ICS 29.020
J 07

中华人民共和国国家标准

GB/T 34136—2017/IEC/TR 62061-1:2010

机械电气安全 GB 28526 和 GB/T 16855.1 用于机械安全相关控制系统设计的应用指南

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

(IEC/TR 62061-1:2010,Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery,IDT)

2017-07-31 发布　　2018-02-01 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

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 IEC/TR 62061-1:2010《ISO 13849-1 和 IEC 62061 中用于机械的安全相关控制系统设计的应用指南》(英文版)。

本标准做了下列编辑性修改：

——为了与其他相应的标准名称相协调，标准名称改为《机械电气安全 GB 28526 和 GB/T 16855.1 用于机械安全相关控制系统设计的应用指南》。

本标准由中国机械工业联合会提出。

本标准由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本标准负责起草单位：国家机床质量监督检验中心。

本标准参加起草单位：中国科学院沈阳计算技术研究所有限公司、山东大学。

本标准主要起草人：薛瑞娟、黄祖广、赵钦志、尹震宇、胡天亮、蒋峥、黄麟。

机械电气安全 GB 28526 和 GB/T 16855.1 用于机械安全相关控制系统设计的应用指南

1 范围

本标准规定了 GB 28526 和 GB/T 16855.1 用于机械安全相关控制系统设计的应用指南。

2 概述

2.1 GB 28526 和 GB/T 16855.1 均规定了机械安全相关控制系统设计和实施的相关要求。这两项标准规定的方法虽然不同,但正确使用时,均可降低风险至相应等级。

2.2 这两项标准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 5 个性能等级(PL):a、b、c、d 和 e;而 GB 28526 则分为 3 个安全完整性等级(SIL):1、2 和 3。

2.3 产品标准(C 类)技术委员会规定的安全相关控制系统的安全要求,建议这些技术委员会按照 PL 和 SIL 所要求的置信度等级进行分类。

2.4 机械设计人员可按照具体的应用特点选用 GB 28526 或 GB/T 16855.1 标准。

2.5 选择和使用哪一项标准需要考虑以下因素确定,例如:

——在机械安全相关控制系统设计中,以往的知识和经验是基于 GB/T 16855.1—2008 描述的类别概念,则可能意味着使用 GB/T 16855.1—2008 更合适;

——基于介质不是电气技术的安全相关控制系统,则使用 GB/T 16855.1 更合适;

——用户要求以术语 SIL 证明机械安全相关控制系统的安全完整性等级时,则使用 GB 28526 更合适;

——机械安全相关控制系统用于例如过程工业领域时,当其他安全相关系统(例如符合 GB/T 21109 的安全仪表系统)以 SIL 表征,则使用 GB 28526 更合适。

3 标准对比

3.1 GB/T 16855.1 和 GB 28526 的技术要求对比如下:

——术语;

——风险评估和性能分配;

——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,这两项标准均给出了用于评估的每小时危险失效概率(PFH_D)和平均失效间隔时间($MTTF_d$)的简化数学公式。

3.3 标准对比结论如下：

——通过集成按照 GB 28526 或 GB/T 16855.1 标准要求设计的非复杂的安全相关电气控制系统(SRECS)的子系统或控制系统安全相关部件(SRP/CS)，使用这两项标准中的任一项设计的安全相关控制系统均能达到可接受的功能安全等级；

——通过集成按照 GB/T 20438 设计的电气/电子/可编程电子设备的子系统，这两项标准也可用于为复杂的 SRECS 和 SRP/CS 提供设计的解决方法；

——目前机械行业使用这两项标准是有意义的，经验表明使用者将受益。一段合理时期的实际应用反馈，对于推动 GB 28526 和 GB/T 16855.1 这两项标准内容的合并是必需的；

——由于细节上存在着差异，及某些概念(例如功能安全管理)需要进一步工作以建立各自设计方法和一些技术要求之间的对应关系。

4 风险评估和所需性能分配

4.1 对具体安全功能分配 SIL 和/或 PL_r 的方法进行比较。每个标准的附录 A 中各自提供的方法之间有很好的对应等级。

4.2 无论使用哪种方法，注意确保对风险参数进行适当的判断，以确定能够适用于具体安全功能的 SIL 和/或 PLr。这种判断最好让相关人员(如设计、维护和操作人员)共同参与，以确保正确理解机械可能出现的危险。

4.3 有关风险评估过程和性能目标分配的更多信息可见 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安全功能由安全相关控制系统实现。

