ICS 25.040.01
P 72
备案号：J319-2004

SH

中华人民共和国石油化工行业标准

SH/T 3018—2003
代替 SH 3018—1990

石油化工安全仪表系统设计规范

Design code for safety instrumented system in petrochemical industry

2004-03-10 发布　　2004-07-01 实施

中华人民共和国国家发展和改革委员会　发布

目　次

前　言

本规范是根据原国家经贸委《关于下达 2002 年石化行业标准制修订项目计划的通知》（国经贸厅行业[2002]36 号）和中国石化建标[2003]94 号文的通知，由中国石化工程建设公司对原 SH 3018－1990（SHJ 18－90）《石油化工企业信号报警、联锁系统设计规范》进行修订，由中国石油化工集团公司工程建设管理部组织审定。

本规范共分 11 章和 1 个资料性附录。

本规范与 SH 3018－1990（SHJ 18－90）《石油化工企业信号报警、联锁系统设计规范》相比，主要变化：规范内容深度和广度作了较大部分调整，原规范为 5 章，本规范为 11 章。

本规范在实施过程中，如发现需修改或补充之处，请将意见和有关资料提供给主编单位（地址：北京市朝阳区亚运村安慧北里安园 21 号，邮政编码：100101），以便今后修订时参考。本规范由主编单位负责解释。

本规范主编单位：中国石化工程建设公司

主 要 起 草 人：黄步余　王建民　王玉华

石油化工安全仪表系统设计规范

1 范围

1.1 本规范适用于新建、改扩建石油化工装置(或工厂)安全仪表系统的工程设计。储运系统、公用工程及辅助设施等工程设计可参照执行。

1.2 安全仪表系统的工程设计必须满足石油化工装置(或工厂)安全度等级的要求。

1.3 相关标准如下:

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511 Functional safety: safety instrumented systems for the process industry sector

ANSI/ISA-84.01 Application of safety instrumented system for the process industries

DIN V 19250 Programmable safety system

IEC 61131 Programmable controller

1.4 执行本标准时,尚应符合国家现行有关强制性标准规范的要求。

2 术语和定义

下列术语和定义适用于本规范。

2.1

危险故障 dangerous failure

能够导致安全仪表系统处于危险或失去功能的故障。

2.2

安全故障 safe failure

不会导致安全仪表系统处于危险的故障。

2.3

安全仪表系统 safety instrumented system (SIS)

用仪表实现安全功能的系统。系统包括传感器,逻辑运算器,最终执行元件及相应软件等。

2.4

安全度等级 safety integrity level(SIL)

用于描述安全仪表系统安全综合评价的等级。

2.5

最终执行元件 final element

安全仪表系统的一部分,执行必要的动作,使过程达到安全状态。

2.6

逻辑运算器 logic solver

安全仪表系统或过程控制系统中完成一个或多个逻辑功能的部件。

2.7

可编程电子系统 programmable electronic system（PES）

由一个或多个可编程电子设备组成，用于控制、保护或监视的系统。

2.8

过程控制系统 process control system（PCS）

用于直接或间接控制过程及相关设备的控制系统。

2.9

冗余 redundancy

用多个相同的模块或部件实现特定功能或数据处理。

2.10

容错 fault tolerant

功能模块在出现故障或错误时，仍继续执行特定功能的能力。

2.11

表决 voting

用多数原则确定结论。

2.12

故障安全 fail to safe

安全仪表系统发生故障时，使被控制过程转入预定安全状态。

2.13

显性故障 overt fault

能够显示自身存在的故障。

2.14

隐性故障 covert fault

不能显示自身存在的故障。

2.15

平均故障间隔时间 mean time between failures(MTBF)

相邻故障间隔的平均时间（包括平均失效时间和平均修复时间）。

2.16

平均修复时间 mean time to repair(MTTR)

故障修复所需要的平均时间（包括诊断，确认及等待时间）。

2.17

平均失效时间 mean time to failure (MTTF)

功能单元实现规定功能失效平均时间。

2.18

可用性 availability(A)

