



安全技术的发展 及安全产品对比分析

中国工控网 (www.gongkong.com)

安全技术的发展

今天, 安全技术经常应用于许多不同的领域, 比如机器制造、运输系统、过程工业和建筑领域。这意味着人员的健康和安全的、工厂设备的正常运行、生产环境的保护都依靠实现安全技术的自动控制系统。虽然一个完整设备或系统的安全技术水平会根据特殊的应用而不同, 但安全系统总是由一系列传感器、安全控制单元和用于安全停车的执行器组成。

过去, 根据是否功能安全, 一个设备或系统所采用的技术可分为标准技术和安全相关技术, 这两者是严格分开的。通常, 不同的工程技术和工具被用于这两个层次。这不仅导致较高的人员培训成本, 同时在这许多时候这两个层次不能以适当的方式连接起来。现在的安全技术不再基于独立于标准控制系统以外的硬连线安全控

制系统, 而是在同一总线上传送标准的数据和安全相关的信息。这样不仅节约了用于诊断和反馈信号的配线成本, 同时在整个系统中同一标准工程工具和方法的使用保证了系统在设计、安装和维护等各阶段的成本节约。

安全技术的特征可以是功能性的(例如温度超过 500°C 时关闭设备), 固定性的(例如人与机床旋转部件的距离是1m)或者描述性的(例如资质和文化)。近年来, 功能安全受到世界各地各个领域学者和生产厂家的关注, Siemens公司的创立者Werner von Siemens在1880年就提出“阻止事故发生不应被看作仅仅是立法的问题, 而应被看作我们对于人类和经济的责任”。国外发达国家的安全技术发展、应用都已经达到较高的水平, 我国为了应对有关安全问题

的强制条款和安全事故频发的现状, 对建立以功能安全为核心的工业安全体系提出了迫切的需求。

1. 安全技术的目标

安全技术的目标是通过应用和使用适当的技术, 把对人类和环境存在的潜在危险降至最低。然而, 应该是在对工业生产、机械设备的使用和化学制品生产方面不强加任何不必要限制的条件下来实现。通过国际间协调的标准和规范, 每一个国家的人和环境都应当受到同一程度的保护。

2. 安全技术的发展

随着计算机技术、通信技术、先进制造技术等不断发展, 工业安全技术也取得了很大的进步。

1) 基于计算机系统的智能安全技术

基于计算机系统的智能安全技术提供更高的安全性:

- 新型取样传感器允许对于特定应用, 采取针对特殊功能的最优安全技术;

- 带有高时钟频率计算机通道保证极短的响应时间;

- 智能软件允许老化过程在产生危险影响前被检测到;

- 安全现场总线系统极大减少了配线数量, 因而减少了潜在的故障并降低了故障发生时查错的难度。

2) 产品生命周期的安全设计和测试

80年代我们通常使用测试方法来保证复杂的安全技术。现在只在产品生产结束时进行检测已不能满足要求, 取而代之的是伴随产品生命周期每一阶段,

从最初概念设计到最终产品制造, 甚至产品维护和报废的同步安全设计和测试步

骤。这种方法在产品生命周期的特定里程碑中进行相关安全标准的符合性测试, 这也就是当代安全技术更应被看作一个过程而非产品的原因。

3) 集成安全技术

新技术允许安全功能直接集成在一个机器或设备中, 作为其功能控制的一部分。比如, 集成了安全技术的新型CNC控制系统在人员进行安装操作时, 会自动降低其工作速度以避免对工作人员造成伤害, 其安全停车通过相应软件实现, 不需要任何外部的监视设备。这意味着对于使用者, 由于安全集成在控制系统中, 因而故障发生的概率大大降低。同时使用安全相关的数据通信概念, 标准硬件能被用于安全网络的不同控制系统, 甚至是完整的生产系统, 这完全

消除了附加的人工操作, 比如组态安全设备。安全相关数据可以在中央处理器中统一管理和报告, 消除了安全技术使用的障碍, 提高了其被接受的程度。

4) 分布式安全技术

安全停车系统提供的高水平安全性和DCS等传统基本控制系统提供的安全性之间有很大的差距。同样, 基本控制系统提供的复杂控制与停车系统的简单功能之间也有着很大的差距。很多工厂使用现场总线技术使基本过程控制系统可以在整个系统生命周期内, 提供卓越的控制策略、高度的有效性和更高的安全性, 从而填补了这些差距。使用现场总线技

术, 工厂还可以采用附加的测量和安装规范来增加系统的有效性和安全性。

3. 安全系统设计方法

对于大多数企业的生产来说, 只需要一个过程控制系统。如果根据事故分析和危险分类, 工程安全级系统的一些回路必须在发生故障时中断, 则应该与过程控制系统并行配置一套安全相关系统。安全相关系统有自己的、独立于控制系统并基于传统技术的变送器和切断阀(当今技术的发展已使在同一标准现场总线上传输标准数据和附加的安全信息成为可能, 但缺乏必要的安全相关设备和被认可的成功应用案例, 因而其应用还有待进一步验证和推广)。安全相关系统监测危险回路, 如果过程中一部