5.2 对控制电路执行的每一项安全功能应进行评估，例如使用 GB/T 16855.1 附录 A 或 GB 28526 的附录 A。宜确定每台机械的具体安全功能提供怎样的风险降低水平，依次确定执行该安全功能的控制电路所要求置信度等级。

5.3 PL 和/或 SIL 给定的置信度等级与具体的安全功能有关。

5.4 以下显示的与安全功能相关信息宜由产品标准(C 类)提供：

由控制电路要执行的安全功能：

——安全功能的名称；

——功能的描述；

——按 GB/T 16855.1 要求的性能等级：PL_r a～e ；或/和

——按 GB 28526 要求的安全完整性等级：SIL 1～3。

6 性能目标分配：PL 与 SIL 比较

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。然而对于这些概率目标，两项标准还规定了其他要求(如系统安全完整性等)，同样也适用于安全相关控制系统。这些要求的严酷等级与各自的 PL 和 SIL 有关。

表 1　基于每小时平均危险失效概率的 PL 和 SIL 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	10^{-5}～<10^{-4}	无特殊安全要求
b	3×10^{-6}～<10^{-5}	1
c	10^{-6}～<3×10^{-6}	1
d	10^{-7}～<10^{-6}	2
e	10^{-8}～<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

当设计一个 SRECS/SRP/CS 时，应考虑下列方面：

——当在各自限定范围内使用时，两标准的任一个都可用于设计具有合适功能安全的安全相关控制系统，用 SIL 或 PL 表示。

——按照 GB/T 16855.1 设计具有相关 PL 的非复杂的安全相关部件可以作为子系统集成到按照 GB 28526 设计的安全相关电气控制系统中。任何按照 GB/T 16855.1 设计相关 PL 的复杂安全相关部件都可以集成到按照 GB/T 16855.1 设计的控制系统的安全相关部件。

——任何按照 GB 28526 设计实现具有相关 SIL 的非复杂子系统都可以作为安全相关部件集成到按照 GB/T 16855.1 设计的 SRP/CS 组合中。

——任何按照 GB/T 20438 设计具有相关 SIL 的复杂子系统都可以作为安全相关部件集成到按照 GB/T 16855.1 设计的 SRP/CS 组合中，或者作为子系统集成到按照 GB 28526 设计的 SRECS 中。

7.2　PFH_D 和 $MTTF_d$ 的估计以及故障排除的使用

7.2.1　PFH_D 和 $MTTF_d$

7.2.1.1　GB/T 16855.1 中的 $MTTF_d$ 值与不带诊断的单通道 SRP/CS 相关时，只在这种情况下为 GB 28526 中 PFH_D 的倒数。

7.2.1.2　$MTTF_d$ 是不考虑任何给定因素(如诊断或架构)的部件和/或单通道的参数，而 PFH_D 是考虑了由设计结构决定的诊断和架构因素的子系统的参数。

7.2.1.3　GB/T 16855.1 的附录 K 给出了以类别和诊断覆盖率分类的不同架构 SRP/CS 中 $MTTF_d$ 和 PFH_D 的关系。

7.2.1.4　按照 GB/T 16855.1 串联组合的 SRP/CS 的 PFH_D 的估计，可以采用 GB 28526 中子系统使用的相似方法，以累加各 SRP/CS 的 PFH_D 值(例如源于 GB/T 16855.1 的附录 K)的方法计算。

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的使用，见 GB 28526 的 6.7.7 和 GB/T 16855.1 的 7.3。GB 28526 不允许 SRECS 在无硬件故障容错(在无硬件故障容错的情况下要求达到 SIL 3)的情况下，使用故障排除。

7.2.2.2 使用故障排除，重要的是对它们的正确判断和 SRP/CS 或 SRECS 预期生命周期有效。

7.2.2.3 通常，通过 SRP/CS 或 SRECS 实现安全功能为 PLe 或 SIL 3 等级的地方，不应仅单独依赖于故障排除获得这样的性能等级。这取决于采用的技术和预期操作的环境。因此，设计者使用故障排除来增加 PL 或 SIL，需要额外小心。

7.2.2.4 在 SRP/CS 或 SRECS 设计中为达到 PLe 或 SIL 3，故障排除不适用于机电位置开关和手操作开关（例如，紧急停止装置）的机械部分。这些故障排除可以应用的特定机械故障条件（如：磨损/腐蚀，断裂）在 GB/T 16855.2—2007 已经描述。

7.2.2.5 例如，须达到 PLe 或 SIL 3 的门联锁系统通常不通过排除故障（例如停止开关操动器）来判断，为了达到这样的性能等级，将需要合并一个最小故障容错 1（例如两个传统的机械位置开关）。然而，排除按相关标准设计的控制面板内布线电路短路的故障是可以接受的。

