Dynamical Systems and Control 动力系统与控制, 2016, 5(3), 80-85
Published Online July 2016 in Hans. http://www.hanspub.org/journal/dsc
http://dx.doi.org/10.12677/dsc.2016.53009

Hans汉斯

Study and Application for Performance Evaluation of SRP/CS

Huiyong Wang[1], Xiangnan Li[1], Dayong Bao[1], Li Xing[1], Haipeng Zheng[1], Bin Wang[1], Xiaodong Liu[2]

[1]Shandong Inspection and Quarantine Technology Center, Qingdao Shandong
[2]Technical Center for Mechanical and Electrical Product Inspection and Testing of SHCIQ, Shanghai
Email: why2325@163.com

Received: Jun. 15th, 2016; accepted: Jul. 8th, 2016; published: Jul. 18th, 2016

Abstract

Process of performance evaluation of safety-related part of a control system (SRP/CS) was reported. Required performance level (PLr) of SRP/CS was determined by hazard based approach. Determined methods for category of SRP/CS, MTTFd, DCavg and CCF were reported. Performance evaluation was taken for control system of movable guard of CNC lathe.

Keywords

SRP/CS, Performance Level, Evaluation, Application

控制系统有关安全部件性能评估研究及应用

王会永[1]，李向男[1]，包大勇[1]，邢　力[1]，郑海鹏[1]，王　彬[1]，刘晓东[2]

[1]山东检验检疫局检验检疫技术中心，山东 青岛
[2]上海检验检疫局机电产品检测技术中心，上海
Email: why2325@163.com

收稿日期：2016年6月15日；录用日期：2016年7月8日；发布日期：2016年7月18日

文章引用: 王会永，李向男，包大勇，邢力，郑海鹏，王彬，刘晓东. 控制系统有关安全部件性能评估研究及应用[J]. 动力系统与控制, 2016, 5(3): 80-85. http://dx.doi.org/10.12677/dsc.2016.53009

摘　要

本文阐述了SRP/CS性能评估流程，确定了采用基于危险的方法确定SRP/CS要求的安全性能等级(PLr)，介绍了SRP/CS控制回路的类别、平均危险失效时间(MTTFd)、平均危险失效的诊断覆盖率(DCavg)及共因失效(CCF)四个参数的确定方法，并对数控车床可移动式防护门控制系统进行了性能评估。

关键词

控制系统有关安全部件，性能等级，评估，应用

1. 引言

随着制造技术和控制技术的发展，集成了机械、电气及电子等技术的复杂安全控制系统正逐渐在各领域中得以应用。控制系统中有关响应安全输入信号并产生有关安全输出信号的部件称为控制系统有关安全部件(SRP/CS)，为机器提供安全功能。风险评价是分析机器在使用时可能产生的各种危险状态及对每种危险状态下可能损伤或危害健康的概率和程度进行全面评估[1]。SRP/CS 性能评估就是通过风险评价，识别由 SRP/CS 执行的安全功能，并确定 SRP/CS 的性能等级，验证其性能等级是否能够实现安全目标。

2. SRP/CS 性能评估流程

由 SRP/CS 执行的安全功能，应根据风险评价的结果，确定“要求的性能等级”(PLr)。SRP/CS 实现的风险减小总和越多，PLr 就越高。SRP/CS 完成安全功能的能力通过性能等级(PL)来表示。PL 应不低于 PLr，才能实现由 SRP/CS 执行的安全功能，达到风险减小的目的在所提供的安全功能中，SRP/CS 一般通过作为本质安全设计的一部分或安全装置和保护装置的方式实现风险减小。SRP/CS)性能评估流程如图 1 所示。性能等级定义为每小时危险失效的概率[2]。

3. SRP/CS 性能评估方法

3.1. 确定要求的性能等级(PLr)

对于每种由 SRP/CS 执行的安全功能，应确定“要求的性能等级”(PLr)。本文选择基于 HBA 的评估方法，并通过风险图确定 PLr，影响因素包括伤害的严重度(S)、暴露于维修的频率和时间(F)，以及避免危险或限制伤害的可能性(P)，确定方法见图 2。

图中：1——估计安全功能对风险减小影响的起始点。L——对风险减小的影响小。H——对风险减小的影响大。风险因素：S——伤害的严重度；S1——轻微(通常是可恢复的伤害)；S2——严重(通常是不可恢复的伤害或死亡)；F——暴露于危险的频率和(或)时间；F1——很少发生和(或)暴露时间短；F2——频繁和(或)暴露时间长；P——避免危险或显示伤害的可能性；P1——特定条件下可能；P2——几乎不可能。PLr——所需的性能等级；a、b、c、d、e——性能等级级别。