分出错, 系统将被停车。

以下的设计方法经常被用于安全相关系统的设计:

1) 使用满足安全等级要求的安全产品, 实现功能安全

在IEC61508中, 把系统所能达到的安全级别分4级别, 如图1中SIL (Safety Integrity Level) 1、2、3、4, 或根据EN 954规定, 把功能安全分为6个等级, 即AK (Requirement classes) 1、2、3、4、5、6。根据系统所要求达到的安全等级, 即根据SIL或AK需求进行系统设计, 选择符合等级的安全产品, 功能安全实现的方法可以用图1表示。

2) 通过诊断获得安全性

增强的诊断意味着系统中更多的危险故障会被发现, 尤其在现场仪表中。没有被发现的故障很危险, 因为此时过程不会停车, 而是继续运行在“没有保护”的状态下。用户应确保使用高级的仪表诊断和联锁来提高系统的安全性。在传统手段无法发现的故障发生时现场总线能够发现其它需要停车的状况, 中断回路运行, 从而使系统更加安全。安全现场总线技术的应用极大提高了工业控制系统的安全性, 其中最重要的特点是现场仪表内的诊断可以成为安全联锁的有机部分, 在仪表发生故障时, 将回路中断。

3) 诊断代替差异检查

过去, 变送器故障是通过中央控制器比较连接到同一点的两个模拟变送器的读数来发现的。如果发现两个数值差异很大, 则变送器之一必然有故障, 从而回路不得不停车。但是系统无法知道哪个变送器发生故障, 故障在哪里, 以及故障的严重程度。

使用现场变送技术, 通过变送器内部自检查得到的诊断可以用来

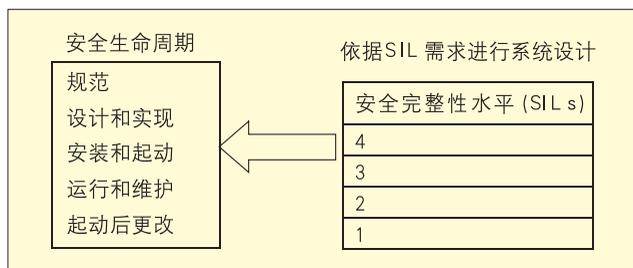


图1 功能安全实现方法

指示测量数值的有效性，并在故障发生时中断回路。换句话说，诊断独立于中央控制器在现场仪表中进行，每个制造商都有自己专有的诊断方法，但是诊断结果会用标准的方式予以表示。应确保使用现场总线技术的诊断功能来发现故障并对其采取措施。

4) 保证正确组态

如果连锁组态不正确，设备可能不会按要求工作。用户如果使用了现场总线技术来管理设备组态，就可以提供设备组态的安全性。比如，更换智能仪表时可能产生的一个严重错误，就是不能将新设备中的所有参数设置得与原设备一致。使用能在一个数据库中存储所有设备参数设置和修改的组态工具是非常重要的。这可以确保更换设备后，新设备的组态信息和原来完全一致。

5) 通过分散得到安全性

如果停车连锁在一个共享中央处理器中执行，就会存在一种偶然性，即一个没有被察觉的硬件故障会使几个回路安全连锁不能发挥作用。通过分散这些连锁功能，工厂就可以

6) 使操作安全，平衡有效性和安全性

某些应用中，如果操作人员无法看到过程中发生的情况，则是不安全的。对于不危险的回路，如罐中的水位，回路长时间的“盲目”运行可能是允许的。然而对于其它回路，即使短时间内无法看到实际情况而进行控制动作都是不能接受的。因此如果与操作员的通信中断，一些回路必须中断，而其它回路则允许继续运行。对于有危险回路的网络而言，不在现场设备中设置冗余可能更好。在设计阶段，最好弄清楚哪些网络从有效性(available)方面获益更多，哪些网络从安全性(safety)方面获益更多，然后根据需要在现场设置冗余结构。

安全性和有效性是两个相互矛盾的目标。安全性意味着回路不得不停车，停止生产并降低有效性。工厂的生产能力和风险管理可以通过每个回路找到恰当的平衡来实施优化。检测仪表故障并对其进行适当处理的能力可以使用户为每个回

7) 失去能源时的安全保证

任何仪表故障或过程问题的停车策略都须依赖能源才能起作用。在电源、气源或液压故障时，最终的控制单元无论如何都必须进入故障安全状态。这意味着在能源丢失时，控制单元的机械设计能够使其输出返回到安全位置。例如，一个阀门必须可以自开或自关。