7.2.2.6 更多关于故障排除使用的信息见 GB/T 16855.2。

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

7.3.1 按照 GB/T 16855.1 或 GB 28526 设计的子系统或控制系统安全相关部分的所有情况，如果满足相关系统等级标准的所有要求，才能声称与系统等级标准一致。

7.3.2 在子系统或控制系统安全相关部件部分的设计应满足相应的 GB 28526 或 GB/T 16855.1 要求。允许符合一个以上充分满足这些标准的要求。

7.3.3 当设计子系统或者控制系统安全相关部件部分时，不允许混合标准的要求。

7.4 使用已由其他标准设计的子系统或 SRP/CS 进行系统设计

7.4.1 在系统设计中，可以选择符合相关产品标准和 GB/T 20438、GB 28526 或 GB/T 16855.1 的子系统（例如，电敏保护设备）。各种型号子系统的供应商，宜依照 GB 28526 或 GB/T 16855.1 提供便于将子系统整合到安全相关控制系统的必要信息。

7.4.2 使用产品标准（例如 GB/T 12668.502—2013）设计的子系统（例如调速电气传动系统）实现了 GB/T 20438 的要求，可以用于依照 GB 28526（见 GB 28526 中 6.7.3）和 GB/T 16855.1 设计的安全相关控制系统中。

