SICK AG 白皮书

根据 EN ISO 14119 设计和选择联锁设备

作者

Otto Görnemann
德国瓦尔德基尔希市 SICK AG 公司
机器安全与法规部经理

总结

新版 EN ISO 14119“机械安全 - 与物理防护设备搭配使用的联锁装置 - 设计和选择原则”取代了之前的 EN 1088,过渡期为 2013 年底起 18 个月。其对不同类型的联锁设备进行了分类,并区分物理上的工作与操控原理。此外,其还引入了对激励元件编码的质量评估,并提供防篡改安装说明。由于这些创新和对 EN 1088:2008 现有内容的实际解释,从用户的角度来看, EN ISO 14119:2013 是实用的,易于实施。虽然新的要求对机器制造商来说是微不足道的,但他们却能从许多有利的具体化中获益。

SICK
Sensor Intelligence.

目录

引言 **3**

有什么变化?EN ISO 14119 和 EN 1088 之间的区别 **4**
应用范围和概念 4

闭锁装置的一般原则 **6**
选择正确的联锁装置 6
正向操作和强制打开 6
安装:激励元件的安装和类型 7
保护锁的特点 7
减少规避的可能性 8

对控制系统的要求 **9**
对故障排除的规范 9
操作频率不高时的功能性 9
共同原因的故障 9
解锁的可靠性 9
联锁装置的逻辑串联和故障屏蔽 10

为用户提供的信息 **10**

结论 **11**

引言

新国际标准 EN ISO 14119 定义了设计和选择与物理防护设备结合使用的联锁设备时无关于具体技术的准则。作为符合 ISO 12100-1(基本安全标准)的 B 类标准原则上适用于所有机器。作为 EN ISO 14119:2013,该标准取代了 1995 年的 EN 1088,过渡期为 2013 年底起 18 个月。

物理防护设备在机械制造中很常见。固定物理防护设备简单,可用于机器正常运行不需要人员进入危险区域的地方。然而,这相当于机器在没有任何功能缺陷或中断的情况下运行!但是,这种情况实际上很少出现。

如果需要通过这种固定物理防护设备进入,很可能导致无法将防护设备重新定位在其位置上,或者无法正确地固定。因此,当保不存在防护效果时,有必要采取额外的措施来防止执行危险的机器功能。经典的解决方案是将这些功能的操作与物理防护设备的状态进行联锁。

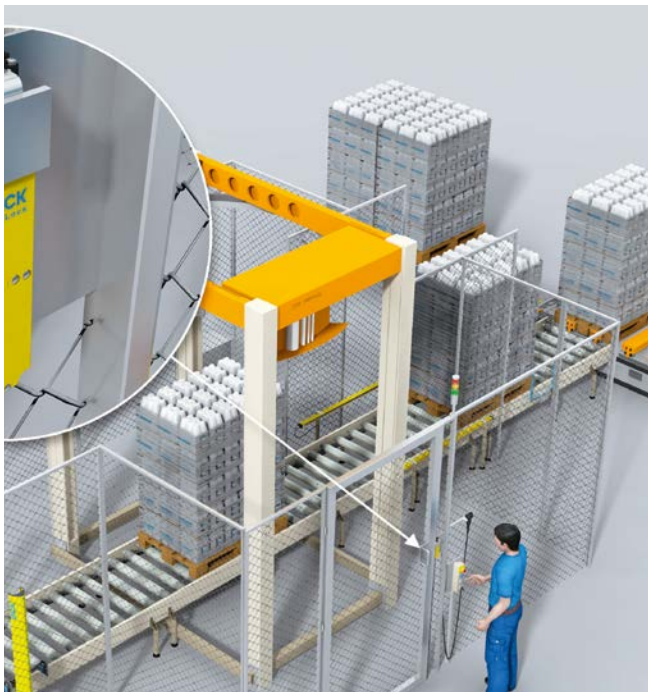

图 1:通过安全锁定装置临时防止进入的防护设备的锁定装置

具体来说,这个国际安全标准描述了以下几点:

- 与物理防护设备搭配的联锁装置的工作原理和典型类型
- 对联锁装置的设计和安装要求
- 选择联锁装置的方法
- 评估规避激励措施的方法
- 对改进避免规避的要求
- 纳入控制系统的要求和
- 对操作人员/用户的信息要求

从标准的标题中已经可以看出,其应用范围并不限于可移动物理防护设备,还包括装有联锁装置的固定物理防护设备。乍一看,这似乎有些矛盾,但如果使用的是物理防护设备,尽管它们不需要在操作时拆除,但必须允许在需要的情况下快速进入,例如在发生故障或维修时。

EN ISO 14119 的应用范围包括所有使用联锁防护设备(如防护门)的机器。在特定机器的 C 标准没有补充或修改 EN ISO 14119 的规定时,该安全标准的规定适用于大量的机器,例如工厂和物流自动化设备。由于其广泛的适用性,新标准具有极其重要的意义。

对旧 EN 1088:2008 的修改和补充对用户有一些相关的影响。

有什么变化?EN ISO 14119 和 EN 1088 之间的区别

与欧洲 EN 1088:2008 相比,现在的国际标准EN ISO 14119:2013 对其基本内容进行了根本性的修订(见图 2)。
主要变化涉及以下几点:

- 由于界定和区分了四种类型的联锁装置,改进了结构
- 说明联锁技术及其各自的优缺点(附件 A 至 E)
- 定义和考虑“以合理可预见的方式规避”
- 评估篡改/规避的动机(附件 H)
- 减少可能的规避行为所需的措施
- 考虑电磁保护锁(5.7.3 节)
- 引入验证锁紧力的测试方法
- 融入控制系统(附件 G)和串联(8.6 节)
- 引入新的防护锁监控触点符号

下面,本文重点介绍了上述对用户(机械制造商)非常重要的创新,并强调了由此产生的新意义。

应用范围和条件
原则上,新标准也针对联锁装置的制造商和用户。与 EN 1088:2008 相比,EN ISO 14119:2013 的应用范围只扩大了两点。除了经典的联锁装置外,还考虑了带电磁保护锁的联锁装置。这一点在应用范围中没有明确解释,但通过将其纳入新的 5.7.3 节来实现。

名称	致动		激励元件		SICK 产品	
	原理	示例	原理	示例	示例	
结构型式 1	机械	物理接触、力、压力	未编码	转换凸轮	i10P	
				转换杆	i10R	
				铰链	i10H	
2 型结构			带编码	成型的激励元件(转换棒)	i16S	
				扳手	–	
结构型式 3	非接触式	感应式	未编码	合适的铁磁材料	IN4000	
		磁式		磁铁、电磁铁	MM12 [1]	
		电容式		所有合适的材料	CM18 [1]	
		超声波式		所有合适的材料	UM12 [1]	
		光学式		所有合适的材料	WT 12 [1]	
结构型式 4		磁式	带编码	编码磁铁	RE11	
		无线射频识别		带编码的 RFID 应答器	TR4 Direct	
		光学式		带编码的光学激励元件	–	

1) 这些传感器不是为安全应用开发。在锁定装置内应用时,设计者必须非常谨慎地考虑可能的系统失效和共因故障并相应采取附加措施。

图 2:类型(型号 EN ISO 14119:2013 的联锁装置结构型式

新列入的要求还包括减少篡改的可能性,即故意和可合理预见的规避行为。需要注意的是,虽然该标准适用于密钥传输系统,但它并不包含所有必要的产品要求。这一点仍需在单独的标准化文件中进行。

定义中增加了一些术语,其他术语则更加精确。这尤其涉及到联锁装置及其元件的定义、激励元件的编码以及由此产生的四种类型的分级。对于激励元件的编码,无论采用何种技术,EN ISO 14119 首次对编码深度进行了划分。如果激励元件的版本数量在 1 ~ 9 之间,则定义为低级编码。在有 10 到 1000 个版本时,标准为中级编码。高级编码需要 1000 多个版本。这些表示编码深度的极限值是以实践为导向,与各制造商协商确定的。