3.2. 性能等级(PL)评估

性能等级评估的目的是证实 PL 不低于 PLr。一般通过考虑 SRP/CS 控制回路的类别、平均危险失效时间(MTTFd)、平均危险失效的诊断覆盖率(DCavg)及共因失效(CCF)四个参数进行评估。

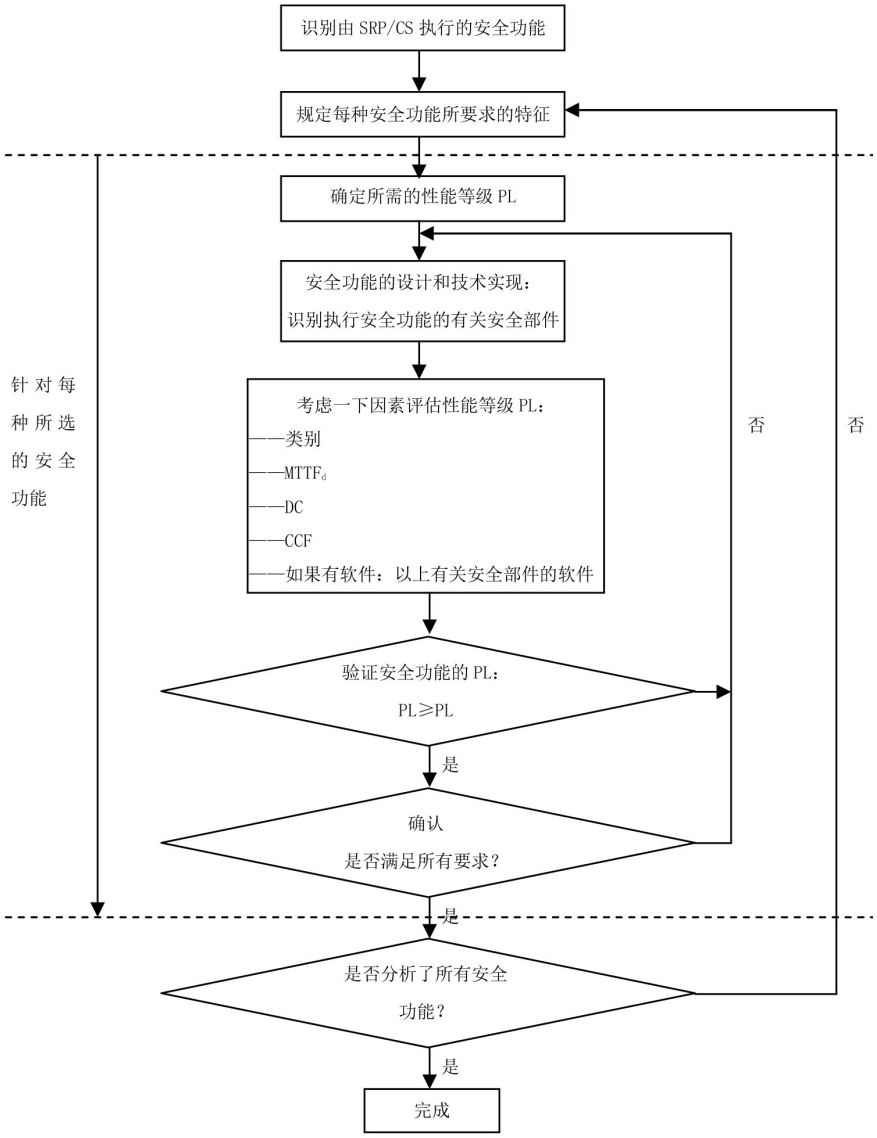


Figure 1. Performance evaluation procedure of SRP/CS
图 1. SRP/CS 性能评估流程

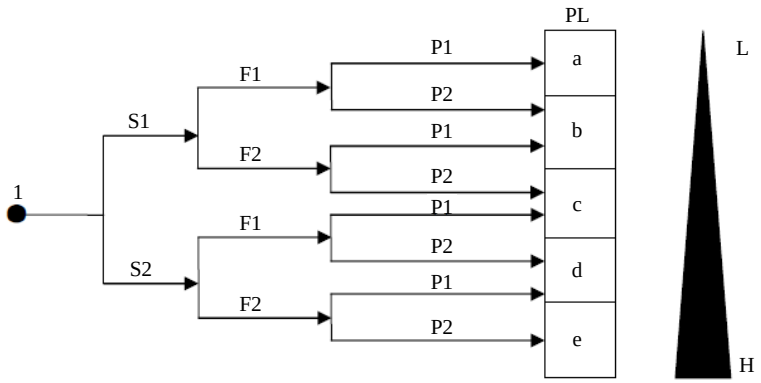


Figure 2. Method for determining PLr
图 2. 确定 PLr 的方法

3.2.1. SRP/CS 控制回路的类别确认

SRP/CS 控制回路的类别分为 5 类[2]。B 类是基本类别，当出现故障时，能导致安全功能的损失。1 类主要是通过选择和应用合适的元件来实现改进耐故障的能力。2 类、3 类和 4 类提高规定安全功能方面的性能主要是通过改进 SRP/CS 的结构来实现。SRP/CS 的结构是对 PL 有重大影响的关键特征，每种类别的指定结构都能够用有关安全模块图象征性表出来。出现在机器上的大部分结构能够映射到一种类别。

3.2.2. 平均危险失效时间(MTTFd)估算

MTTFd 是指预期的危险失效平均时间。MTTFd 为定量指标，单位为年，可从元器件制造商处获得。如果没有，则需要根据元器件的工作条件，通过 B10d (10%的元器件达到危险失效的平均周期数)、hop (平均工作时间，小时/天)、dop (平均工作时间，天/年)和 t 周期(元器件两个相继周期的起始点之间的平均工作时间，秒/周期)计算得出。根据计算得出的 MTTFd，判断其是低、中或高。

