功能安全系统技术在工业衡器的最新应用

上海大和衡器有限公司　陈日兴

【摘　要】　产品功能安全系统设计与应用目前在国外工业发达国已经发展到相当先进的水平，我国工业界近几年也紧跟国际潮流，相应制定了相关的国家标准与实施计划。在我国工业衡器技术的发展历程中，同样离不开衡器功能安全技术的发展。本文针对目前国内衡器行业对于产品功能安全的理念和相关技术比较陌生的实际情况，试图根据最新国际 IEC/EN、ISO/EN 相关标准内容，结合衡器产品设计与应用，以最简洁的方式阐述工业衡器“功能安全”概念及衡器技术的发展与应用。

【关键词】　工业衡器功能安全；CAT 危险等级；SIL 安全完整性水平；PL 控制系统安全性能等级

概述

从传统的基于继电器与人工防护的安全系统到目前发展起来的功能安全集成系统，使得我国工业产品的安全技术在不断进化。产品功能安全系统设计与应用是目前我国工业技术革命向纵深发展的必由进程。近几年 IEC 国际电工技术委员会与 ISO 国际标准化技术委员会相继发布了“与安全相关的电气、电子和可编程电子控制系统的功能安全”，“机械安全—控制系统的安全相关部件”等标准，我国也根据上述国际标准等同采用制定或正在制定相应的国家标准。2011 年 11 月初在上海举办的“2012 中国国际工业博览会”上，主办部门举办的“OEM 机械设计技术高峰论坛”上就产品功能安全系统作了专题交流与研讨，研讨会上许多国际知名公司如：Rockwell，ABB，Omron，Pilz 等相继推出了最新功能安全应用的控制产品。由于目前国内衡器行业对于产品功能安全的理念比较陌生，本文拟结合我国衡器行业正在制定的唯一的衡器产品强制国家标准《电子衡器安全技术要求》，从产品功能安全系统设计的概念开始结合衡器产品的设计与应用，特别是对于较复杂的工业称重系统谈谈自己的看法。

一、功能安全概念

由于产品研发人员在开发制造中由于可靠性风险管理意识的不足，自身安全性能存在缺陷的产品已经造成人身安全、财产损失和环境危害等影响，给社会带来了无法挽回的损失，为此引出了功能安全的设计理念。

功能安全——无论产品的零部件或者整体系统发生失效是随机失效、系统失效还是共因失效，都不会导致安全系统的故障，进而不会对操作人员或者环境产生危害，那么这个系统在功能上就是安全的。

无论是在正常工作状态或者是故障工作状态，控制系统都必须保证其安全功能。

二、功能安全相关标准

目前许多有关安全的设备供应商均在其说明书或样本中声明其产品符合 EN 954-1 安全标准的规定。EN 954-1 和 IEC、ISO 有关的安全标准之间的关系如何，有何区别。为了搞清楚这个问题我们有必要先分别介绍一下相关标准的内容。

1、EN 954-1 标准

EN 954-1“机械安全——控制系统有关安全的部件”是由欧洲标准委员会（CEN）制定的欧洲标准，最早于 1992 年 11 月公布，它设定了一个流程来选择和设计安全措施，这个流程包括以下 5 个步骤：（1）危险分析与风险评估；（2）确定措施以减少风险；（3）通过控制系统的与安全相关的部件实现指定的安全要求；（4）设计；（5）验证。

EN 954-1 也提供了一个典型的安全功能的列表：（1）停车；（2）紧急停车；（3）手动重置；（4）启动和重启；（5）响应时间；（6）安全相关的参数；（7）本地控制功能；（8）供电系统的波动，损失和复位；（9）暂时失效；（10）安全功能手册。

EN 954-1 将危险等级分为 CAT.B、CAT.1、CAT.2、CAT.3、CAT.4 五个等级。等级 B 是最低，对安全系统没有特别的要求，等级 4 为最高的危险等级。控制等级分为 4 级，安全控制等级必须大于等于其危险等级。EN954-1 通常适用于机械的低复杂性的安全系统。

EN 954-1 存在的问题：没有覆盖 PLC 可编程系统及单片机系统；没有涉及系统故障概率；安全等级划分不明确；有效期至 2011 年 12 月 31 日。

2、IEC 61508 标准

IEC 61508“电气／电子／可编程电子（E/E/PE）安全相关系统的功能安全”是由国际电工委员会在 1998 年 12 月发布的国际标准，该标准包括电气/电子/可编程电子安全系统的要求，包括对设备和系统的要求，对软件的要求，描述避免失效的方法，给出一些确定安全完整性水平的方法示例，给出测试方法。