7.4.3 根据 GB 28526 中的要求，使用其他标准设计的子系统要符合 GB 28526 中 6.7.3 的规定。

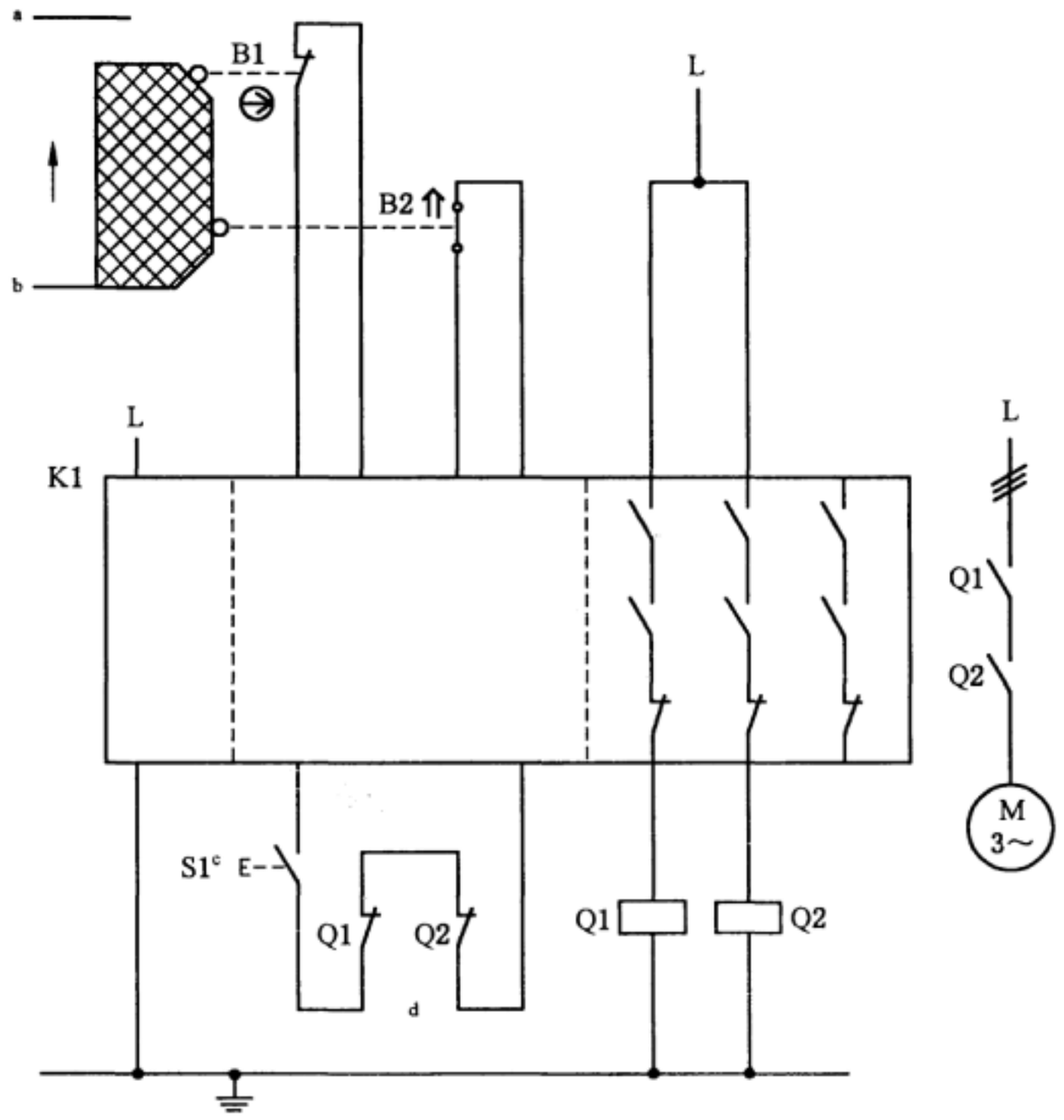
8 示例

8.1 概述

以下示例假定已满足两项标准的所有要求。这个示例只是为了演示标准应用的特定方面。

8.2 执行规定的安全相关控制功能的安全相关控制系统的设计和确认的简化示例

8.2.1 这个简化的示例，意为演示符合 GB 28526 和/或 GB/T 16855.1 的子系统或 SRP/CS 在 SRECS/SRP/CS 中的使用。这个示例是以实现安全功能为基础，是与活动式防护装置的位置监控关联的安全相关停止功能，并且规定了安全完整性等级 SIL 3 或所需的性能等级 PL$_r$ e，如图 1 中所示。



说明：

⇑——显示动作位置；

a ——打开 ；

b ——闭合 ；

c ——起动 ；

d ——反馈电路。

图 1　安全功能的实现示例

8.2.2　以下为本示例的安全要求规范相关信息：

安全功能

——安全相关停止功能，由保护装置引发：活动式防护装置的打开引发安全功能 STO(安全转矩取消)。

功能描述

——通过活动式防护装置(防护栅)防护。联锁防护装置的打开靠两个位置开关 B1/B2 检测，使用断开触点/接通触点组合，并由中央安全模块 K1 进行评估。K1 使两个接触器 Q1 和 Q2 动作，退出中断或阻止危险运动或状态；

——位置开关被监测是为了 K1 故障检测的合理性。Q1 和 Q2 中的故障由 K1 起动试验来检测。只有当 Q1 和 Q2 已经退出，起动命令才能执行。不需要通过打开和关闭联锁防护装置进行起动测试；

——万一元器件失效，安全功能应保持完整。在可导致 Q1 和 Q2 退出和操作失效的联锁防护装置的操作或执行(打开和闭合)期间可检测故障；

——两个连续执行之间的两个以上故障累加，可导致安全功能丧失。

8.2.3　下列特性要求也宜提供：

——基本的和经验证过的安全规则得到遵守(例如，接触器 Q1 和 Q2 的负载电流为其定额的 50%)，类别 B 的要求得到满足。保护电路被执行(例如，触点保护)；

——保护装置的牢固安装,以确保位置开关正常动作;

——依照 GB 14048.5—2008 附录 K,开关 B1 是带有直接断开功能的位置开关;

——位置开关 B1 和 B2 的供电导线单独放置或带有保护。

8.2.4 下列是来自制造商的 SRP/CS 设计内的每部分有效信息:

——由制造商声明,安全模块 K1 满足类别 4、PLe 和 SIL CL 3 的要求;

——接触器 Q1 和 Q2 具有符合 IEC 60947-5-1:2003 中附录 L 的要求的机械连接接触元件。

8.2.5 SRP/CS 和/或 SRECS 的设计宜注意:

——只有在不同保护装置的数个机械位置开关不是串联(即不级联)连接的场合,才能实现类别 4。否则,开关的故障检测不到。

8.2.6 按照 GB/T 16855.1 失效概率的计算:

图 2 示连有双通道输入输出单元的逻辑子系统(安全模块 K1)。由于硬件层的抽象概念已经在安全相关框图中给出了,子系统序列原则上可以互换。因此,建议共用相同结构的子系统组合在一起,如图 3 所示。在评估时,通过减少通道的 $MTTF_d$ 次数限制到 100 年,可以简化 PL 的计算。

