Safety Is of Paramount Importance

安全就是唯一

www.TSxPlus.com

GNS中山

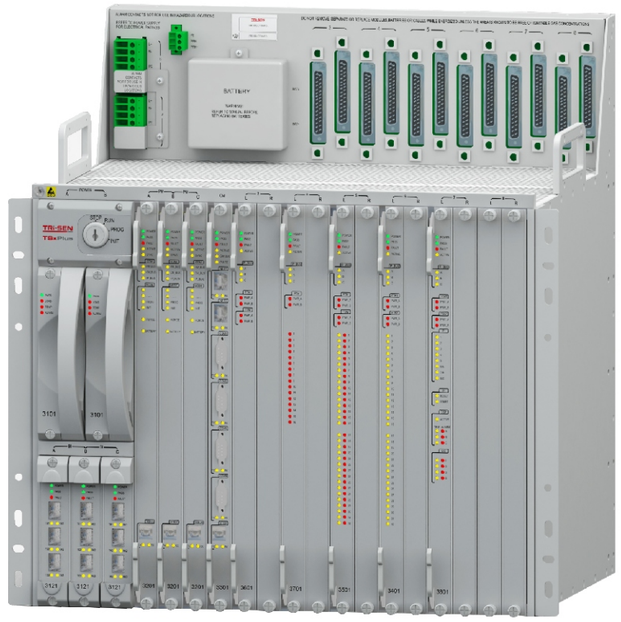
杭州中山电子工程有限公司

地址：杭州市西湖区西园一路8号3A幢六楼
电话：0571-89000880
传真：0571-89000887
专线：13958089945
邮件：sis@TSxPlus.com
微信：TSxPlus
Q Q：1489000880

GNS中山

TSxPlus

安全控制系统
产品样本



杭州中山电子工程有限公司

中山简介

杭州中山电子工程有限公司即原“杭州中山自动化成套工程有限公司”，以杭州龙山化工有限公司计量仪表室整体改制成立，信奉“科技兴中，立信为山”作为公司行为准则。

GNS中山　　龙山化工

十多年来，中山公司服务于集散控制系统工程，自动化仪器仪表工程，自动化成套。主要承接了DCS\PLC\SCADA\SIS系统安装、调试，仪器仪表安装、调试，控制柜成套等业务。

2012年3月对公司进行重组，并更名为“杭州中山电子工程有限公司”，精准定位做“您身边的安全自动化专家”，专注于安全自动化技术、服务及平台解决方案供应商。同时提供工业自动化、建筑智能化、工厂信息化等技术、服务及平台解决方案；自动化系统、仪器仪表、工业防爆、工业监控、工业广播等成套设备供应商。业务涉及医药生产、精细化工、水务、智能楼宇、弱电监控等行业。

中山公司在工业自动化领域秉持“科技兴中”的初心，以成为全球顶尖的“自动化服务器”的愿景，铸造“技术、服务、平台”为基石的自动化全生态体系。专注于本地化服务，强化“Gold Nonstop Service 服务无止境”理念。注重产品、服务及解决方案的专业性、适用性、实用性。通过对工艺的深度解读、专家级风险评估、纵深产品优选、专业工程经验，最终为您提供量身定制的自动化技术、服务及平台解决方案。

近几年，中山公司重点推出以TSxPlus系统为平台开发的安全技术产品，主要针对SIS、ESD、FGS、ITCC、IGCC、DEH、BMS、HIPPS等关键设备控制的全系列解决方案。我们奉行“Safety Is of Paramount Importance 安全就是唯一”

面临挑战

更好的兼顾安全性和可用性

不同于工厂自动化中的功能安全应用，过程自动化中的安全仪表系统（简称“SIS”）关注系统可用性的程度不亚于系统安全性。一旦由于系统本身故障导致误停车，将带来重大经济损失。如何降低系统自身故障导致的误停车概率，同时在系统降级后维持安全回路的安全等级不变一直是供应商在系统设计时重点考虑的问题。

预测性维护

传统工厂主要采用事后控制的方式来解决设备维护问题，即在故障出现后及时解决。由于流程行业的工艺特点，一旦非计划停车就会造成巨大的经济损失，因此，如何实现预测性维护，减少非计划停车就成了用户现实而迫切的需求。

