仪表SIL认证

产品名称	仪表SIL认证
公司名称	上海镭朔信息科技有限公司
价格	.00/个
规格参数	
公司地址	上海市嘉定区曹安公路3918号
联系电话	4006285882 13167050230

产品详情

评估总是从关于IEC 61508的审核/诊断开始；

SIL认证是依据IEC
61508标准进行认证的，这是由以下部分组成，电气/电子/可编程电子安全相关系统的功能安全：

对于需要SIF的PHA和LOPA识别的每种危害，使用相同的方法分配目标SIL水平。请注意，您可能会有各种目标SIL等级。该过程的下一步是设计一个能够实现所需SIF并达到目标SIL水平的SIS。

对于安全管理，引入IEC61508提出的安全生命周期概念，就是说对于安全相关系统的安全部分，在设计时按照该步骤进行设计，并且需要进行全程的安全评估和验证，目的是进一步减少和安全相关的人为失误，进而减少系统故障风险。

基于IEC 61508标准基础上，ISO 26262标准定义了电气、电子系统的使用安全性。仪表S仪表SIL认证IL设计中的一大难点是如何预先评估潜在的危害和风险，并且采取适当的方法来减小这些风险。为了促进这一过程，ISO规定在开发工作的开始必须要进行“ 危害和风险分析 ”。

1, 执行IEC 61508种安全相关数据通讯的要求基本原则，包含潜在的错误传输，应对措施和影响数据完整性方面的规定

3 1,000至10,000（103至104）

IEC61800-5-2:

6部分：2部分和3部分的应用指南

仪表SIL工业均使用高性能的电子器件进行车辆的安全控制，知名各大仪表SIL厂商所共同制定并认可的ISO 26262 功能安全标准即针对车辆用电子零件、软硬件产品设计的要求进行规范。随着 ISO 26262 的颁布和实施，未来亦能够降低车辆可能发生的风险及意外发生时的危害仪表SIL认证程度，近而使国内的车辆工业提升国际未来的适应力与竞争能力。

目标SIL级别通过使用图4中的表格直接从所需的RRF确定。注意SIL级别和RRF之间的关系。
SIL1的小RRF为101，SIL2的小RRF为102，依此类推。

IEC61800-5-2定义了集成安全驱动器的安全功能，其中定义了一系列停车功能（Stop），即：

业务流程评估

机械安全.控制系统的相关安全部分.1部分:设计用一般原理

IEC 61326-3-1和IEC 61326-3-2标准已经发布，其中规定了安全相关设备的抗扰度水平的附加要求，包括概率非常低的可能发生在任何场所的极端情况。试验模拟设备工作状态下严酷的电磁现象，如瞬时脉冲是模拟数字电路或者数字信号传输的瞬变状态。为了增加安全完整性等级仪表SIL认证（SIL）的电磁抗扰度的可置信度，在进行抗电磁现象性能试验时相对于基础标准要施加更多数量的脉冲或者加长试验的时间以及提高试验等级。例如对用于SIL3的设备，电快速瞬变试验的等级为4kV，试验持续时间应为基础标准规定时间的5倍。

如果需要改善该反应堆的过压保护的PFD，安全工程师可以选择各种方法。

项目文件评估

新版 ISO13849-1 标准即将在2011年底正式生效实施，这将是机械功能安全领域全新的里程碑。在以往要求系统的确定性上，增加了一些系统故障概率方面的评估，从而可以实现从零部件到系统进行全面性安全评估。同时该标准也为设计人员提供了更多的，可以量化的设计实现方法，如增加了系统安全等级 (PLr)、系统平均无危险故障时间 (MTTFd)、系统诊断检测范围 (DC)、共因仪表SIL认证故障预防 (CCF)等参数，从而有效的解决了原有 EN954-1 标准无法实现定量化判断系统安全性的问题。

