统
PI	Pulse Input	脉冲量输入
PLC	Programmable Logic Controller	可编程序控制器
RTD	Resistance Temperature Detector	热电阻
RAID	Redundant Array of Independent Disks	独立硬盘冗余阵列
SAT	Site Acceptance Test	现场验收
SIS	Safety Instrumented System	安全仪表系统
TC	Thermocouple	热电偶
UPS	Uninterruptible Power Supply	不间断电源
VLAN	Virtual Local Area Network	虚拟局域网

4 设计原则

4.1 一般规定

4.1.1 DCS 应是成熟的、经过实际应用检验的系统，应便于扩展，应能满足石油化工装置大规模生产的过程控制、检测、操作与管理的需要。

4.1.2 DCS 应能实现工艺装置、公用工程单元及储运单元等过程的连续控制、间歇控制、批量控制、逻辑控制等类型的过程控制功能。

4.1.3 DCS 应能实现工艺过程的检测、控制、显示、操作、报警、数据和事件记录、数据存储等功能。

4.1.4 DCS 作为各类控制系统显示的公共数据和信息平台，应能实现与其他控制设备或系统的数据通信、数据应用和处理、数据记录及存储等功能。

4.1.5 DCS 应能通过网络将过程控制的各类设备构成统一的整体，应能实现全系统数据和控制指令的共享、互通、处理、存储、通信等信息集成，不应有硬件、软件或功能限制。

4.2 系统性能

4.2.1 过程控制层各设备（单元）的平均失效前时间 *MTTF* 不应小于 5×10^5h，控制器的 *MTTF* 不应小于 1×10^6h，操作监控层设备的 *MTTF* 不应小于 8×10^4h。

4.2.2 控制单元、供电单元和通信单元均应采用冗余结构。

4.2.3 过程控制层的模件应采用带电插拔结构，并能在系统正常工作情况下在线更换。

4.2.4 过程控制层的单元或部件应能独立运行，在出现故障或异常情况时，不应影响对其他单元或部件的运行和功能，并应满足下列要求：

a) 模件带电插拔或更换不应影响其他部件和系统的正常运行和功能。

b) 模件本身的电源故障不应引发其他部件和系统的电源故障。

c) 过程控制网络的中断不应影响控制器的运行和功能。

4.2.5 控制器、模件、电源、网络设备等宜根据不同的工艺装置、单元或使用功能等独立设置。

4.2.6 DCS 系统的硬件和软件应满足以下兼容性要求：

a) DCS 的硬件和软件应能向低版本兼容。

b) DCS 硬件和软件的不同版本、系列之间应能做到数据交换。

c) DCS 软件版本应兼容硬件和操作系统，并且兼容时间应与硬件运行期一致。

d) DCS 硬件和软件版本维护和供应时间不应少于 15 年。

e) DCS 应能与同一品牌 20 年以内生产的产品进行网络连接及数据交换。

4.2.7 DCS 的抗干扰能力不应低于表 5.2.7 中的要求。

表 5.2.7 DCS 抗干扰能力要求

抗扰度试验项目	试验端口	抗扰度试验值	抗干扰能力分级	试验标准
静电放电	外壳	接触放电 6kV，空气放电 8kV	B 级	GB/T 17626.2-2018
射频电磁场辐射	外壳，信号端口，电源端口	10 V/m @ 80MHz 以上	A 级	GB/T 17626.3-2023
电快速瞬变脉冲群	信号端口，电源端口	电源端 2kV，信号端 1kV	B 级	GB/T 17626.4-2018
工频磁场	外壳	30 A/m	A 级	IEC 61000-4-8

4.2.8　对于需要接入 DCS 的信号，不应额外增加外接功能设备或仪表取代 DCS 本身已有的控制、显示、报警、计算和管理等功能，所有相关功能均应在 DCS 内部实现。

4.3　系统功能

4.3.1　DCS 的过程控制站应能满足石油化工装置常规过程控制的功能及速度要求，应能满足所有过程变量检测的需要。

4.3.2　DCS 应有数据存储的功能，可将各种工艺变量、系统参数、操作模式、DCS 设备运行状态、控制回路状态等数据按需要存入存储设备，并可根据需要调用。

4.3.3　DCS 应具有连续控制、间歇控制、批量控制、逻辑控制等控制功能，至少包括：

a)　常规（PID）控制、串级控制、比值控制、超驰控制、前馈控制、批量处理、顺序控制、分程控制；

b)　输入/输出线性化；

c)　运算（包括加、减、乘、除、方根、乘方、对数、指数、多项式等）；

d)　范围控制（包括高选、低选、高限、低限等）；

e)　动态控制（包括超前/滞后、死区、速度限制等）。

4.3.4　控制功能宜通过标准化功能模块组态完成，不宜采用程序语言编写方式。

4.3.5　在组态文件下装时，DCS 应能进行二次确认。

4.3.6　DCS 应具有硬件及软件的状态监测和故障诊断功能，应自动记录故障并发出报警。

4.3.7　过程控制层的状态监测和故障诊断功能至少应包括：I/O 模件，过程数据通信，控制单元，电源，网络通信。

4.3.8　DCS 系统管理应包括系统数据的管理、系统各设备的在线诊断、系统软件数据的维护、系统组态及修改、图形管理等内容。

4.3.9　DCS 宜具备在线或离线组态和调试的功能。

4.3.10　DCS 应能定期备份软、硬件组态数据、PID 控制参数和历史数据。

4.3.11　DCS 宜具备快速数据恢复功能。

4.3.12　DCS 内部应具备准确、稳定、可靠的时钟及时钟同步功能，应使系统网络中各个节点的时钟保持一致，时钟同步系统设置应遵循下列原则：

a)　DCS 的正常运行不应依赖时钟服务器或外部时钟，需要时间标记的单元应具备内部时钟，其功能不应受到外部时钟信号变化的影响。

b)　与工艺运行过程相关的第三方应用计算机或网络的同步信号应由时钟同步服务器或 DCS 系统发布。

c)　用于 DCS 系统的时钟同步服务器不应与工艺运行过程无关的第三方计算机或网络（包括工厂信息网）进行连接或共享。

d)　时钟同步服务器应内置时钟源，授时精度不应低于 10ms，守时精度不应低于 10ns/s。

e)　当时钟同步服务器需要外部时钟校正源时，宜采用北斗卫星。

f)　时钟同步服务器应专门用于为 DCS 提供辅助时钟源，并向 DCS 外部的系统分发时钟信号。为使系统安全和数据隔离，该服务器宜设置在数据服务层或数据缓冲层，并且不应直接接入过程控制数据网。

g)　时钟同步基准时间应采用北京时间，并应采用广播或点播形式向各端口发送授时数据。

h） DCS 网络宜直接与时钟同步服务器授时端口连接，时钟同步服务器各数据授时端口之间应相互隔离，各端口之间不应有数据交换；当采用路由器或交换机拓展时钟同步服务器数据端口数量时，不同的第三方应用计算机或网络之间应采用防火墙或安全网关进行隔离。

4.4 报警和事件记录

4.4.1 DCS 应具备对过程变量的报警分级、分区、分组的功能，不同的分级、分区、分组应能设置不同的报警设定、报警声音、显示颜色及标识、报警抑制、报警停用和启用、分类筛选等功能，级间、区间、组间的功能互相不应影响或关联，应能临时组成报警显示组图形用以观察。

4.4.2 DCS 宜按顺序和时间标记自动显示和记录所有的报警发生、消失、消除事件，以及报警变量的属性、位置、描述、实时数值等报警信息。

4.4.3 DCS 宜按顺序和时间标记自动记录对设定值改变、报警确认等操作事件。

4.4.4 DCS 对过程变量报警和系统故障报警宜有属性和位置的区别功能，不应单纯采用故障代码的形式。

4.4.5 DCS 应能记录和输出报警信息，报警信息应能按时间顺序显示、滚动、记录。

4.4.6 DCS 宜具有对报警和事件记录分类、过滤、筛选、检索、统计的功能，并宜能按照报警的形式、时间、分类、组别等自定义方式输出单独的数据表文件。

4.4.7 DCS 宜具备防止对报警和事件记录的删除和修改功能。

4.4.8 DCS 报警功能不应依赖于其他报警管理设备或软件。

4.4.9 报警显示和声音图像宜具有下列方式：

a） 操作画面上部报警区；
b） 过程报警一览表；
c） DCS 自诊断报警图表
d） 报警分级图表；
e） 报警分区图表；
f） 报警分组图表；
g） 报警分时段图表；
h） 报警统计表（具有索引、筛选、过滤、排序、分类、汇总、制表、输出等数据处理功能）；
i） 报警变量恢复正常记录；
j） 特定观察报警组；
k） 报警抑制图表；
l） 报警停用图表；
m） 长期报警及频繁报警专用图表；
n） 报警分级、分区、分组目录；
o） 报警启停设定表；
p） 报警声音、色彩种类设定表；
q） 报警设置变更记录；
r） 其他报警图表。

4.4.10 过程变量报警的设定应综合评估多项因素，包括工艺变量的具体条件、过程变量可能出现的变化情况、工艺设备及工艺过程本身的容忍程度、报警处理所需的时间，以及变量超限时的危险程度等，并应遵循下列原则：

a） 在设定报警时，应为每个报警变量明确其性质、位置、名称、属性、所属报警组、报警级别以及相应的提示信息，并可附加处理方案和指南，以提供操作人员在报警发生时的参考；每个过程变量应能够同时归属于不同的报警组。

b） 对于开停工期间与工艺正常运行期间过程变量的变化区间和程度不一致的情况，应将报警组分为开停工报警组和正常运行报警组；在开停工期间和正常运行期间，应分别启用和停止相应的报警组，以适应不同的工艺运行过程和条件。

c） 当存在一种以上工艺过程、逻辑提量、降负荷运行等具有不同报警要求的过程变量时，应将这些变量分为不同的报警组；在需要时，应启用或停止相应的报警组，以满足不同过程控制场景下的报警需求。

4.4.11 DCS 过程变量报警宜根据报警变量的重要程度、处理响应时间和后果严重性分为不同的优先级，同一过程变量的不同报警应能划分到不同的优先级，优先级设置宜遵循下列原则：

a） DCS 宜具备通过图例形状、颜色、数字区分不同报警优先级的功能。

b） DCS 报警管理界面宜能根据报警优先级和时间顺序进行排序。

4.4.12 DCS 过程变量报警宜能根据工艺过程及控制系统的功能、生产操作的区域划分等因素进行报警信息分区。

4.4.13 DCS 过程变量报警宜能根据开工过程、设备启停过程、工段操作过程，相关报警等划分报警分组，并宜能按照分组整体进行报警抑制和报警停用操作。

4.4.14 当同一过程变量在多个报警组中同时触发报警时，DCS 应给出提示，要求操作人员调整该变量所属的报警组，并选择唯一启用的报警。

4.4.15 DCS 宜能对过程变量报警设定值设置迟滞区，以减少检测变量在报警设定值上下频繁波动造成的重复报警。

4.4.16 DCS 宜按变量和时间顺序自动记录对设定值改变、报警确认等操作事件及操作人员信息。

4.4.17 DCS 宜能记录和输出控制回路手动、自动、串级等状态信息，应能按照时间统计各状态的占比。

5 系统结构

5.1 功能结构

5.1.1 DCS 功能结构可分为过程控制层、操作监控层、数据服务层和数据缓冲层。

5.1.2 过程控制层应完成 DCS 对过程的直接控制以及过程变量的数据采集、实时存储和传输功能。

5.1.3 DCS 的操作站和工程师站应位于操作监控层，应能对过程控制层的数据进行各种显示、报警、记录、调节、确认、存储等监控操作，实现集中操作管理的功能。

5.1.4 操作监控层设备不应直接带有过程接口单元。

5.1.5 过程变量应接入到 I/O 模件或通信模件。

5.1.6 与生产操作或系统管理直接相关的数据服务（如：报警、历史记录、诊断等）应在过程控制层或操作监控层实现。

5.1.7 数据服务层可用于各操作分区设备的全局数据服务（如数据备份恢复、网络管理、用户权限管理和访问控制、时钟同步等）。

5.1.8 数据服务层应通过操作监控层的服务器、工程师站等设备与过程控制层进行数据交换，不应直接建立数据通信。

5.1.9　数据缓冲层应为 DCS 内部网络与外部网络数据交换的中间层，可向间接参与生产过程的用户提供数据服务和应用服务。

5.1.10　数据缓冲层设备可根据需要在管理员授权后安装与 DCS 功能无关的第三方应用软件或模块，但安装前应对安装软件或模块进行安全检验。

5.1.11　与 DCS 功能相关的第三方应用计算机应设置在数据缓冲层，设备和数据的安全应在 DCS 系统安全保护范围内，并满足第 7 章中的安全要求。

5.2　网络结构

5.2.1　DCS 网络可由过程控制网、系统数据网和服务数据网等组成，DCS 网络结构示意图可参见附录 A。

5.2.2　过程控制网可用于过程控制层与操作监控层之间工艺过程检测控制数据、DCS 系统组态数据、仪控设备状态数据的传输，过程控制网设置应遵循下列原则：

a）过程控制网宜独立设置，并且宜与其他 DCS 网络相互隔离，不宜与其他 DCS 网络共用交换机、网卡等网络设备，不应与其他非 DCS 系统共用交换机、网卡等网络设备。

b）不同操作分区的过程控制网络应相互隔离，与 DCS 功能无关的第三方设备或网络不应接入过程控制网络。

c）过程控制网应采用冗余配置，冗余网络不应共用交换机、网卡等网络设备。

d）与 DCS 功能相关的第三方的设备应通过过程数据服务器与过程控制网络交换数据。过程数据服务器的设置应符合 11.3 条要求。过程数据服务器与第三方的应用计算机或网络之间应设置防火墙，对网络通信协议、流量和端口地址进行限制。

5.2.3　系统数据网可用于操作监控层和数据服务层设备之间工艺过程检测控制数据、仪控设备状态数据、备份恢复数据、设备和用户配置数据、时钟数据以及间接参与生产操作的高级应用数据的传输，不宜用于生产操作控制直接相关的数据传输。

5.2.4　系统数据网应通过防火墙与服务数据网连接，并应限制允许访问的通信协议和设备端口地址。

5.2.5　服务数据网应用于 DCS 内部网络与外部网络进行数据交换的 DCS 的数据缓冲层，服务数据网设置应遵循下列原则：

a）服务数据网不应与过程控制网络进行直接连接。

b）工厂信息网以及其他与 DCS 功能无关的外部网络不应直接与服务数据网络连接（即使采用安全网关或防火墙等设施），应通过隔离网闸与 DCS 数据缓冲层的数据服务器采用数据同步的方式进行数据交换。

c）非授权访问、入侵行为、异常流量等异常信息可送至安全管理系统进行集中管理和监控。

5.2.6　过程控制层和操作监控层宜按照操作或管理进行网络分区，划分为不同的子网，DCS 网络划分示意图可参见附录 B。

5.2.7　网络分区应能独立构成系统。

6　系统安全

6.1　信息安全

6.1.1　DCS 应有身份验证和访问控制功能，应能根据用户或设备的不同身份赋予不同的权限，防止

非授权使用网络信息资源，并应根据访问权限，限制用户或设备对系统的访问。

6.1.2 DCS 应有启用/关闭登录窗口、限制登录密码输入错误次数、登录超时自动退出、修改登录密码等功能。

6.1.3 DCS 系统与其他控制系统之间采用基于 TCP/IP 协议的通信时（如 OPC，Modbus TCP 等），应设置网闸、安全网关或防火墙等访问控制设备，配置访问控制策略，不应采用穿越区域边界的 HTTP、Telnet、Rlogin、FTP 等通用网络服务。

6.1.4 DCS 宜具备系统组态数据（如配置、控制方案、PID 参数等）和历史数据的手动和自动备份功能。

6.1.5 操作监控层和数据服务层设备应遵循最小安装原则，仅安装完成 DCS 功能所需的组件和应用程序，不应安装与 DCS 功能和安全防护功能无关的第三方软件。

6.1.6 DCS 设备应关闭与 DCS 功能无关的系统服务、默认共享和高危端口。

6.1.7 DCS 网络中宜设置恶意代码防护服务器。

6.1.8 恶意代码防护宜采用白名单技术。

6.1.9 安装在 DCS 设备中的所有软件应为合法授权的正式版本，安装前均应经过安全性检测。

6.1.10 恶意代码库和补丁文件在升级和更新前应首先进行数据校验，并进行与 DCS 系统兼容测试，确定无害、无妨后方可安装。

6.1.11 DCS 设备在上线使用前应经过安全性检测，避免设备固件和软件中存在恶意代码。

6.1.12 列入国家互联网信息办公室等部门联合发布的《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应由具备资格的机构按照 GB 42250 等相关国家标准的强制性要求进行安全认证或者安全检测，证实其符合相关要求。