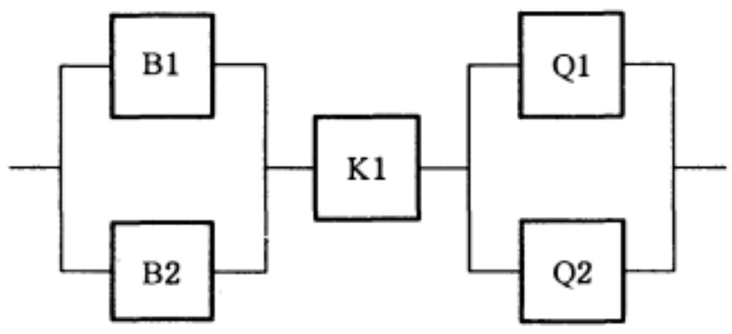
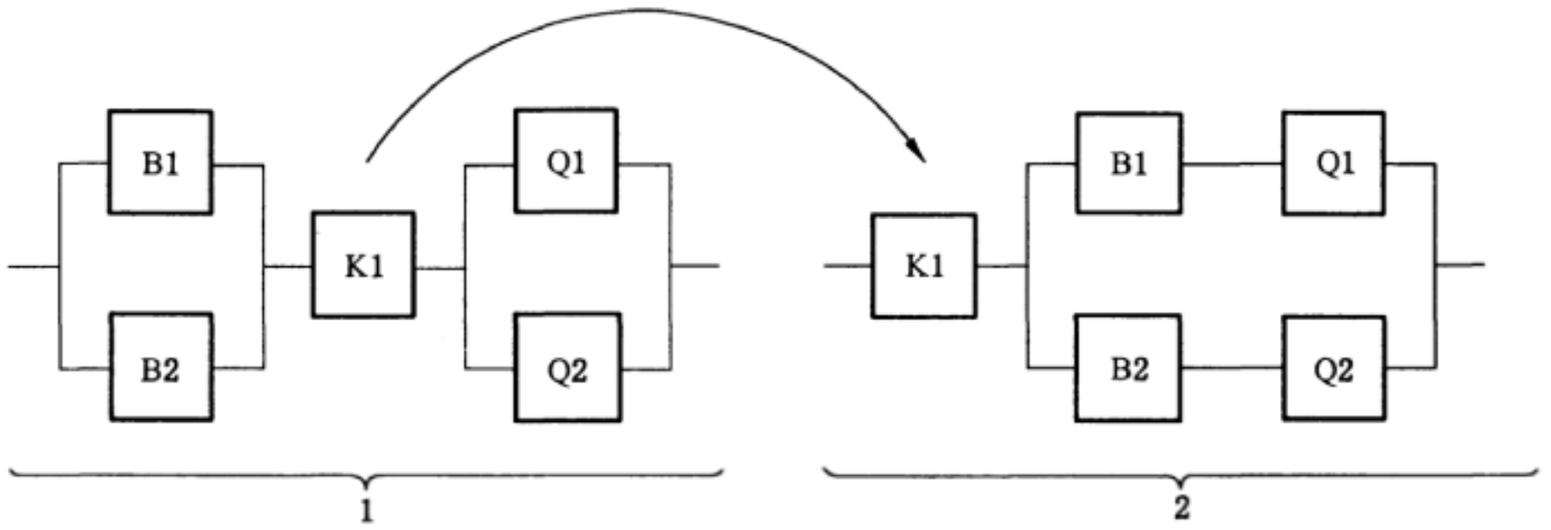


图 2 安全相关框图



关键点:

1——硬件相关表示:三个 SRP/CS 作为子系统;

2——简化的逻辑表示:两个 SRP/CS 作为子系统。

图 3 按照 GB/T 16855.1 进行计算的安全相关框图

安全模块 K1 失效概率,由制造商声明并加至计算结果[每小时 2.31×10^{-9}(制造商给定值),适用于 PLe]。其余子系统,失效概率的计算如下:

——$MTTF_d$:1 000 000 个周期的 B_{10d} 值(制造商给定值)是为说明 B1 的机械部分。对于位置开关 B2,B_{10d} 值为 500 000 个周期(制造商给定值)。以一年 365 个工作日,一天 24 个工作小时,以及 900 s(15 min)的周期时间,由 GB/T 16855.1 中式(C.2)和式(C.7)计算的部件每年的工作周期 n_{op} 是 35 040。

$$n_{op}=\frac{d_{op}\times h_{op}\times 3\,600\text{秒}/\text{小时}}{t_{周期}}=\frac{365\text{天}/\text{年}\times 24\text{小时}/\text{天}\times 3\,600\text{秒}/\text{小时}}{900\text{秒}/\text{周期}}=35\,040\text{周期}/\text{年}$$

$$\mathrm{MTTF_{d,B1}}=\frac{B_{10d}}{0.1\times n_{op}}=\frac{1\ 000\ 000\ 周期}{0.1\times 35\ 040\ 周期/年}=285\ 年$$