信息安全

基于以下原因，工业控制领域的信息安全形势日益恶化：

■更多的工控系统正受到网络攻击；

■工控技术越来越多使用标准的IT技术（比如OS、Ethernet、WiFi）；

■供应商通过网络直接对现场设备进行访问正变成系统维护的标准方式，这给恶意软件和非授权访问等带来了新的传播途径；

安全系统由于本身的重要性，当受到网络安全威胁时往往会带来更大的人员财产损失和名誉损失。

安全功能的集成

响应时间是安全功能的关键属性之一，不同的安全功能对于响应时间的要求是不同的，这取决于被保护对象允许的从触发保护阈值到保护输出起效之间的最长时间。

当装置或设备中的安全功能存在不同的响应时间要求时，供应商需要评估这些安全功能能否在一套系统中实现。很多情况下，为了确保响应时间短的安全功能在两套系统中实现，这对终端用户来讲往往会带来额外的成本支出。

TÜVRheinland CERTIFIED　　TSxPlus SIL3

Safety Is of Paramount Importance
安全就是唯一

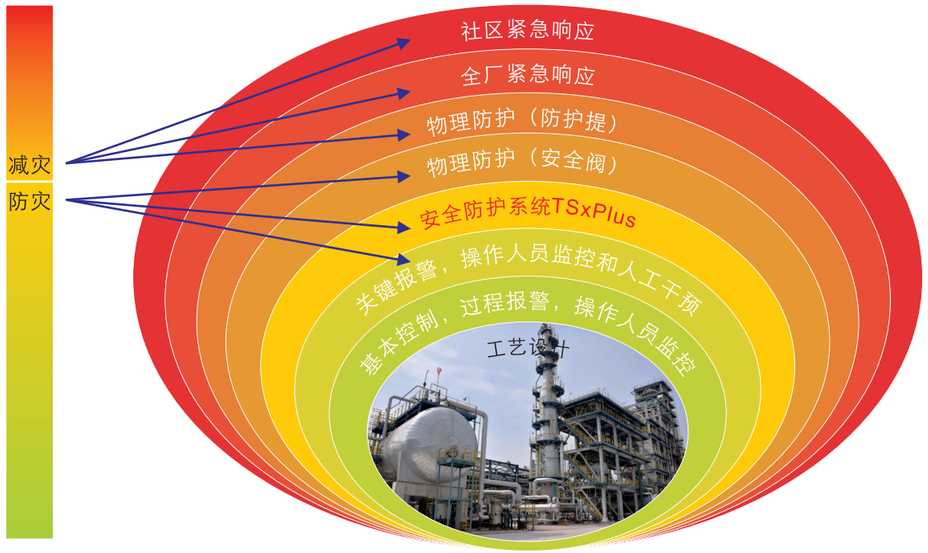
符合IEC和ISCI标准的国际信息安全认证

除了莱茵TUV的SIL3等级功能安全认证外，还拥有莱茵TUV和ISASecure EDSA 双重信息安全认证，符合最新版IEC62443和EDSA标准要求。

信息安全技术要求

功能安全系统和关键控制系统中的信息安全漏洞一旦被利用，可能造成的经济财产损失会更大，因此在取得功能安全认证的同时还应取得国际上权威第三方机构的信息安全认证，这可以进一步帮助用户降低风险。

信息安全和功能安全联合认证



支持快速回路和慢速回路集成运行

安全级的操作系统内核支持真正的多任务运行，快慢任务周期可任意设置。快任务的运行周期最快可设置为5ms。将快速安全回路和慢速安全回路集成在同一套系统中可有效降低终端用户的初始投入成本和后期维护成本。

产品特色

3-2-1-0降级模式

无论主控制器还是I/O部分，全部支持3-2-1-0降级模式，最大程度提升安全回路的可用性。同时，3-2降级后可维持SIL等级不变，无维修时间要求，最大程度降低安全回路输出拒动的风险。

针对机组应用的优化设计

根据API 670标准和国家安全监督总局“安监总管三【2014】116号”文件要求，机组的控制部分和保护部分应物理上相互独立，避免由于两者耦合过多造成控制功能和保护功能同时失效。为此，系统中设计了独立闭环运行的超速保护模块（简称“OSP”）执行保护功能，OSP的运行不受系统中其他组成部分的影响，自成闭环回路，周期性上报自身运行状态供上位机显示。

此外，系统提供适用于不同机组类型的专业库函数，确保顺利开车和机组平稳运行。

更可靠的扩展通讯方式

机架间的通讯扩展采用光纤通讯的方式，光信号与电信号相比有更好的抗电磁干扰能力，可以实现更可靠的通讯传输，从而提高系统的可用性。光信号的其他优势还体现在高速、远距离传输，无需区分本地机架和远程机架，系统的集中式和分布式布置可根据实际应用需要灵活设计方案。

