

安全标准

机器安全标准的改变

机器制造业各企业能够在其根据机器设备指导方针争取 CE 标识的过程中节省资金和时间。因为一再出现在最终的标准合格评审中暴露出疑问的情形，机器设备与安全相关的控制部分，是否所有的安全功能均符合标准，在该方面，缺失必要的证明文件问题突出。通过前后一致地运用 DIN EN ISO 13849-1 标准，审核验证能有效地达成合格。本文就付诸实施的重点加以阐述。

文 | Pascal Staub-Lang



更多精彩请扫描二维码

台机器必须设计得安全。因此除系统性错误之外还必须掌控安全控制部分的偶然性错误。为此一种适用的途径就是安全性专业标准 DIN EN ISO 13849-1 “机械设备的安全 - 关于控制系统安全相关部分。”它是关于机器设备控制功能安全的核心标准。然而该标准的应用对于计划人员，设计人员而言可能意味着挑战。如果风险评价和审核验证在规划和设计阶段被忽略，则可能导致在最终的标准合格审核中过不了关。当制作者无法通过汇编文献资料证明其产品符合 EG 标准时，那么它将被授予 CE- 标识 并且不予签发合格证书。这就意味着：这台机器不准进入欧洲市场。

必要的证明材料直到生产之后才生成，这可能使事情变得困难；即使当各个组成部分本身是安全可靠的，却也可能由于规划错误或专业能力不足而致它们的能力（合格）没有得到正确的检验或者没有按照实际的标准对要求加以调整。保护回路所达到的性能等级（PL）没有给出计算上的证明或者没有正确地以文献和资料加以说明是十分常见的现象。所以，在一台机器的规划阶段就应优先考虑标



准合格问题，而且必须在设计阶段之前就确定下来。

缺乏对安全功能组件的相关规定

相关标准不仅仅只是在设计新机械设备时重要。同样在现有机器和设备更新改造时也经常需要重新匹配安全纲要。在进行设备翻新改进时必须达到使安全技术措施符合当前的技术水准这一目标。这意味着，在必要时应对安全技术加以补

充，以满足操作安全法规以及在一定情况下机器设备指导方针的要求。这涉及到所有的安全功能以及这些功能之下与安全相关的所有组件（控制系统安全相关部分；SRP/CS）。

DIN 13849 标准虽然包含了设计指导原则，但却回避了有关安全控制实施的具体规定。风险评估采用的是概率理论计算方法。作为规划人员就必须对可能带来危险的安全功能失效的概率，也包

括组件和保护回路失效的概率进行计算。此后作为设计人员就必须能够证明所设计保护回路的能力。虽然该标准允许对用于规划设计的参数采取估算。但是参考相关的标准值还是必要的。这些参考值，例如关于组件的过载能力，理想情况下应该由组件供应方在技术参数说明书、安全手册或者部分情况下的组件合格证书中提供。

在作为安全保护用的组件上，这已经形成了常规。然而在标准组件方面情况却有所不同，在这方面有效的说明和数据有时很难得到。当这些组件在设备控制系统中担当重要的安全功能时，这将会带来问题。于是设计人员往往必须向生产厂家询问一些重要的参数说明，但是并不能每次都得到所需要的答复。通过那些可用于性能等级 PL 计算的数据，可以推测到产品的性价比以及不同生产厂家之间在质量，失效概率和使用寿命等方面的差距。正因为如此组件生产厂家有时在一些具体的和关键的数据上存在保留，因为害怕暴露竞争缺点。在有疑问的情况下机器制造者必须耗费很大精力去设法获得必要的参数。因此，从一开始就把安全功能的布局作为规划过程中固有组成部分来考虑显得更加重要。

新标准的变化

现行 DIN EN ISO 13849-1 文本自 2016 年 7 月生效并代替原先 2008 年的老版本。老版本标准在应用中凸显出一些问题。因此，标准委员会对章节划分和结构作了修订，包括重新对一些概念作了更为明确的定义。现行版本还根据欧洲机械设备指导方针 2006/42/EG 进行了调整。因此，凡根据该标准的规定和结构指导原则开发，设计和制造的机器设备，均遵从推测效应。也就是说，机器产品视同达到了现技术水准并且由此而具备了安全性。

下面是新标准最重要的几点变化：
● 风险评估：风险图表现在还考虑到了故障事件的发生概率。这对于所要求的



图 1 在进行设备翻新改进时必须达到使安全技术措施符合当前的技术水准这个目标。这意味着，在必要时对安全技术加以补充，以满足操作安全法规以及可能的情况下机器设备指导方针的要求

性能等级的分级产生了影响 (PLr- 要求的性能等级)。如果上述发生概率估算结果为“低”，将使得要求的性能等级 PLr 降低一级。这就意味着，对于组件可靠性的要求也随之降低。此外，对于失效发生概率关系密切的还有人为失误的可能性以及可靠性特征参数的正确性。