$$T_{10d,B1}=\frac{B_{10d}}{n_{op}}=\frac{1\ 000\ 000\ 周期}{35\ 040\ 周期/年}=28.5\ 年$$

$$\mathrm{MTTF_{d,B2}}=\frac{B_{10d}}{0.1\times n_{op}}=\frac{500\ 000\ 周期}{0.1\times 35\ 040\ 周期/年}=143\ 年$$

$$T_{10d,B2}=\frac{B_{10d}}{n_{op}}=\frac{500\ 000\ 周期}{35\ 040\ 周期/年}=14.3\ 年$$

B2 的 T_{10d}值为 14.3 年。如果整个 SRP/CS 的预期任务时间为 20 年，当超过 14.3 年时，B2 将被替换。

——对于接触器 Q1 和 Q2，在感应负载(AC 3)下，B_{10}值相应为 1 000 000 个周期的电气寿命(制造商给定值)。如果假定 50%失效是危险的，B_{10d}的值为 2 倍的 B_{10}值：

$$\mathrm{MTTF_{d,Q1/Q2}}=\frac{B_{10d}}{0.1\times n_{op}}=\frac{2\ 000\ 000\ 周期}{0.1\times 35\ 040\ 周期/年}=571\ 年$$

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

——对于两个通道，$\mathrm{MTTF_d}$ 通过使用 GB/T 16855.1 中的式(D.1)计算：

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

$$\frac{1}{\mathrm{MTTF_{d,Ch1}}}=\frac{1}{285\ 年}+\frac{1}{571\ 年}=\frac{1}{190\ 年}$$

$$\frac{1}{\mathrm{MTTF_{d,Ch2}}}=\frac{1}{143\ 年}+\frac{1}{571\ 年}=\frac{1}{114\ 年}$$

这里给定 $\mathrm{MTTF_{d,Ch1}}$值为 190 年，$\mathrm{MTTF_{d,Ch2}}$值为 114 年。依照 GB/T 16855.1 两个通道的 $\mathrm{MTTF_d}$ 被限制到 100 年，在这种情况下，限制后两个通道的 $\mathrm{MTTF_d}$ 是相等的，不必执行对称。

——$\mathrm{DC_{avg}}$：B1 和 B2 取 99%的 DC 是基于 K1 中断开/连接触点组合的合理监测。接触器 Q1 和 Q2 取 99% 的 DC 是源自 K1 起动期间的定期监测。对于每一个子系统陈述的 DC 值相当于 $\mathrm{DC_{avg}}$。$\mathrm{DC_{avg}}$值可以根据 GB/T 16855.1 中的式(E.1) 计算。由于每个单独的 DC 都是 99%，所以 $\mathrm{DC_{avg}}$也是 99%。

——在子系统 B1/B2 和 Q1/Q2 中有足够的防共因失效措施(70 点)：分离(15)，经验证的部件(5)，防止过压等(15)和环境条件(25+10)。

——任务时间：作为 GB/T 16855.1 的简化方法，假设任务时间为 20 年。

——子系统 B1/B2/Q1/Q2 对应具有高 $\mathrm{MTTF_d}$(100 年)和高 $\mathrm{DC_{avg}}$(99%)的类别 4。这导致每小时 2.47×10^{-8}的危险失效平均概率(见 GB/T 16855.1 中表 K.1)。下列附加的子系统 K1，危险失效平均概率为每小时 2.70×10^{-8}。这相当于 PLe。

8.2.7 按照 GB 28526 计算失效概率。

8.2.7.1 依照 GB 28526 中 6.6.2，电路安排可分成三个子系统：B1/B2，K 和 Q1/Q2，如安全相关框图所示。

8.2.7.2 对于子系统 K 的失效概率为每小时 2.31×10^{-9}和安全模块 K1 的安全完整性等级 3 是由制造商给定的。

8.2.7.3 对于其他的子系统，失效概率可以估计如下：

——子系统 B1/B2：B_{10d}值为 1 000 000 周期(制造商给定值)是为 B1 的机械部分规定的。对于位置开关 B2，B_{10d}值为 500 000 周期(制造商给定值)。以每年 365 个工作日，每天 24 个工作小时和 15 min 的周期时间，这些部件的 C 值为每小时 4 周期。失效率计算为：$0.1\times C/B_{10d}=4\times10^{-7}$每