支持供电质量监测

机架内供电电源可实时监控网络电能质量，并将监控结果存储在非易失性存储器中。主控制器周期性读取监控结果并可在上位机显示。当由于供电质量原因导致系统故障时，监测结果有助于故障的追根溯源。被监测的参数包括：最大输入电压，瞬态脉冲次数等。

支持智能仪表通讯功能

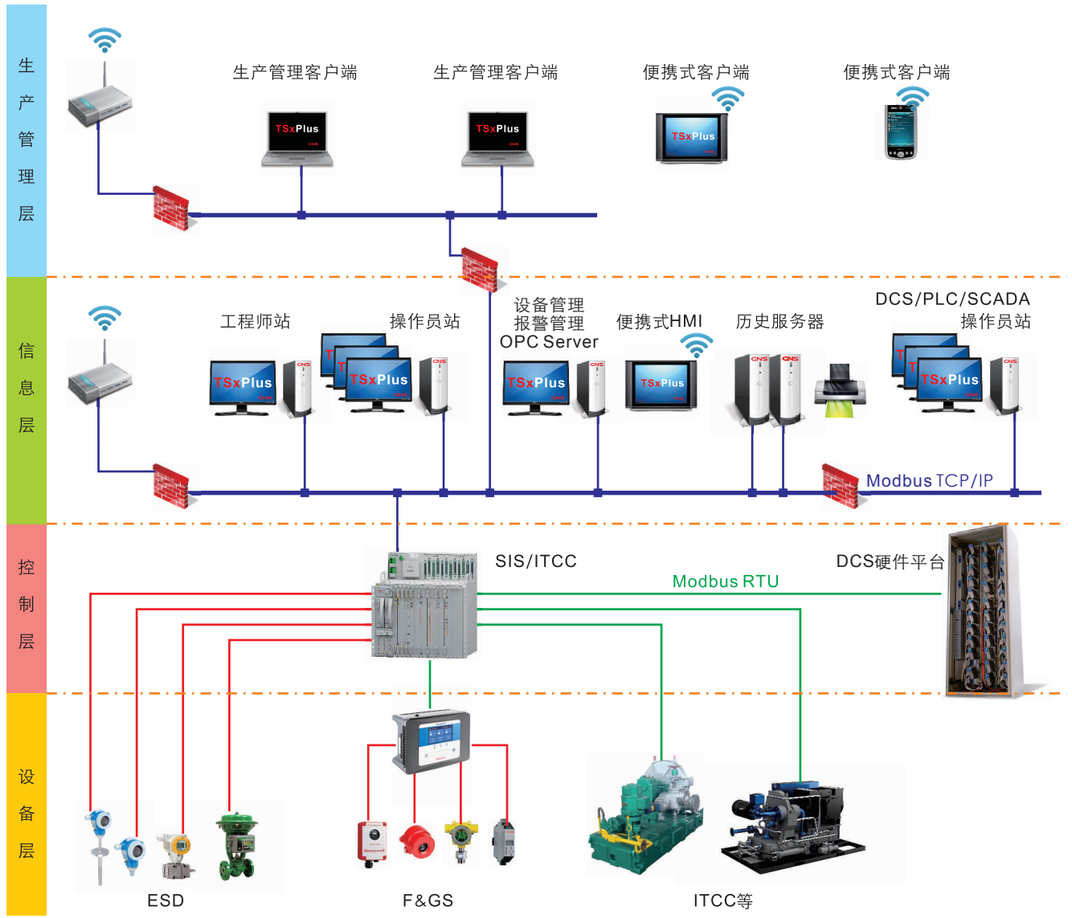
模拟量模块可直接连接HART智能仪表。硬件模块内部支持HART协议解析，通过复用卡件自身与主控制器通讯的链路来传输HART命令，HART信号分配与协议转换和系统物理上融为一体。

支持远程诊断与预测性维护

远程诊断通过在线收集系统监测的关键数据，并利用大数据分析技术对不同应用项目中类似应用的数据进行挖掘，可以更快速准确的定位故障，节省用户的维护成本，同时提高维护的时效性。