6.2 网络安全

6.2.1 DCS 网络设置应遵循下列原则：

a） DCS 网络宜采用横向分区、纵向分层（纵深防御）、区间隔离、层间防御、网络专用的基本防护策略，网络结构示意图参见附录 C。

b） 过程控制网和系统数据网是实现 DCS 必要功能的内部网络，应能在与服务数据网等其他网络切断后保证 DCS 功能的完整性、可靠性和可用性。

c） 不同建筑物之间的 DCS 网络宜采用光缆连接。

d） 包括工厂信息网在内，与 DCS 功能无关的外部网络不应直接接入 DCS 网络。

e） 不应以任何形式将 DCS 网络接入到系统外网络或公共互联网。

f） 当需要 DCS 系统进行网络安全测试或认证时，应由国家授权的机构进行，测试报告应保密。

6.2.2 DCS 各级网络不应采用无线通信方式，当 DCS 需要与无线仪表或其他采用无线通信的控制系统进行通信时，应遵循下列原则：

a） 采用无线网络的控制系统及仪表设备不应直接接入 DCS 各级网络。

b） 采用无线网络的控制系统应通过通信模件与 DCS 交换过程数据，采用基于 TCP/IP 协议的通信时（如 Modbus TCP），还宜设置防火墙或隔离网闸进行隔离，限制网络通信协议、流量和端口地址。

c） 采用无线网络的控制系统及仪表设备与 DCS 的数据通信可参见图 7.2.2。

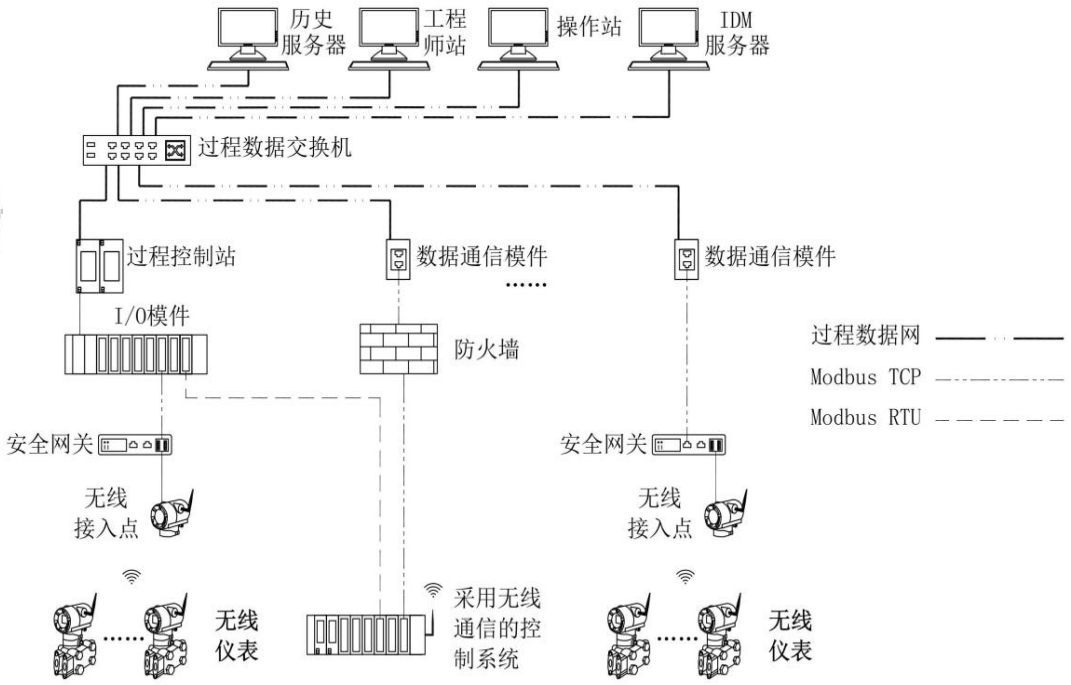

图 7.2.2　无线网络通信示意

d） 无线仪表设备的数据应首先接入安全网关，通过 DCS 的 I/O 通信模件或数据通信模块与 DCS 进行数据传输。

e） 安全网关应内置防火墙功能，对数据类型、通信协议和流量进行监测和限制。

f） 安全网关应具备接入认证功能，应能禁止未认证的无线设备进行数据传输。

g） 安全网关及相关的 DCS 通信模件宜采用热备或同步冗余。

6.3　安全管理措施

6.3.1　不应采用包括互联网在内的外部网络对 DCS 设备进行远程操作、管理。

6.3.2　不应采用包括互联网在内的外部网络对过程控制层和操作监控层设备进行软件升级和恶意代码库更新。

6.3.3　所有人机界面的外部数据接口均应设置操作访问权限措施，未经授权的用户不应使用移动存储设备。

6.3.4　操作监控层和数据服务层所有人机界面的外部数据接口应处于禁止使用状态，只有在设备需要安装和维护时方可由授权用户解除禁用状态，并应在安装和维护后恢复禁止使用状态。

6.4　安全管理系统

6.4.1　安全管理系统可用于对 DCS 各设备的网络安全监控、报警，审计日志的集中管理以及用户和软件的获准管理，安全管理系统各设备功能见附录 C。

6.4.2　安全管理系统应能对 DCS 系统中异常访问、异常操作、网络和设备流量、网络冗余机制等状态进行监控、报警、记录和存储。

6.4.3　除安全管理客户端外，安全管理系统设备宜设置独立机柜进行管理和维护。

6.4.4　安全管理系统不宜用于对过程控制层设备和过程控制网的监控、安全管理以及网络设备配置。

6.4.5　安全管理系统设备的外部数据接口应处于禁止使用状态，只有在设备需要安装和维护时方可由授权用户解除禁用状态。

6.4.6　安全管理系统设备不应与包括互联网在内的 DCS 外部网络连接，并宜设置专人进行管理和维护。

6.4.7　安全管理客户端应为 DCS 安全管理岗位专用人机接口，不应安装与安全管理功能无关的其他应用。

6.4.8　安全管理网可用于网络安全设备（如防火墙、网闸）的状态信息、设备配置等安全管理数据与安全管理系统之间的数据传输，以及安全管理系统内部设备之间的数据传输。

6.4.9　安全管理网应独立设置，不应与包括 DCS 网络在内的其他网络连接。网络连接方式见附录 C。

6.4.10　安全数据网可用于 DCS 设备的安全策略、恶意代码特征文件、审计日志、用户权限等安全数据以及网络设备（如交换机、路由器等）的状态信息、流量监控数据与安全管理系统之间的传输。

6.4.11　安全数据网应通过防火墙与系统数据网连接。

7　系统技术要求

7.1　过程控制站

7.1.1　除了常规 PID 控制外，控制器还应具备串级控制、比值控制、超驰控制、前馈控制、批量处理、顺序控制、分程控制、逻辑运算、数值计算等控制功能和计算功能。

7.1.2　控制器应具备控制周期为 0.1s 的快速回路控制的能力。

7.1.3　控制器宜具备 PID 参数自整定功能。

7.1.4　控制器应采用同步冗余配置。

7.1.5　相互冗余的控制器均应处理输入数据，同时执行控制运算，由工作控制器控制最终执行单元。

7.1.6　当工作控制器和冗余控制器的运算结果不一致时，各控制器的自诊断功能及切换控制模块应具备判断错误位置和选择控制器的功能。

7.1.7　控制器的实际运行最大负荷不应超过额定负荷的 60% 。

7.1.8　过程控制站宜按工艺装置、工艺单元或控制区域分别配置。

7.1.9　各过程控制站 I/O 模件插槽应预留不小于 20%的余量。

7.1.10　不宜单独设置备用控制器。

7.2　过程接口单元

7.2.1　I/O 模件应具备输入信号滤波功能，应进行 250V 共模干扰、50Hz 工频、≥10MHz 高频噪声的抗干扰功能试验，并且信号变化应在精度范围内。

7.2.2　根据不同的 I/O 模件类型，所有输入、输出端都应带有信号过载保护功能。

7.2.3　模拟量 I/O 模件及数字量 I/O 模件宜具有通道间隔离方式或组隔离方式。

7.2.4　模拟量输入模件应满足下列要求：

a）模拟量输入模件（AI 卡）应能接收 4mA～20mA DC 等标准信号，并应能用于二线制、三线制和四线制的信号制式。

b）AI 卡的接线端子宜采用三端子式。

c）AI 卡应包括 4mA～20mA DC 叠加 HART 通信信号的标准类型。

7.2.5　模拟量输出模件应满足下列要求：

a）模拟量输出模件（AO 卡）应能输出 4mA～20mA DC 等标准信号。

b）AO 卡输出电流信号时，负载阻抗不应小于 700Ω，并应具有正向和反向输出功能。

c） AO 卡应包括 4mA～20mA DC 叠加 HART 通信信号的标准类型。

7.2.6 热电偶输入模件（TC 卡）应能接收采用 GB/T 16839.1 标准分度号的各种热电偶信号，应具备线性化和冷端补偿功能，可设置断线上下限报警。

7.2.7 热电阻输入模件（RTD 卡）应能接收包括 GB/T 30121 标准铂电阻和 JB/T 8623 标准铜电阻在内的二线制、三线制或四线制热电阻信号，可设置断线上下限报警；Pt100 铂热电阻的测量电流不宜大于 1mA，其余热电阻的测量电流不宜大于 5mA。

7.2.8 数字量输入模件（DI 卡）应能接收开关信号，输入信号电压应包括 24V DC 和 220V AC，并应有“有源”和“无源”两种规格。DI 卡宜具有抗 250V 共模电压和抗静电干扰的品种，应能直接接收非隔离的外部开关电压信号。

7.2.9 数字量输出模件（DO 卡）应输出开关信号，DO 卡接点电压应包括 24V DC 和 220V AC，并应有供电与非供电两种规格。DO 卡宜具有数字开关（晶体管开关）品种，应具有代替继电器接点直接驱动外部开关设备的品种。

7.2.10 脉冲量输入模件应满足下列要求：

a） 脉冲量输入模件（PI 卡）应能接收脉冲信号，脉冲信号的可用频率下限不应大于 10Hz；上限不应小于 10 kHz。

b） 脉冲信号的高触发、低触发电压应可组态设定，高电压信号的下限不宜小于 4V DC；低电压信号的上限不宜大于 3V DC。

7.2.11 通信模件（COM 卡）应满足下列要求：

a） 通信模件应能接收和输出与其他设备兼容的通信信号。

b） 通信模件的通信协议至少应包括 MODBUS RTU，通信接口至少应包括 RS485。

c） 通信模件宜具备热备冗余配置功能。

d） 通信模件通信协议采用 MODBUS RTU 时，接口宜采用端子型接线。

7.2.12 通用 I/O 模件功能应符合本规范 8.2.1~8.2.10 的要求。

7.2.13 I/O 模件配置原则应满足下列要求：

a） 不同应用类型（本安与非本安、模件供电和外供电、不同电压等级等）的 I/O 模件不应混用。

b） 各种 I/O 模件的最大通道数量应满足表 8.2.13 中要求：

表 8.2.13 I/O 模件最大通道数量

I/O 模件类型	AI	AO	TC	RTD	DI	DO	PI	通用 I/O	COM	其他
最大通道数量+	16	16	32	32	32	32	16	32	4	32

7.2.14 I/O 模件接口的标称交流电压等级不应超过 220V AC，标称直流电压等级不应超过 24V DC，I/O 模件的开路电压不应超过 30V DC。

7.2.15 I/O 模件可根据外部信号的具体情况、模件的耐电压特性以及信号类型采用继电器或隔离器进行隔离。

7.2.16 I/O 模件的配置应遵循下列冗余原则：

a） 用于控制功能的多通道 AO 卡应采用同步冗余，其余用于控制和工艺联锁功能的多通道 I/O 模件应采用热备或同步冗余。

b） I/O 模件不宜采用串联接入额外的信号转换模件的方式来实现冗余配置。

c） 冗余的 I/O 模件应为相互独立的模件。

d） 同一控制回路的输入输出 I/O 模件宜分配在同一个过程控制站中。

7.2.17 I/O 模件的备用应遵循下列原则：

a） I/O 模件的备用宜采用模件备用的方式，不宜采用通道备用的方式。

b） 每种备用 I/O 模件应根据实际需要和可预期的补充留有适当的备用数量。

c） 备用 I/O 模件应根据工艺装置、公用工程单元、储运单元或控制区域，按照模块类型分别配置。

d） 每种备用 I/O 模件的数量不应少于 1 块。

7.2.18 远程 I/O 设备应是 DCS 控制器的远距离安装的 I/O 系统，应适用于室内或室外特定的应用场景及环境条件，并应满足下列要求：

a） 远程 I/O 设备与 DCS 控制器的通信宜采用控制器的 I/O 总线，不宜采用通信模块经由过程控制网络进行通信的方式。

b） 用于室外安装的远程 I/O 设备应配备适应环境的防护箱，应具备适应当地极端环境条件的性能，并应适应安装区域工业环境及腐蚀环境条件。

c） 安装在室外的远程 I/O 设备宜装在单独的机箱，不宜采用机柜，不应与非仪表设备混装。

d） 用于室外的远程 I/O 设备不应安装在爆炸危险环境 0 区或 1 区；安装在爆炸危险环境 2 区的远程 I/O 设备与机箱应取得整体防爆认证。

e） 远程 I/O 设备宜采用冗余通信方式，可采用电通信或光通信的方式，安装在室外或通信路径复杂电磁场环境宜采用光通信方式。室外安装的远程 I/O 设备机箱不应采用串联通信方式与控制器进行连接。

f） 远程 I/O 模件的冗余配置应根据检测及控制变量的重要程度进行设计。

g） 室外安装的远程 I/O 设备机箱内宜配备箱内温度、湿度检测元件，并宜将信号送到控制器。

h） 远程 I/O 设备的交流供电模件宜采用符合 GB/T 16895.21-2020 规定的双重绝缘或加强绝缘结构，距离控制室大于 300 米时宜采用就地供电的方式。

i） 安装在室外的远程 I/O 设备机箱应使机箱内温湿度变化维持在设备正常运行的允许范围之内，远程 I/O 设备机箱宜采用非机械式的温湿度调节方式。

j） 实施防雷工程的远程 I/O 设备应根据 SH/T 3164-2021 第 7 章、第 8 章的规定，按照控制室仪表防雷模式装备电涌防护器。

7.3 操作站

7.3.1 作为 DCS 系统的人机交互界面，操作站应具备全面、准确地显示工艺过程、过程变量、控制流程及设定参数等数据的功能，并且具备图形显示、报警、记录、调节、处理以及存储等功能。

7.3.2 操作站可用作专用报警功能操作站。

7.3.3 操作站不应用于软件开发、数据管理以及文档处理等其他用途。

7.3.4 操作站应具备操作控制、画面浏览、图形显示、报警、数据处理、数据存储、信息调用、报表调用等功能。

7.3.5 操作站应能安装并运行工程师站软件，并可通过修改用户权限的方式兼做工程师站。

7.3.6 操作站的配置应满足下列要求：

a） 操作站宜采用通用的、兼容的、非专用机型，其硬件配置应能充分满足操作站的功能要求并留有余地。

b） 中心控制室或现场控制室内宜按工艺装置、公用工程单元、储运单元或操作分区配置操作站，每个独立操作的工艺装置、单元或操作分区宜至少配置 2 台操作站。

c） 同一工艺装置、公用工程单元、储运单元或操作分区的操作站软硬件配置宜相同，并互为备用。

d） 每台操作站应带主机。

7.3.7 操作站应能显示下列标准画面：

a） 总貌及链接目录；

b） 图面及图示分组；

c） 操作回路；

d） 报警列表图、分级、分区、分组图及报警统计与检索图；

e） 实时和历史趋势；

f） 事件记录；

g） 系统状态和概貌；

h） 诊断信息；

i） 控制点或检测点细节；

j） 操作流程图。

7.4 工程师站

7.4.1 工程师站作为用于系统管理和组态维护及修改的人机接口，应具有以下功能：

a） 系统测试与诊断；

b） 硬件的组态和功能定义；

c） 控制软件的组态与下装；

d） 工程师站不应用于软件开发、数据管理以及文档处理等其他用途。

7.4.2 工程师站的机型、硬件配置和性能宜与操作站的配置相同。

7.4.3 当采用分散布置方式时，现场机柜室应按操作分区配备现场工程师站，并应至少配备一台现场工程师站；中心控制室中每个操作分区宜至少设置 1 台工程师站，不同操作分区的工程师站不宜共用。