被广泛使用的"安全开关"这一概念并未出现在标准中,因为适用于锁定装置的传感器设计和技术众多,无法定义通用要求。无论采用哪种技术(机械、电气、气动、液压),均适用以下定义:

- 锁定装置至少由激励元件和位置开关组成。
- 位置开关由操作系统和输出系统组成。
- 新的附件 A 至 E 介绍了不同类型的联锁装置及其优缺点,并展示了各种应用示例。

根据所用位置开关的技术和功能安全要求,物理防护设备需要一个或多个锁定装置。

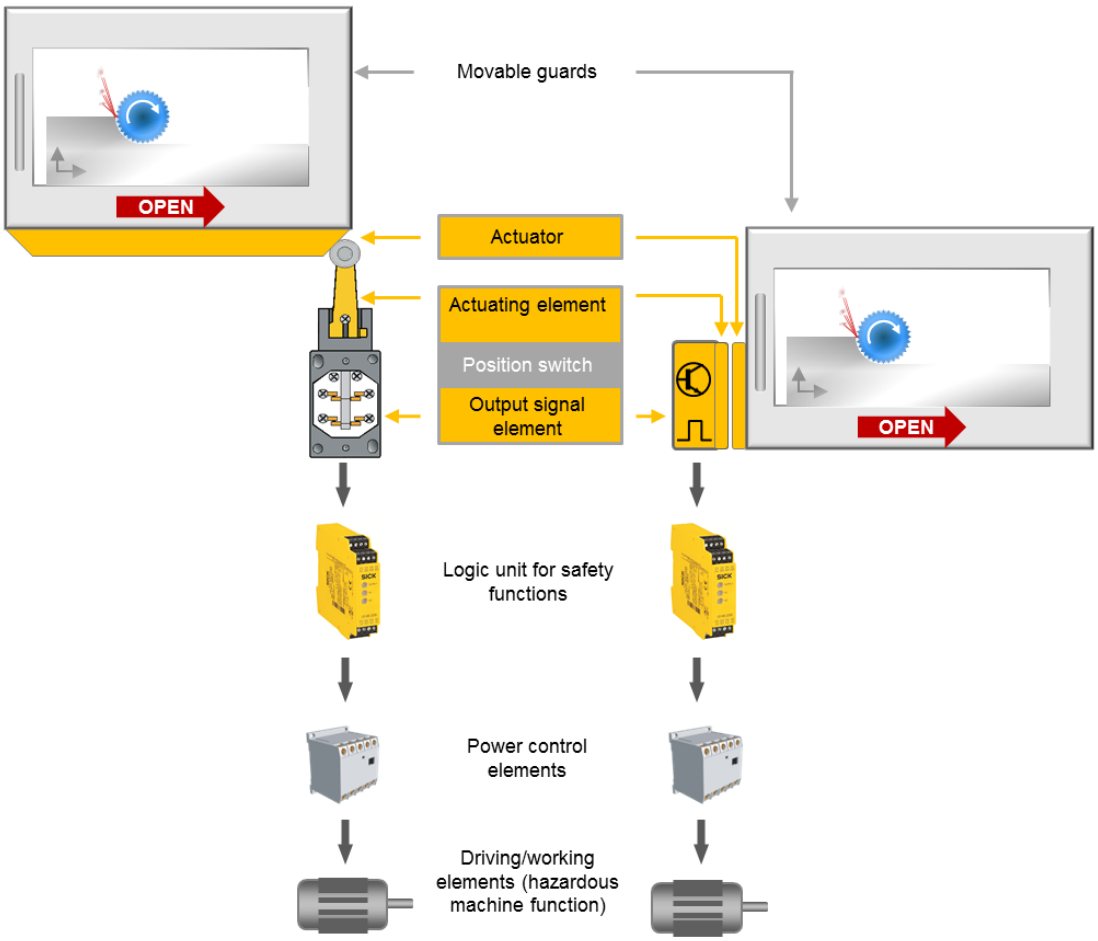

图 3:结构型式 1(左)和结构型式 3(右)联锁的示例。

锁定装置的一般原则

锁定装置是指当防护设备不在保护位置,即安装和关闭时,监测物理防护设备的位置(保护位置)并防止危险机器功能运行的装置。这可以通过防止防护设备不在保护位置(即关闭)时启动,或在防护设备打开时触发停止指令来实现。如果打开可移动物理防护设备,危险的机器功能已经发生,必须在人员到达相关危险点之前及时停止。停止需要一定时间,所谓的"停止时间"。这影响了作业危险点和物理防护设备之间的最小距离要求(见 EN ISO 13855)。