系统可以使用工作时间的概率。

2.19

可靠性 reliability(R)

系统在规定的时间间隔内发生故障的概率。

2.20

传感器 sensor

用于测量过程变量的单一或组合设备。

3 基本原则

3.1 安全仪表系统独立于过程控制系统，独立完成安全保护功能。

3.2 当过程达到预定条件时，安全仪表系统动作，使被控制过程转入安全状态。

3.3 根据以下要求确定安全仪表系统的功能：对过程危险性及可操作性分析；人员、过程、设备及环境的保护；安全度等级。

3.4 安全仪表系统可按照安全度等级的要求分为1、2、3、4级。安全等级越高，安全仪表系统的安全功能越强。

3.5 安全仪表系统应设计成故障安全型。

3.6 安全仪表系统应具有硬件和软件诊断和测试功能。

3.7 安全仪表系统构成应使中间环节最少。

3.8 安全仪表系统的传感器、最终执行元件宜单独设置。

3.9 安全仪表系统应能与过程控制系统、工厂管理系统进行通信。

3.10 安全仪表系统宜提供独立于逻辑运算器的手动设施，直接操作最终执行元件。

3.11 当多个单元的保护功能在一套安全仪表系统内完成时，其共用部分应符合最高安全等级要求。

3.12 安全仪表系统的人机接口宜与过程控制系统相同。

4 传感器

4.1 传感器的独立设置原则

4.1.1 1级安全仪表系统，其传感器可与过程控制系统共用。

4.2.2 2级安全仪表系统，其传感器宜与过程控制系统分开。

4.2.3 3级安全仪表系统，其传感器应与过程控制系统分开。

4.2 传感器的冗余设置原则

4.2.1 1级安全仪表系统，可采用单一的传感器。

4.2.2 2级安全仪表系统，宜采用冗余的传感器。

4.2.3 3级安全仪表系统，应采用冗余的传感器。

4.3 传感器的冗余方式选用

4.3.1 当重点考虑系统的安全性时，应采用“或”逻辑结构。

4.3.2 当重点考虑系统的可用性时，应采用“与”逻辑结构。

4.3.3 当系统的安全性和可用性均需保障时，宜采用三取二逻辑结构。

4.4 安全仪表系统的传感器宜采用隔爆型。

5 最终执行元件

5.1 最终执行元件可以是安全仪表系统用的切断阀，与过程控制系统共用的控制阀或电动阀等。气动控制阀或气动切断阀均应带接受安全仪表系统控制信号的电磁阀。

5.2 阀门的独立设置原则

5.2.1 1级安全仪表系统，其阀门可与过程控制系统共用，应确保安全仪表系统优先于过程控制系统的动作。

5.2.2 2级安全仪表系统，其阀门宜与过程控制系统分开。

5.2.3 3级安全仪表系统，其阀门宜与过程控制系统分开。

5.3 阀门的冗余设置原则

5.3.1 1级安全仪表系统，可采用单一的阀门。

5.3.2 2级安全仪表系统，宜采用冗余的阀门，如采用单一的阀门，配套的电磁阀宜冗余配置。

5.3.3 3级安全仪表系统，宜采用冗余的阀门，配套的电磁阀宜冗余配置。

5.3.4 冗余配置的阀门，可采用一个控制阀和一个切断阀。

5.4 电磁阀的设置原则

5.4.1 控制阀上的电磁阀应安装在阀门定位器与执行机构之间。

5.4.2 电磁阀放空口应有防护措施。

5.4.3 当重点考虑系统的安全性时，冗余电磁阀宜采用与逻辑连接。