7.4.4 工程师站可运行操作站软件，但不宜兼做操作站；操作站也不宜兼做工程师站。

7.4.5 组态应用程序应具备以下功能：

a） 系统结构定义组态；

b） 数据库组态；

c） 控制回路组态；

d） 编制程序；

e） 画面绘制；

f） 过程变量的参数（包括：零点、量程及报警限值等）设定；

g） 实时和历史数据库组态；

h） 报表组态；

i） 组态下装；

j） 组态在线修改。

7.5 历史服务器

7.5.1 历史服务器应能存储与管理过程数据、报警记录和事件记录，并可为其他应用提供存储的数据。

7.5.2 历史服务器宜采用服务器机型；硬盘应采用 RAID 1 或 RAID5 冗余配置，应能热插拔更换，MTTF 不应小于 2×10^6h。

7.5.3 历史服务器数据存储单元的存储能力应为：

a) 存储变量的数量不少于所有 I/O 点数的 4 倍；

b) 模拟量类型数据存储的最小间隔周期不大于 1s；

c) 每一变量存储的数量不少于 2×10^5 条；

d) 存储时间不少于 180 天。

7.5.4 历史服务器的硬盘存储能力应根据所保存的图形数据、历史趋势数据以及其他相关数据的格式要求及系统自身占用情况进行综合估算，并确保其空闲存储空间不得少于总存储容量的 40%。

7.5.5 历史服务器应按工艺装置、公用工程单元、储运单元或操作分区分别设置，不同操作分区的历史服务器不宜共用。

7.5.6 采用分散布置方式时，中心控制室或现场控制室应设置历史服务器，现场机柜室可根据需要设置备用历史服务器。

7.5.7 历史服务器应独立设置，工程师站、操作站等其他功能的工作站不应同时兼做历史服务器。

7.5.8 历史服务器作为过程数据交换的核心设备，应用于过程数据、历史数据、报警和事件信息的存储和检索，不应兼用于高级应用或其他用途。

7.5.9 历史服务器的软件应为通用数据库型，应具备数据库管理和操作的功能。

7.5.10 历史服务器软件应能记录存储过程变量、报警记录和事件记录。

7.5.11 历史服务器软件应具有数据处理和统计运算的功能，应能按需要调用数据、显示曲线、显示统计、制图及制表等。

7.6 网络管理服务器

7.6.1 网络管理服务器宜根据 DCS 的网络类型和运行需要配备，用于 DCS 网络中设备和用户的管理，应具备以下功能：

a) 设置和配置网络参数及网络节点，全面执行网络管理的各项任务；

b) 定义和分配用户访问权限，并执行用户身份认证，确保网络安全；

c) 管理网络资源服务，优化网络性能；

d) 对操作系统的域设置、用户账户管理以及服务策略实施等进行统一的集中管理。

7.6.2 网络管理服务器应独立设置，不应兼做高级应用或其他用途。

7.7 安装条件

7.7.1 安装在可能有腐蚀性气体场合的 DCS 模件，应能在符合 ISA 71.04 标准 G3 等级的环境中正常工作至少 5 年。

7.7.2 室内安装的 DCS 模件应能在环境温度 0℃～50℃和相对湿度 10%～90%（无结露）的条件下正常工作。

7.7.3 DCS 的室内安装条件应满足 SH/T 3006 的规定。

7.8 供电及接地要求

7.8.1 直流电源装置应带有故障报警功能，并应将报警信号接入到 DCS 模件中。

7.8.2 直流电源装置应按 1：1 冗余配置，任一单个直流电源装置应能独立满足全部负荷需求，且在

该状态下运行的负荷不应超过 50%。

7.8.3 直流电源装置电源输出宜能直接并联，不宜设置额外的并联设备。

7.8.4 供电开关、端子等宜预留不少于 20%的余量。

7.8.5 用于给控制器、I/O 模件供电的系统直流电源装置应与用于外部设备供电的直流电源装置分开设置。

7.8.6 DCS 的供电设计应符合 SH/T 3082 的规定。

7.8.7 DCS 的接地设计应符合 SH/T 3081 的规定。

7.9 备品备件

7.9.1 开车备件的种类和数量宜由供货商推荐并提供。

7.9.2 DCS 供货商应保证系统所需的备品备件 15 年的供应期。

8 网络系统

8.1 网络特性

8.1.1 操作监控层和数据服务层的通信网络应符合 ISO/IEEE 802.x 的通信标准。

8.1.2 过程控制网带宽不应小于 100Mbps。

8.1.3 系统数据网和服务数据网带宽不宜小于 1Gbps。

8.1.4 应能在线接入或摘除网络设备而不影响网络中其他设备的运行。

8.2 网络设备

8.2.1 用于 DCS 系统的数据服务器应满足下列要求：

a) 服务器的硬件配置应能充分满足数据存储和访问的要求。

b) 操作监控层的数据服务器宜按操作分区配备。

c) 发生故障后会引起过程控制层或操作监控层其他设备功能失效的网络数据服务器应采用冗余配置。

d) 网络数据服务器宜采取冗余供电方式。

8.2.2 用于 DCS 系统的交换机应具备以下功能：

a) 用于过程控制层、操作监控层和数据服务层的交换机应具备网络互联、错误校验以及流量控制的功能，应采用符合 GB/T 30094 标准的工业以太网交换机；

b) 当需要在控制网络中设置子网或虚拟局域网时，相应的交换机还应具备路由或 VLAN 功能；

c) 对于网络节点数量大于 50 的 DCS 网络，系统应能对交换机的工作状态、运行负荷等进行监测，并应设置具有网管功能的网络管理服务器；

d) 系统数据交换机和数据服务交换机宜具备路由和管理功能。

8.2.3 用于 DCS 系统的交换机配置应遵循下列原则：

a) 除级联端口和管理端口外，单台交换机端口数量不宜大于 24 个；

b) 交换机的背板带宽不应低于包括可扩展端口在内的所有端口最大通信速率总和的 2 倍；

c) 交换机需要扩展端口数量时，应利用背板进行扩展（如采用级联口或堆叠）；

d) 当级联或堆叠的交换机总数超过 6 台时，宜采用集群技术进行管理。

e) 用于不同操作分区的交换机不宜共用；

f) 非冗余配置的交换机宜采取冗余供电方式，冗余配置的交换机可采用非冗余供电方式；

g） 过程控制网交换机应按 1:1 冗余配置，应采用无风扇散热结构。

8.2.4 用于 DCS 系统的防火墙应采用工业控制系统专用防火墙，应至少满足 GB/T 37933 中基本级的安全技术要求。

8.2.5 用于过程控制网的防火墙应采用无风扇自然散热设计，并应采取冗余供电方式。

8.2.6 用于 DCS 系统的隔离网闸应采用内、外网处理系统加隔离硬件的结构，实现可信任网络和不可信任网络之间的完全隔离，并应具备以下功能：

a） 隔离网闸应满足 GB/T 37934 中增强级的安全技术要求。

b） 隔离网闸应能够阻断 TCP/IP 及其他网络协议。

c） 隔离网闸应具备应用协议控制、数据包过滤、访问控制、入侵检测和流量控制等功能。

d） 隔离网闸安全策略应包含基于 MAC 地址、IP 地址、端口、协议类型的访问控制。

e） 隔离网闸应支持对数据库的安全访问和同步，并应支持单向和双向同步模式。

f） 隔离网闸应能对通信协议进行深度内容检测，禁止不符合协议规约的通信。

g） 隔离网闸应具备安全管理功能，包括日志记录、安全审计、异常情况的分析和处理等。

8.2.7 在 DCS 系统的光通信设计及光缆配置中，应遵循以下原则：

a） 光通信宜采用交换机的光端口接口，不宜采用 RJ45 端口加光电转换器。

b） 光电转换器应支持 DCS 的网络协议。

c） 室外敷设的光缆宜采用符合 GB/T 9771.1 标准的 B1.1 类单模光纤。

d） 用于室内敷设的光缆宜采用符合 GB/T 9771.7 标准的 B6 类单模光纤。

8.2.8 用于 DCS 系统的网络连接电缆配置应遵循下列原则：

a） 采用 IEEE802.3 系列协议的网络连接电缆应满足网络传输速率要求，传输速率超过 10Mbps 时不应采用同轴电缆。

b） 网络连接电缆宜采用 4 对屏蔽双绞线，机械和电气特性应不低于 IEC 61156-5 标准中关于 6_A 类屏蔽线的规定，冗余的网络宜采用不同颜色的网络连接电缆。

c） 网络传输距离超过 90 米时，应采用光缆连接以确保信号的稳定传输并降低信号衰减的影响。

8.2.9 用于过程控制网的网络通信设备应采取同步冗余或热备冗余配置。

8.2.10 各级网络通信设备和部件应预留至少 20%的端口。

8.3 网络负荷

8.3.1 采用 IEEE802.3 系列协议的网络，最大负荷不应超过网络标称负荷能力的 30%。

8.3.2 采用其他协议的网络，最大负荷不应超过网络标称负荷能力的 50%。

8.3.3 在正常操作状态下，过程控制网的网络负荷宜小于其网络标称负荷能力的 50%。

8.4 与第三方设备通信

8.4.1 过程控制层和操作监控层设备不宜采用标准以太网协议直接与 SIS、CCS 及其他 PLC 设备进行数据通信，宜通过通信模件将外部通信协议转换为 DCS 内部通信协议。

8.4.2 当 DCS 采用 MODBUS 协议与第三方设备通信时，除 MODBUS TCP 协议外，对于其他类型的 MODBUS 协议，每个通信接口的通信报文不宜超过 100 条。

8.4.3 DCS 在与第三方设备通信时，若使用 OPC、MODBUS TCP 或其他基于 TCP/IP 的协议，应采用防火墙或隔离网闸等网络隔离措施，限制网络通信协议和流量，控制端口地址。

8.4.4　与 DCS 控制和保护功能无关的数据宜通过通信模块与操作监控层设备进行通信，不宜通过过程控制站。

9　辅助设备

9.1　辅助操作台

9.1.1　应采用 DCS 的辅助操作台来安装 DCS 的辅助开关、按钮、报警显示等辅助操作设备。

9.1.2　辅助操作台的外形、尺寸及颜色宜与 DCS 操作台相同。

9.1.3　辅助操作台宜按工艺装置、公用工程单元及储运单元的需要分别配备。

9.2　机柜

9.2.1　宜根据各工艺装置、公用工程单元及储运单元的控制范围，按 I/O 点总数配置相应的控制单元及机柜。

9.2.2　不同工艺装置、公用工程单元及储运单元的 I/O 模件、控制器等不宜装于同一机柜内。

9.2.3　DCS 的系统机柜不应与其他控制系统的机柜混用。

9.2.4　DCS 机柜宜采用钢铁材料。

9.2.5　各类机柜宜留有 20%的备用安装空间。

9.2.6　室内安装机柜的防护等级不应低于 GB/T 4208 规定的 IP30。

9.2.7　半敞开厂房内安装的机柜防护等级不应低于 GB/T 4208 规定的 IP54。

9.2.8　室外安装机柜、机箱的防护等级不应低于 GB/T 4208 规定的 IP66，并应能具备适应当地极端气象及局部环境条件的能力，否则应采用适当的补充防护措施。

9.2.9　机柜内辅助照明设施不应与控制系统共用 UPS 供电，应设置单独的安全用电及短路保护器。

9.2.10　机柜内不应设置非用于 DCS 设备的电源插座。

9.2.11　机柜风扇宜通过柜内温度控制启停。

9.3　打印机

9.3.1　打印机宜能实现操作站、工程师站等人机接口进行屏幕打印、图形打印、报表打印和报警打印的要求。

9.3.2　打印机宜采用网络打印机形式。

9.4　其他辅助设备

9.4.1　安全栅所在机柜一侧除接线端子和 I/O 接口模块外，不宜安装隔离器、继电器等非本安信号接口设备。

9.4.2　电涌防护器应采用金属导轨安装型，并应以此导轨作为接地汇流条。

9.4.3　电涌防护器应做为室外电缆接入系统的第一道连接端口（接线端子除外），宜与后续连接的仪表设备安装在同一机柜内。

9.4.4　通过继电器向外供电的电源不应使用 DCS 的系统电源。

9.4.5　继电器的线圈侧或触点侧采用非安全电压时，继电器应独立安装，不应与安全电压用电设备安装在机柜的同一侧，并应在机柜外设置明显的标识。

10 高级应用

10.1 智能设备管理系统

10.1.1 智能设备管理系统的功能应至少包括智能仪表设备组态、状态监测及诊断、校验管理和自动文档记录管理等功能。

10.1.2 智能设备管理系统应能自动读取系统连接的智能设备数据，应能自动完成系统的数据存储和管理，应能自动显示系统及设备的连接状态和诊断信息。

10.1.3 智能设备的状态信号和规格数据不应用于过程控制和检测。

10.1.4 智能设备管理系统应兼容标准智能设备的通信和数据交换，支持 EDDL 或 FDT/DTM 协议。

10.1.5 智能设备管理系统应使用标准化的数据库和文件，并宜采用标准化的设备描述文件。

10.1.6 智能设备管理系统应具备对其连接的智能设备进行诊断的功能，应具有异常状态报警功能。

10.1.7 智能设备管理系统应能识别信号线路的短路和断路，并发出报警。

10.1.8 智能设备管理系统维护操作站宜根据智能设备数量配置，每台维护操作站管理的最大设备数量不宜超过 2000 台。

10.1.9 智能设备管理系统宜提供开放的数据接口，以支持第三方系统或软件的接入和数据获取，并应至少支持以下标准接口协议：OPC DA、OPC AE）、以及 OPC UA。

10.2 实时数据服务

10.2.1 实时数据服务器作为高级应用的数据接口，应能获取过程控制层及操作监控层的实时数据或中间数据，并应能将数据传输至数据缓冲层设备。

10.2.2 实时数据服务器应设置在操作监控层。

10.2.3 实时数据服务器应通过防火墙或网闸与系统外服务器进行数据交换，并应通过访问控制机制控制两网之间的数据交换行为，仅允许交换符合安全策略的指定格式的数据，网络连接方式参见附录 A。

10.3 过程数据服务

10.3.1 过程数据服务器作为高级应用或管理的数据接口，应能获取来自操作监控层的过程数据（包括实时数据和历史数据），并应能将数据传输至高级应用及生产管理层设备。

10.3.2 过程数据服务器的网络接口带宽不宜小于 1Gbps，宜根据存储的数据量配置硬件，满足过程数据交换的需要。

10.3.3 过程数据服务器应设置在数据缓冲层，应通过防火墙或网闸单向获取操作监控层设备的数据。

10.4 先进控制

10.4.1 先进控制服务器作为专用控制软件的运行或数据交换平台，应通过实时数据服务器读写 DCS 网络中的过程变量，并应符合 11.2.3 条的规定。

10.4.2 先进控制工作站作为软件的运行及人机接口，应通过先进控制服务器和实时数据服务器与 DCS 进行数据交换；先进控制服务器可兼做先进控制工作站。

10.4.3 先进控制服务器及工作站不应直接与过程控制层设备进行数据交换。

10.4.4 先进控制服务器及工作站的机型和硬件配置宜与操作站相同，应能满足先进控制软件运行、计算和数据存储的需要。

10.5 储运管理

10.5.1 储运管理软件宜在 DCS 上运行，实现储运自动化管理。

10.5.2 运行储运管理软件的非 DCS 设备不应直接接入 DCS 的过程控制层或操作监控层的网络，应通过实时数据服务器交换数据，并应符合 11.2.3 条的规定。