IEC 61508 标准主要适用于对安全系统有较复杂要求的系统，根据发生故障的可能性分为 4 个 SIL（安全完整等级 Safety Integrity Level）等级。

表 1　SIL 与故障概率

SIL 等级	具有高等的或连续要求的操作
	危险故障概率【1/小时】
SIL 1	$\geq 10^{-6} < 10^{-5}$
SIL 2	$\geq 10^{-7} < 10^{-6}$
SIL 3	$\geq 10^{-8} < 10^{-7}$
SIL 4	$\geq 10^{-9} < 10^{-8}$

SIL 以故障率表示如下表：

表 2　SIL与PFH_d关系

SIL	PFH_d	可接受的最大故障率
None	$\geq 10^{-5}<10^{-4}$	每 10,000 小时发生一起危险故障
SIL 1	$\geq 10^{-6}<10^{-5}$	每 100,000 小时发生一起危险故障
SIL 2	$\geq 10^{-7}<10^{-6}$	每 1000,000 小时发生一起危险故障
SIL 3	$\geq 10^{-8}<10^{-7}$	每 10,000,000 小时发生一起危险故障
SIL 4	$\geq 10^{-9}<10^{-8}$	每 100,000,000 小时发生一起危险故障

其中：PFH_d——每小时发生危险故障的概率。

3、IEC 61511 标准

IEC 61511 是适用于工艺过程工业的安全仪表系统的国际化标准，是 IEC 61508 的补充。

4、IEC/EN 62061、ISO/EN 13849-1 风险评估标准

安全标准主要依据应是风险、故障概率的描述和安全等级，现 IEC/EN 62061 将注意力集中在机械设备安全功能的量化上，是 IEC 61508 标准的简化版。与 IEC 61508 标准相同由每小时故障率 PFH 决定安全完整性等级 SIL，如上表 2 所示。

ISO/EN 13849-1 旧版本（1999）与EN 954-1 是相同的，ISO/EN 13849-1 新版本（2006 版）引入控制系统安全性能等级的新概念PL（Performance Level），是一种定性故障评估的方法，考虑了控制系统外在因素的可变性。新的安全控制标准EN /ISO13849-1 在 2009 年 12 月取代EN 954-1 强制执行，标准覆盖了气压系统、机械安全控制系统。还引入了B_{10d}，$MTTF_d$等概念。

（1）PL（Performance Level）——控制系统执行安全功能的能力，以每小时发生危险故障的概率表示，并划分 5 个等级，依次为 PL a、PL b、PL c、PL d、PL e。