5.4.4 当重点考虑系统的可用性时，冗余电磁阀宜采用或逻辑连接。

5.4.5 电磁阀应采用长期带电型，电磁阀电源应由安全仪表系统提供。

5.4.6 安全仪表系统的电磁阀宜采用隔爆型。

5.5 电动阀的配置原则

5.5.1 安全仪表系统和过程控制系统可共用电动阀。

5.5.2 电动阀不采用冗余配置，必要时可采用冗余的接点接入电气控制回路。

6 逻辑运算器

6.1 安全仪表系统的逻辑运算器可由继电器系统或可编程序电子系统构成，也可由其混合构成。

6.2 逻辑运算器的技术选择原则

6.2.1 继电器系统

继电器系统用于输入输出点较少、逻辑功能简单的场合。

6.2.2 可编程序电子系统

a) 可编程序电子系统用于下列场合：

1) 输入输出点较多；

2) 逻辑功能复杂；

3) 与过程控制系统进行数据通信；

b) 可编程序电子系统可以是可编程序逻辑控制器(PLC)、分散型控制系统(DCS)或其它专用系统。

6.3 逻辑运算器的独立原则

6.3.1 1级安全仪表系统，其逻辑运算器宜与过程控制系统分开。

6.3.2 2级安全仪表系统，其逻辑运算器应与过程控制系统分开。

6.3.3 3级安全仪表系统，其逻辑运算器必须与过程控制系统分开。

6.4 逻辑运算器的冗余原则

6.4.1 1级安全仪表系统，可采用单一的逻辑运算器。

6.4.2 2级安全仪表系统，宜采用冗余或容错的逻辑运算器，其中央处理单元，电源单元，通信系统等应冗余配置，输入/输出模块宜冗余配置。

6.4.3 3级安全仪表系统，应采用冗余或容错的逻辑运算器，其中央处理单元，电源单元，输入/输出模块及通信系统等应冗余配置。

7 通信接口

7.1 安全仪表系统与工程师站通信可采用RS－232,RS－485/RS－422串行通信方式。

7.2 安全仪表系统管理网络可采用工业以太网通信方式。

7.3 安全仪表系统与过程控制系统通信可采用RS232,RS－485/RS－422串行通信方式；过程控制系统为主站，安全仪表系统为从站。

7.4 安全仪表系统负荷不应超过60%。

8 人机接口

8.1 操作站

8.1.1 操作站可采用过程控制系统操作站。

8.1.2 应确保操作站失效时，安全仪表系统的逻辑处理功能不会受到影响。

8.1.3 操作站不能修改安全仪表系统的编程软件。

8.2 辅助操作台

8.2.1 用于安装紧急停车按钮、开关、信号报警器等。

8.2.2 信号报警器宜采用一体化的闪光报警器。

8.2.3 灯光显示应采用闪光、平光或熄灭表示报警顺序的不同状态。

8.2.4 红色灯光表示越限报警或紧急状态；黄色灯光表示预报警；绿色灯光表示运转设备或过程变量正常。

8.2.5 宜选择区别第一信号记忆的闪光报警器（有顺序事件记录或历史记录的情况可不设置），信号报警顺序如表1所示。

表1 区别第一信号的闪光报警顺序

过程状态	第一信号的灯光显示	其余灯光显示	声响	备注
正常	不亮	不亮	不响	
第一信号输入	闪光	平光	响	其余信号输入
按确认按钮	闪光	平光	不响	
报警信号消失	不亮	不亮	不响	运行正常
按试验按钮	亮	亮	响	试验检查

