ICS 13.110
J 09

中华人民共和国国家标准

GB/T 30175—2013/ISO/TR 23849:2010

机械安全　应用 GB/T 16855.1 和 GB 28526 设计安全相关控制系统的指南

Safety of machinery—Guidance on the application of GB/T 16855.1 and GB 28526 in the design of safety-related control systems

(ISO/TR 23849:2010, Guidance on the application of ISO 13849 and IEC 62061 in the design of safety-related control systems for machinery, IDT)

2013-12-17 发布　　2014-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照 GB/T 1.1　2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/TR 23849:2010《应用 ISO 13849-1 和 IEC 62061 设计机械安全相关控制系统的指南》(英文版)。

本标准等同翻译 ISO/TR 23849:2010。为便于使用,本标准做了下列编辑性修改:

——标准名称修改为《机械安全 应用 GB/T 16855.1 和 GB 28526 设计安全相关控制系统的指南》;

——删除了国际标准的前言并按照我国标准的要求重新起草了前言;

——对 GB 30175　2013 引用的其他标准,用已被等同采用为我国的标准代替对应的国际标准,未被等同采用为我国标准的直接引用国际标准。

本标准由全国机械安全标准化技术委员会(SAC/TC 208)提出并归口。

本标准起草单位:苏州澳昆智能机器人技术有限公司、欧姆龙自动化(中国)有限公司、深圳市华测检测有限公司、中机生产力促进中心、广西柳工机械股份有限公司、西门子(中国)有限公司、皮尔磁工业自动化贸易(上海)有限公司、国家机床质量监督检验中心、南京林业大学光机电仪工程研究所、罗克韦尔自动化(中国)有限公司。

本标准主要起草人:李政德、李立言、朱平、杨军、张天强、洪刚、罗广、褚卫中、王己妍、徐凯、黄之炯、赵钦志、华镕、张晓飞、李勤、王学智、居荣华、李建友、程红兵、宁燕、刘治永、付卉青、戴群亮、王旭光。

引　言

机械领域安全标准的结构如下：

- A 类标准(基础安全标准)　给出能适用于机械的基本概念、设计原则和一般特性的标准；
- B 类标准(通用安全标准)　规定能在较大范围应用的机械的一种安全特性或一类安全装置的标准：
  1) B1 类标准　规定特定的安全特性(如安全距离、表面温度、噪声)的标准；
  2) B2 类标准　规定安全防护装置(如双手操纵装置、联锁装置、压敏装置、防护装置)的标准。
- C 类标准(机器安全标准)　对一种特定的机器或一组机器规定详细安全要求的标准。

根据 GB/T 15706，本标准属于 B 类标准。

本标准的首要目的是帮助 GB 28526 和 GB/T 16855.1 的使用者理解两项标准之间的关系，以使其有信心根据其中一项标准设计安全相关的控制系统。

机械安全　应用 GB/T 16855.1 和 GB 28526 设计安全相关控制系统的指南

1　范围

本标准规定了如何应用 GB 28526 和 GB/T 16855.1[1] 设计安全相关控制系统的指南。

本标准适用于所有控制系统安全相关部件，无论其使用何种类型的能源，例如电力的、液压的、气动的、机械的等。

2　概述

2.1　GB 28526 和 GB/T 16855.1 均规定了安全相关控制系统在设计和使用方面的要求。这两项标准给出的方法虽然不同，但如果正确使用，都可以达到相似的风险减小水平。

2.2　这两项标准都将所执行安全功能的安全相关控制系统根据每小时的危险失效概率进行分级。GB/T 16855.1 分为五个性能等级(PL)：a、b、c、d 和 e，而 GB 28526 则分为三个安全完整性等级(SIL)：1、2 和 3。

2.3　产品标准(C 类标准)的技术委员会(TC)详细说明安全相关控制系统的安全要求，并建议这些技术委员会根据 PL 和 SIL 明确安全系统的等级。

2.4　机械设计者可根据具体的应用特点选择使用 GB 28526 或 GB/T 16855.1。

2.5　选择和使用哪一项标准可能需要通过以下因素来确定，例如：

——之前设计机械安全相关控制系统的知识和经验是基于 GB/T 16855.1—2005 中给出的类别时，则使用 GB/T 16855.1—2008 更合适；

——安全相关控制系统不是基于电气技术时，则使用 GB/T 16855.1—2008 更合适；

——客户需要以 SIL 说明机器安全相关控制系统的安全完整性时，使用 GB 28526 更合适；

——机器安全相关控制系统用于过程工业等领域时，此时安全相关的系统(如符合 GB/T 21109 的安全仪表系统)是以 SIL 来规定特征的，则使用 GB 28526 更合适。