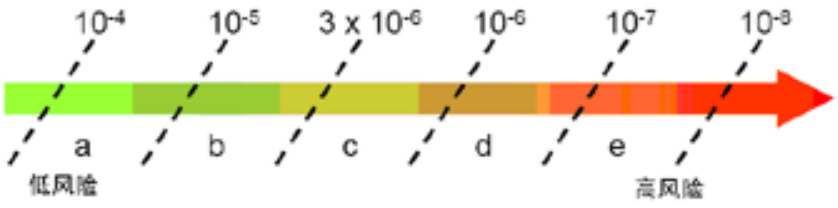

图 1　PL 等级与危险故障概率关系

上图中 PL e 为最高等级，PL a 为最低等级。

（2）风险评估图

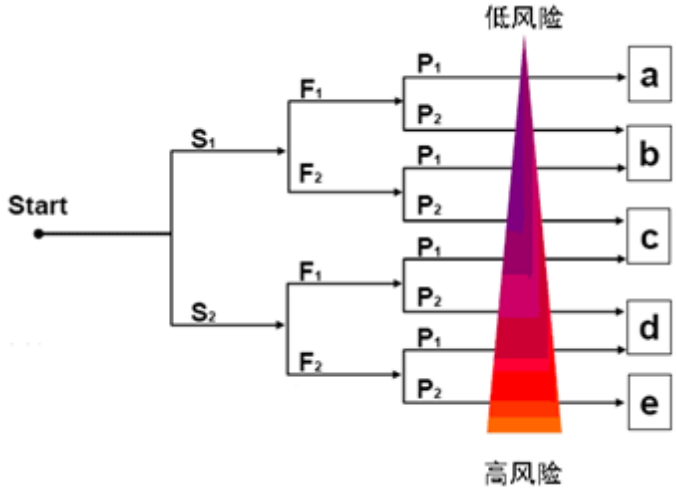

图 2　风险评估图

上图中：S——伤害的严重性。其中 S1：轻微的；S2：严重不可恢复的。

F——风险发生的频率或暴露的时间。其中 F1：很少；F2：频繁。

P——避免风险的可能性。其中 P1：可能；P2：几乎不可能。

（3）PL 评估参数

A．B_{10d}值——发生 10%故障概率时，开关动作的次数。

$$B_{10d}=0.5\times B_{10}$$

其中B_{10}——制造商提供的 10%故障概率开关动作的次数。

B．$MTTF_d$——每个通道的平均无危险故障时间（mean-time-to-dangerous failure of each channel），是统计值，不是可以保证的寿命值。

$MTTF_d$可以分为 3 级。

表 3　$MTTF_d$范围

$MTTF_d$等级	范围
低	3-10 年
中	10-30 年
高	30-100 年

此范围值低于 3 无法接受。

$MTTF_d$的大小取决于实际开关动作的频率。

C．DC——诊断覆盖率（diagnostic coverage）。

D．Architecture——类别（the category）。

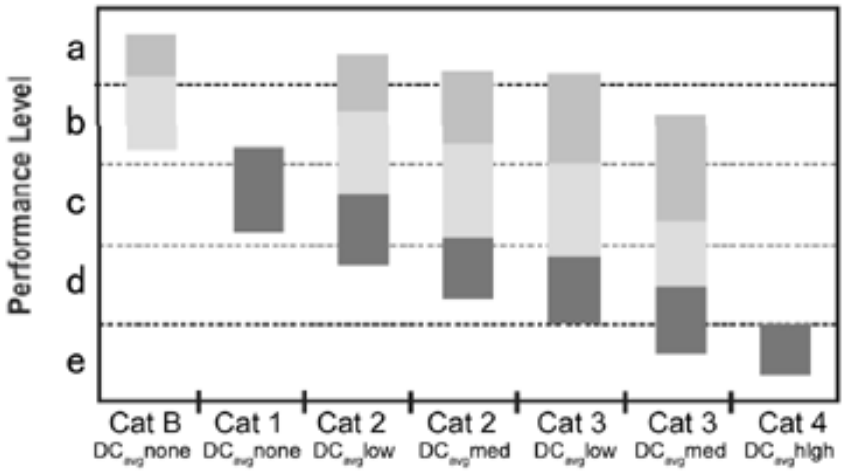

图 3　DC 与 PL、Cat 等级的关系

三、风险评估的流程

首先要确定当前或者发展中可能存在风险的等级，通过评估、设计、选择、验证以及维护等一系列程序来建立真正安全的生产环境，这些都要遵循相关的国际安全标准和规则。较为复杂的工业产品系统能够达到何种安全等级一般是需要由第三方机构进行认证的。目前我国主要由一些权威的外资机构如德国 TUV 公司等在中国开展了产品安全等级测试及认证工作。基于 IEC 61508，IEC 61511，IEC 13849-1，IEC 62061 等标准，对安全设备的安全完整性等级（SIL）或者性能等级（PL）进行评估和确认的一种第三方评估、验证和认证。功能安全认证主要涉及针对安全设备开发流程的文档管理（FSM）评估，硬件可靠性计算和评估、软件评估、环境试验、EMC 电磁兼容性测试等内容。以下是风险等级评估的流程。