8.2.6 一般信号报警采用 DCS/PLC 实现，重要报警除操作站上显示外，在辅助操作台上宜设置灯光显示。

8.2.7 紧急停车按钮宜采用红色，旁路开关宜采用黄色，确认按钮宜采用黑色，试验按钮宜采用白色。

8.3 工程师站

8.3.1 工程师站完成安全仪表系统编程组态及维护。

8.3.2 工程师站可采用台式 PC 机，也可采用便携式 PC 机。

9 过程接口

9.1 过程接口包括输入输出卡、顺序事件输入卡、配电器、安全栅、开关、继电器等关联设备。

9.2 输入输出卡应带光电或电磁隔离，每个通道应互相隔离，带故障诊断。

9.3 若采用三取二过程信号应分别接到三个不同的输入卡。

9.4 安全仪表系统不应采用现场总线通信方式。

9.5 输入输出卡相连接的传感器和最终执行元件应设计成故障安全型。

10 软件组态

10.1 软件组态

编程语言应符合 IEC 61131—3 工业标准。

10.2 软件组态的安全性

10.2.1 采用 PROM 或 EPROM 存储器存储应用软件，提供防止未被授权人员修改程序的功能。

10.2.2 软件应能在线修改及下载。

10.3 软件组态的审查

10.3.1 软件组态的程序应与逻辑图一致。

10.3.2 在系统投用前应对软件组态进行 100%的功能测试。

10.4 软件组态文件

10.4.1 功能逻辑图。

10.4.2 软件采用的主要参数及变量。

10.4.3 软件程序说明、用户手册、使用说明等。

11 工程设计

11.1 基础工程设计

11.1.1 根据安全度等级，确定安全仪表系统的功能和方案。

11.1.2 根据工艺安全功能说明或因果表、管道仪表流程图（P&ID），确定安全仪表系统逻辑功能图。

11.1.3 编制安全仪表系统规格书（参见附录 A）。

11.1.4 编制安全仪表系统硬件配置图。

11.2 详细工程设计

11.2.1 编制安全仪表系统规格书（参见附录 A）。

11.2.2 评审安全仪表系统报价书。

11.2.3 签订安全仪表系统合同及技术附件。

11.2.4 准备软件组态所需数据、工程图纸等文件。

11.3 应用软件组态、编译下载、调试投用

11.3.1 编制应用软件组态文件。

11.3.2 审查应用软件组态文件。

11.3.3 编译下载，工厂验收测试（FAT）。

11.3.4 现场安装、调试，验收测试（SAT）。

附 录 A
（资料性附录）
安全仪表系统规格书编制提纲

1 范围

1.1 概述
1.2 目标
1.3 系统组成

2 定义和缩写

2.1 定义
2.2 缩写

3 标准规范

3.1 国际、中国标准规范
3.2 工程规定
3.3 相关规格书

4 通用要求

4.1 系统环境
4.2 系统的可用性和可靠性
4.2 系统冗余
4.4 电源要求
4.5 接地
4.6 防雷保护
4.7 系统备件、负载和扩展要求
4.8 标准硬件和软件

5. 硬件要求

5.1 系统总貌
5.2 认证
5.3 中央处理器要求
5.4 存储器
5.5 输入输出模件要求
5.6 顺序事件记录
5.7 安全网络要求
5.8 标准规定

用 词 说 明

对本标准条文中要求执行严格程度不同的用词，说明如下：

（一）表示要求很严格、非这样做不可并具有法定责任时，用词为“必须”（must）；

（二）表示要准确地符合标准而应严格遵守时，用词为：

正面词采用“应”（shall）；

反面词采用“不应”或“不得”(shall not)。

（三）表示在几种可能性中推荐特别合适的一种，不提及也不排除其他可能性，或表示是首选的但未必是所要求的，或表示不赞成但也不禁止某种可能性时，用词为：

正面词采用“宜”(should)；

反面词采用“不宜” (should not)。

（四）表示在标准的界限内所允许的行动步骤时，用词为：

正面词采用“可”（may）；

反面词采用“不必”（need not）。

中华人民共和国石油化工行业标准

石油化工安全仪表系统设计规范

SH/T 3018—2003

条 文 说 明

2004 北 京

目　次

石油化工安全仪表系统设计规范

1 范围

1.2 安全仪表系统的工程设计包括基础工程设计、详细工程设计、安装和调试、预投运检查、投运操作及维护程序、修改或更新等。

1.3 安全仪表系统的工程设计，尚应符合现行 GB 50058－92《爆炸和火灾危险场所电力装置设计规范》，GB 3836－2000（IEC－60079－1990）《爆炸性气体环境用电设备》的有关规定。

1.4 IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.

主要用于安全仪表系统制造和供应商。

IEC 61511 Functional safety：safety instrumented systems for the process industry sector.