作为额外的安全保证，应确保所选择的阀门为机械的“故障时开”或“故障时关”。在动力故障时，将提供最后一道安全防线。

8) 冗余解决不一致现象

仪表诊断对于安全性起着重要作用，然而，仪表不可能发现外部问题，例如，那些发生在设备连接处的问题(比如，变送器没有确定的方式来发现设备连接的阻塞或损坏)。此时必须使用两个变送器，如果两个“好的”数值彼此有偏差，问题很有可能是外部的，比如，压力传感器膜片的阻塞或“结块”。

9) 前瞻性维护方案

设备的维护方式分为4种：反应性维护(reactive maintenance)、预防性维护(preventive maintenance)、预测性维护(predictive maintenance)和前瞻性维护(proactive maintenance)，其区别如表1所示。

前瞻性维护方案是把维护的目标指向实际需要维护的仪表，也就是以设备的状况为基础，资源不会浪费在不需要维护的设备上。这个方案需要的资源最少，成本最低，人力资源的使用最有效。利用通信技术，再加上自诊断，可以连续监视因磨损、受力、极端的环境条件和运转的次数等原因出现的“先导性指示”，在不需要人工收集和输入数据的情况下，预测将要出现的故障。

表1 各种设备维护方式比较

维护方式	维护时机	安全性	有效性	成本
反应性维护	损坏以后维护	非常低	低	低
预防性维护	固定时间维护	高	较高	很高
预测性维护	统计时间维护	高	高	低
前瞻性维护	需要设备维护	高	最高	最低

减少这个未被发现的故障所能影响的回路数。

将安全连锁放到最终的控制单元内还有额外的好处，那就是阀门定位器能够不依赖于任何集中的连锁，自己来中断回路。换句话说，即使故障发生在控制设备或去往阀门定位器的通信中，它仍然能采取正确的动作，这是传统定位器或没有内置安全连锁功能的定位器所无法做到的。

路在安全性和有效性之间建立恰当的平衡。适时的诊断使系统安全并减少虚假停车，对安全性和有效性同样重要。

有些场合可能会采取折中方案，在足够长的限定时间内，允许系统在无监视的情况下继续运行，以便纠正故障接口或完成批过程，对于持续时间更长的监控中断，则应该停车。

10) 其它安全性措施

作为一个系统来说，整体的安全性受多方面的影响，如硬件安全设计、软件安全设计、网络安全设计等，以网络安全设计为例，安全现场总线技术包含很多设计良好的技术可以用来提高控制系统的安全性，通常只选择一种安全现场总线就是一种安全性措施。在工厂里混合多重协议可能会带来协议转换的问题和其它安全性方面的顾虑，而使用单一标准总线则可以避免。

功能安全标准的应用

1. 国外安全技术标准

在世界各个地区和国家中，对安全有着不同的概念和要求。对机器制造商和设备制造公司来说，安全标准就是本地的法律和规章，比如，一个机器的控制系统，如果在美国运行和使用的話，即使机器制造商(比如：OEM)是基于欧洲生产的，也必须遵守美国的要求。即便达到安全的技术概念，符合安全技术原则，检测其是否符合本地的法律或具体限制依然是很重要的。

1) 欧盟(EU)的规章和标准

欧盟立法规定了“工作场所的健康和安全”。立法要求这个目标和类似目标要在欧洲委员会(EC)指

南中所列的各个地区实现。为了达到这些目标，立法对这些设备的操作者和使用者、设备和机器的制造商都作了相关规定。立法也规定了他们对可能发生的伤害或损坏所应承担的责任。

EC指南中规定：

- 对设备、系统和其操作者/使用者的要求做了具体的规定，保护个人的健康和**安全以及环境质量；
- 包含了关于工作场所的健康和安全的规章(最低要求)；
- 定义了产品特性和参数以保证使用安全；
- 对产品的生产和使用规定做了区分。

实现EC指南是基于一个新的全球的概念，得到EC(CEN, CENELEC)正确授权的标准化委员会定义了标准的技术细节。当标准被执行时，就假定指南中相关的安全要求也被执行(一致性假设)，立法不再规定特殊的标准必须被满足。但是，要能够进行“合理性的假设”，即当特殊的标准被遵守时，EC指南的相关安全标准目标也是满足的，EC指南规定成员国都要互相承认对方成员国规章和法律。

2) 美国关于工作安全的法律要求和标准

美国和欧洲在“工作安全”立法要求方面的一个重要区别是：在美国，全国没有一个统一的立法能够适用于所有机械安全，并且完全覆盖制造商/供货商。实际上，总的要求是雇主能够提供一个安全的劳动场所。1970年职业安全与健康法案(OSHA)在这方面做了管制，如雇主应该为每一个雇员提供工作和工作场所，这个工作场所可以使其雇员免于遭受已知的危险，这些危险可能造成死亡，或者可能对雇员造成严重的身体伤害；雇主应该遵守这个法案公布的职业安全与健康标准。