所需安全可用性（RSA）值与可靠性同义：安全仪表功能在面对危险过程条件时将履行其职责的概率。

评估验证和验证活动

对于我们的油箱溢流示例，小RRF为25，SIF的目标SIL水平为SIL1，因此，这是SIL1危险。

4部分：定义和缩写

SIL认证内容

目标SIF的SIL级别

ISO13849-1:

该标准定义了系统的RAMS（reliability、availability、maintainability和safety），即可靠性、可用性、可维护性和安全性，并且规定了安全生命周期内各个阶段对RAMS的管理和要求，RAMS作为系统服务质量衡仪表SIL认证量的一个重要特征，是在整个系统安全生命周期内的各个阶段通过设计理念、技术方法而得到的。

IEC62061:

RSA的数学补充（PFD = 1 - RSA），

安全完整性等级（SIL）定义为安全功能提供的相对风险降低水平，或指定目标风险降低水平。
简而言之，SIL是安全仪表功能（SIF）所需性能的度量。

铁路应用：可靠性、可用性、可维护性和安全性（RAMS）规范和说明

· 建立概念统一、协调一致的标准架构和体系。

新版 ISO13849-1 标准针对一些新型的控制方法，提供了更有效的安全评估解决方案。可提升控制系统越来越复杂的机械设备的安全等级，保证生产安全性和率，并且结合新技术和设计经验，帮助企业在总体效率、生产力和灵活性方面得到仪表SIL认证提升，保证连续性生产，减少意外停机时间，并降低开发、操作和维护成本。尽快执行该项标准，可保证机械制造商在激烈竞争中抢得市场先机。

SIL是“ 安全完整性等级 ”的首字母缩写，来自工厂所有者/运营商用于量化危险操作的安全性能要求的两个自愿标准：

SIL认证一共分为4个等级，SIL1、SIL2、SIL3、SIL4，包括对产品和对系统两个层次。
其中，以SIL4的要求高。

所有这些步骤完成后，将颁发SIL证书。

IEC61800-5-2标准主要针对安全编码器，安全仪表SIL器，交流伺服系统，伺服驱动器，伺服马达等系统提出了功能安全要求。例如，符合功能安全技术要求的马达控制器将支持安全扭矩停止（STO）以及安全停止 1 (SS1) 等安全功能，防止意外启动的发生，产品设计必须仪表SIL认证符合 EN 61800-5-2 标准中的要求。IEC61800-5-2标准已经转化成为国标，标准号为GB/T 12668.5.2，国内对口的标委会为全国电力电子学标准化技术委员会调速电气传动系统半导体电力变流器分技术委员会(TC60/SC1)。

IEC61326-3-2:

方便地，SIL编号与所需安全可用性（RSA）值中的小“ 9 ”数相匹配。

IEC61508标准的主要目标为：

IEC 61511：过程工业部门的安全仪表系统

SIL认证的步骤是

EN50129

铁路应用：铁路控制和防护系统的软件

过程工业领域安全仪表系统的功能安全要求

运行安全评估的分析和研究

7部分：技术和措施概述

IEC 61508：电气/电子/可编程电子仪表SIL认证安全相关系统的功能安全

- 评估故障模式，影响和诊断分析（FMEDA）分析

SIL要求降低风险因素

机械安全.与安全有关的电气、电子和可编程序电子控制系统的功能安全

· 提供确定安全相关系统安全功能要求的方法;

该PFD值包括传感器，逻辑解算器，终控制元件和工艺管道（包括反应堆容器本身以及任何减压阀和其他辅助设备）的故障概率。

铁路应用：安全相关电子系统

反馈（经验教训）评估的相关性

IEC61511是专门针对流程工业领域安全仪表系统的功能安全标准，它是国际电工委员会继功能安全基础标准IEC61508之后推出的专业领域标准，IEC61511在国内的协调标准为GB/T 21109。在过程工业中，仪表安全系统都被用来执行仪表安全仪表SIL认证功能，IEC61511标准解决了仪表应达到怎样的安全完整性和性能水平的问题。