3　标准的比较

3.1　根据以下几个方面比较 GB/T 16855.1 和 GB 28526 的技术要求：

——术语；

——风险估计和性能分配；

——安全要求规范；

——系统完整性要求；

——诊断功能；

——软件安全要求。

3.2　此外，对根据这两项标准通过简化的数学公式如何确定危险失效概率(PFH_D)和 $MTTF_d$ 进行了评价。

---

1)　本标准考虑的是 GB/T 16855.1—2008，而不是已被其代替的 GB/T 16855.1—2005。

3.3 上述工作得出以下结论：

通过集成分别按照 GB 28526 和 GB/T 16855.1 设计的不复杂的安全相关的电气控制系统(SRECS)子系统或控制系统安全相关部件(SRP/CS)，使用两项标准其中一项均可设计出达到功能安全可接受水平的安全相关控制系统。

通过集成按照 GB/T 20438 设计的电气/电子/可编程电子子系统，这两项标准也可用于提供复杂 SRECS 和 SRP/CS 的设计方案。

目前机械行业的使用者均可利用这两项标准，并且经验表明将得到很大的好处。一定阶段内，这两项标准实际应用情况的反馈将推动与 GB 28526 和 GB/T 16855.1 等同的国际标准 IEC 62061 和 ISO 13849-1 的合并。

目前还存在细节上的差异，一些概念(如功能安全管理)需要进一步研究，以达到各自设计方法和一些技术要求之间的平衡。

4 风险估计以及所要求性能的指定

4.1 已对确定具体安全功能 SIL 和/或 PL_r 使用的方法进行比较，并且已明确每项标准的附录 A 中各自给出的方法之间存在很好的对应关系。

4.2 不管使用了哪种方法，很重要的一点是注意确保对风险参数进行合适的判断，以确定可能适用于具体安全功能的 SIL 和/或 PL_r。通常，这种判断最好是使相关人员(如设计者、维护人员、操作者)共同参与，以确保正确理解机械上可能存在的危险。

4.3 关于风险估计和性能确定过程的更多信息可参见 GB/T 15706 和 GB/T 20438.5。

5 安全要求规范

5.1 GB/T 16855.1 和 GB 28526 各自的方法在第一阶段均要求规定由安全相关控制系统执行的安全功能。

5.2 宜对控制电路执行的每种安全功能进行评估，如使用 GB/T 16855.1 的附录 A 或 GB 28526 的附录 A。宜确定需要机器每种特定的安全功能减小多少风险，然后确定执行安全功能的控制回路需要的等级。

5.3 以 PL 和/或 SIL 规定的等级与具体的安全功能有关。

5.4 下面给出了宜由产品标准(C 类标准)给出的与安全功能相关的信息。

由控制电路执行的安全功能：

安全功能的名称

功能的描述

符合 GB/T 16855.1 所需的性能等级：PL_r a～e

和/或

符合 GB 28526 所需的安全完整性等级：SIL 1～3

6 性能目标指定：PL 与 SIL

表 1 给出了基于每小时平均危险失效概率的 PL 和 SIL 之间的关系。然而，除了这些同样适用于安全相关控制系统的概率目标之外，两项标准都规定了其他要求(如系统安全完整性等级)。这些要求的严格程度与各自的 PL 和 SIL 有关。

表 1 基于每小时平均危险失效概率的 PL 和 SIL 之间的关系

性能等级(PL)	每小时平均危险失效概率(1/h)	安全完整性等级(SIL)
a	$\geqslant 10^{-5} \sim < 10^{-4}$	无特殊的安全要求
b	$\geqslant 3\times 10^{-6} \sim < 10^{-5}$	1
c	$\geqslant 10^{-6} \sim < 3\times 10^{-6}$	1
d	$\geqslant 10^{-7} \sim < 10^{-6}$	2
e	$\geqslant 10^{-8} \sim < 10^{-7}$	3

7 系统设计

7.1 使用 GB 28526 和 GB/T 16855.1 进行系统设计的一般要求

在设计 SRECS 和 SRP/CS 时，宜考虑以下几个方面：

——当在两项标准各自限定范围内使用时，可采用任意一项标准设计具有可接受安全功能的安全相关控制系统，用达到的 SIL 或 PL 表示。

根据 GB/T 16855.1 相关的 PL 设计的不复杂安全相关部件可作为子系统集成到按照 GB 28526 设计的 SRECS 中。任何按照 GB/T 16855.1 相关的 PL 设计的复杂安全相关部件可集成到按照 GB/T 16855.1 设计的 SRP/CS 中。

——任何按照 GB 28526 相关的 SIL 设计的不复杂子系统都可作为安全相关部件集成到按照 GB/T 16855.1设计的 SRP/CS 组成中。

——根据 GB/T 20438 相关的 SIL 设计的复杂子系统都可作为安全相关部件集成到按照 GB/T 16855.1设计的 SRP/CS 中，或者作为子系统集成到按照 GB 28526 设计的 SRECS 中。