各种标准的应用和使用在OSHA 29 CFR 1910.xxx “标准的适用性”中有规定。这个概念和欧洲相似。只要产品相关安全方面被加以规定，则具体产品标准比一般的标准有优先级，当按照标准要求去完成，就可以认为雇主已经达到了OSHA法案的核心要求。

3) 日本机械安全要求

日本的情况不同于欧洲和美国。根据功能安全对立法要求的比较，会发现用于欧洲的一些规则在日本不适用，生产责任不能起到和美国相同的作用。日本JIS(日本工业标准)出台了相应的行政建议。

日本标准基于欧洲思想，并且已经把欧洲基本的标准作为国家标准。

2. 我国的功能安全标准转化工作

IEC61508系列标准的制定为工业控制领域注入了新的活力，功能安全逐渐成为IEC/TC65乃至整个IEC的发展重点。在贸易技术壁垒协定(TBT协定)生效后，一些国家根据本国利益设置技术壁垒以限制进口。如欧盟通过《技术协调与标准新方法》规定，只有在涉及到产品

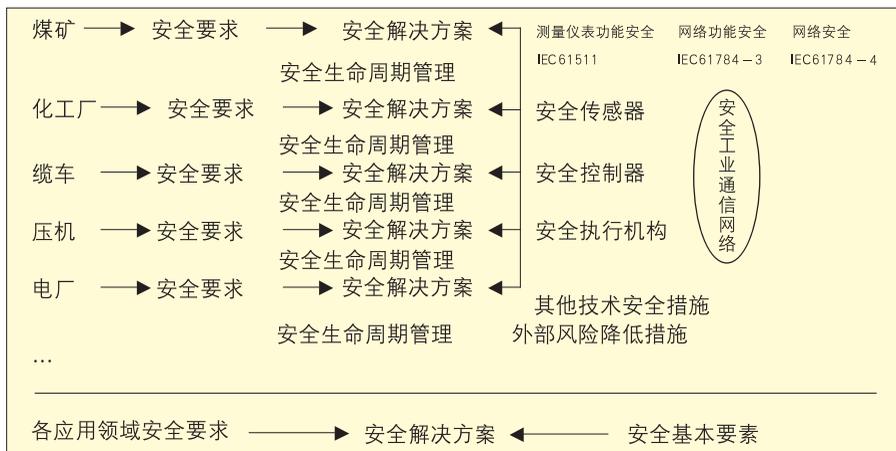


图2 基于功能安全的工业安全标准体系

安全、工业安全、人体健康、消费者保护和环境保护5个方面的技术要求时，才制定相关的技术法规，而且只写出基本要求，细节将由协调标准规定。因此，国外的贸易保护措施多存在于保护人类安全和健康及保护环境等方面所制定的法规和标准中。随着国际上功能安全标准体系的建立以及已经开始的功能安全认证，以功能安全技术为核心的技术性贸易壁垒正在形成。

与安全有关的电器、电子设备、可编程序产品、紧急故障停车（ESD）等系统功能安全的国际标准是在1998年末发布，即IEC(International Electro technical Commission) 615081 Functional Safety of electrical/electronic/programmable electronic safety-related system，主要适用于流程业、机械制造业、交通运输业等产业。1996年，国际测量仪表与控制学会（ISA, The Instrumentation Systems and Automation Society）的SP84委员会，发布针对化学等流程工业的安全仪表系统（SIS, Safety Instrument System）的安全标准，ISA-4.01。SIS包括紧急停车系统（ESD, ESS, Emergency Shutdown System）、安全停车系统（SSD, Safety Shutdown System）、安全连锁系统（SIS, Safety Interlock System）等。

功能安全标准是可靠性技术在



系统功能安全领域的延伸，解决了困扰工业界多年的对系统要执行的功能进行安全评价和管理的理论依据和实践问题，在系统可靠性与器件(软硬件)、子系统的可靠性之间建立了量化关系。功能安全标准为国家进行安全监管提供了理论依据，为企业进行安全控制提供了手段和方法。国内迫切需要对功能安全标准进行制定和执行，已经针对功能安全标准的行业应用领域标准，如对IEC61511系列标准《功能安全——过程工业部门的安全仪表系统》等进行研究并制定我国标准。目前，全国工业过程测量和控制标准化技术委员会和机械工业仪器仪表综合技术经济研究所的有关专家已经积极转化此套标准。

3. 基于功能安全的工业安全标准体系

功能安全概念的提出对我国工

业安全提出了新的挑战 and 机遇，我国已经提出基于功能安全的工业安全标准体系，其基本框架如图2所示。

4. 功能安全标准在我国的应用情况

与世界工业发达国家相比，我国还处在工业化的进程中，机器设备的自动化程度较低，安

全保护技术的应用还不广泛。虽然我国早在上个世纪90年代就颁布了相应的安全标准，但与欧盟各国相比，我们尚未把它强化。从根本上说，由于我国目前在绝大多数行业还没有把机器安全保护标准上升为法令，工人、厂家和设备制造商并没有真正意识到安全保护的重要性。很多企业为了降低成本，不愿意增加安全保护装置的投入；一些设备制造商为了获得价格优势，通过省略安全保护装置来压缩成本，给事故的发生埋下了隐患。操作工人往往缺乏自我保护意识，不能清楚判别自己所处工作条件的危险性。在我国，依据功能安全标准实现“安全工厂”的理想还需要很长时间，这取决于我国经济、社会发