选择认证其工程流程并获得完整IEC 61508认证的公司也将遵守与软件开发相关的3节。

· 对所有的包括软、硬件在内的安全相关系统的元器件，在生命周期范围提供安全监督的系统方法;

IEC61800-5-2同样定义了一些监控功能，这些监控功能方面有:加速度安全限制；步程安全限制；运动方向安全限制；速度安全限制；矩/力安全限制；位置安全限制；电动机温度安全限制。

1部分：一般要求

测量、控制和实验室用电气设备.电磁兼容性(EMC)的要求：与安全相关的系统和用于与执行安全相关功能(功能安全)

对于与安全相关的装置安全功能的确认，SIL等级是认可度较高的安全完整性定义方法。针对过程仪表SIL认证控制行业，与之相关的国际标准主要有IEC 61508
标准（设计和运行安全仪表系统的基础根据），IEC 61511
标准主要关注过程控制应用的系统，针对装置设计人员遵照 IEC 61511 标准并根据 IEC 61508
标准来完成设计。

SIL级别适用于整个系统。 单个产品或组件没有SIL等级。
在实施SIF时使用SIL级别，该SIF必须将现有的不可容忍的过程风险级别降低到可容忍的风险范围。

4. 规定了几种安全通讯层,作为IEC61784-1和IEC61158系列标准中通讯服务行规部分。

IEC/EN 62061与EN ISO 13849-1:2008标准均包含了与安全有关的电气控制系统。采用这两种标准后，可获得同样等级的安全性能与安全完整性。每种标准采用的方法存在差异，仪表SIL认证但都适于各自的读者。EN ISO 13849-1:2008在其说明部分的表1中给出一种限定情况。当采用复杂的可编程技术时，应将高PL性能等级定义为PLd。

相反，随需应变概率（PFD）与不可靠性同义：

SIL认证依据标准

产品制造商通常满足2节要求，通过FMEDA分析确定其产品适合在给定的SIL水平内使用。

为了能够采用复杂的、可由先前非传统系统结构执行的安全功能，IEC/EN 62061标准提供相应的方法。

为了提供采用传统的系统结构执行更传统的安全功能所需的更直接、更简单的路径，EN ISO 13849-1:2008标准也给出了相应的方法。这两种标准的重要区别是适用于不同的技术领域。IEC/EN 62061标准仅限于在电气系统领域。EN ISO 13849-1:2仪表SIL认证008标准则适用于启动、液压、机械以及电气系统。主要定义的参数为PFH、MTTF、DC、SFF等。

开发和产品设计评估

EN50126

IEC 61784-3：

· 建立基础标准，使其可直接应用于所有工业领域。同时，亦可指导其他领域的标准，使这些标准的起草具有一致性(如基本概念、技术术语、对规定安全功能的要求等);

IEC 61508:

进行数据计算得出结论符合SIL认证哪种等级；

EN50156

EN50128

图4：SIL水平与所需风险降低因子的函数关系。

2 100至1,000（102至103）

测量和控制数字数据通信 三部分 工业网络功能安全行规

- 评估危险失效的可能性（PFD）和每小时危险失效概率（PFH）的仪表SIL认证计算

可调速的电动设备标准.5-2部分: 功能安全要求

5部分：确定安全完整性水平的方法示例

该标准主要定义了如下内容：

2. 各种技术实现的通用内容

例如，具有0.00073的按需故障概率（PFD）的安全仪表功能的RSA值为99.927%，相当于SIL 3等级。

1 10到100（101到102）

IEC61508标准规定了常规系统运行和故障预测能力两方面的基本安全要求。这些要求涵盖了一般安全管理系统、具体产品设计和符合安全要求的过程设计，其目标是既避免系统性设计故障，又避免随机性硬件失效。

3部分：软件要求

什么是SIL水平？

· 鼓励运营商和维护部门使用以计算机为基础的技术;