7.2 PFH_D 与 $MTTF_d$ 的估计以及故障排除的使用

7.2.1 PFH_D 与 $MTTF_d$

7.2.1.1 GB/T 16855.1 中的 $MTTF_d$ 值只有在与不带诊断的单通道 SRP/CS 相关时，才是 GB 28526 中 PFH_D 的倒数。

7.2.1.2 $MTTF_d$ 是一个或多个组件和/或不考虑任何给定因素(如诊断和结构)的单通道的一个参数，而 PFH_D 是考虑了多种因素(如诊断和依赖于设计构架的结构)的子系统的一个参数。

7.2.1.3 GB/T 16855.1 的附录 K 给出了按照类别和诊断覆盖率(DC)分类的不同结构的 SRP/CS 的 $MTTF_d$ 与 PFH_D 之间的关系。

7.2.1.4 对于符合 GB/T 16855.1 的串联 SRP/CS 的组合，其 PFH_D 的估计也可按照 GB 28526 中子系统的类似方式，即通过累加每个 SRP/CS 的 PFH_D 值(如来自 GB/T 16855.1 的附录 K 中的值)来完成。

7.2.2 故障排除的使用

7.2.2.1 两项标准都允许故障排除，见 GB 28526 的 6.7.7 和 GB/T 16855.1 的 7.3。对于要求达到 SIL3 且不带硬件故障裕度的 SRECS，GB 28526 不允许故障排除。

7.2.2.2 故障排除的正确性和有效性对于 SRP/CS 或 SRECS 的预期寿命是非常重要的。

7.2.2.3 通常，当 SRP/CS 或 SRECS 执行的安全功能规定为 PLe 或 SIL3 时，单独依靠故障排除达到该性能等级是不正常的。这取决于所使用的技术和预定的使用环境。因此，在 PL 或 SIL 提高时，设计者需要特别注意故障排除的使用。

7.2.2.4 设计 SRP/C 或 SRECS 时，为了达到 PLe 或 SIL3，故障排除通常并不适用于机电位置开关和手动开关（如急停装置）的机械部分。可应用于特殊机械故障情况下（如磨损/腐蚀、破裂）的故障排除在 GB/T 16855.2 中给出。

7.2.2.5 例如，由于通常不能对开关执行器损坏等故障进行故障排除，因此为了达到 PLe 或 SIL3，已实现 PLe 或 SIL3 的门联锁系统需要的最低故障裕度为 1（如两个常规的机械位置开关）。然而，在按照相关标准设计的控制面板内，对线路短路等故障的排除可能是可接受的。

7.2.2.6 更多关于使用故障排除的信息将在修订后的 GB/T 16855.2 中给出。

7.3 使用符合 GB 28526 或 GB/T 16855.1 的子系统或 SRP/CS 进行系统设计

7.3.1 在任何情况下，按照 GB/T 16855.1 或 GB 28526 设计的子系统或 SRP/CS，只有满足了所有系统级（相关的）标准的要求，才能声明符合相应的系统级标准。

7.3.2 设计子系统或 SRP/CS 的部件时，应分别满足 GB 28526 或 GB/T 16855.1。假如每项标准都得到完全满足，则应完全遵循这些标准。

7.3.3 设计子系统或 SRP/CS 的部件时，不允许混合使用这两项标准的部分要求。

7.4 使用按照其他标准设计的子系统或 SRP/CS 进行系统设计

7.4.1 在设计过程中，可能需要选择满足其他标准的子系统，这些子系统符合相关产品标准以及 GB/T 20438、GB 28526 或 GB/T 16855.1 的中的任意一个，例如电敏防护装置。这类子系统的销售商宜提供必要的信息，以便于将这些系统集成到符合 GB 28526 或 GB/T 16855.1 的安全相关控制系统中。

7.4.2 根据 GB 28526（也可见 GB 28526 的 6.7.3）和 GB/T 16855.1，满足 GB/T 20438 的要求且已按照产品标准（如 IEC 61800-5-2）设计的子系统，如可调速电气传动系统，可用在安全相关控制系统中。