3.2.3. 危险失效的诊断覆盖率(DCavg)估算

DC 是诊断有效性的度量，是可诊断的危险失效的失效率与所有危险失效的失效率之间的比率。一般可用 FMEA 或类似的方法来估算[3]。DCavg 范围的选择基于 3 个关键值：60%、90%和 99%，从而将 DC 分为低(60% ≤ DC < 90%)、中(90% ≤ DC < 99%)和高(DC ≥ 99%)三级指标。

3.2.4. 共因失效(CCF)估算

CCF 是指同一事件引起的不同产品的失效，这些失效相互之间没有因果关系。能导致共因失效的因素很多，诸如雷同的设计、相同的元件进行冗余、类似元器件的不合理应用等[4]，都可能导致共因失效的出现。具有冗余结构的系统，即类别 2、类别 3 和类别 4 的系统都必须采取措施防止共因失效。估算 CCF 的量化应通过整个系统进行，由工程技术来判定估算数值。如果不是完全符合就不得分。总分在 65 分及以上，满足要求。

3.2.5. 确认 PL 的方法

确认 PL 应综合考虑所有相关参数，并进行适当计算。一般可通过 ISO 13849-1：2006 提供的简化程序来实现，如图 3 所示。

由图 3 可以发现，一个 PL 可以由不同的途径和组合来实现，在进行 SRP/CS 设计时，应根据具体的控制系统以最优化的方式来实现，以控制成本。

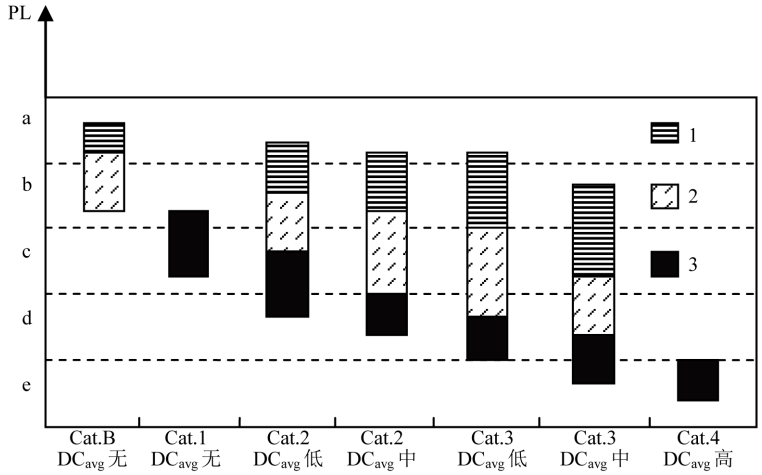
4. SRP/CS 性能评估方法应用

本文以数控车床的可移动式防护门为例，对其控制系统的安全功能进行评估。按照相关标准要求，车床正常工作时，如果打开或移除可移动式防护罩，机床加工工作应停止，以保护操作者的安全。一般通过图 4 所示的电路实现“开门即停”的功能。