10.5.3 储运管理服务器及工作站的机型及硬件配置宜与操作站相同。

10.6 网页浏览服务

10.6.1 网页浏览服务器（Web 服务器）和客户端应设置在数据缓冲层，并通过过程数据服务器读取 DCS 中的过程数据。

10.6.2 网页浏览服务器的硬件配置应满足过程数据和画面的存储容量要求，并宜根据访问用户的数量配置足够的内存容量。

10.6.3 用于外部网络（如工厂信息网）应用的网页浏览服务器和客户端不应设置在 DCS 网络内。

10.7 报警管理系统

10.7.1 报警管理服务器应通过防火墙或网闸单向获取操作监控层设备的报警数据。

10.7.2 报警管理客户端可与数据缓冲层中的其他高级应用客户端共用设备。

10.8 其他高级应用

10.8.1 其他直接参与生产过程的高级应用服务（如油品调和、物料平衡计算等），软硬件配置、网络连接和数据交换要求应同第 11.5 条。

10.8.2 其他间接参与生产过程的高级应用服务，软硬件配置、网络连接和数据交换要求应同第 11.6 条。

10.8.3 视频传输信号应采用独立的信号途径或网络，视频应用系统的控制网络应独立设置，不应利用 DCS 的网络资源，以防止对 DCS 正常数据信号传输造成干扰。

10.8.4 DCS 系统应能采集和存储控制系统状态监测及诊断、控制回路自动化投用率等信息。

11 软件配置

11.1 控制和操作软件

11.1.1 DCS 应配备全套的过程控制软件、过程检测软件和操作软件，软件的容量应按设备的最大配置配备。

11.1.2 在系统运行过程中对软件进行在线修改或下载时，不应对原有软件的正常运行产生扰动，也不应引发软、硬件故障等问题（不包括因修改、下载控制方案对系统的正常扰动）。

11.1.3 DCS 应配备全套的操作系统软件及必要的工具软件。

11.2 工程组态软件

11.2.1 组态软件宜具备在线修改和下装组态数据的功能。

11.2.2 组态软件宜支持离线组态和调试。

11.3 软件版本

11.3.1 DCS 软件应为经过测试并正式发布的版本，不应使用未正式发布的测试版软件。

11.3.2 DCS 软件配置应符合第 5.2.6 条的规定。

11.4 软件授权

11.4.1 DCS 所有相关软件都应为经过授权的正式版本。

11.4.2 DCS 软件配置应满足包括备用模件在内的所有 I/O 模件的全部通道的使用，同时不应受到软件授权点数的限制，并应留有至少 20%的余量。

12 工程实施

12.1 系统开工会

12.1.1 DCS 系统开工会宜包括以下几部分内容：

a) 确定 DCS 软硬件以及备品备件的最终配置、规格和数量；
b) 确定项目中最终用户、设计单位、供货商以及相关的第三方设备供应商各自的工作范围和责任；
c) 确定项目执行过程中各方主要负责人的人员和职责；
d) 明确工程项目需要的所有文件的内容、格式、数量及交付方式，指定文档管理负责人；
e) 制定整个项目的工作计划，确定设备、文件资料的交付时间，以及各个工作段的起始日期；
f) 制定项目进度的管理方案，明确项目进度的主要控制节点，规定项目进度报告所包含的内容以及提交的频次；对可能出现的进度延误情况，应制定明确的应对措施和预案。

12.2 功能设计

12.2.1 DCS 功能设计应至少包括以下内容：

a) 编制 DCS 系统结构图，确定 DCS 网络拓扑结构、节点关联及地址配置；
b) 描述 DCS 硬件和软件的功能；
c) 编制 DCS 各个设备、部件以及功能模块的命名规则；
d) 编制功能组态的通用规定以及各种典型回路的组态示例；
e) 确定 DCS 显示画面的编制规定；
f) 定义报警设置方案；
g) 定义历史数据的预处理、存储周期及存储设备；
h) 定义报警、历史数据、计算统计等各种报表的形式；
i) 确定机柜、操作台以及辅助操作台等设备的外形、尺寸和颜色；
j) 确定安全栅、隔离器、继电器以及电缆进出机柜等排布原则；
k) 确定 DCS 各部分的配电方案。

12.3 组态

12.3.1 在 DCS 组态工作开始之前，应具备下列工作条件：

a) 离线或在线组态所需的软件和硬件已经安装完成；
b) 组态工作人员和工程支持人员已经到位，组态技术资料和其他辅助资料已经配备齐全；
c) 功能设计文件的编制工作已经完成；
d) 已经完成工程项目的 I/O 清单、DCS 索引表、复杂回路框图或说明、逻辑图以及操作画面草图的编制。

12.3.2 DCS 系统组态工作应包括以下内容：

a) 结构组态。根据已制定的系统结构配置 DCS 网络中的各节点，包括名称、描述、地址、相互关系和功能。
b) 参数配置。根据工程需要配置 DCS 各个设备、单元和模块的硬件参数。

c） 安全策略配置。配置 DCS 网络的域和用户组群，定义各个组群及成员的访问权限和密码。定义数据库的存取 限制，以及配置防火墙、安全网关、隔离网闸的数据包过滤、访问控制、安全管理等规则。

12.3.3 功能组态工作应包括以下内容：

a） 基础数据录入。根据 I/O 清单、DCS 索引表等工程设计资料完成各个模块的参数录入，包括：仪表位号、描述、变送器量程，工程单位，硬件地址，输入预处理，滤波常数，偏差和报警限数值等。

b） 控制算法组态。根据每个回路的功能要求完成回路中各个功能模块的调用和连接，并配置功能块的参数，还可 能需要利用 DCS 配备的算法语言编制程序。

c） 通信组态。按照通信协议完成 DCS 与现场仪表设备或其他系统的通信。

12.3.4 显示及操作组态工作应包括以下内容：

a） 静态画面绘制。根据工艺流程图绘制 DCS 操作的静态画面。

b） 数据链接组态。完成静态画面与 DCS 功能模块参数的数据链接以及画面之间的调用链接。

c） 定制报表。定义报警报表、历史数据报表、计算统计报表等各种报表的形式、相关工艺变量和参数。

12.3.5 报警组态应按照报警的重要程度，对工艺变量报警和其他类型的报警进行报警等级的划分，并设定各类报警的报警值。同时，应根据操作与管理的需要定义报警分组。

12.3.6 应结合工艺变量报警和其他报警的具体性质及其处理方式，确定相应的报警功能及报警形式。

12.4 系统集成

12.4.1 DCS 与第三方设备的集成、联调应由 DCS 供货商负责。

12.4.2 DCS 供货商应对 DCS 与第三方设备集成的安装、调试工作负责；

12.4.3 DCS 供货商应对集成后 DCS 的完整性、可靠性和稳定性负责；

12.4.4 DCS 供货商应对 DCS 与第三方设备通信负责。

12.4.5 第三方设备供货商应配合 DCS 设备与第三方设备的集成和联调。

13 工厂验收及集成测试

13.1 工厂验收测试

13.1.1 DCS 工厂验收测试前应具备以下条件：

a） DCS 已经在制造厂调试完毕并提供测试报告；

b） DCS 制造厂根据合同技术附件、功能设计文件和有关标准等已经编制了工厂验收程序；

c） DCS 制造厂根据验收程序已经准备了验收文件和记录文件。

13.1.2 工厂验收测试应包括以下内容：

a） 供货范围检查

1） 文件检查；

2） 软硬件规格数量检查；

3） 供电、通信、网络系统检查；

4） 接线和端子检查；

5） 备件检查。

b) 系统配置检查

1) DCS 各设备、部件的型号、规格和外观应符合要求；

2) 软件的规格和版本应符合要求。

c) 组态检查

1) 操作站的标准功能、流程图画面、分组画面、报警画面、趋势显示等组态应符合要求；

2) 工程师站、历史服务器、智能设备管理系统操作站以及其他应用工作站或服务器等设备应完好投运，软件功能和组态功能应符合功能设计及设计条件的要求；

3) 控制功能应符合要求；

4) 报警状态、记录、处理策略符合要求。

d) 系统性能和功能测试

1) 系统通电运行检查。系统软、硬件、网络全部安装就绪，具备无过程信号运行状态，按照出厂检验程序通电，检查系统所有设备、部件是否正常运行，软件是否运行正常；

2) 部分过程接口信号模拟连接测试及信号处理精度测试（AI、AO、DI、DO 等 I/O 模件应至少抽样 30%）；

3) 部分控制回路仿真测试；

4) 部分联锁回路仿真测试；

5) 系统的冗余和容错功能测试；

6) 系统从故障中恢复测试。

e) 系统安全测试

1) 网络安全相关策略系统性测试；

2) DCS 各设备安全功能测试；

3) 用户登录策略和权限测试。

13.1.3 工厂验收测试报告应包括以下内容：

a) 工厂验收测试的步骤和内容；

b) 检查和测试的结果；

c) 最终验收结论。

13.1.4 工厂验收过程中发现的未完成工作或不符合项应按照以下进行分类和整改：

a) 先整改，然后继续进行 FAT；

b) 在 FAT 的同时进行整改；

c) FAT 后，系统运至现场之前进行整改；

d) 留待现场整改。

13.2 工厂集成测试

13.2.1 工厂集成测试前应具备以下条件：

a) DCS 与第三方设备已经在 DCS 制造厂集成、调试完毕并有测试报告；

b) 对于在 DCS 制造厂集成的第三方设备，已经在 DCS 制造厂完成通信和相关数据测试，并提供测试报告；

c) DCS 制造厂已经提供第三方通信或性能测试设备和软件；

d) DCS 制造厂已经根据合同技术附件、系统硬件配置、系统软件功能、第三方技术资料和有关标准等编制工厂集成验收步骤。

13.2.2 工厂集成测试应包括以下内容：

a) 系统配置检查

1) 第三方供货商提供的设备、部件的型号、规格和外观应符合要求；

2) 第三方供货商提供的软件规格和版本应符合要求。

b) 功能测试

1) 第三方设备与 DCS 集成后的功能应满足要求；

2) 测试 DCS 与第三方设备的通信功能和实际数据交换，第三方的通信设备或模拟通信设备中应带有实际应用的通信数据。

13.2.3 工厂集成测试报告应包括以下内容：

a) 工厂集成测试的步骤和内容；

b) 检查和测试的结果；

c) 最终测试结论。

13.3 现场验收测试

13.3.1 现场验收测试应符合下列要求：

a) 各设备和部件的规格、数量应与装箱单一致，运输过程中应无损坏；

b) 设备安装符合要求；

c) DCS 设备在软件安装和组态数据装载后应正常运行；

d) 所有硬件应按 DCS 制造厂提供的程序进行测试，并应 100%正常工作。

13.3.2 现场验收测试应包括以下内容：

a) 审阅 DCS 工厂验收报告和现场调试记录；

b) 组态检查（同工厂验收内容）；

c) 全部过程接口信号连接测试（包括信号的零点、量程、测量范围、单位等）及系统信号处理精度测试，AI、AO、DI、DO 等 I/O 模件应 100%检查；

d) 全部控制回路功能测试；

e) 全部联锁回路测试；

f) 操作流程图及画面测试、相关操作链接测试；

g) 操作参数的初步设定，包括 PID 参数、报警限数值等；

h) 系统的冗余和容错功能测试；

i) 系统的供电与接地测试；

j) DCS 与第三方设备的通信测试。

13.3.3 现场验收测试报告应包括以下内容：

a) 现场验收的步骤和内容；

b) 检查和测试的结果；

c) 最终验收结论。

14 工程服务

14.1 技术服务

14.1.1 DCS 供货商在整个工程项目进行过程中应提供相关的技术咨询服务。

14.1.2 DCS 供货商应提供其所有交付文件、资料和设备的技术澄清服务。

14.1.3 DCS 供货商在工厂验收和现场验收过程中应提供相关的资料，并配备专门的工程技术人员配合验收工作。

14.1.4 DCS 供货商应对所供货的产品提供必要的组态、操作、使用和维护培训，并提供相关的培训资料。

14.1.5 DCS 供货商应根据控制系统技术方案，提供控制系统的包装、运输、存储、安装等程序文件。

14.1.6 DCS 供货商应根据项目工程服务范围及 DCS 安装、调试、开车进度计划，提供现场服务人力资源计划及责任矩阵文件。

14.2 现场服务

14.2.1 DCS 供货商应配备有资质的工程技术人员配合 DCS 的现场安装、调试、通电等工作，并应对结果负责。

14.2.2 在生产装置开工期间，DCS 供货商应配备有资质的工程技术人员在现场值班，随时解决开工过程中 DCS 出现的故障和应用问题。

工业和信息化部标准报批公示

附 录 A

（资料性）

分散控制系统网络结构示意图

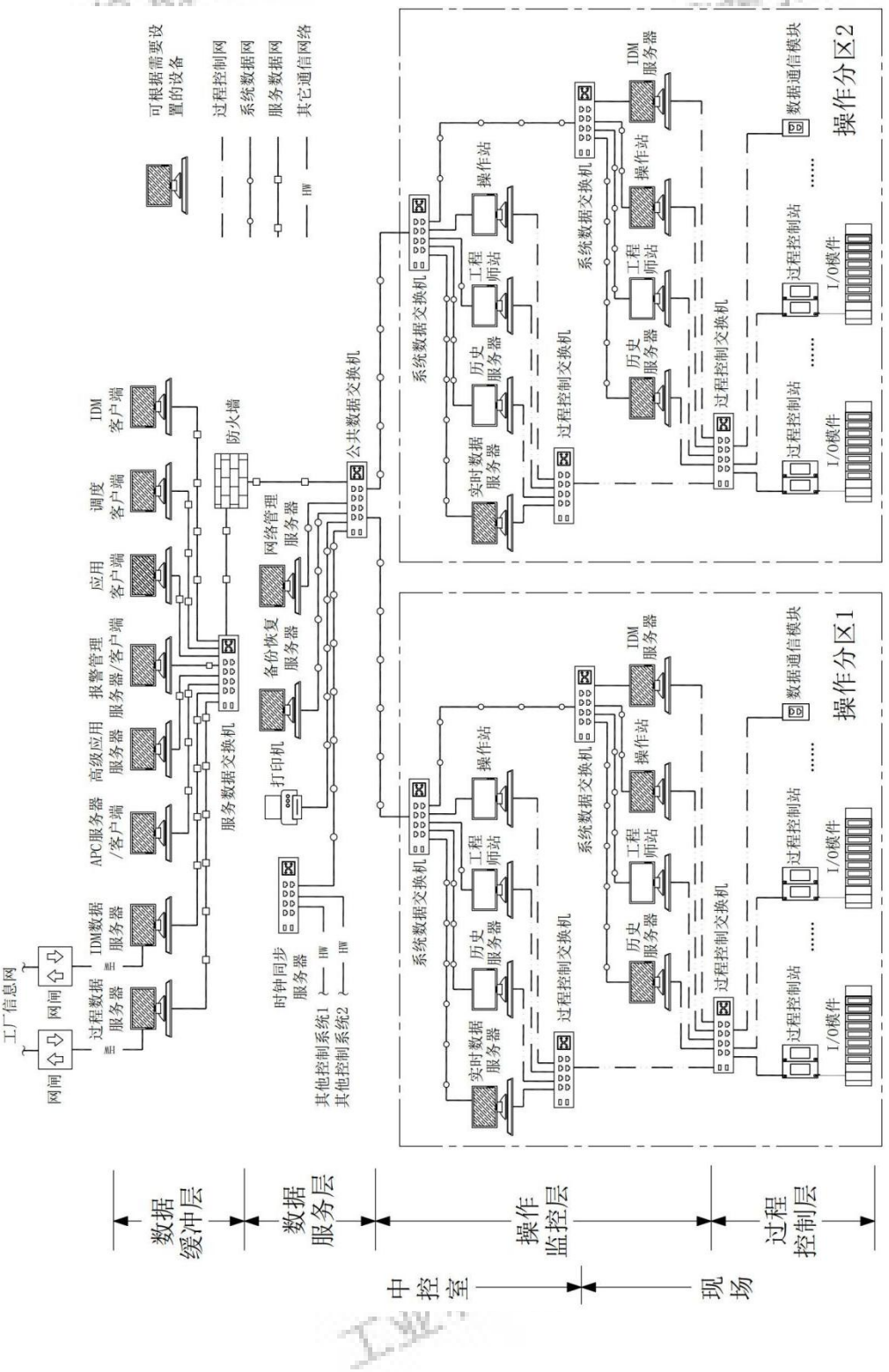

图 A.1 分散控制系统网络结构示意图

图 A.1 以某石化项目分散控制系统网络结构示意图为例，表示了 DCS 网络的结构层次、网络连接以及各层中的典型设备。

A.1 结构层次

图 A.1 中的结构层次是根据生产运行管理需要和数据流及网络管理的可能性划分的，不是 DCS 的网络层次。在不同层次中的 DCS 设备对功能和可靠性要求各不相同，因此配置要求也不同。