在实际操作中,并不总是能够在机器上实现最小距离。在这种情况下,必须防止进入危险区域,直到没有危险的机器功能发生。为此,物理防护设备的开口必须用保护锁闭锁,保护锁的选择必须符合 EN ISO 14119 标准。保护锁可以是联锁装置的组成部分,也可以是单独的。

可由人(如机器操作人员)随时解锁的保护锁称为无条件防护锁。这时重要的是,这个过程需要相应的时间,使访问时间大于停止时间。但是,如果只有在满足某项条件的情况下才能解锁物理防护设备,例如停止危险动作,在标准中称为有条件解锁。

锁定和解锁可以通过受控的能量输入(电能、气动能、液压能)或储存的能量(弹簧力)来实现。

可如下进行通电解锁锁定装置:
- 定时:若使用时间开关,则该装置失效不得减少延迟时间。
- 自动:只有当不存在危险的机器状态时(如通过停机监测器)。
- 手动:物理防护设备解锁与打开之间的时间必须长于机器危险功能的停止时间。

选择正确的联锁装置
物理防护设备是否必须提供带有或不带有保护锁的锁定装置,取决于是否能达到依据 EN ISO 13855 的最小距离。必须仔细考虑可能的机械负荷。根据 EN ISO 14119,在选择联锁装置时,除了传统的静态载荷外,还必须考虑到动态载荷。例如,这些包括在封闭式安全防护设备上的 2 型联锁装置上的振动或在高执行速度下的机械弹跳。
在环境应力的情况下(如由于磨蚀性灰尘、碎片或其他颗粒),新标准要求额外考虑机械操作的联锁装置可能出现的故障,并采取相应的对策,如隐蔽安装。
另一种可能是使用电磁保护锁,其锁定力由电磁铁产生。电磁保护锁已被新纳入 EN ISO 14119:2013 中,并对其适用额外要求。

正向操作和强制打开
可靠动作是对机械锁定装置的重要要求。在正向操作时,锁定装置的移动机械部件由物理防护设备的机械部件正向移动(例如在防护门上)。这可以通过直接接触或刚性部件来实现。锁定装置的强制动作确保位置开关在物理防护设备打开时致动并降低干忧的可能性。
如果直接由执行系统通过非弹性零件(如弹簧)的限定移动隔离开关触点,则接触元件为强制打开常闭触点。在机械动作式位置开关中使用强制打开常闭触点确保当触点磨损或发生其他电气故障时可执行电路隔离。
EN ISO 14119 规定,当使用机械操作的联锁装置(类型 1 或 2)时,其中至少有一个必须满足正向操作和强制打开的要求。若3 型结构 或4 型结构 的锁定装置是物理防护设备上的唯一锁定装置,则其必须满足 IEC 60947-5-3 的要求。在非接触式位置开关上使用两个冗余的电子输出端,如果对其进行相应的监控,则认为相当于强制打开。

图 4:根据 EN 60947-5-1 附件 K,强制打开触点的标识

安装:执行机构的固定和类型

正确固定是对联锁装置的基本要求。因此,新标准中对固定的要求与原标准中的要求没有区别。然而,接触凸轮切换杆和其他类型的激励元件(机械或非接触式)之间是有区别的,因为这些元件是由机器制造商提供的,而不是由模拟量磁性气缸传感器制造商提供的。EN 1088 禁止将位置传感器作为机械挡针,而新的 EN ISO 14119 则允许这样做——但条件是制造商明确说明这一点,并且位置传感器的使用符合制造商的信息。