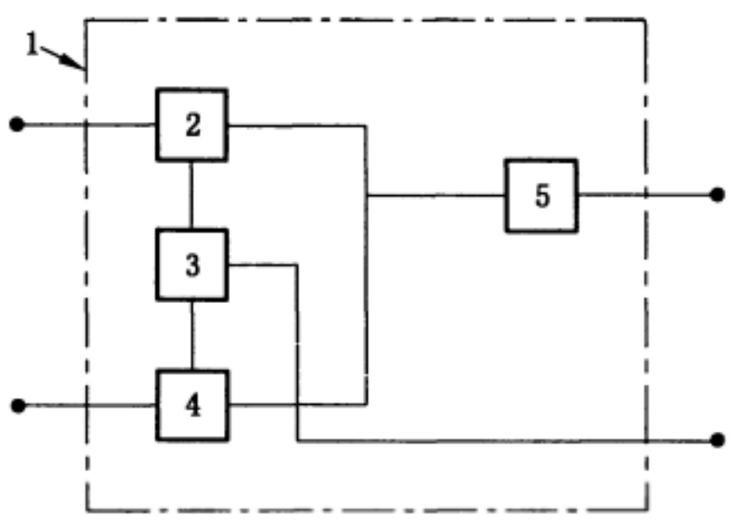
小时 。B2 给定的失效率为每小时 8×10^{-7}。

注：按照 GB 28526 应用的操作周期次数 C 与按照 GB/T 16855.1 的年平均操作次数 n_{op} 相对应。由于 C 确定为每小时的周期数，而 n_{op} 确定为每年的周期数，下列关系适用：

$$C = n_{op} \times \frac{\text{年}}{365 \times 24 \text{ 小时}}$$

因此，以一天中每小时平均操作数和一年中每天平均操作数会影响 C 值和 n_{op}。

——子系统的逻辑结构相当于图 4 中给出的 GB 28526 中 6.7.8.2.5 的图 D。



关键点：

1——子系统 D；

2——子系统元素 λ_{De1}；

3——诊断功能 ；

4——子系统元素 λ_{De2}；

5 ——共因失效。

图 4　子系统 D 的逻辑表示

——子系统元素(开关 B1 和 B2)设计不同，因此以下公式(GB 28526 中的 6.7.8.2.5 的公式 D.1)可用于确定子系统的 PFH_D。

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

$$PFH_{DsD} = \lambda_{DsD} \times 1 \text{ 小时}$$

式中：

T_2 ——诊断试验间隔，对于子系统 B1/B2，它是 15 min；

T_1 ——验证试验间隔或生命周期的较小值。对于子系统 B1/B2，基于最低子系统元素 T_{10d} 值(见 GB/T 16855.1，C.4.2)给定的使用率，生命周期间隔为 125 000 h(14.3 年)。开关 B2 具有最低的 T_{10d} 值。验证试验间隔(见 GB 28526 前言)假定为 20 年(175 200 h)，要比寿命周期长。所以 T_1 为 125 000 h。

β ——共因失效敏感性。由 GB 28526 的附录 F 简化方法中的 42 点导出其值为 5%(0.05)。分离(5+5+5)，评估/分析(9)和环境条件(9+9)。

λ_{De1} ——子系统元素 1 的危险失效率。对于开关 B1，它等于每小时 4×10^{-7}(见上述)。

DC_1 ——子系统元素 1 的诊断覆盖率。基于与 K1 相连的 B1 和 B2 的断开/连接触点的合理性监测，开关 B1 的估计值应为 99%。

λ_{De2} ——子系统元素 2 的危险失效率。对于开关 B2，它等于每小时 8×10^{-7}(见上述)。

DC_2 ——子系统元素 2 的诊断覆盖率。基于与 K1 相连的 B1 和 B2 的断开/连接触点的合理性监测，开关 B2 的估计值应为 99%。

8.2.7.4　将上述数据输入公式得出 PFH_D 值为 3.04×10^{-8}。

8.2.7.5　同样，对于子系统 Q1/Q2：接触器 Q1 和 Q2 在感应负载(AC 3)下有 10^6 周期电气寿命相应的

B_{10}值(制造商给定)。如果假设50%的失效是危险的,那么B_{10d}的值为2倍的B_{10}值。对于上述假定值C,每个接触器的失效率均为每小时2×10^{-7}。

8.2.7.6 子系统Q1/Q2的逻辑结构相当于GB 28526中6.7.8.2.5的图D。子系统元素(接触器Q1和Q2)设计相同,因此式(D.1)用于确定子系统的PFH_D:

$$\lambda_{DssD}=(1-\beta)^2\{[\lambda_{De}^2\times2\times DC]\times T_2/2+[\lambda_{De}^2\times(1-DC)]\times T_1\}+\beta\times\lambda_{De}$$

$$PFH_{DssD}=\lambda_{DssD}\times1\text{ 小时}$$

式中:

T_2 ——诊断试验间隔;对于子系统Q1/Q2,该值为15 min;

T_1 ——验证试验或生命周期中的较小值;对于子系统Q1/Q2,基于子系统元素T_{10d}值(见GB/T 16855.1, C.4.2)给定的使用率,生命周期为500 000 h(57.1年)。验证试验间隔(见GB 28526前言)假定为20年(175 200 h),比生命周期短。所以T_1的值为175 200 h。

λ_{De} ——每个子系统(接触器Q1和Q2)的危险失效率每小时2×10^{-7}(见上述)。

DC——基于由K1起动期间对机械连接的镜像触点的定期监测,每个子系统元素(接触器Q1和Q2)的诊断覆盖率为99%。

β ——共因失效敏感性。由GB 28526的附录F简化方法中的42点导出其值为5%(0.05)。分离(5+5+5),评估/分析(9)和环境条件(9+9)。

将上面的数据输入公式得出PFH_D值为1.01×10^{-8}。

8.2.7.7 子系统B1/B2和Q1/Q2受GB 28526中表5给出的结构限制,见表2。

表2 使用子系统的SRCF可能要求的子系统最大SIL CL的结构限制

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

[a] N级硬件故障容错意味着N+1个故障可导致安全相关控制功能的丧失;

[b] 本标准不考虑SIL4要求限度(有关SIL4见GB/T 20438.1);

[c] 见GB 28526的6.7.6.4,或对可能导致危险失效的故障使用了故障排除的子系统,见6.7.7。

8.2.7.8 每个子系统都有安全失效系数99%(基于他们的DC)和硬件故障容错1。那样为每个子系统产生SIL CL(SIL声明限制)3。

8.2.7.9 对于子系统K1,PFH_D值为每小时2.31×10^{-9},SIL CL 3由制造商声明(见上述)。

8.2.7.10 基于最低SIL CL声明的最大SIL值为3。

8.2.7.11 每个子系统的PFH_D值加到一起:

3.04×10^{-8}(子系统B1/B2)$+2.31\times10^{-9}$(子系统K)$+1.01\times10^{-8}$(子系统Q1/Q2)$=4.28\times10^{-8}$

这满足GB 28526表3中给出的从10^{-8}至小于10^{-7}范围。因此,如果GB 28526所有其他要求得到满足,那么安全功能可以达到SIL 3。

8.3 结论

8.3.1 上述简单示例,用GB/T 16855.1的方法计算的结果是危险失效平均概率为2.70×10^{-8}/h(即与

PLe 相对应),而用 GB 28526 的方法计算的结果是危险失效概率为 4.28×10^{-8}/h(即与 SIL 3 相对应)。这些结果之间的差异在预期允差范围内,因此说明这两标准之间的可接受水平相一致。

8.3.2 应当注意,两标准之间对冗余系统的 β(共因失效敏感性)处理的方法存在一些差异。这可能会在依照两标准取得的 PFH_D 值之间,产生小的但可以接受的偏差(如示例中所示)。GB/T 16855.1 中的方法假设 β 因子为 2%,如果满足标准中表 F.1 的措施。GB 28526 在附录 F 中使用不同的结构表,使用该表的 β 因子的变化范围为从 1%～10%。任何 β 因子值的确定方法,只可在各自标准子系统设计方法的范围内使用。

参 考 文 献

[1] GB/T 12668.502—2013 调速电气传动系统 第5-2部分:安全要求 功能(IEC 61800-5-2:2007,IDT)

[2] GB/T 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(IEC 60947-5-1:2003,MOD)

[3] GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小(ISO 12100:2010,IDT)

[4] 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(ISO 13849-1:2006,IDT)

[5] 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(ISO 13849-2:2003,IDT)

[6] 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[IEC 61508(所有部分),IDT]

[7] 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(IEC 61511-1:2003,IDT)

[8] 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(IEC 62061:2005,IDT)

中华人民共和国
国家标准
机械电气安全 GB 28526 和
GB/T 16855.1 用于机械安全
相关控制系统设计的应用指南
GB/T 34136—2017/IEC/TR 62061-1:2010
*
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(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
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 字数 24 千字
2017 年 8 月第一版 2017 年 8 月第一次印刷
*
书号:155066·1-57118 定价 18.00 元

GB/T 34136-2017