A.2 操作分区

操作分区是根据生产操作和数据管理的需要划分的 DCS 网络分区（网络分区的意义和方式见附录 B）。不同操作分区之间可以通过公共数据交换机进行数据交换，但功能设备和网络应相对独立，应能做到在必要时可以各自形成操作控制功能完备的独立网络。

在划分操作分区时，应避免不同操作分区之间有跨区控制或关联操作。

A.3 现场机柜室

当 DCS 设备采用分散布置方式时，现场机柜室与中心控制室的通信一旦发生中断，现场机柜室内的网络和设备应能构成基本的 DCS 功能单元，能够独立运行，依然能满足维持工艺装置、公用工程单元或储运单元正常生产的基本功能要求。

A.4 网络设备

按照结构层次划分，交换机可分为过程数据交换机、系统数据交换机、公共数据交换机和服务数据交换机。

A.4.1 过程控制交换机

过程控制交换机用于是 DCS 网络中最基础的交换机，控制层交换机的故障会导致过程数据通信和（或）操作监控层设备数据通信的中断，从而导致 DCS 系统功能的失效。

过程控制交换机应冗余配置。

A.4.2 系统数据交换机

系统数据交换机用于操作监控层与数据服务层之间以及操作监控层设备之间的数据通信。

系统数据交换机的故障会导致操作监控层设备数据通信的中断。

当过程控制网与操作监控网共用同一交换机时，操作监控层设备之间的数据通信将增加交换机的负荷，不可避免地影响到过程控制层的数据通信。因此分别设置过程控制网和系统数据网的交换机有利于保护过程控制层数据通信的可靠性。当 DCS 网络规模较小时，系统数据交换机也可与过程控制交换机共用，分散控制系统网络结构示意图可参考图 A.2。系统数据交换机与过程控制交换机共用时，应冗余配置。

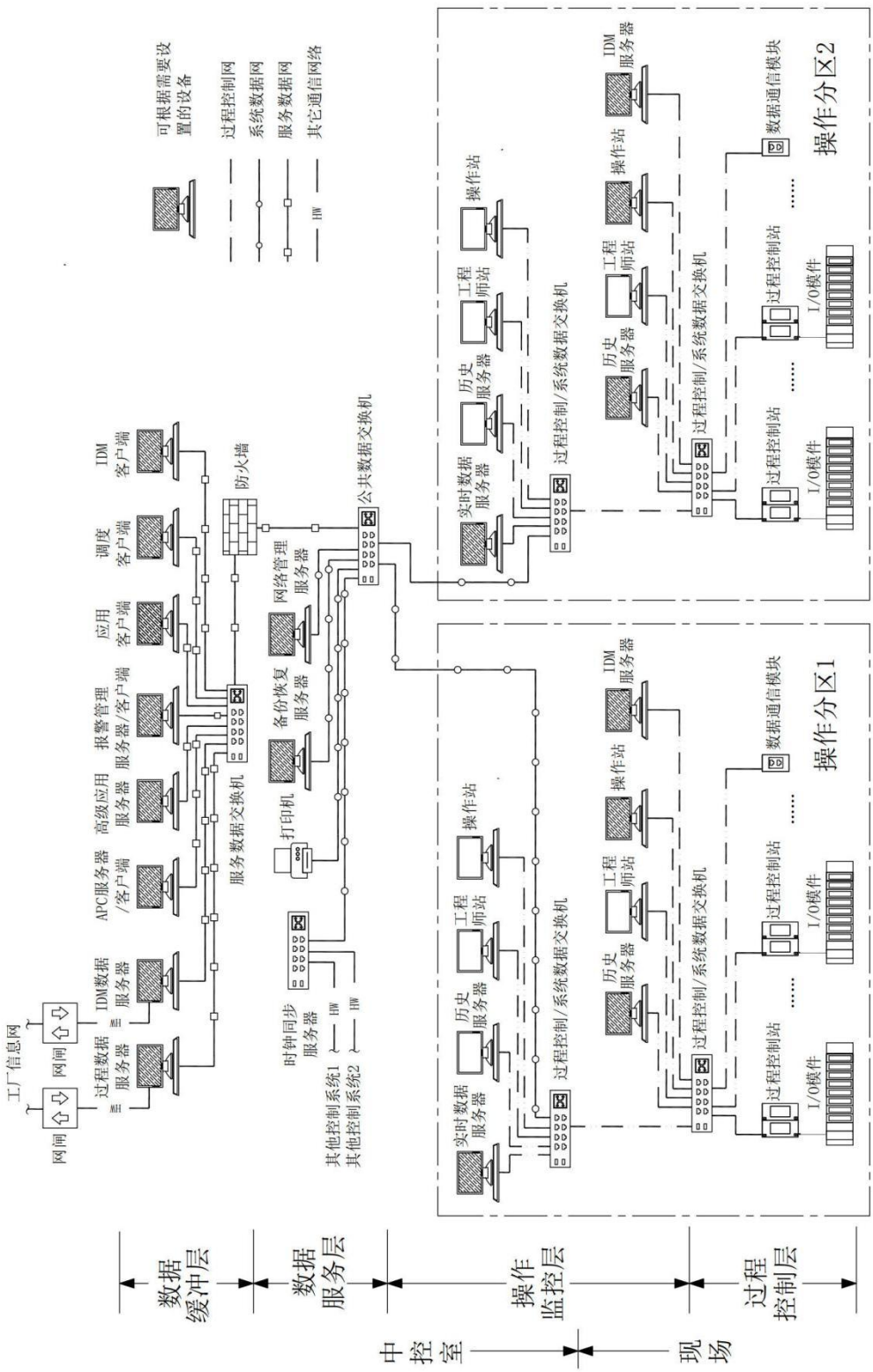

图 A.2　分散控制系统网络结构示意图（系统数据交换机与过程控制交换机共用）

A.4.3 公共数据交换机

公共数据交换机用于数据服务层与操作监控层之间以及操作监控层不同网络分区之间的数据通信，是全厂过程数据的交换中心。同时公共数据交换机也用于全厂各分区共用的操作监控层设备（如网络管理服务器、全厂的 GDS 监控站等）的网络连接。

公共数据交换机的故障会引起各操作分区之间以及操作监控层与数据服务层之间数据通信的中断，但不会影响操作监控层、数据服务层本身的网络通信。

过程控制层设备不应直接接入公共数据层交换机。

当 DCS 网络规模较小，没有必要进行网络分区时，公共数据交换机和系统数据交换机可以共用。

A.4.4 服务数据交换机

服务数据交换机用于数据缓冲层与操作监控层之间以及数据缓冲层设备之间的数据通信。

服务数据交换机的故障会引起数据服务层设备数据通信的中断。

过程控制层和操作监控层设备不应直接入服务数据交换机。

当 DCS 设置数据缓冲层时，服务数据交换机应单独设置，不能与其他层交换机混用。

工业和信息化部标准报批公示

附 录 B
（资料性）
分散控制系统网络分区

B.1 网络分区的意义

对于大型 DCS 网络（节点数量大于 200），网络分区有以下意义：

a） 减轻网络负荷、增加网络能力、降低对核心交换机的配置要求。

b） 网络分区可以独立运行，分散并隔离网络故障、分散网络安全风险、分区之间避免网络干扰。

c） 提高网络运行效率、提高网络可靠性和可用性。

d） 便于网络维护，便于排除网络故障及清除恶意代码。

DCS 网络分区的方式一般有两种，划分子网或设置虚拟局域网(VLAN)。由于虚拟局域网所定义的分区不能构成绝对意义上的独立网段，因此对于大型 DCS 网络各操作分区不宜采用 VLAN 进行网络分区。

根据项目的规模和操作工艺安排，网络分区可能与操作分区一致，也可能不一致。

B.2 子网

B.2.1 子网划分方式

如图 B.2.1 所示，在同一个 IP 网络中划分子网能将一个大型 DCS 网络分成若干个较小的网络，每个子网由路由器（或带路由功能的交换机）界定并分配一个新的子网网络地址。