表2 智能安全设备对比

智能安全的种类	目的	功能	联网能力	输入输出能力	编程能力
安全控制器	具有机器和安全控制的多功能性	安全监视、诊断、联网，常用于小型机器控制	可连接多种总线	多个(40或更多的)，且可扩展	基于软件编程(IEC61131-3)或同类型软件
安全监控器	多功能安全控制和监控	监控和诊断	可选连接总线，采用AS-i等接口标准	主要用于监控，但可以通过远程安全节点扩展	功能块编程或类似软件
安全I/O	复杂的安全互锁	监视、诊断	可选连接总线	根据所采用的技术，如光缆	Dip开关或旋转开关
安全继电器	简单或复杂的逻辑任务	特定于设备之间的安全互锁	无	1~12个I/O	无

展水平提升的速度。

我国工业生产的安全形势十分严峻，其重要原因是缺乏科学有效的安全管理，而不是因为没有采用安全相关系统。不过观念的转变正催生着一个潜力巨大的市场，例如作为安全产品最大的应用行业，我国汽车行业的迅猛发展带动了为汽车提供产品的OEM厂商的发展，由于这些OEM厂商被要求使用安全型产品，从而带动了安全观念的转变；另外中国机器设备出口的增长，导致对安全产品的需求量增加。随着国内、国际市场的逐步接轨，国际市场蕴藏的商机无疑充满诱惑，但要使机器设备能够进入欧盟或北美市场，前提却必须通过相关的安全标准认证。随着国家政策法规的制定，特别是一些行业法规陆续出台，某些行业将强制性使用安全产品和系统，以达到功能安全标准的要求。

安全产品

为了实现功能安全，根据图2所示的工业安全标准体系，在功能安全标准系列的执行过程中，会逐渐形成一个功能安全产品供应链。安全传感器、安全继电器、安全PLC、安全通讯网络、安全I/O、安全执行器等产品供应商会被要求对安全产品进行IEC61508标准认证，以区分不同的安全等级。系统集成商会趋向于选择通过认证的设备与子系统来构建安全系统，用户也会要求集成的系统必须通过安全审核。一般来说，安全控制系统应该包括安全输入设备（如急停按钮、安全门限位开关或联锁开关、安全

光栅或光幕、双手控制按钮），安全控制元件（如安全继电器、安全PLC和安全总线、安全I/O）和安全输出控制（如主回路中的接触器、继电器或阀、声光报警装置等），另外常见的还有安全栅、ESD系统、本安防爆产品等。

安全产品已经应用到各种自动化系统中，一些传统的标准自动化产品供应商，如ABB、FOXBORO、SIEMENS、YOKOGAWA等，纷纷展出其满足IEC61508（功能安全的基本标准）和IEC61511（过程的功能安全标准）的功能安全产品和实现办法及措施。ABB的Industrial IT 800xA自动化系统体现了ABB在油气、石化、化工、电力行业从事安全系统的设计、实现和维护的经验，可在IEC 61508/61511安全生命周期的各个阶段，在风险分析、安全规划及系统设计、运行以及维护等方面随时提供支持。800xA系统提供了一整套安全仪表系统（SIS）的解决方案，符合IEC61508/61511标准，其针对的范围不仅限于解决保证安全的逻辑和顺序问题，而且还包括整个安全回路，覆盖现场仪表、集中控制器和I/O模块，以及现场执行器。德国SIEMENS公司产品SIMATIC S7-400F/FH，400F和400FH分别为1个CPU和

2个CPU运行fail-safe(F)用户程序，均取得TUV认证，安全等级为AK1~AK6。SIEMENS在实现现场总线的功能安全方面，起着引领作用，PROFIsafe既可用在过程安全方面，又可用在机械安全方面，甚至还考虑了用于驱动和传动方面的功能安全，作为安全行规PROFIsafe还适用于PROFINET工业以太网。YOKOGAWA收购Moore QUADLOG系统后开发出的安全仪表系统ProSafe-RS实际上是一种运行在该公司主推的DCS系统Centum CS 3000系统平台上的软件系统，再加上专用的具有丰富的自诊断功能和高可靠性的CPU和I/O模块，即使选择非冗余配置，也达到了SIL3。据称，ProSafe-RS是符合IEC 61511功能安全标准，并已取得安全认证（TUV、SIL3）的安全仪表系统。ProSafe-RS具有安全联锁保护功能，紧急停车ESD功能与DCS控制功能无缝集成，便于操作人员全面掌握DCS和SIS的信息。安全产品中常见的ESD紧急停车系统还有美国Honeywell公司的FAIL SAFE CONTROL (FSC) 系统，由