7.4.3 根据 GB 28526，已按照其他标准设计标准设计的其他子系统满足 GB 28526，6.7.3 的要求。

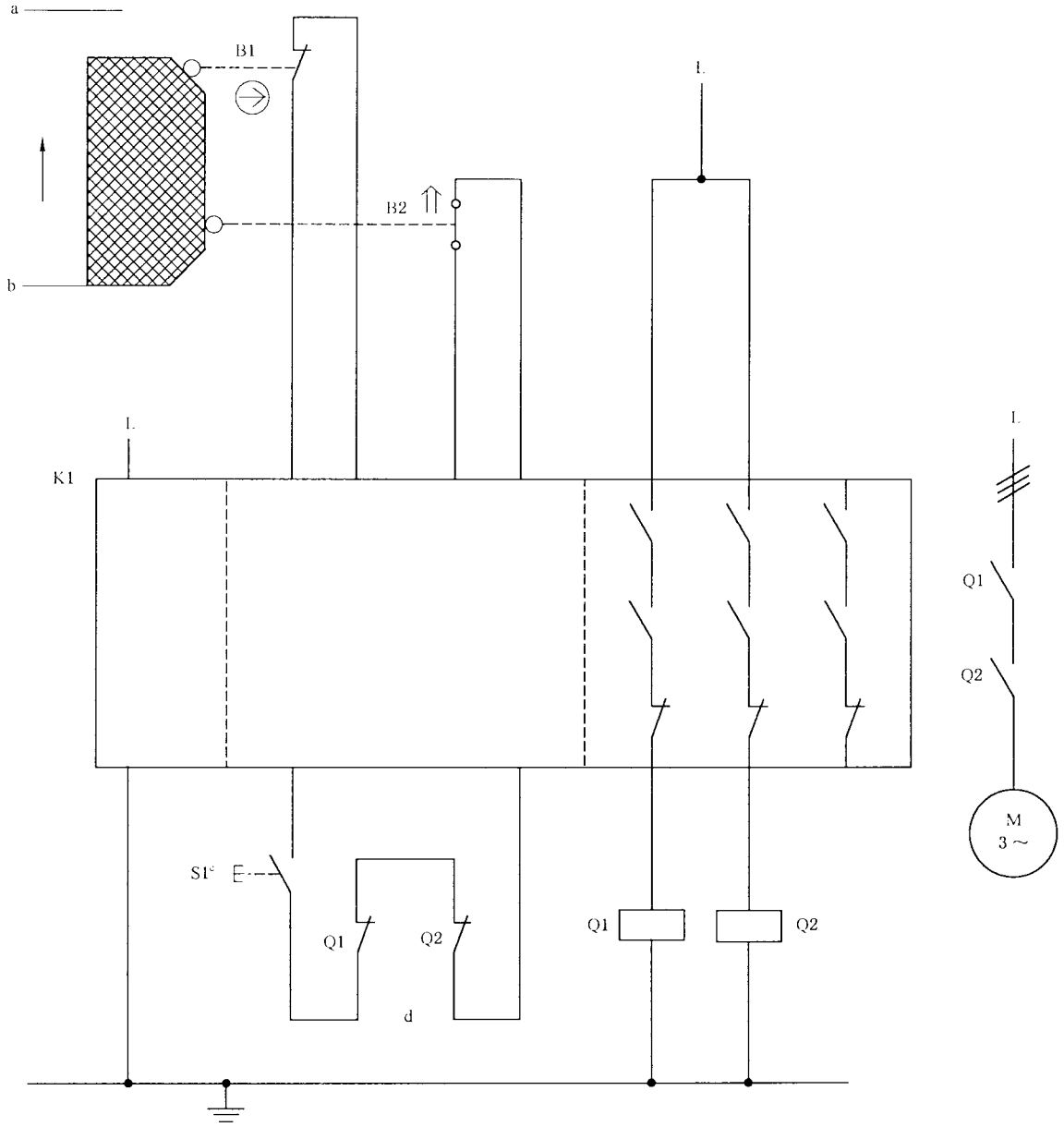
8 示例

8.1 概述

以下示例假定已满足两项标准中的所有要求。示例只用于演示标准应用的特定方面。

8.2 设计和确认执行规定安全相关控制功能的安全相关控制系统的简化示例

8.2.1 这个简化示例用于演示如何使用符合 GB 28526 和/或 GB/T 16855.1 的子系统或 SRP/CS。本示例基于一种安全功能的执行，该安全功能是与活动式防护装置位置监控相连的安全相关停止功能，规定的安全完整性等级为 SIL3/所需的性能等级为 PL,e，见图 1。



说明：

⇑ ——驱动位置；

[a] ——打开位置；

[b] 关闭位置；

[c] 启动；

[d] 反馈电路。

图 1 执行安全功能的示例

8.2.2 以下是与本示例的安全要求规范相关的信息。

安全功能

由保护装置触发的安全相关停止功能：打开活动式防护装置触发 STO 安全功能(安全扭矩卸除)。

功能描述

通过活动式防护装置(保护栅栏)来防护陷入式危险。由两个动断触点/动开触点组合的位置开关 B1/B2 探测联锁防护装置的打开,并通过主安全模块 K1 进行评价。K1 驱动 Q1 和 Q2 两个接触器,使中断或防止危险运动或状态的接触器断开。

为了进行故障探测,K1 监控位置开关的合理性。Q1 和 Q2 中的故障由 K1 中的启动测试进行检测。只有 Q1 和 Q2 已可靠切断,启动指令才有效。通过打开和关闭联锁装置进行启动测试,则不是必需的。

发生组件失效时,安全功能保持完好。操作期间或驱动(打开和关闭)联锁防护装置导致 Q1 和 Q2 可靠切断,以及无法操作时,故障被探测到。操作期间或驱动(打开和关闭)联锁防护装置时如果检测到故障,Q1 和 Q2 会被切断并且操作无效。