主要用于安全仪表系统设计、集成和用户。

2 术语和定义

主要参照 IEC 61511－1 General framework, definition, system, software, hardware requirement 进行编制的。

3 基本原则

3.1 安全仪表系统不同于批量控制、顺序控制及过程控制的工艺联锁。当过程变量越限，机械设备故障，系统本身故障或能源中断时，安全仪表系统能自动（必要时可手动）地完成预先设定的动作，使操作人员、工艺装置及环保转入安全状态。

安全仪表系统（SIS）也称为紧急停车系统（ESD）、安全停车系统（SSD）、安全联锁系统（SIS）或安全保护系统（SPS）。

安全仪表系统宜采用经权威机构认证的可编程序控制系统。

3.3 对过程危险性分析，设备及环境的保护要求，安全度等级确定不属于本规定的范围。

3.4 国外类似标准中将过程的危险或过程安全度进行了分级，如德国标准 DIN V19250 将过程危险定义为 8 级（AK1－AK8）；国际电工委员会 IEC61508 将过程安全度等级定义为 4 级（SIL1－SIL4）；美国国家标准学会/美国仪表学会 ANSI/ISA－S84.01 将过程安全度等级定义为 3 级（SIL1－SIL3）。IEC61508 定义的 SIL4 用于核工业。见附表Ⅰ、附表Ⅱ、附表Ⅲ。

附表Ⅰ　各种标准规范有关安全度等级划分对照表

IEC61508 SIL	ANSI/ISA S84.01 SIL	TÜV AK	DIN V19250
1	1	AK2、AK3	1、2
2	2	AK4	3、4
3	3	AK5、AK6	5、6
4	—	AK7、AK8	7、8

附表Ⅱ　安全仪表的性能要求（要求低的操作模式）

安全度等级	平均故障率	可 用 度
1	10^{-2}～10^{-1}	90.00%～99.00%
2	10^{-3}～10^{-2}	99.00%～99.90%
3	10^{-4}～10^{-3}	99.90%～99.99%

附表Ⅲ　安全仪表的性能要求（要求高或连续操作模式）

安全度等级	平均故障率	可 用 度
1	10^{-6}～10^{-5}	99.999 000 0%～99.999 900 0%
2	10^{-7}～10^{-6}	99.999 900 0%～99.999 990 0%
3	10^{-8}～10^{-7}	99.999 990 0%～99.999 999 0%

安全度等级的确定

1级：装置可能很少发生事故。如发生事故，对装置和产品有轻微的影响，不会立即造成环境污染和人员伤亡，经济损失不大。

2级：装置可能偶尔发生事故。如发生事故，对装置和产品有较大的影响，并有可能造成环境污染和人员伤亡，经济损失较大。

3级：装置可能经常发生事故。如发生事故，对装置和产品将造成严重的影响，并造成严重的环境污染和人员伤亡，经济损失严重。

4　传感器

4.1　传感器分开独立设置，指采用多台仪表将控制功能与安全联锁功能隔离，即安全仪表系统与过程

控制系统的实体分离。

4.2 传感器冗余设置，指采用多台仪表完成相同的功能，通过冗余提高系统的安全性。

不宜采用信号分配器，将模拟信号分别接到安全仪表系统和过程控制系统。

安全仪表系统和过程控制系统共用一个传感器时，宜采用安全仪表系统供电。

5 最终执行元件

最终执行元件（切断阀，电磁阀）是安全仪表系统中可靠性低的设备。由于安全仪表系统在正常工况时是静态的、被动的，系统输出不变，最终执行元件一直保持在原有的状态，很难确认最终执行元件是否有危险故障。在正常工况时过程控制系统是动态的、主动的，控制阀动作是随控制信号的变化而变化，不会长期停留在某一位置。因此，当符合安全度等级要求，可采用控制阀及配套的电磁阀作为安全仪表系统的最终执行元件。当安全度等级为3级时，可采用一台控制阀和一台切断阀串联连接作为安全仪表系统的最终执行元件。