预测性维护通过帮助工厂的运营管理人员制定和实现高效的维护方案，可显著提高工厂重要资产的寿命，明显降低非计划停车的概率，给工厂的运营者带来更大收益。

系统总貌



如图中所示，产品方案主要包括工厂控制层的硬件平台和工厂信息层的软件平台两大部分。硬件平台从设备层获取输入数据，经过处理将控制信号输出到设备层。硬件平台的组成和逻辑由软件平台配置实现，硬件平台的运行状态和数据也会上传到软件平台显示和管理，必要时软件平台可以提供实时的下行数据通道控制硬件平台的运行。

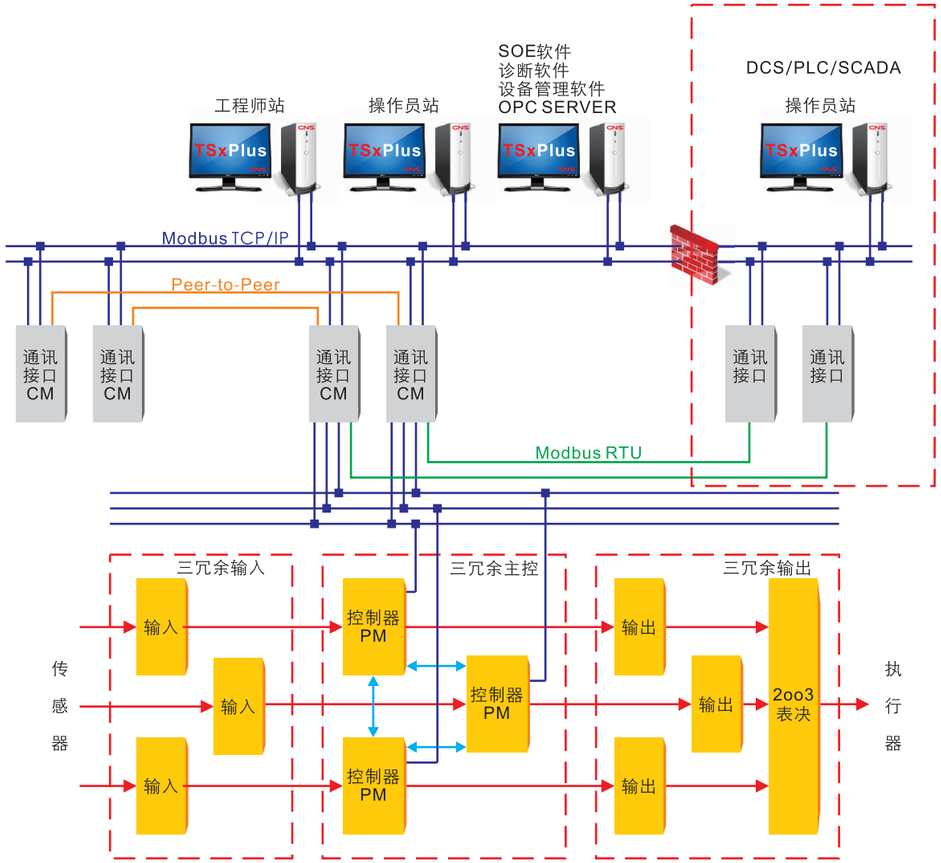
系统介绍

符合标准

标准分类	标准编号
功能安全	IEC 61508 Parts 1-7 IEC 61511 Parts 1-3
信息安全	IEC 62443-3-3 IEC 62443-4-1 IEC 62443-4-2 ISASecure EDSA 311 ISASecure EDSA 312
防爆	EN 60079-15 (Zone2,nA,IIC,T4) EN61010-1 ISA 12.12.01(Class I,Division 2,T4,Groups A,B,C,D)。
防腐蚀	ANSI/ISA-S 71.04（G3等级）
应用标准	API670 NFPA72 EN54-2 EN298 NFPA85 NFPA86 EN230 EN50130-4
EMC/EMI标准	EN 61000-6-2 EN 61000-6-4 EN 61326-3-1。

系统硬件

硬件采用完全的三冗余架构，包括输入模块、主处理器模块和输出模块。三冗余架构、高质量自诊断、3-2-1-0降级模式、单系独立物理卡件、简单易用性等多方面的结合带来了高安全性、高可用性和高维护性的有机融合。