两次连续驱动之间的时间段内,两个以上的故障积累可导致安全功能丧失。

8.2.3 还宜给出以下特性:

遵循基本的和经验证的安全原则(如接触器 Q1 和 Q2 的负载电流通过乘以 50% 的系数降低额定电流),并且满足 B 类的要求。配备保护回路(如接触保护)。

保护装置的稳定布置用以确保驱动位置开关的动作。

开关 B1 是符合 GB 14048.5 2008,附录 K 的具有直接打开动作的位置开关。

分开放置位置开关 B1 和 B2 的导线,或者予以保护。

8.2.4 SRP/CS 每个部件的设计过程中,可从制造商处获得以下信息:

制造商声明满足类别(Cat.)4、PL e 和 SIL CL 3 要求的安全模块 K1[2)]。

接触器 Q1 和 Q2 是具有机械连接的基础元件,并且满足 GB 14048.5—2008,附录 L。

8.2.5 对 SRP/CS 和/或 SRECS 的设计可进行以下观察:

只有用于不同保护装置的几个机械位置开关没有串联连接(即无级联)时,才能达到类别 4。这是有必要的,否则不能检测开关中的故障。

8.2.6 按照 GB/T 16855.1 计算失效概率

图 2 给出了与双通道输入和输出元件相连的逻辑子系统(安全模块 K1)。由于已提取出安全相关模块图中的硬件,从而子系统的顺序原则上是可互换的。因此,建议将同一结构的子系统分为一组,如图 3 所示。这可以将单通道 $MTTF_d$ 的时间限制降低至 100 年,从而实现估计过程中的 PL 计算简化。

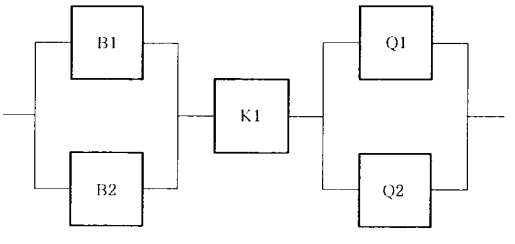
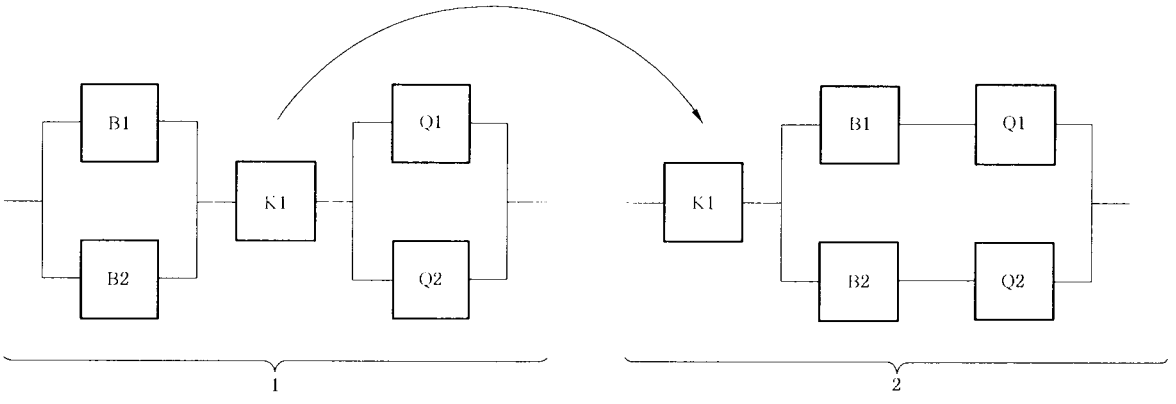


图 2 安全相关模块图

2) 该模块作为子系统,同样,不需要给出其单个通道的 $MTTF_d$(见 7.2.1.1)。



说明：

1　硬件相关的表示：作为子系统的三个 SRP/CS；

2　简化的逻辑表示：作为子系统的两个 SRP/CS。

图 3　符合 GB/T 16855.1 的计算用安全相关模块图

安全模块 K1 的失效概率由制造商声明，并在计算结束时加上此概率[每小时 2.31×10^{-9}（制造商给定值），适用于 PLe]。对其余子系统，其失效概率的计算如下：