6 逻辑运算器

6.2 继电器系统通常只能处理开关量信号，不宜用于要求故障安全场合。

6.2.2 安全仪表系统故障有两种：显性故障（安全故障）和隐性故障（危险故障），当系统出现显性故障时，可立即检测出，系统产生动作进入安全状态。显性故障不影响系统的安全性，影响系统的可用性。当系统出现隐性故障时，只能通过自动测试程序检测出，系统不能产生动作进入安全状态。显性故障影响系统的安全性，不影响系统的可用性。

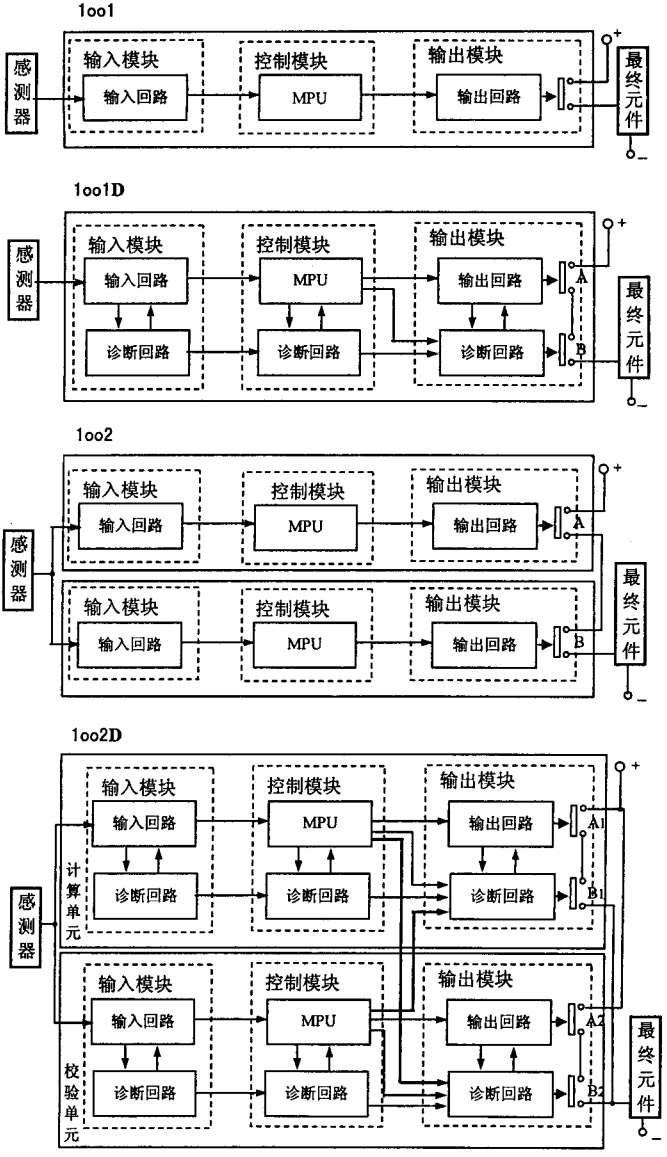
6.3 专用的控制系统(如透平机控制系统)中有保护功能和控制功能，该系统应符合安全度等级要求，宜采用容余或容错逻辑运算器。