虽然对危险点正确距离的要求不属于标准的应用范围,但只有在正确设计联锁装置的情况下,才有可能符合这些要求。

EN ISO 14119 要求物理防护设备的保护作用在每个位置都有效,但引起位置传感器状态变化的位置除外。必须遵守 EN ISO 13857 规定的安全距离或 EN ISO 13855 规定的最小距离。

保护锁的特点

对于与安全相关的应用,必须始终使用通过可控能源输入来解锁的保护锁。根据 EN ISO 14119,只有在风险评估不允许使用这种类型的保护锁时,才可以使用弹簧力解锁。然而,这必须具有同样的安全水平。

如果保护锁用于人身保护以及机器、工件或过程保护,新标准优先考虑人身保护的要求。

物理防护设备的位置监测输出系统和保护锁监测输出系统必须兼容符合 EN ISO 13849-1 或 EN 62061(IEC 62061) 的控制系统上的用途。因此,制造商绝对有必要规定所需的安全参数,如 B10d 或 MTTFd。

虽然 EN 1088 基本要求对通过受控能量释放的保护锁用工具手动解锁,但新标准不再规定这一要求。但是,如果在紧急情况下需要手动解锁,所使用的保护锁必须包含该功能。应该指出的是,风险评估很少能揭示这种必要性。EN ISO 14119 中新增了对辅助和紧急解锁的要求。

如前所述,电磁保护锁已被列入应用范围。新标准在这方面有特殊要求:必须监测锁紧力,以确保达到应用所需的锁定力。在确定所需锁定力时,可参考附件 I 中的表格。它显示了可移动物理防护设备在典型操作情况下的最大驱动力的示例。只有当物理防护设备处于保护位置并达到要求的锁定力时,电磁保护锁才能启用危险机器功能。

与机械式防护锁相反,机电式保护锁可以在不被损坏或破坏的情况下被克服。作用力只能高于锁定力。借助简单的辅助工具就可以实现,并带来规避风险。在这种情况下,EN ISO 14119 要求危险机器的功能不能立即直接重新启动。这一要求的目的是确保在这类规避之后重新启动所需的时间与修复损坏的机械保护锁的时间相符。

根据 EN ISO 14119,可以通过以下措施之一来实现:

- 激活内置复位锁,延迟 10 分钟。
- 产生故障状态,只能通过修理或更换保护锁来终止
- 机器控制系统中造成类似延迟的措施

EN ISO 14119 的另一个新特点是要求独立于所使用的技术来测试锁定力。新标准还规定了相应的安全系数。因此,所使用的保护锁的锁紧力至少应是应用所需锁定力的1.3 倍。

减少规避的可能性

EN 1088 规定的减少物理防护设备上的互锁规避可能性的要求在 EN ISO 14119 中分为一般设计措施和附加设计措施。

新标准还规定了评估规避激励措施和选择所需额外措施的方法。首先,标准的用户必须应用基本的设计措施来减少对联锁的规避。新标准中总结了 EN 1088 中规定的不同类型联锁的措施。在进一步的步骤中,标准的用户必须评估规避锁定装置的激励措施有多强。为此,EN ISO 14119 采用了德国社会事故保险(DGUV/IFA)职业安全与健康研究所开发的方法,在信息性附件 H 中,还展示了一个评估示例。

如果对规避激励措施的评估表明,规避风险需要采取额外的措施,新标准在第 7.2 节中说明了这些措施,并在表 3 中列出了相关的最低要求。

原则和措施	类型 1*和类型 3	第 1 类**	第 2 类和第 4 类, 包括编码等级			包括编码等级的密钥传输系统	
			低	中等	高	中等	高
在正常扫描范围外安装	X		X	X			
可接触性差, 屏蔽							
遮盖式安装							
状态监控或循环测试							
编码器和激励元件的不可拆卸固定							
位置传感器的不可拆卸固定		M				M	M
激励元件的不可拆卸固定		M	M	M	M	M	M
额外的锁定装置, 包括可信度检查	R		R	R			