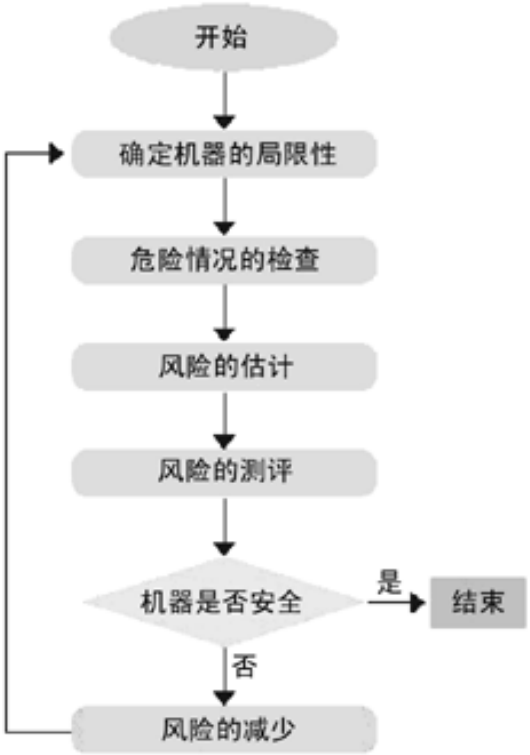

图 4　风险评估流程图

对机器进行过危险性分析后，制造商可以采取如下三种措施来减少事故的可能性，将机器的危险性降低到可以承受的程度：

（1）在设计机器时将可能出现的危险降低到最少；（2）对于无法避免的危险，采取必要的安全保护措施；（3）对用户进行培训，避免剩余危险可能导致的伤害。

为达到上述标准的各类安全等级，最常用的设计方法为热备份的冗余设计方法。例如：安全开

关的双触点结构、安全继电器的双通道输入、安全 PLC 的双 CPU 结构、控制软硬件的冗余设计。此类设计方法已经或正引起越来越多的产品设计与应用部门的重视。

四、功能安全在工业衡器中的应用

功能安全控制系统的宗旨是提高工业产品的可靠性与安全性。目前在我国工业自动衡器的产品中采用功能安全集成控制系统已初露端倪。例如：重量自动分选衡器、连续累计自动衡器中皮带秤、给煤机、皮带配料秤、重力式自动装料衡器中的大型称重配料系统、产品称重包装生产线、动态滚道秤、动态胶料秤等产品中，一些卓有远见的用户已经提出了功能安全集成控制系统的要求。

图 5　功能安全集成控制系统的应用实例

在上图的产品生产称重系统中，安全锁、安全急停按钮、拉线急停开关、感应式安全光幕以及控制柜中的安全继电器、安全 PLC 等部件动作互相关联，组成了一个完整的功能安全集成控制系统。

作为一个设计人员应该在机器的设计上把危险减少到最小，就必须采用安全控制类产品。以下将结合上海大和衡器有限公司近期在工业自动衡器产品设计中的一些应用实例，分别介绍各种安全功能部件的应用。

1、安全互锁开关

安全互锁开关是指通过强制断开动作结构，即使在接点熔接时也能确保功能安全。

产品分为非接触式、机械连锁式两种。例如：安全门锁、舌簧互锁开关、安全限位开关、非接触式安全开关等。上述用于安全互锁开关的共同特点是必须要有两个并列的安全回路。如：两路常开或两路常闭。

图 6 安全门锁在料斗秤中的应用

图 7 安全舌簧互锁开关在皮带秤中的应用

2、安全继电器

安全继电器与一般继电器不同，具有强制导向的接点结构，即使在接点熔接时也能确保功能安全。安全继电器一般与安全开关配套使用，具有双通道检测功能。

安全继电器的主要技术指标如下：

（1）接点间隔不仅在通常运行状态而且在发生故障胡状态也应达到 0.5mm 以上；

（2）接点负载开关应符合 AC15、DC13 的要求；

（3）机械寿命为 1000 万次以上。

下面为应用在工业衡器上的安全继电器实例。

图 8 安全继电器在称重控制柜中

图 9　安全继电器外观及认证标志

3、急停装置

该装置主要用于紧急停车系统。产品主要有安全拉绳开关、急停按钮等。该类设备用于一旦系统出现异常故障，使操作者能在最短的时间，最近的位置实施紧急停车。例如在产品的包装线上、物料配料称重输送线上、皮带秤和定量给料机、给煤机的侧面需使用安全拉绳开关。