系统介绍

系统主要特性指标

TSxPlus是基于硬件容错安全控制技术的逻辑与过程控制系统，为确保最高可能的系统完整性，系统包括如下特性：

TMR架构；

支持3-2-1-0降级模式；

可承受严酷的工业环境；

系统正常运行中可进行模块级现场安装和维护，更换I/O不需拆卸现场接线；

目标应用为安全完整性等级SIL3及以下的过程控制应用，如ESD、BMS、FGS、HIPPS、ETS等安全相关应用，及ITCC等复杂过程控制应用；

最多支持64个控制站。单控制站在最大规模配置情况下，最多支持16个PC软件（包括工程师站、操作员站、SOE站、诊断站等）。单控制站最多支持1个主机架加14个扩展机架。主机架中最多支持安装4个通讯模块，最大支持118对I/O。单控制站硬件测点开关量点最大支持3776点，模拟量点最大支持1248点；

支持远程扩展机架互连，单模SFP光模块可以支持传输距离达到20Km，多模SFP光模块可以支持传输距离达到2Km；

提供控制站与第三方系统通讯的RTU/ASCII master/slave 及Modbus TCP Server/Client接口；

使用Architect系列软件进行控制程序的开发及调试；

提供智能化输入输出模块降低了PM的负荷。每个I/O包括三个MCU，输入模块MCU对信号进行转换处理，并能诊断模块自身硬件故障。输出模块MCU对三系输出数据进行处理，提供给硬件表决电路，并对回读检测结果进行判断，进行最终输出的确认，并对现场连线进行诊断；

OSP配合FTA，既可实现独立的工业旋转设备的超速保护（OSP）功能，也可实现脉冲量输入（PI）采集功能。超速保护（OSP）功能可独立实现无需PM参与；

PM支持在线更换，更换后的PM会自动从其他工作PM上同步工程、运行数据及运行状态，同步完成后，新PM自动运行；

系统在三系或两系PM运行时可满足SIL3要求；

冗余I/O支持无扰切换，不影响现场设备正常运行。

系统重要特性指标

容错是系统的重要特性，它是系统能诊断到故障并采取必要措施的能力。采用故障容错技术，可有效提升系统及被控过程的安全性和可用性。

系统采用TMR安全架构，除电源模块为双重冗余架构外，PM及I/O均包含独立三系。三系并行，每系可独立执行控制程序。DI/AI/TMR-PI从现场采集信号后分配到三重化的输入通道，发送给三系PM进行表决；DO/OSP-DO从三系PM接收输出数据，通过硬件表决电路得到表决后的输出信号；AO三冗余现场侧通道合路后对外输出，采用切换式输出方式，即任一时刻仅有一系通道电路输出电流，另外两系不输出。OSP-PI通道电路共3路，每路对应一个现场探头，三路OSP-PI信号分别送入三系系统侧电路，组成三冗余信号处理电路。

系统具有多种故障诊断与报警功能，系统诊断到故障后，模块指示灯会显示故障状态，也可在上位机显示故障报警信息。用户可根据诊断信息采取纠正或维修措施。

系统架构

主机架提供2个系统PW槽位、3个BI槽位、3个PM槽位、1个CM专用槽位和12个（6对冗余）I/O槽位。主机架中I/O和CM共用I/O槽位，主机架中最多支持安装4个CM。主机架底板提供IP_BUS、PM_BUS、CM_BUS通讯链路，以实现各模块之间的通信互连。主机架底板上提供I/O与端子板之间互连的接口。扩展机架提供2个系统PW槽位、3个BI槽位、16个（8对冗余）I/O槽位。

系统介绍

系统架构说明

每个机架内配备两个冗余的PW，分别经过机架底板独立的输入端子，每个电源均可支持机架内系统侧电源要求。PW具备输出过压和过流保护。

系统包括三个独立的PM，三系并行，独立执行控制程序。作为IP_BUS协议主站，从AI、DI和PI获取现场数据，经过运算和2oo3表决后，将输出到现场的数据发送给DO或AO。

每个AI包括独立的三系，每系读取输入数据，进行处理通过IP_BUS发送给本系PM。AO三系分别从三系PM收到输出数据。三系中只有一系输出电流，电流回读诊断电路对通道电路进行诊断。

每个DI包括独立的三系，每系读取输入数据，进行处理通过IP_BUS发送给本系PM。DI仅支持NC信号为安全应用。

DO三系MCU分别从三系PM获取输出数据，执行表决，用于对4个输出开关进行控制。4个输出开关搭成硬件表决电路，表决后的结果通过FTA输出到现场执行单元。OSP用于超速防护功能时，支持3路OSP-PI输入，4路OSP-DO输出及2路非安全OSP-DI输入。