它执行安全连锁系统的控制部分代替原来在DCS中执行的连锁内容，按照规范将安全连锁系统独立出来，以确保人身和设备的安全；该系统硬件基于双重化结构，软硬件均通过IEC的IEC61508认证。美国Triconex公司开发的Tricon、Trident系统用于压缩机综合控制（ITCC）和紧急停车，安全等级为AK6。GE Fanuc公司开发的Fanuc 90-70系列，其中GMR（模块式冗余容错系统）的安全等级为Class5(2v3)、Class4(1v2)和Class5(2v2)等。

根据生产商的定义和设备的功能，表2列出了常用安全设备和特性比较。受篇幅限制，下面仅对安全控制器、安全继电器进行对比分析。

1. 安全控制器

安全控制器主要是指安全PLC，市场上常见的安全控制器有Pilz公司的PSS系列、Siemens公司的SIMATIC S7-400F/FH S7-300F系列等，目前的安全PLC产品几乎都符合IEC61508标准并得到了SIL3的等级认证。

安全PLC是一种专门为条件苛刻的任务或是安全相关的应用而设计的可编程逻辑控制器；如果一台安全PLC失效了，它不会对人员安全或过程安全带来危险。一个安全PLC需要利用各种水平的冗余结构、利用安装在不同区域的芯片来设计和构造成为事故安全的PLC，它还需要经过第三方的认证以达到IEC61508标准。在一台安全PLC根据要求达到了特定的可靠性/故障概率等级时，就意味着它具有广泛的自诊断能力，可以监测各个方面的硬件状态、程序执行状态和操作系统状态。此外，安全PLC还必须能够执行标准机构（例如TUV、FM等）认证中所必须的故障安全动作，而这些故障安全动作都是根据特



定的原则设计，并满足国际安全标准（如IEC61508和EN954-1等）中定义的要求。另外，安全PLC还可能包括入侵保护预警和权限管理的内容，用来保护安全PLC不受来自外界干扰。

安全IO常用于安全PLC组成的系统中以扩展系统的控制点数，也用于在普通PLC中实现部分IO的安全要求，如PSS universal、ET200S/ET200M、CQM1-SF200。

从安全PLC供应商方面看，既包括专门生产安全产品的厂商，如Pilz；也有传统PLC的生产厂商，如Rockwell、Omron、Siemens等巨头，各大厂商纷纷采取一系列措施，推出自己的安全PLC产品。市场上常见的安全PLC及性能对比见表3所示。

2. 安全继电器

安全继电器具有一种称为强制导引接点的构造，其他部分基本上与一般的继电器相同，安全继电器用传统的方法为人员和机器提供保护，常用于监控与安全保护相关的控制系统。其内部结构包括：电源模块、电子处理模块和继电器，有的安全继电器内部采用两个互为冗余的继电器，这两个继电器具有确定动作的触点，用于安全输出通道和信号通道。安全继电器满足广泛的安全应用需要，

可与安全门开关、安全电磁开关、安全连锁开关、双手控制设备、安全地毯、磁编码传感器、安全边、安全光幕、急停按钮和紧急拉线开关配合使用，以增强机器安全保护系统的可靠性。它通过检测出安全保护电路中的故障，可以切断电源使机器停止运行，直到故障被排除。为保护操作者及机器的安全，Pilz公司早在1987年就率先研制出了第一个PNOZ型急停继电器，以后又陆续推出了不同品种。目前我国市场上的安全继电器主要是国外产品，产品系列和性能对比见表4。

安全产品市场分析

安全产品类别比较多，目前各大安全产品提供商都有自己的行业和产品定位，如Pilz在安全门开关、急停和双手控制等产品以及多种应用的解决方案都拥有着很强的市场竞争力。而专业从事安全产品的美国科学技术有限公司（STI）的产品主要以安全输入和输出设备为主，同时也提供过程保护设备，主要的应用领域则是机械设计和工业操作过程中的安全应用。从安全PLC供应商方面看，Pilz、Siemens、Rockwell、Omron等都推出了符合IEC61508标准并得到了SIL3的等级认证的安全PLC。同时，都试图将安全PLC与其他机械安