X = 至少需要采取所列措施中的一项

M = 需要采取这一措施

R = 建议使用这一措施

* 铰链开关除外

** 仅限铰链开关

注 1: 应根据表 3 选择适当的措施来防止归避联锁装置。根据对应用的风险评估, 可能需要采取一种以上的指定措施

注 2: 当一个工厂内使用的密钥数量已知时, 在以下条件下, 可将激励元件的编码作为充分的措施:
- 编码在设备上标明, 每个联锁装置有不同的编码
- 激励元件的编码水平为中度或高度

注 3: 必须明确区分密钥激励元件的编码等级和密钥传输系统的"闩销或脱扣机构"。本表只涉及密钥激励元件的编码。

注 4: 根据表 3 采取的措施只是最低要求。

图 5:EN ISO 14119 表 3,为减少归避联锁装置的可能性而采取的额外措施

对控制系统的要求

EN ISO 14119 的基本创新之一是对评估或实现联锁装置输出的控制系统的要求进行了规范。该标准明确了物理防护设备和保护锁上的联锁装置是控制系统中与安全相关的零件(EN ISO 13849-1),或者是作为子系统(EN IEC 62061)的安全相关电气控制系统的一部分。因此可以避免错误解释。

对错误排除的规范

在新标准中,尽可能地对经常涉及的可能的故障排除问题进行了规范。标准的用户必须牢记,B 标准只能提出适用于大多数机器的一般要求和声明。如果要求控制系统的可靠性水平达到 PL e 或 SIL3,则当某一种故障发生时,安全功能不得失效。根据新的标准,一般情况下,排除某些故障是不合理的,比如激励元件损坏。然而,允许采取根据 EN ISO 13849-2 的错误排除方法。对 PL d 或 SIL2 必须遵守同样的要求。在实践中,这意味着通常需要两个联锁装置才能满足 PL e 或 SIL3 的要求。对于 PL d 和 SIL2,如果按照 EN ISO 13849-1 或 EN IEC 62061 进行的故障分析允许采用相应的故障排除方法,那么一个联锁装置可能就足够了。

操作频率不高时的功能性

在EN ISO 14119 标准中还新增了对很少操作的物理防护设备的联锁功能的检查要求。对于这样的防护设备,在两次操作之间的时间内,有可能出现错误的累积,导致安全功能失效。因此,如果需要进行手动功能测试(以避免这种累积),必须在以下时间间隔内进行:

- 每月 1 次,适用于 PL e(根据 EN ISO 13849-1)或 SIL 3(根据 EN 62061)的应用
- 每年 1 次,适用于 PL d 和 3 类(根据 EN ISO 13849-1)或 HFT=1 的 SIL2(根据 EN 62061 的硬件容错率)的应用

建议机器控制系统显示所需的测试何时被触发,并且这些测试的设计方式应使机器只有在测试成功后才能重新启动。

共同原因的故障

当避免由于具有共同原因的故障引起的故障时,EN ISO 14119 描述了 EN 1088 中已经描述的冗余机械联锁装置的多样化执行的经典解决方案。新标准还一致提到使用不同的驱动能量。例如,采用冗余联锁装置,其中一个通道直接作用于液压动力传输,而第二个通道通过电子位置传感器控制另一个液压阀。

解锁系统的可靠性

在新标准的说明中,对保护锁解锁的可靠性等级要求进行了说明。乍一看,这似乎有些简略——但是,标准的用户应该记住,标准的所谓规范性文本主要应包含各项要求。因此,标准中对用户有帮助的信息只能以备注的形式提供。以下几点非常重要:

- 在大多数情况下(并非总是如此!),保护锁功能所需的 PL 或 SIL 低于锁定装置功能。
- 可以认为,在所需访问时间点,保护锁失效的概率非常低。
- 对于保护锁功能,即使在所需的 PL e 下,一般也可以接受故障排除。
- EN ISO 13849-2:2013 的表 D.8 不适用于保护锁,因为它只适用于联锁装置。