B.2.2 子网的优点

采用划分子网的方式对 DCS 网络进行分区具有以下优点：

a） 减轻网络负荷。每个子网都是一个单独的多网段广播域，将网络节点分散到各子网中，分散了网络通信量。

b） 子网内仅传输同一操作分区的相关数据，不需要与其他子网进行数据交换，减少了网间数据传输，分散并减轻了网络负荷。

c） 当网络中存在恶意代码时，可将安全的子网从总网络中拆离，便于维护，待网络中恶意代码彻底清除后再重新接入。

d） 各个子网相对独立，主要数据的传输不需要经过核心交换机，对核心交换机的配置要求不高。

B.2.3 子网的设计原则

DCS 的子网划分应遵循以下几个设计原则：

a） 每个子网不宜过大，应留有足够的空闲地址，以便于网络的扩展和调整。

b） 子网应根据操作或管理分区划分。对于数据量交换较大的节点应设置在同一子网中，减少子网之间的数据交换。

c） 每个子网都可以采用物理方式切断与主网络的联系，形成独立的网络。

d） 对于实现分区内正常工艺操作功能（检测、控制、报警、联锁以及历史记录）相关的设备（如操作站、过程控制站、历史服务器等），应在子网内分别独立设置。

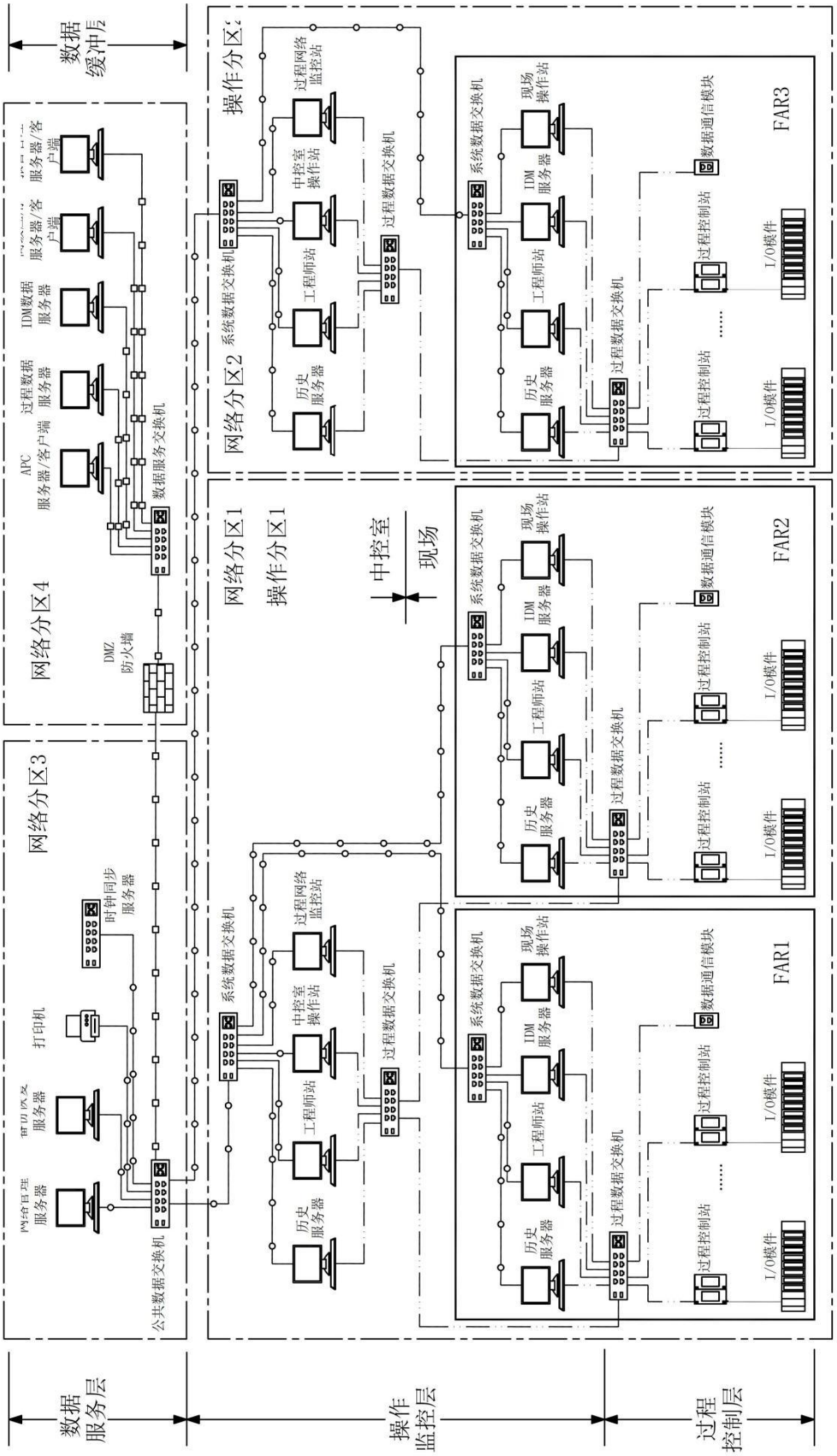

图 B.2.1 子网划分示例图

附 录 C
（资料性）
分散控制系统网络安全结构示意图

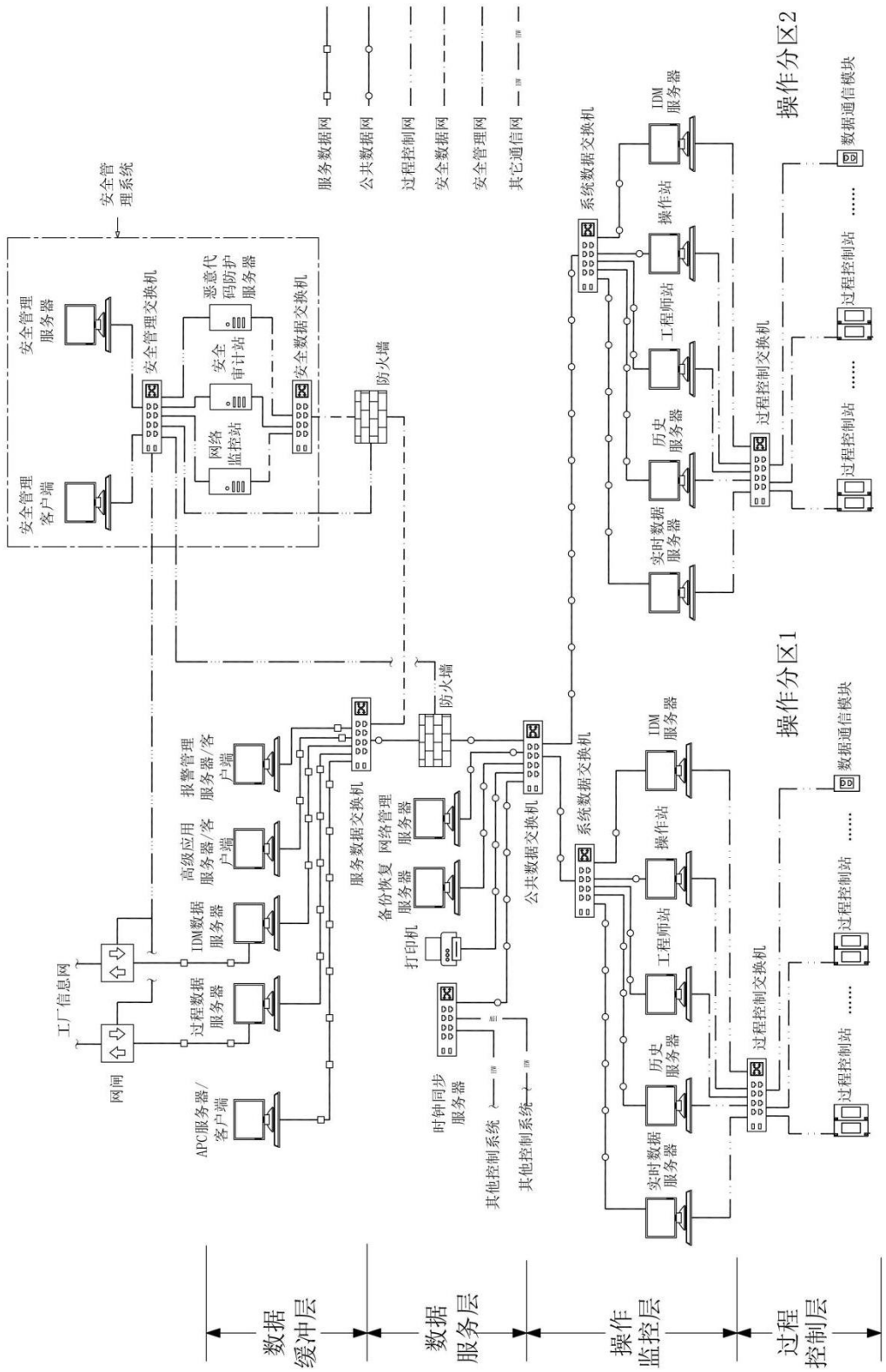

图 C.1 分散控制系统安全管理网络结构示意图一

图 C.1 以某石化项目分散控制系统安全管理网络结构示意图为例，表示了 DCS 安全管理系统的网络连接和设备。

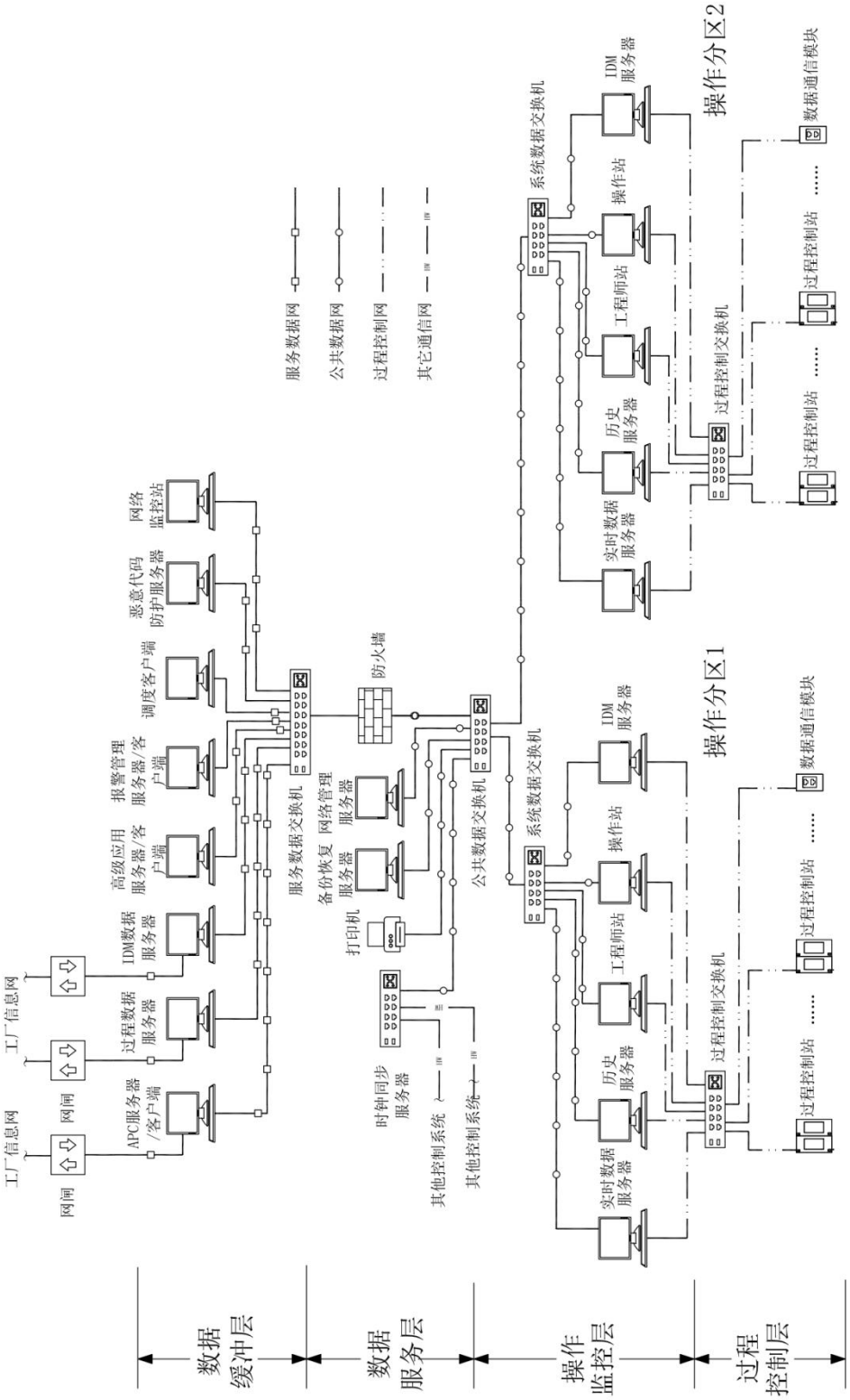

图 C.2　分散控制系统安全管理网络结构示意图二

图 C.2 以某石化项目分散控制系统安全管理网络结构示意图为例，表示了在不设置安全管理系统时，DCS 的安全设备和网络连接。

C.1 安全管理系统

安全管理系统一般由安全审计站、网络监测站、恶意代码防护服务器、安全管理服务器和安全管理客户端组成，用于 DCS 系统网络安全、设备安全、数据安全、访问安全等状态的监测。

DCS 系统安全是由 DCS 网络结构和各层设备的功能来保证的，安全管理系统仅用于 DCS 系统安全的监测和报警，可以便于用户对 DCS 网络及设备进行集中监控和管理，但不是实现 DCS 系统安全的必要配置。在不设置安全管理系统时，应至少设置网络监控站、恶意代码防护服务器和网络管理服务器，用于 DCS 的网络状态监测、恶意代码防护、访问控制和入侵防范。

C.2 DCS 安全管理设备

C.2.1 安全审计站

安全审计站是用于 DCS 设备的审计日志数据管理的专用硬件设备，主要功能包括：

a) 收集、存储和管理系统中的审计日志。

b) 实时监控系统中的安全事件，包括异常登录尝试、未授权访问、系统错误等。

c) 通过对工业控制协议和网络通信协议的数据进行还原，查看数据在事件发生时的原始状态。

d) 在发生安全事件时自动触发报警，通知管理员，并记录事件的相关信息。

操作监控层、数据服务层以及数据缓冲层设备可通过服务数据交换机（无数据缓冲层时可通过系统数据交换机）和安全数据交换机将审计日志数据接至安全审计站。

C.2.2 网络监控站

网络监控站是用于 DCS 各级网络的流量监测、入侵防范的专用硬件设备。

系统数据网络交换机和服务数据交换机分别设置交换机管理口的镜像口，镜像口将复制的网络监测数据传输至网络监控站。

设置镜像口可以将 DCS 功能数据网络与安全管理网络进行隔离。

C.2.3 恶意代码防护服务器

恶意代码防护服务器可用于 DCS 设备的恶意代码防护、白名单控制、资源监控。

恶意代码防护服务器可通过系统数据网络交换机和服务数据将安全策略下发至操作监控层、数据服务层、以及数据缓冲层设备。

C.2.4 安全管理服务器

安全管理服务器可用于来自交换机、防火墙、网闸、安全审计站、网络监测站、主机防护站等网络安全数据的集中存储、分析，应能对 DCS 网络和设备中的攻击行为、异常流量、非法用户登陆的异常行为报警。

C.2.5 安全管理客户端

安全管理客户端是安全管理平台的人机界面，用于用户安全管理员对 DCS 系统安全的监控和管理。

安全管理客户端一旦受到外部入侵或恶意代码侵害，有可能导致防火墙、网闸等安全设备功能失效，严重威胁 DCS 的网络安全。因此安全管理客户端应专岗专用，隔离一切外部网络和数据接口。在条件允许时，安全管理客户端宜设置在单独的岗位房间。

安全管理客户端可与安全管理服务器共用设备。

C.3 安全管理网络

DCS 各级数据网络与 DCS 安全管理网络应相互隔离。交换机、防火墙、隔离网闸、安全审计站、网络监测站、防护主机通过设备管理口（或管理镜像口）接至安全管理交换机与安全管理服务器和客户端连接。

C.4 安全数据网络

安全数据网用于 DCS 设备（操作站、工程师站、历史服务器等）的安全策略、恶意代码特征文件、审计日志、用户权限等安全数据与安全管理系统之间的双向传输，因此需要设置防火墙通过访问控制机制限制数据交换行为，仅允许交换符合安全策略的指定格式的数据，以确保网络和数据安全。

工业和信息化部标准报批公示

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”；

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”。

工业和信息化部标准报批公示

中华人民共和国石油化工行业标准

石油化工分散控制系统设计规范

SH/T 3092—202X

条文说明

202x 年　北　京

工业和信息化部标准报批公示

修 订 说 明

《石油化工分散控制系统设计规范》SH/T 3092-202×，经工业和信息化部202×年××月××日以第××号公告批准发布。

本规范修订过程中，编制组进行了比较广泛的调查研究，总结了我国石油化工工程建设在分散控制系统方面的实践经验，特别是进入21世纪我国新建、扩建千万吨级炼油项目和百万吨级乙烯项目的经验，归纳了多次招标和项目执行的过程和结果，同时参考了国外技术规定、技术标准，征求了有关设计、施工、生产等方面的意见，最终经审查定稿。

为便于广大设计、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，《石油化工分散控制系统设计规范》编制组按章、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标准正文同等的法律效力，仅供使用者作为理解和遵循标准规定的参考。

工业和信息化部标准报批公示

目　　次

修 订 说 明 41
3 术语和缩略语 44
3.1 术语和定义 44
3.2 缩略语 45
4 设计原则 45
4.1 一般规定 45
4.2 系统性能 45
4.3 系统功能 45
4.4 报警和事件记录 46
5 系统结构 46
5.1 功能结构 46
5.2 网络结构 47
6 系统安全 48
6.1 信息安全 48
6.2 网络安全 48
6.3 安全管理措施 49
6.4 安全管理系统 49
7 系统技术要求 49
7.1 过程控制站 49
7.2 过程接口单元 50
7.3 操作站 51
7.4 工程师站 51
7.5 历史服务器 51
7.6 网络管理服务器 52
7.8　供电要求 52
8 网络系统 52
8.1　网络特性 52
8.2　网络设备 52
8.3　网络负荷 53
8.4　与第三方设备通信 53
9 辅助设备 53
9.1　辅助操作站 53
9.4　其他辅助仪表 53
10 高级应用 54
10.1　智能设备管理系统 54
10.3　过程数据服务 54

10.4 先进控制 54
10.5 储运管理 54
10.6 网页浏览服务 54
10.8 其他高级应用 54
11 软件配置 54
11.1 控制和操作软件 54
12 工程实施 55
12.1 系统开工会 55
12.2 功能设计 55
12.3 组态 55
12.4 系统集成 55
13 **工厂验收及集成**测试 ..... **错误！未定义书签。**56
13.1 工厂验收测试 56
13.2 工厂集成测试 56
14 工程服务 56
14.1 技术服务 56

工业和信息化部标准报批公示

3.1 术语和定义

3.1.5 同步冗余

同步冗余与热备冗余相比除了诊断机制不同外，主要的区别是采用同步冗余的备用设备的运行和输出与工作设备保持相同，容易做到无扰动切换。

3.1.6 冷备冗余

冷备冗余的缺点是备用设备启动时间较长，无法做到无扰动切换。冷备设备正常状态下不工作，运行负荷产生的故障率会不同，平时检测相对麻烦。

3.1.13 失效率

失效率通常用来表示一批受测元件单位时间内的失效次数：

$\lambda(t)$ = 单位时间内的失效次数/受测元件总数

当把产品的失效率看做是常数时，可以反映产品在特定时间内发生失效的概率：

$$\lambda(t) = \frac{1}{MTTF}$$

串联系统的失效率 $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n$；（$\lambda_1, \lambda_2, \lambda_n$ 是各个子系统的失效率。）

3.1.17 输入/输出模件

也称为输入/输出卡件，本规范统一称为输入/输出模件。

3.1.25 防火墙

用于网络的防火墙是计算机网络借喻的专用词汇，有特定的含义，类似的词汇还有病毒、木马等。防火墙一般分为硬件防火墙和软件防火墙。路由器、交换机或杀毒软件等产品有时也会配置简单的防火墙功能。本规范中的防火墙特指不依附于其他设备或软件独立运行的硬件防火墙。

3.1.26 隔离网闸

隔离网闸是使用带有多种控制功能的通道开关连接两个独立主机系统的信息安全设备。隔离网闸以“摆渡”（转交） 的方式将需要交换的数据导入到内部主机系统，实现信息的交换。由于隔离网闸所连接的两个独立主机系统之间不存在通信的物理连接、逻辑连接、信息传输命令及信息传输协议。

网闸通过数据隔离卡将交互数据进行数据转交结合专有协议实现数据交互安全，及物理隔离的两个不同网络的数据交互。隔离网闸主要用于两个安全级别不同的网络之间的数据安全传输，如信任网络（DCS网络）和非信任网络（工厂信息网）。

3.1.17 安全网关

网关按其功能可分为协议网关、应用网关和安全网关三类。协议网关用于在使用不同协议的网络之间进行协议转换。应用网关可以在应用层连接两个不同的应用，适用于特定应用的协议转换。安全网关通过执行既定的安全策略和流量限制来提供通信数据保护。本规范中的安全网关特指工业控制系统边界安全专用网关，具备接入管理、协议转换、数据处理、网关设备管理、标识管理、安全管理等功能。

3.1.28 恶意代码

恶意代码是一种程序，常常通过把代码隐蔽到另一段程序或数据文件中的方式，借机运行，达到干扰正常程序功能、破坏数据、盗窃数据、运行破坏性程序等目的。恶意代码按传播方式可分成五类：病毒、木马、蠕虫、移动代码和复合型病毒。

3.2 缩略语

智能设备管理系统（IDM）用于智能设备的数据采集和管理，曾有过其他缩略语，例如： AMS 或 PRM。

4 设计原则

4.1 一般规定

本规范中对 DCS 制定了一些原则上的、定性的规定，目的是限制和约束在石油化工工厂应用的 DCS 的品质、功能、性能和水平。但是，不同品牌的 DCS 硬件配置、软件功能、网络拓扑、系统结构、组态方式和操作特点都有区别。随着相关技术的快速发展，很难定量规定和约束。所以，本规范多处规定了一些定性的基本功能。

本条特别规定了应在 DCS 中实现的、DCS 应具备的基本功能，明确 DCS 应是一个具有多种完备功能设备的整体系统。

4.1.1 鉴于石油化工应用的情况，新建项目的 DCS 的硬件和软件的年代版本应该在正式公布一年以上，三年以内。

4.1.2 集中布置方式的 DCS 过程控制层和操作监控层的主要硬件设备均位于同一建筑物或安装区域内。采用集中布置方式的控制室，DCS 的 I/O 模件、过程控制站、操作站、工程师站以及各种数据服务器等主要设备均安装在同一建筑物内。仅有个别不影响 DCS 正常功能的设备位于其他位置（如远程操作站、第三方应用设备等）。分散布置方式的 DCS 过程控制层和操作监控层的主要硬件设备分别位于不同的建筑物或安装区域内，主要应用于操作与控制功能分开，以达到分散控制、集中管理的目的。例如：中心控制室结合现场机柜室方式，DCS 过程控制层的设备安装在现场机柜室内，操作监控层与生产操作监控有关的大部分设备安装在其他区域的在中心控制室内。

4.2 系统性能

4.2.2 控制器、供电单元和通信单元等下游单元相对集中，故障时会影响多个下游单元，为减少这种集中关联影响到过程控制、工艺操作、设备运行等，为提高系统的整体或部分设备的可用性，采取冗余结构。