——$MTTF_d$：B1 机械部件的 B_{10d} 规定为 1 000 000 个周期（制造商给定值）。位置开关 B2 的 B_{10d} 为 500 000 个周期（制造商给定值）。每年工作 365 天，每天工作 24 小时，并且一个周期为 900 s（15 min）时，根据 GB/T 16855.1 的公式(C.2)和公式(C.7)计算得出的这些组件的 n_{op} 为每年 35 040 个周期：

$$n_{op}=\frac{d_{op}\cdot h_{op}\cdot 3\,600\,\frac{s}{h}}{t_{cycle}}=\frac{365\,\frac{d}{y}\cdot 24\,\frac{h}{d}\cdot 3\,600\,\frac{s}{h}}{900\,\frac{s}{cycle}}=35\,040\,\frac{cycles}{y}$$

$$MTTF_{d,B1}=\frac{B_{10d}}{0.1\cdot n_{op}}=\frac{1\,000\,000cycles}{0.1\cdot 35\,040\,\frac{cycles}{y}}=285y$$

$$T_{10d,B1}=\frac{B_{10d}}{n_{op}}=\frac{1\,000\,000cycles}{35\,040\,\frac{cycles}{y}}=28.5y$$

$$MTTF_{d,B1}=\frac{B_{10d}}{0.1\cdot n_{op}}=\frac{500\,000cycles}{0.1\cdot 35\,040\,\frac{cycles}{y}}=143y$$

$$T_{10d,B2}=\frac{B_{10d}}{n_{op}}=\frac{500\,000cycles}{35\,040\,\frac{cycles}{y}}=14.3y$$

B2 的 T_{10d} 值为 14.3 年。如果整个 SRP/CS 的任务时间预期为 20 年，则在 14.3 年之后应替换 B2。

对于接触器 Q1 和 Q2，感性载荷（AC 3）下的 B_{10} 为 1 000 000 个周期的电气寿命（制造商给定值）。如果假定 50%的失效是危险的，则 B_{10d} 为 B_{10} 的两倍：

$$MTTF_{d,Q1/Q2}=\frac{B_{10d}}{0.1\cdot n_{op}}=\frac{2\,000\,000cycles}{0.1\cdot 35\,040\,\frac{cycles}{y}}=571y$$

$$T_{10d,Q1/Q2} = \frac{B_{10d}}{n_{op}} = \frac{2\ 000\ 000 \text{cycles}}{35\ 040 \frac{\text{cycles}}{\text{y}}} = 57.1\text{y}$$

根据 GB/T 16855.1 的公式(D.1)计算两个通道的 $MTTF_d$：

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}}$$

$$\frac{1}{MTTF_{d,Ch1}} = \frac{1}{285\text{y}} + \frac{1}{571\text{y}} = \frac{1}{190\text{y}}$$

$$\frac{1}{MTTF_{d,Ch2}} = \frac{1}{143\text{y}} + \frac{1}{571\text{y}} = \frac{1}{114\text{y}}$$

计算结果得出 $MTTF_{d,Ch1}$ 为 190 年，$MTTF_{d,Ch2}$ 为 114 年。根据 GB/T 16855.1，两个通道的 $MTTF_d$ 限定在 100 年内，此时，由于限制后两个通道的 $MTTF_d$ 相等，因此，不必实现对称。

DC_{avg}：基于 K1 中动断触点/动开触点组合的可靠监控得出 B1 和 B2 的 DC 为 99%。由启动期间 K1 常规监控得出触点 Q1 和 Q2 的 DC 为 99%。DC 值根据每个子系统的 DC_{avg} 予以规定。根据 GB/T 16855.1 的公式(E.1)计算 DC_{avg}。由于每个单独的 DC 为 99%，因此 DC_{avg} 也为 99%。

——子系统 B1/B2 和 Q1/Q2(70 分)中需要采取充分的措施防止共因失效：隔离(15)、经验证的元件(5)，过压保护等(15)，以及环境条件(25+10)。

——任务时间：根据 GB/T 16855.1 中的简化方法，假定任务时间为 20 年。

子系统 B1/B2/Q1/Q2 对应于高 $MTTF_d$(100 年)和高 DC_{avg}(99%)的 4 类。这使得每小时的平均危险失效概率为 2.47×10^{-8}(见 GB/T 16855.1 的表 K.1)。后面附加的子系统 K1，其每小时的平均危险失效概率为 2.47×10^{-8}。这对应于 PLe。