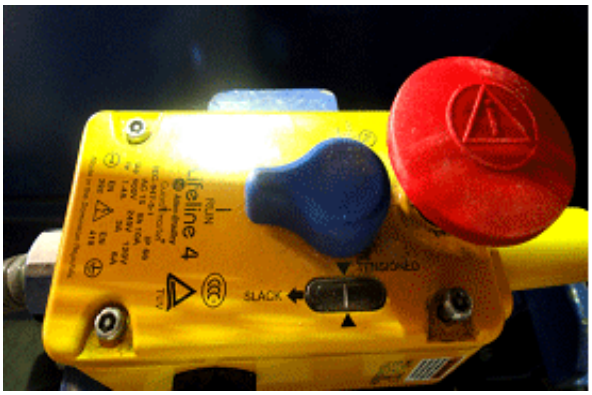

图 10　拉绳式急停开关外观

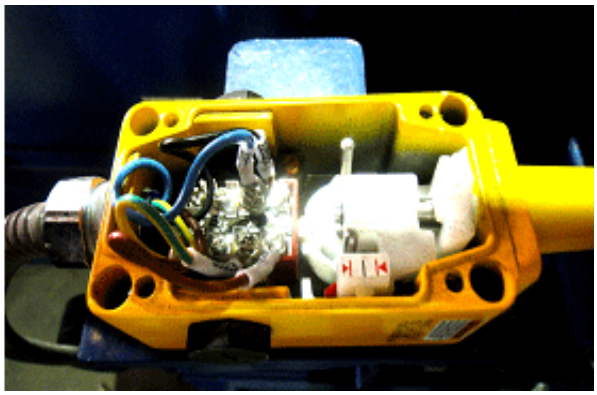

图 11　拉绳开关内部安全双回路

4、感应式安全装置

该类装置属于主动安全防护，无需在设备和操作者之间设置硬件防护。主要感应生产线上的操作者或移动设备。较为典型的产品有安全光栅/光幕、安全扫描仪等。在衡器行业应用最多的是安全检测光栅/光幕。在产品包装热封设备前用于防止操作者手动误操作的红外线安全光栅；设置在动态公路称重收费站秤台边的车辆检测光幕。

安全光幕还有光束屏蔽功能，由于工艺需要把光幕中的个别光束屏蔽不起作用。光幕输出为 OSSD 信号，该信号有短路输出、过载保护、PNP 输出及交叉检测等功能。安全光幕还有外部设备监控功能：通过外部执行器的断开检测是否正常工作。

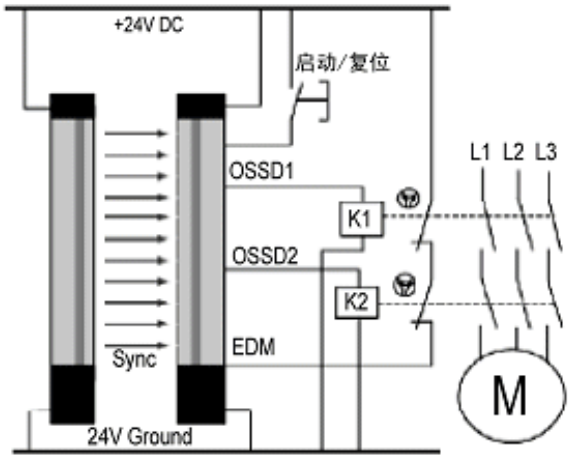

图 12　安全光幕外部设备监控原理

图 13　安全光幕用于包装袋热封机

5、安全 PLC

目前市场上已有封装型可编程安全控制器、集成安全控制器和安全 I/O，通过 RSNetWork 编程，通讯采用 DeviceNet 和 EtherNet/IP，该类产品最大的特点是采用标准与安全的两套 CPU 控制，并实现安全通讯。

(a)　(b)　(c)

图 14 安全 PLC 种类

(a) 可编程安全控制器；(b) 集成安全控制器；(c) 安全 I/O

上述各种安全部件可以组成一个完整的功能安全集成控制系统。在工业衡器的系统设计中应根据现场的不同安全等级要求选择不同的功能安全器件及功能安全系统。

五、结尾

在功能安全控制系统的应用已经风靡全球工业界的今天，工业衡器特别是自动衡器如何紧跟这一时代发展的新潮流，已经成了我国衡器行业技术发展急需提出的新课题。尽管越来越多的衡器产品最终用户和制造商已经意识到安全的重要性，但并未认识到应从系统上根本解决安全的问题，安全理念和相关技术与标准的实施在我国衡器行业推广的道路仍然漫长。愿本文能在衡器行业起到一定的推动促进作用。

参考文献

1．慧桥自动化《机器安全解决方案》，张宏涛。

2．功能安全标准介绍资料，德国莱茵公司。

3．《机械安全——控制系统有关安全的部件》EN 954-1（1996 版）。

4．《电气/电子/可编程电子（E/E/PE）安全相关系统的功能安全》IEC 61508（1998 版）。

5．《机械安全——控制系统与安全相关的电气/电子/可编程电子（E/E/PE）功能安全》IEC/EN 62061、ISO/EN 13849-1（2006 版）。

作者简介

陈日兴，男，上海大和衡器有限公司，总工程师/高工；

研究方向：衡器研发与计量技术，享受国务院政府特殊津贴专家；

国内外发表论文近 70 篇。