● 2 类保护回路：对于测试率的要求作了调整，该测试率用于监视 2 类保护回路功能通道的逻辑单位以及为此进行数据流分析 (传感器、逻辑单位、执行器)。类别中结合它们抵御故障的能力和故障状态下的表现划分出与安全相关的各控制系统部件 (SRP/CS)，基于这些部件的可靠性和 / 或结构上的要求。在 2 类保护回路中安全功能的执行情况按照一定的时间间隔，通常通过技术装备自动进行检验。

● 估算性能等级 PL：通常对于机械的，液压的或气动的部件 (或者包含各种工艺的混合体的一些部件) 没有现成的应用专有可靠性数据。因此就使得 PL 值的估算方法趋于简化，以至于可不必计算平均危险失效时间 MTTFd (Mean Time to Dangerous Failure)。必要的安全功能可靠性可以借助于从属的每小时危险失效概率 PFHd- 值 (Probability of Dangerous Failure per Hour) 来估算。

● 带有安全功能的液压部件：对于于

推算 MTTFd 的特性参数值切合实际作了调整。在先前的标准中，像单位时间内操作次数等对于那些应用于安全功能的液压部件并不重要。现在，动作的次数 (所谓操作次数，英文缩写 nop) 这个参数在估算各单个部件的 MTTFd 值时被纳入计算并且为 MTTFd 明确了典型的结合实际的数据值。

● 诊断覆盖率 (DC)：对于冗余路径的综合考虑被表明目的不明显。现在，诊断覆盖率必须对每个关断路径分别予以估算。诊断覆盖率 DC 的计算结果由所有可能导致危险失效的总和来决定。为了简化 PL 的计算，平均诊断覆盖率 (DCavg) 也得到应用。

关于新旧标准的区别以及选择

在 13849-1 标准之前很长一段时间一直是 DIN EN 954-1 作为机械设备功能安全的基本标准，然而该标准相对于目前的技术水准来讲存在缺陷。例如它并没有覆盖依靠电子类可编程系统来保证安全的应用情形。由于该标准已经不合时势，于是便起草了适应现技术水平的新标准。在机械设备安全领域除了 ISO 13849-1，主要要面对的还有 DIN EN/IEC 62061。

这两个标准在功能安全设计应用上都是适用的，要明确的是，哪些技术措

施对于降低安全风险是必需的和适用的。风险评估在两种情况下均依据一个风险图表来进行。IEC 62061 标准 在 2016 年也作了修正和补充，并且根据欧洲机械设备指导方针进行了调整。

到 2019 年年底，一个联合的 ISO-IEC 控制委员会会将两个标准合并。但直至今在这两个标准仍然平行并列同时有效。因此设计人员在任何特定情况下有权选择采用哪一个指导原则来进行风险评估和对自己的安全功能进行证明。根据任务不同，两个标准存在着各自的优点和缺点，这就需要认真地作出权衡，还要看规划人员，设计人员和文献资料汇编全权代表对于规定的熟悉和精通程度。决定性的一点还在于，任何时候仅只应用一个标准而非两个。否则会由于要求和结构指导原则混淆而导致标准合格评审不必要的复杂化。

功能安全专家们在选型上帮助企业并且对其提出的关于应用问题作出解释。专业鉴定人员熟悉这些新标准，了解它们的变化、要求和对于风险评估以及安全相关组件定型的影响。

现行标准 DIN EN ISO 13849-1 相对于老标准有诸多优点。规划人员和设计人员在开发控制系统架构时具有了更多灵活性，这一点也同样体现在组件的选择上。机械设备制造者由此通过更好的选型和比较可能性而节约成本。

所选解决办法的可计算性为机械设备制造者提供了确证，要求的安全等级能够得到遵守。他们怎样做才能在机器的预期使用寿命内保持一定的安全水准，对此设备使用者得到明确的规定。因为各部件危险失效的时间能够很好地估计到，所以人们也能够更好地计划维护。此外，正确的审核验证在处理损失和质保情况时能给予制作者司法保障。

为此，风险评估必须伴随从规划之前直至设备验收的整个开发过程。风险评估是一个重复的过程。也就是说，安全纲要必须持续不断地更新以适应现实情况。



图 2 现行的 DIN EN ISO 13849-1 相对于老的标准提供了诸多优点。规划人员和设计人员现在在开发控制系统架构时具有了更多的灵活性，这一点也同样体现在组件的选择上

为了保持对于分过程有一个清晰总览和必要时对其进行优化，可借助一种功能管理系统（FMS）。第三方，例如来自 TUV

Sud（TUV 南德）的专家们在标准合规核验方面还包括在合适的功能管理系统的选择上能为企业提供帮助。[MM]

COTAO® 科道打印贴标机
4008-213-863 www.cotao.com

广告