OSP-PI支持磁阻探头，有源探头，涡流探头三种信号。来自现场三个探头的PI信号通过FTA送入OSP-PI，3路OSP-PI信号分别进入三系系统侧电路。

FTA 被用来连接现场设备，输入模块配合FTA可完成输入信号的采集，输出模块配合FTA可实现信号输出功能。

Cm完成控制站与上位机软件之间的通讯，控制站之间安全通讯的黑通道，控制站与第三方控制系统之间的通讯。CM具备校时功能，根据外部时间源的校时信息校准本地系统时间，然后通过CM_BUS校准PM的系统时间。

每个CM支持2个Ethernet接口和4个串口。Ethernet接口可被配置为System Net与上位机软件进行通讯，或者可配置为Safety Net与其他控制站通讯，或者配置成Modbus TCP与第三方控制系统进行通讯。串口可配置为Modbus RTU/ASCII与第三方控制系统通讯。

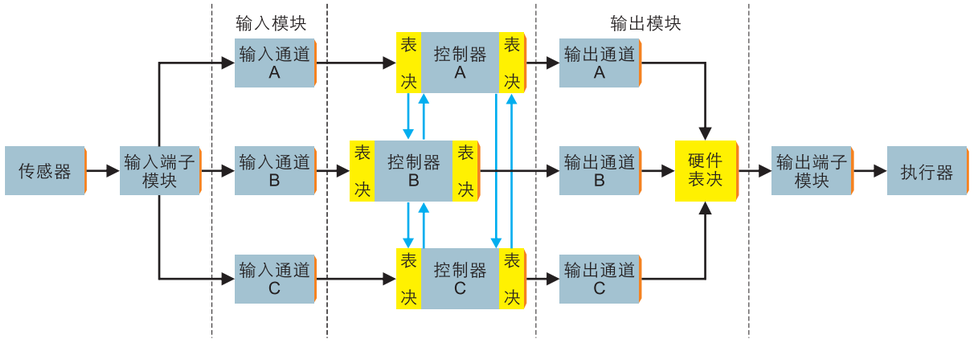
BI作为IP_BUS通讯链路的中继模块，机架内每条IP_BUS链路对应一块BI模块。机架内部通过背板总线互连，机架间通过光纤互连。BI模块提供3个SFP光模块，支持星型连接和总线型连接。

主控制器数据流

每个I/O包括独立的三系，输入模块每系读取输入数据，通过IP_BUS发送给本系PM。三系PM通过PM_BUS交换输入数据，从而每系PM都得到三份输入数据，每系PM分别对三份输入数据进行表决，表决得到的结果用于用户程序的运算，分别得到每系的输出数据。

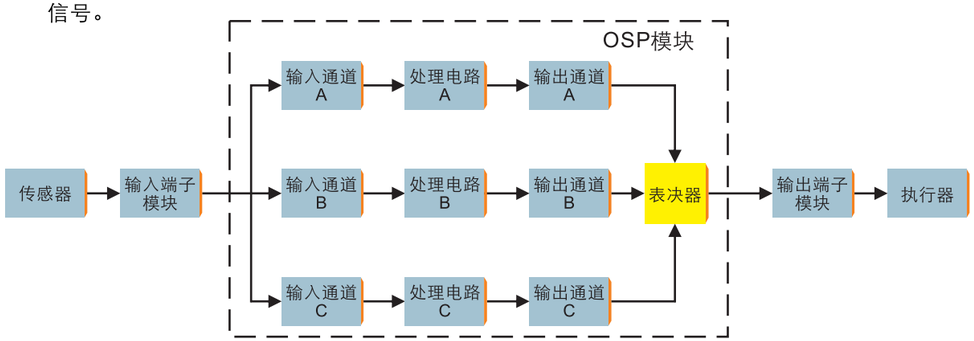
每系PM分别将本系输出数据通过IP_BUS发送给DO，DO将三系输出数据转化为三系输出信号，通过硬件表决电路，得到表决后的输出信号。

AO从三系PM收到三份输出数据后，将数字量信号转换为模拟量信号。三系采用切换式输出方式，即任一时刻仅有一系输出电流，另外两系不输出。



OSP数据流

来自现场传感器/变送器的三系输入信号通过OSP端子板的传输，分别送到OSP的三系输入通道电路，输入信号被处理分别送到三系MCU，每系MCU分别将本系输入数据用于用户程序的运算，分别得到每系的输出数据，每系MCU分别将本系输出数据发送给本系输出通道电路，输出通道电路分别对三系数据进行处理，通过硬件表决电路，得到表决后的输出信号。