6.4 安全仪表系统的逻辑运算器结构选择，见附表Ⅳ、附图Ⅰ。

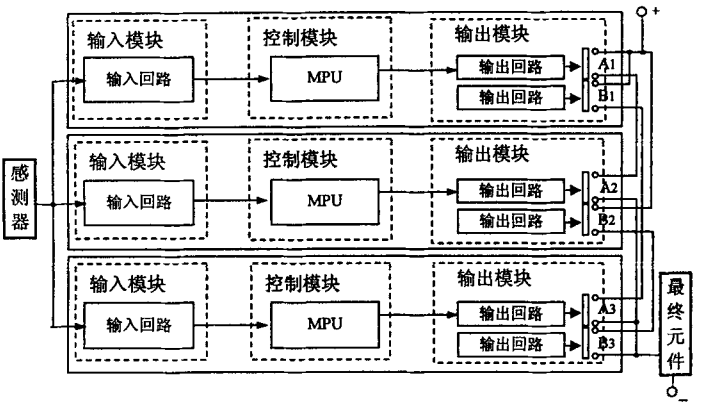
附表Ⅳ 安全仪表系统的逻辑运算器结构选择表

逻辑单元结构	IEC61508 SIL	TüV AK	DIN V19250
1oo1	1	AK2、AK3	1、2
1oo1D	2	AK4	3、4
1oo2	2	AK4	3、4
1oo2D	3	AK5、AK6	5、6
2oo3	3	AK5、AK6	5、6
2oo4D	3	AK5、AK6	5、6

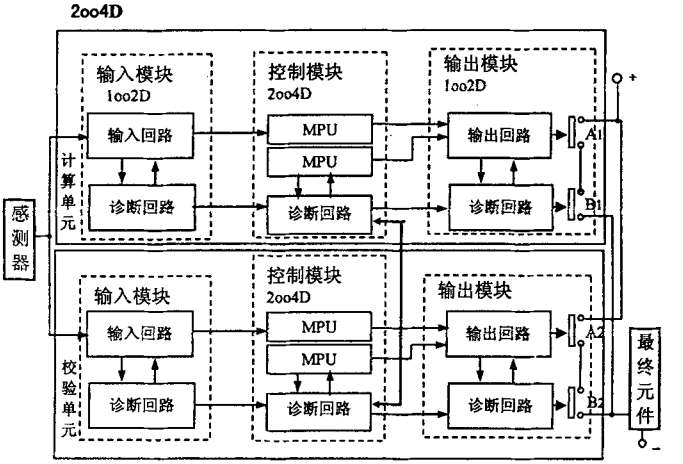
附图 I　安全仪表系统逻辑结构框图



2oo3



2oo4D



注 1：三取二 2oo3（2 out of 3）

系统故障时性能递减方式：3－2－0

采用三取二表决方式，即三个 CPU 中若一个运算结果与其它两个不同，该 CPU 故障，其余两个继续工作；若其余两个 CPU 运算结果再有不同时，则无法表示出哪一个是正确，系统停车。

注 2：二取一带自诊断 1oo2D（1 out of 2 with Diagnostic）

系统故障时性能递减方式：2－1－0

当一个 CPU 被检测出故障时，该 CPU 被切除，另一个 CPU 继续工作；若第二个 CPU 再被检测出故障时，

系统停车。

注 3：双重化二取一带自诊断 2oo4D（2 out of 4 with Diagnostic）

系统故障时性能递减方式：4—2—0

系统中二个控制模块各有二个 CPU，同时工作又相对独立。当一个控制模块中 CPU 被检测出故障时，该 CPU 被切除，切换到 2—0 工作方式；其余一个控制模块中二个 CPU 以 1oo2D 方式投入运行，若这一个控制模块中再有一个 CPU 被检测出故障时，系统停车。

7. 通信

7.1 通信是指安全仪表系统内部，安全仪表系统与过程控制系统之间，安全仪表系统与工厂管理系统之间的信息传输。

通常采用对安全仪表系统进行只读通信或带写保护的读/写通信。

8 人机接口

8.1 操作站是操作员与安全仪表系统之间信息通信的媒介，显示安全仪表系统有关状态信息。

8.2 辅助操作台是操作员与安全仪表系统之间通信的媒介。辅助操作台安装紧急停车按钮，开关及信号报警器等。

8.3 工程师站是维护工程师进行软件组态，编程、下载、测试诊断等的设备。

9 过程接口

9.3 当安全性为重点时，宜采用二取一配置；当可用性为重点时，宜采用二取二配置；当安全性和可用性均应保证时，宜采用三取二配置。

9.6 安全仪表系统宜采用 4mA～20mA DC 模拟信号，不采用现场总线、HART 或其它串行通信信号。