SIL 3认证-SIL3安全完整性等级认证指南

产品名称	SIL 3认证-SIL3安全完整性等级认证指南
公司名称	深圳市贝华检测技术有限公司
价格	.00/件
规格参数	检测周期:5--7天 送样地址:深圳宝安 检测认证费用:电话咨询，根据产品评估
公司地址	深圳市宝安区新安街道布心社区74区布心二村商住楼6栋三单元503
联系电话	18824158163 18824158163

产品详情

SIL3认证是什么意思？

SIL3 或安全完整性等级(SIL认证) 是基于与防止特定危险事件的安全仪表功能 (SIF)
相关的风险降低值，或必须如何降低风险才能达到可接受的水平。

SIL认证确定基于定量和定性因素，例如：

1.发展历程

2.安全生命周期管理

安全仪表系统(SIS)的实施是解决危险的常用方法，必须始终确定对此类仪表保护的最终需求。如果需要，必须确定适当的安全完整性等级(SIL)以达到所需的安全等级，这个过程对于实现安全至关重要。

安全完整性等级 SIL3：

安全完整性等级(SIL)基于与防止特定危险事件的安全仪表功能 (SIF)
相关的风险降低值，或必须如何降低风险以达到可接受的水平。

因此，它是安全功能提供的风险降低的相对水平，换言之，提供了对安全仪表功能 (SIF) 性能的衡量。

在IEC 61508 标准中，安全性被定义为“ 免于不可接受的伤害风险 ”，而风险是伤害发生概率和伤害严重程度的组合（R=FxC，其中 F 是事故频率，C是它们的后果，评估为成本；因此 R 定义为每时间单位的成本）。

并非所有功能安全标准都对给定的 SIL 提供相同的要求，IEC 61508 定义了四个 SIL，其中 SIL 4 最可靠，SIL 1 最低。

SIL 是几个国际标准中使用的可靠性和风险降低量度：

ANSI/ISA S84（过程工业部门安全仪表系统的功能安全）

IEC 61508（电气/电子/可编程电子安全相关系统的功能安全）

EC 61511（过程工业部门的安全仪表系统）

IEC 61513（核工业）

IEC 62061（机械安全）

EN 50128（铁路应用——铁路控制和保护软件）

EN 50129（铁路应用——用于信号的安全相关电子系统）

EN 50402（固定气体检测系统）

ISO 26262（汽车行业）

MISRA，各种（汽车应用中的安全分析、建模和编程指南）

国防标准 00-56 第 2 期——事故后果

SIL 的确定基于定量和定性因素，例如开发过程和安全生命周期管理。例如，安全生命周期包括危害和风险评估阶段，在该阶段必须识别所有重大危害事件，然后进行评估以确定安全仪表功能 (SIF) 实现目标所需的风险降低水平风险水平。

SIL 表示 SIF 所需的风险降低或性能，此评估称为 SIL 确定，定义了 SIF 所需的性能或“ 目标 SIL ”，以及目标平均按需故障概率 (PFD)，表示目标 SIL 范围内允许的最大值。

常用的SIL确定方法有：

安全层矩阵（SLM）；风险图（RG）；保护层分析（LOPA）；故障树分析（FTA）；和事件树分析（ETA），它们通常结合使用，LOPA是大型工业设施最常用的，SLM最简单，FTA和ETA最灵活，因此适用于复杂的情况。

SLM 和 RG 用于初步筛选评估，由于其灵活性和注重细节，FTA 特别适用于在确定 SIL 2、SIL 3 或 SIL 4

级别时所需的重新评估。

一般而言，SIL 的分配如下：

计算与特定危害相关的风险，而没有 SIF
的风险降低效果。然后，将确定的风险与认为可接受的风险目标进行比较。SIF
的风险降低必须解决未缓解风险和可容忍风险之间的差异，SIL
目标对应于所需风险降低的相关关系，其中所需的降低越大，所需的 SIL 越高。

国际电工委员会(IEC)标准 IEC 61508 将要求分为硬件安全完整性和系统安全完整性两类。根据标准，设备必须满足这两个类别的要求才能达到特定的 SIL。对于硬件安全完整性，要求是统计的，具有要达到的特定目标，例如危险故障的最大概率和最小安全故障分数。

在I EC EN 61508中，针对低需求操作的不同 SIL
的PFD（按需故障概率）和RRF（风险降低因子）的要求是：

SILPFDPFD（功率）RRFSIL10.1-0.0110-1 – 10-210-100SIL 20.01-0.00110-2 – 10-3100-1000SIL 30.001-0.00110-3 – 10-41000-10.000SIL 40.0001-0.0000110-4 – 10-510.000-100.00

以及对运行或连续运行的高要求（每小时故障概率）

SILPFHPFH（功率）RRFSIL10.00001 – 0.00000110-5 – 10-6100.000 – 1.000.000SIL 20.000001 – 0.000000110-6 – 10-71.000.000 – 10.000.000SIL 30.0000001 – 0.0000000110-8 – 10-910.000.000 – 100.000.000SIL 40.00000001 – 0.00000000110-9 – 10-10100.000.000 – 1.000.000.000