系统介绍

硬件部件列表

硬件名称	型号	规格
主机架	MC01	220VAC输入（宽电压输入），24VDC输出 2个供电电源专用槽位； 3个主处理模块专用槽位； 3个总线接口模块专用槽位； 最多支持4个通讯模块，其中3个通讯模块槽位 与I/O槽位通用； 最多支持12个I/O槽位。
扩展机架	EC01	2个供电电源专用槽位； 3个总线接口模块专用槽位； 最多支持16个I/O槽位。
机架电源	PW01	1+1冗余配置，单电源功率（240W满足整机架内负荷）； 冗余电源分别独立输入到被供电模块； 供电质量检测功能（过压值、过压次数、瞬态脉冲次数）； 掉电保持时间＞50ms@24V 10A； 支持机架故障指示； 支持高温报警指示
主控制器	PM01	Power PC双核处理器，800MHZ主频，带浮点协处理器； 512MBytes内存，独立ECC内存； 32MBytes用户工程存储空间，32位CRC保护； 内部通讯总线数据吞吐量100Mbps。
通讯模块	CM01	内置防火墙； Power PC双核处理器，800MHZ主频，带浮点协处理器； 512MBytes内存，独立ECC内存； 64MBytes非易失存储空间，32位CRC保护； 冗余1000M以太网，支持MODBUS-TCP协议， 支持Peer-to-peer通讯； 支持MODBUS-RTU协议，最多支持单卡4个DB9接口通讯。
总线接口模块	BI01	3组光纤接口，可灵活实现总线拓扑和星形拓扑； 最大传输距离20km。

系统介绍

硬件部件列表

硬件名称	型号	规格
数字量输入模块	DI3201	32位双核SIL3等级安全CPU,180MHz主频； 单卡32通道，TMR架构； 支持硬SOE功能，分辨率1ms; 支持现场接线故障诊断。
模拟量输入模块	AI3281	32位双核SIL3等级安全CPU,180MHz主频； 单卡32通道，TMR架构； 允许输入信号范围0～22mA,采集精度0.15%; 通道支持HART协议； 支持硬SOE功能； 支持通道断线和短路故障诊断。
数字量输出模块	DO3201	32位双核SIL3等级安全CPU,180MHz主频； 单卡32通道，TMR架构； 输出硬件表决； 单通道最大2A驱动能力； 支持输入状态回读并指示灯显示； 支持通道断线、短路和过载故障诊断。
模拟量输出模块	AO1681	32位双核SIL3等级安全CPU,180MHz主频； 单卡16通道，TMR架构； 允许输出信号范围0～22mA,输出精度0.2%; 通道支持HART协议； 支持通道断线和过载故障诊断。
超速保护模块	OSP01	32位双核SIL3等级安全CPU,180MHz主频； 超速保护功能响应时间＜12ms; 8通道脉冲输入（PI）,支持无源磁阻探头、有源逼近探头、涡流探头，支持差分电压信号和单端电压信号； PI通道支持计数功能，支持方向检测； 4通道数字量输出（DO）,单通道最大2A驱动能力； 2通道数字量输入(DI)。

软件部件列表

软件名称	功能简介
组态软件 Architect	符合IEC61131-2标准，支持标准的LD、FBD和ST编程语言； 同一项目支持多个控制站和用户库工程同时组态； 控制站支持多任务组态，每个任务可单独下装及调试； 支持无忧增量下装； 独立的仿真软件完美仿真硬件平台，支持并发多站仿真； 图形化组态风格，直观易用。
诊断软件 Architect_Monitor	全方位的硬件监视，包含状态、故障、版本等； 实时监视系统运行状态，包括版本、轮询时间、内存占用等。
顺序事件管理软件 Architect_Event	强大事件管理能力； 支持单控制站级别事件收集和管理； 支持软、硬实时SOE事件分类与筛选； 支持快照功能。
设备管理软件 Architect_AMS	HART智能仪表的参数设置、状态监测及诊断。
OPC Server Architect_Server	同时支持OPC DA和OPC UA； 支持组态软件点表直接导入； 支持冗余切换； 支持从多个控制站读/写数据。
HMI软件 TriView	基于Windows平台的一站式可视化软件; 为工业安全领域提供完备的监控与数据采集功能； 涵盖单用户系统，多用户系统直到由冗余、客户机/服务器和浏览器/服务器构架组成的复杂的分布式系统； 具有可扩展、开放、灵活的特点。