4.2.6 系统的硬件和软件应具有版本兼容性。

a) 对于版本较早的系统，如果不能做到与新版本的系统完全兼容，则新版本的系统应能采用通信及数据连接设备将新、老系统进行连接，在过程控制层实现数据传输。

b) 不同版本间硬件和软件的兼容性对已有 DCS 的设备维护和更新尤其重要。本规范规定了软件维护版本和补充版本与硬件的兼容时间应与设备运行寿命一致。

4.2.8 采用外接功能设备代替 DCS 已有的功能会增加信号处理环节，降低系统的可靠性。

外接功能设备是指在现场仪表和控制系统之间接入的、为实现某种特定功能（如温压补偿计算或报警设定）的设备或仪表。

4.3 系统功能

4.3.5 工程师站组态下装时应进行二次确认后再进行下装操作，以减少差错。

4.3.7 故障诊断是系统提高可靠性和可用性的必要手段和措施，也是智能化电子设备的特点。

4.3.9 在线组态和调试是指在本项目的系统上工作，离线是指在非本项目的系统或设备上组态和调试，然后在本项目的系统复制及下载。

4.3.11 DCS 应具备某些局部故障时的的快速数据恢复功能（例如：单个模件软件下载、冷备冗余部件更换、操作站启动、工艺控制参数复制等）。

4.3.12 DCS 系统的正常运行不应依赖时钟同步，特别是不应依赖外部时钟。

a) DCS 系统内部已具备时间同步机制，为使不同系统之间的时钟同步，便于不同系统间的数据对照，可以配置外部时钟源进行同步校正。

b) 时钟同步的目的是使系统内部和系统之间的时间标记数据一致。系统时间的同步并不追求与某一特定地域时间的绝对一致性，而是侧重于实现时间标记的相对一致性。在实际应用中，当需要具有时间标记记录数据的第三方计算机设备与 DCS 同步时，宜采用由 DCS 发布同步信号的方式。对于不需要记录时间标记数据的第三方设备，不必设置时钟同步。

本规范中“第三方”定义为除 DCS 系统本身及其直接控制或管理的组件之外的任何实体或设备。这些第三方实体包括其他计算机系统、设备、服务提供商或任何需要与 DCS 系统进行信息交互或数据交换的实体或设备。

d) 授时精度是指时钟同步服务器向各个节点发出时钟同步信号的精度。守时精度是指时钟同步服务器本身在一定时期内时间的准确度。

f) 过程控制数据网络中的设备（如过程控制站）通过工程师站或历史站时钟同步信号，而不直接从时钟同步服务器获取，是为了通过分层保护来降低外部网络威胁的风险。

4.4 报警和事件记录

4.4.2 报警和事件记录是 DCS 必备的基本功能。由于石油化工过程的复杂，区别各类报警事件对于及时处理异常过程、防止事故至关重要，本规范强调对过程变量报警的分级、分区、分组及数据处理的功能。

报警事件的记录是分析报警过程、分析工艺过程和设备状态的重要条件，特别是分析和确定事故原因和事故过程的重要条件和关键依据。

4.4.12 报警分区是为了便于操作岗位的报警监视和管理，减少不同岗位间报警信息的相互干扰。分区的原则是与操作岗位的职责范围一致，在操作站中不会显示与当前操作岗位无关的报警。

4.4.13 报警分组是为了在工艺装置的非正常运行过程中，避免正常操作触发的报警对异常操作过程的干扰。可根据装置的不同运行阶段，如投运过程、停工期间、水联运、油联运、从投料初期到达到标称处理量期间、工艺提量运行、工艺降量运行等，设定报警分组，操作人员可以根据运行阶段和预设的规则，启用适合的报警组，并暂停（约束、限制）其他报警组的运行。这样的设计减少了无效报警，有助于操作人员准确获得报警信息，了解当前工艺装置的运行状态，减轻操作负担，准确并及时操作。

5 系统结构

5.1 功能结构

5.1.1 DCS 总体结构的分层是根据生产运行管理系统的需要和数据流及网络管理的论述方便，并不是 DCS 的固有层次，也不是 DCS 产品的网络层次。本规范层次划分的目的是为了便于说明系统安全配置。

生产运行管理层主要实现生产数据和管理数据的高层次应用和集成，对生产过程进行优化操作。生产运行管理层承担企业的调度管理和协调工作等。本规范涉及的范围不包括生产运行管理层的相关内容。

DCS 系统结构配置可参考附录 A（分散控制系统网络结构示意图）。

5.1.3 操作监控层内的设备与生产操作或 DCS 系统管理相关，包括操作站、工程师站、历史服务器、智能设备管理站等计算机，还包括其他相关的网络设备。

5.1.4 为了过程控制的安全，过程控制层不应直接接入人机接口，但某些成套设备的控制系统是带有人机接口的。这种情况下，成套设备的控制系统不应直接通过网络与装置的 DCS 相连接，可以通过串行接口数据通信的方式进行数据传输。

5.1.7 数据服务层主要用于对各操作分区的公共数据进行传输和管理，如用户权限管理、设备备份和恢复数据管理、打印服务管理、时钟同步数据管理等。

设置在数据服务层中的设备或通信故障不会影响到工艺过程的正常生产操作。主要包括：网络管理服务器、备份恢复服务器、时钟同步服务器等。打印机可根据管理需要整体设置在数据服务层，也可分别设置在各操作分区的操作监控层。

5.1.9 过程控制层和操作监控层的数据需要传输至生产运行管理及企业管理等各个层次和部门。由于数据传输的目标设备往往位于非安全网络环境中，增加了网络安全风险。通过设置数据缓冲层，运用服务器、安全网关、防火墙等一系列技术手段，使非安全环境的网络与 DCS 内部网络在物理层隔离，同时严格限制访问的数据类型和对象。数据缓冲层成为一个独立的网络区域，提升系统的安全防护能力。

位于数据缓冲层中的设备特征：

a) 设备或通信的故障不会影响工艺过程的正常生产操作；

b) 仅从操作监控层单向读取数据，避免了对过程控制或工艺操作的数据篡改或非法访问风险。

数据缓冲层主要包含以下几类服务器：恶意代码防护服务器、网页浏览服务器、过程数据服务器、应用数据服务器以及IDM数据服务器等。

5.1.11 安装在DCS网络中的第三方应用计算机归入到DCS安全管理的范围内。可由DCS供货商提供预装操作系统、安全软件和必需办公软件的计算机，然后由第三方通过授权的用户登陆计算机，安装经过验证的应用软件或模块并进行配置和调试。安装后的软件和模块经过验证后归入到白名单系统。

5.2 网络结构

DCS 网络分为生产过程控制网和工厂管理网。本规范的设计要求不包含工厂管理网的相关内容。

为提高 DCS 的网络运行及信息安全，减少故障风险、减低网络负荷，DCS 的网络结构采用“纵向分层、横向分区”的结构。

近年来的 DCS 趋向于采用 IEEE802.3 的通信协议，增加了 DCS 的网络负荷，个别全厂网络出现了网络通信故障。对大型 DCS 网络按操作和管理分区的网络结构方案，各网络分区可以自成系统，独立运行，减少网络故障的风险，便于网络维护。

5.2.1 DCS网络的分层是为了实现专网专用和网络隔离，在不同层次的网络边界设置安全保护措施，实现对DCS设备和网络的纵深防护。

5.2.2 过程控制网作为 DCS（分散控制系统）的核心网络，稳定性和安全性至关重要，关系到生产过程的“安、稳、长、满、优”。过程控制网与系统数据网隔离，可以减少网络通信故障和外部影响。

5.2.7 操作分区是 DCS 中基础和重要的分区概念。DCS 的分区设计不是基于计算机硬件软件运行能力或基于数据管理局限性的“域”的概念。操作分区可根据工厂操作和管理的实际需要来划分。

DCS网络分区与工厂操作分区一致，便于操作、维护和管理、降低网络负荷等，在设计和实施DCS分区时，应坚持操作和管理的主导地位，而不是被动地适应DCS的数据结构和网络结构。

6 系统安全

DCS 系统的安全关系到网络的稳定运行和数据的畅通无阻，涉及对外部网络威胁的防御以及工厂内部数据的保密和完整，需要采取多层次、综合性的安全防护策略。DCS 系统的基本安全策略是多层保护的分布式纵深防御：

a) 分层保护策略：制定差异化的层次防护措施，以防止攻击或异常影响长驱直入或对单一防护策略的突破。

b) 双重安全防护：当过程控制层设备与第三方设备进行数据传输时，应至少实施两重安全防护措施，实现数据在传输过程中的安全性。

c) 关键数据与设备的保护：避免与正常安全生产直接相关的数据、设备和网络受外部入侵或恶意代码的破坏。

d) 紧急隔离机制：在面临外部安全威胁时，应能在不影响正常生产操作的前提下，迅速切断 DCS 控制、操作设备和网络与其他所有网络、设备的连接，以减小安全风险。

e) 分区物理隔离：一旦 DCS 网络受到入侵或感染恶意代码，能按操作分区进行物理隔离，以限制异常的影响范围，维持其他区域的安全运行。

除了网络信息的防护措施，还需要考虑环境因素对工厂网络特别是控制网络安全的影响。这包括生产环境、气象条件、自然环境和社会环境，以及自然灾害和人为灾害等极端情况下的应对策略。

采用防护技术是保障系统安全的重要手段，但网络的日常运行管理和规章制度的制定与执行同样重要。

6.1 信息安全

6.1.5 第三方软件是指除操作系统和 DCS 之外的应用软件。操作监控层设备中运行的软件只能用于完成 DCS 自身必要功能和安全防护功能，其他非直接相关的功能（如数据分析、文档处理等）只可在数据服务层或 DCS 系统外的设备上完成。近年来，随着计算机的普及和各种软件的丰富和杂乱，由软件造成的对计算机正常功能的危害越来越严重，为 DCS 不受未知确切安全的软件的影响，特规定在操作监控层的设备中禁止安装与 DCS 功能和安全防护功能无关的软件。

6.1.7 恶意代码防护服务器可以同时用于白名单和黑名单技术，集中制定和管理恶意代码防护策略，统一更新网络设备的恶意代码库，配置安全程序列表。

6.1.8 黑名单机制是禁止已经发现的恶意程序。需要不断更新恶意代码名单和识别特征库。对于未知的恶意代码是不能防范的。更新恶意代码库的过程也有安全风险。白名单技术用于放行已知安全、有权限的程序和应用在用户的设备上运行。白名单技术安全性较高，只需要管理已知安全程序的列表，不需要更新恶意代码库。白名单也需要定期维护更新。在操作站、工程师站、历史服务器等功能相对固定的设备上采用白名单技术，相对简单有效。

6.1.12 具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构。《网络关键设备和网络安全专用产品目录》和《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》由国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会发布更新。已经获得《计算机信息系统安全专用产品销售许可证》的产品在有效期内可继续销售或者提供。

6.2 网络安全

6.2.1

c） 不同建筑物之间的 DCS 网络应采用光缆连接，可以减少电磁干扰。

d） 如果与 DCS 功能无关的计算机和设备直接接入 DCS 网络，不但占用 DCS 网络资源、降低 DCS 的数据通信效率，还可能直接影响和破坏 DCS 网络，影响和威胁工厂过程运行的安全。

6.2.2 过程控制网络是连续、实时的，对生产过程和工厂安全至关重要的基础网络。因此，在没有充分证据证明无线网络能够在所有时间和各种环境条件下保持安全之前，不应采用无线网络作为 DCS 控制系统的各级网络。

虽然本规范规定 DCS 网络不应采用无线网络，并不意味着仪表信号也不能通过无线方式进行传输。采用无线通信方式传输信号的仪表，可以通过网关将无线通信协议转换为有线通信协议（如 Modbus）后接入到 DCS 的 I/O 层。

c） DCS 数据通信模块用于将通用的工业通信协议（如 Modbus）转换成 DCS 内部专用的通信协议。对于不直接参与过程控制及保护功能的检测 数据，可以 DCS 数据通信模块进行传输。

e） 安全网关的作用是将无线仪表的通信协议转换成通用的工业通信协议（例如 Modbus），并设置安全措施保护穿越网关的数据。

6.3 安全管理措施

6.3.1 远程访问服务（Remote Access Services，简称 RAS）采用客户端通过拨号连接或虚拟专用连接的方式登录网络，用于对网络资源或设备进行远程访问和控制，虽然 DCS 故障诊断便捷，但存在安全问题。当确有必要使用远程诊断及排除故障时，在确认网络安全并有效监督下限时进行，工作完成后应及时解除远程介入。

6.3.3 移动存储设备是指可在不同终端间进行数据交换的可存储设备，包括软盘、移动硬盘、光盘、USB 闪存盘（U 盘）以及磁带机等。

6.3.4 外部数据接口和移动存储设备可采用软件禁用、封闭或拆除接口以及机箱设锁等方式限制使用。

6.4 安全管理系统

在 DCS 系统的安全保障体系中，安全管理系统不是必要的。如果安全管理系统未能得到妥善的实施和有效的管理，可能会引入额外的安全风险。

7 系统技术要求

7.1 过程控制站

7.1.4 同步冗余是为了保证控制器在切换过程中保持输出一致，减少切换过程对工艺操作造成的干扰。

7.1.7 负荷计算时，不同扫描周期的 I/O 点数占总点数的一般比例为：0.2s 为 10%，0.5s 为 30%，1s 为 60%。PID 控制模块的数量按各过程控制站 AO 点数的 2 倍计算，控制周期按 1s 计算。当有快速控制功能需求时，控制器负荷应按快速控制的扫描周期和点数进行计算控制器负荷。

7.1.8 如果由于改造等原因对某装置、单元的 DCS 过程控制站的组态数据修改、下装并重新启动时，对共用一个过程控制站的其他装置、单元会造成影响，将不同装置、单元（即使是同一操作分区）的控制回路和检测回路放在不同的过程控制站中可以避免装置、单元之间的相互影响。

对于 I/O 点数较多的工艺装置、公用工程单元及储运单元，为避免控制功能过于集中、控制器负荷过大，可按照过程控制站的处理能力，根据控制、操作要求划分成几个控制区域。

7.2 过程接口单元

7.2.2 过载保护有两种：第一，信号超出工作范围，但仍在模件的正常承受能力内；第二，信号超出模件的正常承受能力，如果由于采用了过电压保护技术，模件不会发生电气损坏。因此，优先选用具有过电压保护技术的过载保护模件。

7.2.3 隔离的作用有三个：第一，提高信号输入端的共模抑制电压；第二，隔断信号的电连接，减少或避免过载电压；第三，隔离地电位，提高抗干扰能力。常用的隔离技术有：光电隔离、电磁隔离、电容隔离和继电器隔离。

I/O 模件的隔离方式分为通道隔离、组隔离。

通道隔离方式的输入与输出、信号与电源、通道之间是电气隔离的，电路是浮空的，通道之间、供电回路没有共用电路。

组隔离方式是将信号通道或供电回路分组，各组的输入与输出、信号与电源、通道组之间是电气隔离的，组内存在共用电路，共用电源、共用地以及共用模数/数模转换器。

7.2.4

b）三端子式是指 AI 卡的接线端子包括电源正、信号正和公共端三种端子。

7.2.5 AO 卡正向和反向输出功能是指，AO 卡应能通过组态设置改变 AO 卡输出信号的变化方向，如通过设置反向输出将输入 0~100%转换为输出 20mA~4mA 信号。

7.2.8 有源数字量输入信号是指由信号端的设备供电的信号，信号源的本质是电压信号；无源数字量输入信号是指信号端设备不对信号供电，而由数字量输入模件或信号接收端的电源设备供电，信号源的本质是“开关”信号。提倡采用能够直接触发的抗干扰型 DI，减少输入隔离继电器环节。若输入输出（I/O）模块的耐电压性能无法满足特定输入信号的电压等级要求（例如 220VDC），则应当采取增设继电器的措施来实现信号的电气隔离。

7.2.9 供电的数字量输出信号对于信号接收端就是有源数字量输入；非供电的数字量输出信号对于信号接收端就是无源数字量输入。提倡采用能够直接驱动的抗干扰型 DO，减少输出隔离继电器环节。

7.2.13

a） 根据本质安全电路的相关规定，本安与非本安的 I/O 模件不应混用。为避免 I/O 模件通道配电的混乱、减少配电失误、防止维护差错，本规范规定不同应用类型的 I/O 模件不应混用，即不同供电形式以及不同供电电压等级的 I/O 通道不应在同一模件中，应分为不同的 I/O 模件。

b） 高密度 I/O 模件元器件通道数量较多，I/O 模件故障影响范围较大，造成系统可用性降低。如果实际配置的 I/O 模件通道数量超过本条文中的要求，应按条文中通道数量的最高限定额使用。例如：64 通道的 DI 卡应当做 32 通道的 DI 卡使用。