8.2.7 根据 GB 28526 计算失效概率

8.2.7.1 根据 GB 28526 的 6.6.2，回路布置可分为三个子系统：B1/B2、K 和 Q1/Q2，如图 2 所示。

8.2.7.2 对于子系统 K，制造商声明每小时的失效概率为 2.31×10^{-9}，安全模块 K1 的 SIL 限定为 3。

8.2.7.3 对于其余的子系统，可按如下方法估算失效概率：

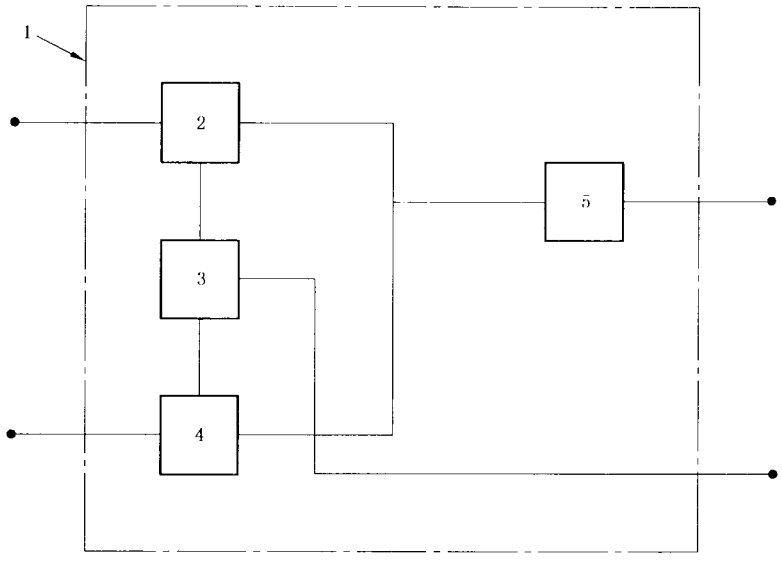
——子系统 B1/B2：B1 机械部件的 B_{10d} 为 1 000 000 个周期(制造商给定值)。位置开关 B2 的 B_{10d} 为 500 000 个周期(制造商给定值)。每年工作 365 天，每天工作 24 小时，并且一个周期为 15 分钟时，这些组件的 C 为每小时 4 个周期。计算出失效率为 $0.1\times C/B_{10d} = 4.00\times10^{-7}$/小时。这就得出 B2 的失效率为 8.00×10^{-7}/小时。

注：符合 GB 28526 的应用中，操作周期的数量 C 对应于 GB/T 16855.1 中的年平均操作次数 n_{op}。因此，C 的单位为周期/每小时，n_{op} 的单位为周期/每年，即存在以下关系：

$$C = n_{op} \cdot \frac{\text{y}}{365.24\ \text{h}}$$

因此，每天的平均运行小时数和每年的平均工作天数影响 C 和 n_{op} 的值。

本子系统的逻辑结构等同于 GB 28526 中 6.7.8.2.5 的模块图 D，如图 4 所示。



说明：

1——子系统 D；

2——子系统元件 λ_{De1}；

3——诊断功能；

4——子系统元件 λ_{De2}；

5——共因失效。

图 4　子系统 D 的逻辑表示(表达方式)

——子系统元件(开关 B1 和 B2)的设计不同，因此，根据 GB 28526 中 6.7.8.2.5 中的公式(D.1)，按照以下计算确定子系统的 PFH_D：

$$\lambda_{DssD}=(1-\beta)^2\{[\lambda_{De1}\times\lambda_{De2}\times(DC_1+DC_2)]\times T_2/2+[\lambda_{De1}\times\lambda_{De2}\times(2-DC_1-DC_2)]\times T_1/2\}+\beta\times(\lambda_{De1}+\lambda_{De2})/2$$

$$PFH_{DssD}=\lambda_{DssD}\times 1\ h$$

式中：

T_2　诊断试验间隔时间；子系统 B1/B2 的诊断时间间隔为 15 min。

T_1　验证试验间隔或寿命，取其中的较小值。对于子系统 B1/B2，根据子系统元件最小的 T_{10d}(见 GB/T 16855.1，C.4.2)，在给定使用率下，寿命间隔为 125 000 h(14.3 年)。位置开关 B2 有最小的 B_{10d}。验证试验间隔(见 GB 28526 的前言)假定为 20 年(175 200 h)，大于寿命。因此，T_1 取 125 000 h。

β　共因失效的敏感度。根据 GB 28526，附录 F 中的简化方法：隔离(5+5+5)、评估/分析(9)以及环境条件(9+9)，得分为 42 分，因此它的值为 5%(0.05)。

λ_{De1}　子系统元件 1 的危险失效率。对于开关 B1，等于 4.00×10^{-7}/h(如上所示)。

DC_1　子系统元件 1 的诊断覆盖率。基于结合 K1 对动断触点/动开触点 B1 和 B2 的合理性监控，开关 B1 的估计值为 99%。

λ_{De2}　子系统元件 2 的危险失效率。对于开关 B2，等于 8.00×10^{-7}/h(如上所示)。

DC_1　子系统元件 2 的诊断覆盖率。基于结合 K1 对动断触点/动开触点 B1 和 B2 的合理性监控，开关 B1 的估计值为 99%。

8.2.7.4　根据上述数据计算得出 PFH_D 的值为 3.04×10^{-8}/h。

8.2.7.5　类似地，对于子系统 Q1/Q2：感性载荷(AC 3)下的 B_{10} 为 10^5 个周期的电气寿命(制造商给定

值)。如果假定50%的失效是危险的,则B_{10d}为B_{10}的两倍。由上面对C的假定值得出每个触点的失效率为2.00×10^{-7}/ h。

8.2.7.6 子系统Q1/Q2的逻辑结构等同于GB 28526的6.7.8.2.5中的模块D。子系统元件(接触器Q1/Q2)的设计相同,因此,用公式(D.1)确定子系统的PFH_D:

$$\lambda_{DssD}=(1-\beta)^2\{[\lambda_{De}^2\times2\times DC]\times T_2/2+[\lambda_{De}^2\times(1-DC)]\}+\beta\times\lambda_{De}$$

$$PFH_{DssD}=\lambda_{DssD}\times1\ h$$

式中:

T_2 诊断试验间隔时间;子系统B1/B2的诊断时间间隔为15 min。

T_1 验证试验间隔或寿命,取其中的较小值;对于子系统Q1/Q2,根据子系统元件的T_{10d}(见GB/T 16855.1,C.4.2),在给定的使用率下,寿命间隔时间为500 000 h(57.1年)。验证试验间隔(见GB 28526的前言)假定为20年(175 200 h),小于寿命。因此,T_1取175 200 h。

λ_{De} 每个子系统元件(接触器Q1和Q2)的危险失效率,等于2.00×10^{-7}/h(如上所示)。

DC 基于启动时K1对机械连接的镜像触点的常规见监控,每个子系统元件(接触器Q1和Q2)的诊断覆盖率为99%。

β 共因失效的敏感度。根据GB 28526,附录F中的简化方法:分离(5+5+5)、评估/分析(9)以及环境条件(9+9),得分为42分,因此它的值为5%(0.05)。

根据上述数据计算得出PFH_D的值为1.01×10^{-8}。

8.2.7.7 因此,子系统B1/B2和Q1/Q2遵从GB 28526的表5中给出的结构限制。

见表2。

表2 使用本子系统的SRCF可声明的子系统最大SIL CL的结构限制

安全失效系数	硬件故障裕度[a]		
	0	1	2
<60%	不允许	SIL1	SIL2
60%~<90%	SIL1	SIL2	SIL3
90%~<99%	SIL2	SIL3	SIL3[b]
≥99%	SIL3	SIL3[b]	SIL3[b]

[a] 硬件故障裕度N意味着$N+1$次故障可能导致安全相关控制功能的丧失。

[b] 本标准并未考虑声明SIL4的限制。对于SIL4,参见GB/T 20438.1。

[c] 见GB 28526的6.7.6.4,或者对于已排除可能导致危险失效的故障的子系统,见6.7.7。

8.2.7.8 每个子系统的安全失效系数为99%(基于其DC),硬件故障裕度为1。因此,每个子系统的SIL CL(SIL声明限制)为3。

8.2.7.9 对于子系统K1,制造商已声明PFH_D为每小时2.31×10^{-9},SIL CL3(如上所示)。

8.2.7.10 因此基于最小的SIL CL,可声明最大SIL为3。

8.2.7.11 将每个子系统的PFH_D加起来:

3.04×10^{-8}(子系统B1/B2)+2.31×10^{-9}(子系统K)+1.01×10^{-8}(子系统Q1/Q2)=4.28×10^{-8}

这满足GB 28526的表3中给出的$\geq10^{-8}$~$<10^{-7}$范围。因此,如果满足了GB 28526中其他所有要求,则该安全功能达到SIL3。

8.3 结论

8.3.1 在上述简单示例中,使用GB/T 16855.1给出的方法计算得出的平均危险失效率为每小时

2.70×10^{-8}(即对应为 PLc),而使用 GB 28526 给出的方法计算得出的危险失效率为每小时 4.28×10^{-8}(即对应为 SIL3)。两个结果之间的差异在预期误差范围内,从而给出了两项标准相应的可接受水平。(从而在可接受水平上给出了两项标准的对应关系)。

8.3.2 宜注意,两项标准都有的变量 β 是针对冗余系统的。这可能导致两项标准得到的 PFH_D 之间存在较小但可接受的差异(如示例中所示)。如果满足 GB/T 16855.1 的表 F.1 中充分的措施,则该标准中的方法假定 β 系数为 2%。GB 28526 使用了附录 F 中不同的结构表。使用该表得出的 β 系数范围在 1%~10%之间。确定 β 系数的每种方法都只有在各自标准的子系统设计方法范围内使用。

参 考 文 献

[1] GB 14048.5 2008 低压开关设备和控制设备 第5-1部分:控制电路电器和开关元件 机电式控制电路电器

[2] GB/T 15706 2012 机械安全 设计通则 风险评估与风险减小

[3] GB/T 16855.1 2008 机械安全 控制系统有关安全部件 第1部分:设计通则

[4] GB/T 16855.2 2007 机械安全 控制系统有关安全部件 第2部分:确认

[5] GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

[6] GB/T 21109.1 2007 过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求

[7] GB 28526 2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[8] IEC 61800-5-2, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*

中华人民共和国
国家标准
机械安全 应用 GB/T 16855.1 和
GB 28526 设计安全相关控制系统的指南
GB/T 30175—2013/ISO/TR 23849:2010
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 23 千字
2014 年 4 月第一版 2014 年 4 月第一次印刷
*
书号:155066·1-48395 定价 21.00 元

GB/T 30175-2013

打印日期:2014年4月17日 F009A