SIS

安全仪表系统，Safety Instrumented System，简称SIS；又称为安全联锁系统（Safety InterLocking System）。主要为工厂控制系统中报警和联锁部分，对控制系统中检测的结果实施报警动作或调节或停机控制，是工厂企业自动控制中的重要组成部分。

安全仪表系统包括传感器、逻辑运算器和最终执行元件，即检测单元、控制单元和执行单元。SIS系统可以监测生产过程中出现的或者潜伏的危险，发出告警信息或直接执行预定程序，立即进入操作，防止事故的发生、降低事故带来的危害及其影响。

ESD

ESD紧急停车系统（Emergency Shutdown System），是为生产过程的安全而设置的，它适用于高温、高压、易燃、易爆等连续性生产作业领域。当生产过程出现意外波动或紧急情况需要采取某些动作或停车时，该系统能精确监测，并及时、准确地做出响应，使装置停在一定的安全水平上，确保装置和人身的安全。

ESD和DCS是完全分离的。DCS主要用于过程工业参数指标的动态控制。在正常情况下，DCS动态监控着生产过程的连续运行，保证能生产出符合要求的优良产品。而ESD则是对于一些关键的工艺及设备参数进行连续的监测，在正常情况下ESD是“静止的”，不采取任何动作。但是当参数发生异常波动或故障时，它会按照已定的程序采取相应的安全动作，使装置停在安全水平线上。所以ESD和DCS在过程工业中所起的作用不同，既有分工，又成互补关系。同时，ESD也不单是实现联锁关系，它应该凌驾于生产过程控制之上，具有独立性，这样降低了两者同时失效的概率。

应用说明

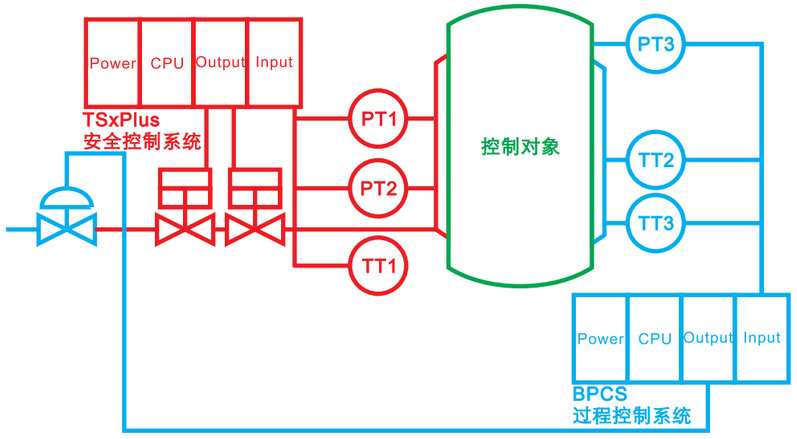
FGS

FGS是火灾报警和气体检测系统（Fire Alarm and Gas Detector System）的简称。FGS是针对火灾和气体探测的安全管理系统，通过对化工装置现场的消防按钮、烟、火、可燃气体、有毒气体的检测信号的采集，经过软件逻辑输出来控制报警灯、报警铃、雨淋阀、泡沫阀以及空调系统的新风入口阀等。

国内和国际上的大项目一般都会采用专用安全系统生产厂家的设备设置独立的火气系统，从而与SIS系统一起构成一体化的工厂综合安全系统。

其他

TSxPlus平台还针对ITCC、IGCC、DEH、BMS、HIPPS等关键设备控制提供安全技术解决方案。



服务体系

我们中山公司提出完整的生命周期服务理念，确保设计、工程、试运行、投运、跟踪一站式服务的质量在项目解决方案具体实施过程中降低了验证的成本。

完整的生命周期程序

计划和定义

- 可行性研究
- URS协助
- 验证审计
- 标准协助

设计和开发

- 开放性整体自动化解决方案
- 全部工程数据管理
- 先进控制系统
- 测试

工程实施和现场服务

- 设备采购
- 技术培训及交底
- 现场安装调试服务

试运行和鉴定

- 现场培训
- 试运行服务
- IQ/OQ/PQ等验证支持

正在进行的操作和生产投运

- 生产投运保障服务
- 项目归档和系统备份
- 服务等级协议

跟踪回访和终身维护

- 备份管理
- 备份和灾难恢复
- 定期和不定期跟踪检查协助
- 变更管理服务

服务保障体系

- 长期的相关优质产品合作伙伴
- 完整的服务程序
- 质量工程服务
- 专家应用技术的共享
- 工业级、专业级、可扩展的整体解决方案

项目流程