表3 安全PLC性能对比

厂商	安全PLC型号	PLC	Invensys triconex	Siemens	Schneider	STI	Rockwell	SICK	OMRON
		PSS 3000	Trident	SIMATIC S7-400F/FH	Preventa XPS MF60 CPU; XPS MFCPU22 金属机架 XPS MFGEH01, 电源模块 XPS MFPS01, 机架型 I/O 模块	F3SX	GuardLogix CPU; 主控制器可选 1756-L61S 或 1756-L62S, 安全控制器是 1756-LSP	UE410, UE440/470	OMRON NE1A
CPU		3, 底板: PSS BMP 8 速度: 平均3ms/千个指令和每个周期5ms自一个报警标志位; 2048 (ST 区) 1152 (FS 区); 定时器: 128; 数据内存: 16KB 非保护性故障保护区; 32KB 标准 Flash EPROM 故障保护区; 512KB 集成式 Flash EPROM	MP 主内存包括: 2M 内部程序和程序和数据内存, 8M 可扩展内存; 数据内存: 256KB 内部 RAM, 可扩展最大 64M FEPROM 或 RAM; 最大 FB 和 FC 达 6144; 最大数据块 8191; 最大数字量 131072; 最大模拟量 8192	417-4H 程序和数据内存均为 500K, 数字量和模拟量 I/O 模块的连接数量根据“机架型” I/O 模块型号而定	F3SX-ER2 本体有 2 个安全输出, 1 个辅助输出, 数字量和模拟量的连接数量根据 I/O 模块型号而定, 可控制 4 个光栅组和 8 个安全开关以及 2 个紧急停止开关	1756-L62S 的用户内存: 4MB (标准), 1MB (安全); I/O 内存: 478K 1756-L61S 的用户内存: 2MB (标准), 1MB (安全)	UE410-MU	NE1A-SCPU02 自带 40 个安全输入和 8 个安全输出, 通过 DeviceNet 可以连接 32 个安全站, 使用 12 点输入模块时, 输入达 384 个, 使用 16 点输出模块时, 输出达 256 个	
系统性能			采用 Motorola MPC860 PowerQUICC™ Quad 处理器						
认证		符合 EN954-1 4 级, DIN V 19 250 01/89 DIN VDE 0116, BG, TUV, UL508	符合 SIL 1 ~ SIL 3, IEC61508 EN954-1 组 2~4, DIN V 19250/DIN V VDE 0801 SIL 1 - 3 (IEC 61508)	符合 IEC 60364-5-53, SIL 3 EN954-1/ISO13849-1 4 类	符合 EN 61508, IEC61508, EN954-1, EN61000-6-2, EN61000-6-4, EN61496-1, IEC61496-1, EN60204-1, IEC60204-1, EN50178, EN55011, UL508, UL1998	符合 UL, CE, C-Tick, CSA Class 1 Div 2, ATEX, FM, TUV 认证 SIL3 Cat.4	符合 IEC61508 (SIL3), EN954-1/ISO13849-1 (Cat.4)		
通信		串口, RS232/485 支持冗余总线, SafetyBUS p, 最高速度 500K Bit/s 长度: 3500m	串口, Modbus, TriStation TCP/IP, 点对点	MPI, Profibus - DP, PROFIsafe	4 个安全通讯端口 (以太网), 1 个 FB2 (Sub-D9 针) 工业通讯端口 (Modbus)	点对点, RS232	CIP 通过 Ethernet/IP, DeviceNet, ControlNet	PROFIBUS - DP, DeviceNet, CANopen	DeviceNet
其他特点		CPU 采用多通道和相似的结构, 带有完整的检测和算法; 能够处理故障保护 (多通道处理 ST 程序), 互不影响, FS 程序只生成一次, 所有编译和功能拷贝都有 CPU 来实现; 所有主要功能均提供了经过认证的模块, 可减少开发和试运行时间 LED 和 4 位数字显示器提供状态和诊断信息	可连接 ET 200S PROFIsafe 分布式 I/O 编程方式支持 STEP 7 (LAD, FBD, STL), SCL, CFC, GRAPH, HiGraph; 有两种配置模式, 故障安全和故障安全容错	集成了双处理器能够接收的安全输入和输出信息进行分析, 并加以对比, 输入和输出信息 (编程值和接收值) 可由两个处理器并行接收, 并进行实时对比, “看门狗”或自监视, 模块型 PLC 持续监视信息处理周期和作业执行情况, 如周期时间超过预定值, 则要对其进行干预, 集成交换机 (专用交换机制) 对于安全以太网所提供的输入和输出信息, 可进行短时间的存储, 并以极高的速度进行发送, 同时避免出现网络中的信号冲突和数据过量的情况, 采用专用 XPSMFWIN 编程	采用专用 F3SX-CD100-E 编程, 自动检测线路断线功能, 带通讯自诊断, LED 指示	主控器和安全控制器为冗余结构, 均提供 LED 状态指示灯, 提供专用特殊功能块完成安全所需的各种功能, 支持安全标签, 安全任务, 安全程序, 安全规则, 内置冗余的 CPU 系统, 利用内部测试电路检查 I/O 模块的运行状况, 而不是直接使用冗余的 I/O 附件。	电源支持 24V DC 19V, 2V, 30V, 可通过旋转开关选择程序, 可通过 PROFIBUS-DP/DeviceNet 进行诊断	可以从 DeviceNet 主站监视安全输入和输出以及状态信息, 系列逻辑功能和特殊功能块, 系统启动和错误恢复支持使用安全网络配置器进行在线监视, 自动检查不完整的接线	