· 安全断开的力矩/仪表SIL认证安全中断扭距(STO- Safe Torque Off)；

制定ISO
26262标准的目的是使得人们对安全相关功能有一个更好的理解，并尽可能明确地对它们进行解释。ISO 26262是从电子、电气及可编程器件功能安全基本标准IEC61508派生出来的，主要定位在仪表SIL行业中特定的电气器件、电子设备、可编程电子器件等专门用于仪表SIL领域的部件，旨在提高仪表SIL电子、电气产品功能安全的国际标准。此标准一经提出，即受到了各大仪表SIL制造商、仪表SIL零部件商的高度重视，并积极推动该标准在产品开发中的执行。

3. 各种通讯行规簇的功能安全行规的独立描述

2部分：电气/电子/可编程电子设备的要求-安全相关系统

SIF的小RRF =有效频率w / o SIS /可接受仪表SIL认证频率= 2.5 / 0.1 = 25。

SIL（Safety Integrity Level）-安全完整性等级。

每次文件评估后进行补充审核；

电气/电子/可编程电子安全相关系统的功能安全性

SIL认证是什么

4 10,000至100,000（104至105）

每个SIF所需的小RRF用于确定SIF的目标SIL等级。

在我们的罐装溢流实例中，我们确定在应用非SIS保护层后，我们的有效频率为每年2.5次。如果我们可接受的危险频率是10年一次，那么SIF必须具有至少25的风险降低因子（RRF）。

表示在需要时SIF将无法按需执行的概率。

对铁路控制和防护系统的软件进行了安全完善度等级(SIL)的划分，针仪表SIL认证对不同的安全要求制订了相应的标准，按不同等级对整体软件开发、评估、检测过程中，包括对软件需求规格、测试规格、软件结构、软件设计开发、软件检验和测试、软硬件集成、软件确认评估、质量保证、生命周期、文档等提出相应的程序制定初相应的规范与要求。

SIL代表安全完整性等级。 SIL是衡量SIF或SIS的安全系统性能或按需故障概率（PFD）的指标。
有四个与SIL相关的离散完整性级别。 SIL级别越高，安全系统需求失败的概率越低，系统性能越好。
重要的是还要注意，随着SIL水平的增加，通常系统的成本和复杂性也会增加。

重要的是要了解什么是SIL，什么SIL不是。
SIL等级是指安全功能的可靠性，而不是系统的各个组件，也不是整个过程本身。

为了符合标准，必须符合1 - 3部分的要求。仪表SIL认证4 -
8部分仅供参考，可用于理解和应用标准，但不具备一致性要求。

IEC61511:

· 安全停车1/SS1(Safety Stop1)/ 安全停车2/SS2(Safety Stop2)

然后，继续评估文件并完成与组件或功能安全相关的每个文件的调查结果报告；

根据IEC 61508标准（SIL认证），安全系统以及传感设备和执行器进行评估和认证。我们将讨论以下主题，以确保对组件进行详尽而一致的评估（通用或特定于“ 安全回路 ”）：

例如，对于SIL等级为2的化学反应器过程的过压保护系统，对于特定的关闭功能整体而言，按需失效概率在0.01和0.001之间。

ISO26262:

· 安全操作停止(Safety Operation Halt)

SIL技术标仪表SIL认证准是由国际电工委员会（IEC）首先颁布制定的，由IEC/TC65归口实施。SIL技术的归口标准化技术委员会为“ 全国过程工业测量控制及自动化 ”标准化技术委员会（SAC/TC124），秘书处单位为机械工业仪器仪表综合技术经济研究所。

根据IEC标准的定义，有四个SIL级别（1-4）。
较高的SIL水平意味着更大的过程危害和SIS所需的更高级别的保护。
概括如何确定SIL水平，参见图1。SIL水平是危险频率和危害严重程度的函数。
可能更频繁发生或具有更严重后果的危险将具有更高的SIL水平。

注1：概率是特定结果可能性的定量测量。概率值为1或100%意味着有问题的结果肯定会发生。概率值为0（0%）意味着结果是不可能的。概率值为0.3（30%）意味着它将平均发生三次中的三次。

道路车辆系统设计功能安全