7.2.16

a） AO 卡采用同步冗余是为了使 AO 卡在切换过程中输出保持一致，减少切换过程对工艺过程造成的干扰。

b） 用于控制回路的 I/O 模件采用冗余配置是为了提高系统的可用性，避免 I/O 模件故障维修期间对正常生产过程带来的影响。当多通道 I/O 模件不能冗余配置时（如某些产品的温度信号输入模件），按照需要点数的 2 倍配置可以减少模件修复时间，降低 I/O 模件密度，在一定程度上提高可用性。

c） 由于串联回路的失效率是回路中各个部件的失效率之和，因此除非串联的信号转换模件的失效率低于 DCS I/O 模件，否则采用信号转换模件串联冗余 I/O 模件的方式，不但增加了系统的配置成本，也会降低整个回路的可靠性。

d） 同一模件中的冗余电路仅仅是模件本身电路冗余的设计，并不是模件间的冗余，不能具备模件之间的冗余功能。冗余模件是指当工作模件发生故障时，由冗余模件代替工作模件的工作，继续完成原模件功能。在同一模件中具有冗余电路方式的模件不应视为冗余模件。

7.2.18

b） 远程 I/O 单元是过程控制站的重要组成部分，设计为可在远离中心控制区的位置进行安装。这些单元在功能上与普通 I/O 单元相同。为适应室外或苛刻环境条件，远程 I/O 单元通常安装在特制的防护箱内。远程 I/O 单元不应取代控制器完成核心功能，如控制算法的执行和复杂计算任务的处理。

h） 由于长距离输电会导致供电的电压下降和电能损耗，影响电能的传输效率和稳定性，增加用电安全的隐患，因此无论是 24VDC 还是 220VAC 都不应用于长距离供电。当远程 I/O 机箱距离现场机柜室/控制室超过 300 米时，宜在现场设置独立的 UPS 配电箱就近供电。

i） 可通过设置遮阳棚和散热片等方式对安装在室外的机箱进行防晒和降温；可采用 IP66 和 IP68 双重认证的机箱或采用限制呼吸型设计的机箱，以保证机箱内的湿度不受外界环境湿度变化的影响。

7.3 操作站

7.3.7

b） 每个操作分区或工艺装置配置 2 台操作站的目的是为了互为冗余，避免因为操作站故障影响工艺过程运行。互为冗余的操作站可不属于同一工艺装置、公用工程单元及储运单元，但应属于同一操作分区，应采用相同的组态。

7.4 工程师站

7.4.1 e） 工程师站应当专机专用，不应用作其他用途，其目的是为了系统安全和数据安全。

7.4.3 现场机柜室和中心控制室按操作分区配备工程师站的目的是减轻组态时人员与计算机的负荷、分散组态的风险，并且便于系统管理和组态维护。

7.4.4 现场机柜室的工程师站和现场操作站宜专机专用，对于较小的工艺装置、公用工程单元及储运单元，工艺流程操作较少、控制回路较少的情况，可以采用工程师站兼做临时现场操作站。

7.5 历史服务器

7.5.5 在工艺装置、公用工程单元及储运单元规模较小时，也可采用 DCS 的其他设备（如工程师、操作站）等同时兼做历史服务器，但每个历史服务器应存储该工艺装置、公用工程单元及储运单元完整的历史数据，其功能和配置还应同时符合本规范第 8.5 条的规定。

7.5.7 对于全厂规模或大型联合装置，可采用历史数据服务器（包括报警和事件记录）的方式存储历史数据。宜采用按操作分区分散配置数据库的方式，也可采用集中数据库冗余方式进行配置，备用数据库可存放在一台或多台设备中，与主数据库实时同步。

采用两台或多台历史数据服务器的方式存储历史数据是为了减轻存取负荷，降低服务器故障风险。采用数据库冗余方式是为了提高可靠性和安全性，同时也为了降低服务器故障风险。

7.5.8 虽然有些 DCS 的操作站和工程师站从功能上也可以兼做历史服务器，但这些工作站相对历史服务器更容易出现软硬件方面的功能失效，导致历史数据丢失，因此不应兼做历史服务器。

7.6 网络管理服务器

7.6.1 网络中的多台计算机有两种组合形式：区域（简称域）和工作组。一般情况下网络管理服务器兼做域服务器，对工作域的用户和设备进行管理。当采用工作组形式时，可不设置网络管理服务器。

7.6.2 对于单体装置的控制室，因网络管理服务器对硬件配置要求不高，不必单独设置。采用分散布置时，因整个 DCS 网络的用户、权限管理等信息需要统一管理，应在数据服务层设置专用的网络管理服务器，不应按照操作分区分别设置网络管理服务器。

7.8 供电要求

7.8.2 直流电是可以在相同电压时并联运行的，供电容量和电流是并联供电装置之和，可用于增加供电容量或冗余。当供电装置的等效内阻近似时，负荷近似分配，可以提高电源装置的寿命。但某些直流电源装置的输出端没有输出电压、电流调节电路，会使得负荷分配不均，甚至发生电压低的供电装置逆流，为此供应商采用二极管并联输出的方式。这种方式虽然可以避免逆流现象，但二极管压降会形成电能消耗并且发热，也不能避免负荷分配不均。所以本规范规定需要采用输出能够直接并联的直流电源装置品种和型号，不应采用附加并联模块的方式。直流电源装置 1：1 冗余是较好的方式，各负担 50%的电流容量，不应采用多台直流电源装置均分负载的方案。

8 网络系统

8.1 网络特性

8.1.2 过程控制层网络带宽是指设备间的网络通信带宽，不包括 I/O 总线带宽。

8.2 网络设备

8.2.1 网络数据服务器是某些型号 DCS 的过程控制网络配备的数据服务设备，不同型号 DCS 的网络数据服务器的功能和作用有所区别。某些型号的 DCS 不需要网络数据服务器。

c) 网络数据服务器提供操作监控直接相关的数据服务，可以根据功能不同采用 1 台或多台服务器。对于失效后不会影响到工艺装置的正常生产操作的其他数据服务器，可根据实际功能需要进行配置。

8.2.3

b) 位于不同位置的交换机对端口通信速率的要求也不同。交换机的端口速率应根据所在位置和应用进行选择。

交换机连接的方式有三种：

1) 级联方式

级联就是使用网线将多个交换机进行连接，连接后仍然是相对独立的交换机，优点是可以延长网络的距离，缺点是多个设备的级联会产生级联瓶颈。如果级联链路中的某个交换机发生故障，可能会导致整个网络中的通信中断。

2) 堆叠方式

堆叠是靠一个提供背板总线带宽的多口堆叠母模块与单口的堆叠子模块相联实现的。采用堆叠方式的交换机组可看做为一个整体，便于维护和管理。

3) 集群方式

集群技术将相互连接的多台交换机作为一个逻辑设备进行管理，从而降低网络管理成本，简化管理操作。

8.2.4 工业控制系统专用防火墙具备以下功能：

a） 具有应用协议控制、数据包过滤、访问控制、入侵检测和流量控制等功能。

b） 防火墙安全策略包含基于 MAC 地址、IP 地址、端口、协议类型的访问控制。

c） 过滤规则具备一致性检测机制，防止各条规则间互相冲突。

d） 防火墙支持常用工业通信协议，如 OPC、Modbus TCP、Profinet 等。

e） 防火墙能对通信协议进行深度内容检测，禁止不符合协议规约的通信。

f） 防火墙具有抗拒绝服务攻击的能力。

g） 防火墙具备网络地址转换（NAT）功能。

8.2.7

c） 光纤按的传输模式分为单模和多模。

在 10M/100Mbps 的以太网中，多模光纤最长可支持 2000 米的传输距离，在 1Gbps 千兆网中，多模光纤最长可支持 550 米的传输距离。单模光纤最大可支持 40 公里～3000 公里的传输距离。

多模光纤最小弯曲半径约为 GB/T 9771.1 标准 B1.1 类单模光纤的一半，应用成本低，但传输速率低、距离短，更适用于室内网络连接。

GB/T 9771.7 标准的 B6 类单模光纤为耐弯光纤，最小弯曲半径更小（5.0mm~10mm），但成本高，适用于作为 GB/T 9771.1 标准的 B1.1 类光纤入室后光缆分配盘后的尾纤。

8.3 网络负荷

网络负荷可以由网络监控站或相应的网络检测软件侦测出。

8.4 与第三方设备通信

8.4.2 不同 DCS 的通信接口的通信能力不同，通信量的计算方法和限制也不一样，可参考相应的通信接口规格。每个通信接口的通信量不宜过多。通信接口的使用应遵循产品手册，包括电气连接、电缆规格、接地方式、通信格式等。

8.4.4 与 DCS 功能无关的数据采用单独的通信模块进行数据传输，可以有效降低 DCS 控制器的通信负荷。

9 辅助设备

9.1 辅助操作台

辅助操作台可用作 DCS 的报警显示屏，可在屏幕上显示定义的报警画面，需要时也作为操作站使用。

9.4 其他辅助设备

本条仅规定安全栅、电涌防护器、继电器等辅助仪表在机柜内的供电与安装，其他事宜应按照设计和有关标准规定实施。

10 高级应用

10.1 智能设备管理系统

10.1.8 不同品牌的 DCS 的智能设备管理系统结构有所不同，数据服务器的配置也有所不同。设备数量较少的项目，在中心控制室配置一台服务器兼维护操作站即可。规模较大的项目，可在机柜室配备数据服务器兼维护操作站，同时在中心控制室配备总的数据服务器兼维护操作站。

10.3 过程数据服务

过程数据服务器用于高级应用或工厂管理网的过程数据接口，设置数据缓冲层并采用过程数据服务器传输数据的方式是提高过程控制网络安全的措施。过程数据服务器从历史服务器和实时数据服务器获取历史数据和实时数据，通信采用单向方式。过程数据服务器不直接与控制器交换数据，也不直接与 DCS 外部的网络或设备通信。当历史服务器支持实时数据服务功能时，不需要在操作监控层额外设置实时数据服务器用于与过程数据服务器之间的实时数据通信。

10.4 先进控制

典型的“先进控制”是多变量预测控制或模型控制。先进控制服务器是先进控制软件运行的硬件平台，有时根据需要会采用服务器/客户端结构。先进控制服务器用于过程数据的采集、处理以及控制算法的运行，并将运算结果输出到 DCS。先进控制客户端用于控制器的组态、建模、整定、分析和仿真，并将制定好的控制策略和算法下装到先进控制服务器中。

对于先进控制、油品调和等需要与过程控制网进行数据交换的第三方应用，采用实时数据服务器进行数据中转，将第三方设备与过程控制网进行隔离并设置边界防护，同时对实时数据服务器的软件、接口、进程、服务等设置安全防护策略，可以效降低第三方设备的安全风险。

10.5 储运管理

储运管理系统采用 DCS，集中处理储运系统的过程数据，主要完成储罐及与储罐密切关联的工艺过程的数据采集、信息处理、过程控制、安全报警及储罐液位、容量（质量）、密度计算等系统功能。

10.6 网页浏览服务

10.6.1 网页浏览服务器也称 Web 服务器，是应用数据服务器的一种，可以采集、存储 DCS 网络中的过程数据。经过授权的外部计算机可通过网页访问的方式，浏览网页浏览服务器中存储的操作数据和画面。

10.6.3 工厂网络不应随意向其他网络开放。同样，为了控制网络的安全，DCS 控制网也只能有限度地向工厂网传送数据，而且应有相应的防范措施。

10.8 其他高级应用

应用程序服务器是指本章未涉及的其他数据服务器，例如油品调和系统的应用程序服务器。

11 软件配置

11.1 控制和操作软件

11.1.1 DCS 配备的过程控制软件和操作软件的容量和控制点数应包括备用设备。

12 工程实施

12.1 系统开工会

DCS 系统开工会的举行标志着 DCS 的设计、制造、集成等工作的正式开始。DCS 的软件和硬件配置和规格在开工会后不应再修改，这意味着设计条件不应有本质上的变化。如果不能确定 DCS 的软件和硬件配置和规格的设计条件，则应待条件成熟时再举行开工会或采取相应的阶段式设计、制造和集成方式。

DCS 系统开工会的结束表示软、硬件等所有设备配置和数量的最终确定。

12.2 功能设计

功能设计的主要内容是制定 DCS 系统软件组态的基本规则，使软件组态的工作和风格统一，对于由 DCS 供货商组态以及多个设计单位共同参加的项目，功能设计对各方工作的统一协调很重要。

功能设计的实质是 DCS 设备集成和软件组态工作的统一规定。基础文件由 DCS 供货商编制，用户及设计单位根据项目的具体情况最终达成一致并批准实施。

鉴于历史数据采集的时间间隔通常长于实时数据的采集周期，为确保历史数据的准确性和可用性，在存储历史数据之前，必须对实时数据执行预处理操作，如计算时间间隔内实时数据的平均值、最大值、最小值等，旨在将处理后的实时数据高效、准确地存储为历史数据。预处理步骤旨在降低数据量，提取关键信息，并为后续分析和决策提供更加清晰和精确的数据支持。

12.3 组态

组态一般有两种方式：第一种方式是由用户和设计单位完成，DCS 供货商指导、检查，并对结果负责；第二种方式是由用户和设计单位提交相应的设计资料，并检查实际组态方案和效果，由 DCS 供货商完成组态，并对结果负责。

12.3.2 系统组态是在软件中完成组成系统的各设备的定义，用软件方式配置 DCS 的硬件构成。

12.3.3 功能组态是利用 DCS 本身的功能模块、控制算法和程序语言完成工艺过程的控制策略。

12.3.4 显示组态是在软件中绘制生产过程的操作、监视和控制的显示画面，并完成数据链接。过程显示画面包括概貌画面、流程图画面、控制组画面、操作面板画面、趋势画面以及报警一览表等。

12.3.5 报警功能是 DCS 最重要的操作和管理功能之一，包括报警分级、分组、分声音和显示方式等。报警功能及形式有屏幕提示和声光报警等。

12.4 系统集成

系统集成有两种情况：

第一种情况是 DCS 内部采用第三方设备，例如：直流电源、机柜、继电器等，这种情况的第三方设备是在 DCS 合同内的，是 DCS 功能必备的。第三方设备的责任直接由 DCS 供货商承担。

第二种情况是 DCS 设备与第三方设备关联，例如：安全栅、关联通信设备等。这种情况的第三方设备不是 DCS 功能必备的，不在 DCS 内部合同中，而是在 DCS 与用户的合同中，或在其他合同中。所以，DCS 供货商对第三方设备的性能没有直接责任，但通常对设备集成负有主要责任。

13 工厂验收及集成测试

13.1 工厂验收测试

根据组态工作方式和责任范围的不同，工厂验收的内容也有所不同。对于由用户和设计单位组态的方式，工厂验收测试只包括系统配置检查和系统硬件性能测试；对于由 DCS 供货商组态的方式，工厂验收测试包括系统配置检查、系统硬件性能测试和组态功能测试。

13.2 工厂集成测试

对于 DCS 与第三方设备的通信，应根据设备的具体情况，将通信设备或模拟通信设备运到 DCS 集成工厂进行实际通信测试。

对于不能在 DCS 制造厂测试的第三方设备，应在第三方设备制造厂进行测试。

14 工程服务

14.1 技术服务

14.1.1 DCS 是由仪表、计算机、网络通信的多种技术结合的高技术复杂产品，供货商的技术咨询服务是必不可少的，本规范不是招标文件，但有必要规定供货商的责任和义务，提示用户注意。

14.1.2 DCS 设备的技术和应用文件、资料很多，特别是在项目执行前后，需要相应的多次技术澄清，这是 DCS 供货商的工程服务内容之一。

14.1.3 在工厂验收和现场验收前，应由 DCS 供货商准备验收程序，提供相关的验收资料和工作记录文件，这是合同执行的重要内容。验收过程中，供货商还需要配备专门的工程技术人员配合验收工作，这也应该是合同规定的。

本规范对 DCS 供货商的规定，实际上是提示用户在合同中对供货商提出要求，完整地实施 DCS 应用工程。

工业和信息化部标准报批公示