表4 安全继电器性能对比

品牌	Pilz	OMRON STI	Schneider	Banner	Siemens	SICK	comitronic	Honeywell	Rockwell
安全继电器型号	PNOZ XV3P	SR101A	Preventa XPSAC	ES-FA-11AA	3TK2 827-2BB41	UE48-3OS2D2	XXL	FF-SRL6025	100S-C100S-C09A23C
标准认证	符合 VDE0113、11/98、EN60204-1、12/97 和 IEC204-1、11/98	符合 EN60204-1、EN954-1 与 VDE 0113-1、CE、UL、C-UL、BG	符合 EN954-1 标准的安全控制等级3	符合 UL991、ISO13850(EN418)、ISO13849-1 (EN954-1)(SafetyCategory4)	符合 EN954-1 B、1、2、3、4	符合 EN954-1、EN60204-1	符合 EN954-1 等级4	符合 EN954-1 等级4	符合 IEC947-5-1
电源要求	24V DC	24V AC/DC、115V或230V AC	24V AC/DC、115V AC或230V AC	24V AC/DC	24V DC	24V AC/DC	24V AC/DC	22V DC	C09可接受9、24、36、48、60、64、72V DC
输入		1个无监测单常闭触点		1~2个常闭触点，1个复位NO				2个	
输出	2个延时常开触点；3个即刻常开触点	2个常开触点	3个常开触点安全输出；1个固态辅助输出	2个常开触点安全；1个辅助输出	2个常开触点；2个常开触点，1个常闭触点	3常开触点，可扩展	2个延时常开触点；1个延时常闭触点；3个即刻常开触点	3常开触点；1常闭触点	2个常开触点；3个常闭触点
监视与诊断	LED指示灯	提供一个SR101A上连接S11与S21的N/C回路和外部装置监测(EDM)；	LED指示灯	LED指示灯；3个绿色LED指示灯和1个红色指示灯	4个诊断LED	3个LED，提供EDM检测	LED可视化，延时时间0~999可调	LED显示电源和内部继电器状态，过载短路保护	
复位模式	受控手动复位、自动复位	自动复位		自动复位、通过复位开关	自动复位	手动复位和自动复位	1个按钮和2个常闭触点激活，自动控制	手动复位、自动复位	
防护等级	固定安装:IP54 机架:IP40 终端:IP20	IP20	IP20	IP40；NEMA1，或IP20	IP20	IP20		IP40、IP20	

全产品一起构成完整的机械安全解决方案，例如2005年11月，Rockwell在美国举办的年度Automation Fair展览会上设立了安全产品线独立展区，产品线覆盖从传感、逻辑判断到执行机构的每个环节，如安全按钮、安全地毯、安全开关、安全继电器、安全光幕、安全镭射扫描器、集成安全功能的马达启动器与伺服电机、安全PLC（模块式与分布式）、安全分布式I/O、安全网络等。Siemens的安全PLC大量应用于Toyota等汽车厂商。实践证明已经采用安全PLC的行业包括汽车、机床、机械、船舶以及过程工业中的石化、炼油、电厂、锅炉控制和燃烧控制、高压应用等行业和场合。此外，它还可以应用在一些远程遥控、无人值守以及维护费用十分昂贵的应用场合（例如大型储罐区）。

在国内，工业安全产品的应用主要集中在机械领域，这些产品其实就是对机械操作过程中的危险进行控制。使用比较多的是在压力机、升降机、电梯、机床等大型的设备上，主要是因为这些设备的应用场合安全要求通常比较高，安全产品被大量应用到存在安全隐患的设备中。比如说在冲压机床模块上下的运动中，就需要安全产品来保护机器的操作者，避免人手被切或者被压。

随着自动化控制设备和系统越来越多地应用于生产环节，为了保证企业中生产线的正常运行和操作人员的人身安全、设备安全，使用安全的产品、设备、系统已经成为企业的迫切要求。今后5年，我国整个安全市场的增长速度将是整体自动化市场增长速度的两倍以

上，而其中的安全元器件，包括安全PLC、安全网络等增长更为明显。从国际上看，欧洲和北美对机械自动化安全装置的大量需求将促进安全PLC的发展和和使用，北美安全PLC产量将由2004年的930万美元上升到2007年的2.07亿美元，年增长率为30.6%，而在欧洲，安全PLC产量将由2004年的4.31亿美元上升到2007的7.88亿美元，年增长率为22.3%。这2个区域的差别主要是欧洲市场较成熟，安全PLC的应用也相对成熟一些。另一方面，纵观整个机械自动化安全装置市场，2007全年欧洲市场的年增长率为7.4%，北美为12.5%。因此相对来说，安全PLC市场增长率远远超过了其他机械安全装置的增长速度。■