联锁装置的逻辑串联和故障屏蔽

如果位置编码器与冗余触点串联起来,则可以通过操作任意开关在故障和连接的作为控制系统的安全相关部件的安全相关分析之间对故障的识别进行复位。这种现象称为故障屏蔽。如果可以预见,在机器操作人员排除故障的过程中,防护门、维护盖或其他可移动物理防护设备,其锁定装置与安全相关的控制系统之间的联锁将被启动,则故障被屏蔽。因此,必须考虑到错误检测率 DC(用于:Diagnostic Coverage,德语:诊断覆盖率)的相应降低。如果要求联锁功能具有较高的可靠性,则必须采取额外的措施来防止或检测故障。

近日,ISO TR 24119 技术报告已发布。这支持标准的用户对逻辑串联的结果 DC 值进行评估。它包含了更多信息,以及两种评估这种串联对整个联锁功能诊断范围影响的方法。

图6:某电子制造厂中带有多个门的晶圆生产机器

为用户提供的信息

新标准将作为 EN ISO 14119:2013 适用于由机器制造商提供的部件制造的联锁装置和保护锁,以及作为成品装置单独投放市场的联锁装置和保护锁。因此,标准中包含了对此的不同要求。原则上,应采用 EN ISO 12100 的标识要求。如果由于空间原因不能满足这些要求,则适当的产品标识(名称、制造商的标志、型号代号)必须参照包含必要的信息的操作指南。

为了更好地识别输出端(触点等),开发了一种新的国际符号,它们发出保护锁位置的信号(保护锁监控):

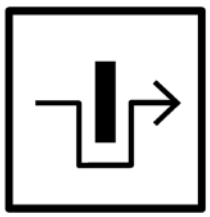

图 7:根据 EN ISO 14119 的规定,标识保护锁监控的符号

除了操作指南中所需的信息和内容(根据机械指令 2006/42 EC 和 EN ISO 12100)外,还根据 EN ISO 14119 增加了更多信息和细节。以下是最重要的几项:

- 用户确定可靠性等级 PL(根据 EN ISO 13849-1)或 SIL(根据 EN 62061)所需的所有信息
- 警告,如果保护锁装置没有紧急或辅助解锁装置,需要为此采取额外措施
- 保护锁作用力 FZh 依据 5.7.4 节
- 允许的操作行程
- 如果联锁装置可用作止动装置,最大允许的冲击能量(J)
- 最大开关电流(峰值)和开关电压
- 编码等级(高-中-低)

结论

结构和编辑的修订,术语的澄清,对 EN 1088 现有内容结合实际的解释和创新,使 EN ISO 14119 变得实用和易于实施。对机器制造商的新要求是可以回顾的。其优势大于众多的具体化,特别是在功能安全和新技术方面。

8025979/2016-01-19 / MK-2M/ITL (2020-09)

参考

EN ISO 14119:2013“机械安全 - 与物理防护设备搭配的联锁装置 - 设计和选择的原则”
EN 1088“机械安全 - 与物理防护设备搭配的联锁装置 - 设计和选择的原则”
EN ISO 13855“机械安全 - 与人体部位接近速度相关的防护设备的布置”
EN 60947-5-2 (IEC 60947-5-3)“低压开关设备 - 控制设备和开关元件 - 对故障条件下具有规定行为的接近设备的要求”
EN ISO 13857“机械安全 - 防止上肢和下肢进入危险区域的安全距离”
EN 62061(IEC 62016)“机械安全 - 与安全有关的电气和电子及可编程电子控制系统的功能安全”
EN ISO 13849-1“机械安全 – 控制系统的安全相关部件 – 第 1 部分:一般设计原则”
EN ISO 13849-2“机械安全 – 控制系统的安全相关部件 – 第 2 部分:验证”
EN ISO 12100“机械安全 - 设计的一般原则 - 风险评估和减少风险”
欧洲议会和理事会 2006 年 5 月 17 日第 2006/42 / EC 号指令“机械指令”

SICK AG | Waldkirch | Germany | www.sick.com

SICK
Sensor Intelligence.