对 SIL 3认证需求：

加工厂很少需要S IL 3 安全功能。

在过程工厂，大多数 SIF 不会要求高于 SIL 1。对于要求高于 SIL 2 的安全功能，必须解决几个问题，关于使用正确的可靠性计算公式，考虑共因故障，使用为共同原因因素选择适当值的正确方法，在计算 PFD
时包括人为错误，在评估中包括所有相关因素，评估所用方法的适当性（如果合适或不；RG、LOPA 和 SLM 不适合 SIL 3，这需要使用故障树审查评估。

事实上，重新评估可能导致将 SIF 的 SIL 3 要求重新分配给较低 SIL 范围内的目标
PFD，从而降低资本和运营成本）。

SIL 3

当需要 SIL 3 时，必须准确检查硬件配置和人机交互与安全功能的组合，确定需要特别注意的需求频率和系统方法（通过使用需求树），涵盖正常操作，异常运行、启动、关闭和从工厂外部发起的需求（服务、电力等），因为这些因素加在一起非常重要。

SIL 3认证测定:

任何预期的 SIL 3 SIF 都需要重新评估，对于 SIL 3，
SIL确定的三个方面值得特别提及：团队能力、警报和人员暴露。

1.关于团队能力

有效的 SIL 确定需要许多专业人员的投入，例如通过与领导者和所有相关学科的代表会面来管理，根据专业技能和个人态度选择，因为他们必须一起工作。此类会议可以很好地用于初步筛选目的，并且可以提供足够的细节来证明 SIL 1 安全功能的合理性，但对于需要更多细节的更高 SIL 来说，任命一名独立专业人员进行评估可能更合适。

2.关于警报

SIL 确定必须考虑操作员对警报响应的潜在风险降低，这可能受到警报进入功能时他的可用性、最终响应时间不足以及在功能中的警报数量的影响。同时。操作员可能难以决定要做什么，必须尽一切努力确保他有所有正确的指示来做出正确的决定并采取正确的行动。

3.关于人员暴露以及故障对工人的潜在后果

有必要考虑处于危险中的人可能在可能发生伤害的工厂区域内的时间比例，同时考虑到，即使对于高危险区，在那里度过的工作日比例非常小（例如低于 10%），也可以在事故发生时要求该人员前往危险区进行调查。在这种情况下，比例会发生巨大变化，因为实际上它会 100% 发生危险事件。

达到SIL 3认证要求:

长期（也就是说，在功能的整个持续时间内）实现和保持 SIL 3 性能是一项非常艰巨的任务。因此，当确定了对 SIL 3 SIF 的需求时，参与风险降低项目的人员发现自己处于复杂的境地，即通过硬件和人机交互的结合来证明 SIL 3 性能，这种情况非常可能会在公司利益相关者或外部监管机构进一步审查时进行讨论。

例如

SIL 3 的主要含义之一是它需要高度重复，这种情况与国际标准中描述为“ 硬件容错 ”的条件有关。或多个故障发生）确定需要多个传感器和多个输出装置，以保证在定期测试之间发生故障的情况下该功能将继续工作。此外，实现 SIL 3 所需的 PFDavg（即在 0.001 到 0.0001 范围内）意味着 SIF 在 1 年 (8760 小时) 期间内无法成功响应的时间最长为 8.76 小时或更短，该值必须包括组织不知道该功能不起作用的时间。

此外，只有在计算 PFD 时满足以下四个条件时，才能达到 SIL 3：

1) 使用的故障率是适当适用于该情况的故障率，如直接现场故障率；

2)对依赖性进行适当的评估，以保证计算不会过于乐观；

3)说明测试期间功能不可用；

4)考虑到人与安全功能的交互，因为人参与了 SIF 的维护、校准和测试以及他们出错的可能性（例如，对 SIL 1 几乎没有影响） PFD) 可能使 SIL 3 无法实现。

因此，与 SIL 1 功能不同，SIL 3 功能需要准确设计人工任务和评估人为错误的概率（并将其包含在 PFDavg 计算中）。此类活动需要专业技能。

SIL 3的总结如下：

SIL 3 是一种安全完整性等级，适用于非常特殊和罕见的情况，其中需要 SIF 的高水平风险降低 性能。

SIL 3 的实际需求必须通过准确和彻底的SIL 确定以及重新评估来确定，同时还要考虑与实现和维持 SIL 3 级别相关的额外成本。

实现 SIL 3 有几个含义，其中包括设计硬件和人机交互组合的安全性能，因此需要来自不同学科的专家参与降低风险的项目。

总之，SIL 3
既是一个目标，也是一个挑战，接近它需要使用个人和组织拥有的最佳技能和专有技术。当确定了对 SIL 3 安全完整性等级的需求时，技术和人类行为必须适应具有挑战性的目标。

实现安全，即“ 免于不可接受的伤害风险 ”，必须是每项生产活动的基本目标，而 SIL 3
是降低风险的新前沿。