图 4 中，B1 和联锁开关的常闭触点，Q1 为控制电动机 M 停转的接触器。当车床正常工作时，联锁开关常闭触点 B1 处于常闭状态，接触器触点 Q1 闭合，电动机 M 正常运转。当防护门打开时，联锁常闭触点 B1 断开，接触器线圈 Q1 失电，接触器触点 Q1 断开，电动机 M 停转。

4.1. 确定 PLr

根据图 2 的方法，如果防护门打开，车床切削加工不停止，容易对操作者造成严重的伤害(S2)，打开防护门干预车床切削工作的情况很少发生(F1)，有经验的操作者可以避免相关的伤害发生(P1)，因此 PLr 为 c，即 $10^{-6} \leq$ 每小时危险失效概率 $< 3 \times 10^{-6}$。确定 PLr 的风险图如图 5 所示。



PL——性能水平；1——每个通道的 MTTFd = 低；2——每个通道的 MTTFd = 中；3——每个通道的 MTTFd = 高。

Figure 3. Relationship between categories, DCavg, MTTFd of each chanel and PL
图 3. PL 和每个通道的类别、DCavg 和 MTTFd 的关系

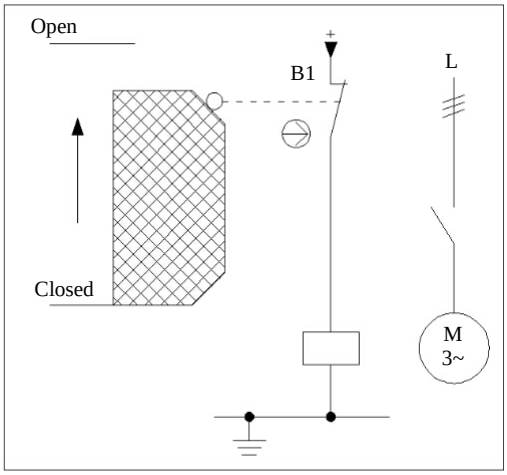


Figure 4. Electrical diagram of stop when opening door
图 4. “开门即停”电气原理图

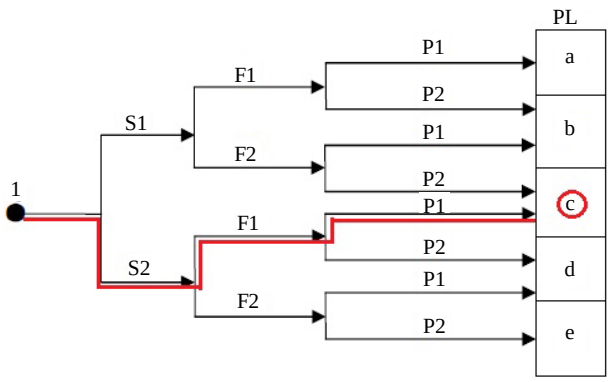


Figure 5. Risk graph for determining PLr
图 5. 确定 PLr 的风险图

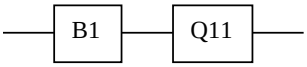


Figure 6. Security module diagram
图 6. 安全模块图

4.2. 确认控制回路的类别

根据控制回路的安全功能和电气原理图，“开门即停”的安全模块图如图 6 所示。联锁开关和接触器均采用国际知名品牌，是经验证的元件。安全模块图符合类别 1 的指定结构。

4.3. MTTFd、DCavg 及 CCF 的量化

从制造商官网查阅相关型号联锁开关和接触器的技术参数，两元器件的 $B10d$ = 20,000,000 周期。一年中，车床的一年的工作时间(dop)为 240 天，每天工作(hop) 8 小时，两元器件两次相继切换起始点之间的平均操作时间估计为 20 s，则可计算单个元器件的 MTTFdi。依据 ISO 13849-1：2006，以联锁开关为例计算过程如下。

联锁开关每年的操作次数

$$nop = \frac{dop \times hop \times 3600\ \mathrm{s/h}}{t_{周期}} = \frac{240 \times 8 \times 3600\ \mathrm{s/h}}{20} = 345600\ 周期/年$$

$$\mathrm{MTTFdi} = \frac{B10d}{0.1 \times nop} = \frac{20000000}{0.1 \times 345600} = 579\ 年$$

由于接触器的相关参数与联锁开关一致，接触器的 MTTFdi 也为 579。根据通道中每个元器件的 MTTFdi，采用“部件计数法”的公式计算每个通道的 $\mathrm{MTTF_d}$。

$$\frac{1}{\mathrm{MTTF_d}} = \frac{1}{\mathrm{MTTF_{d1}}} + \frac{1}{\mathrm{MTTF_{d2}}} + \cdots + \frac{1}{\mathrm{MTTF_{dN}}} = \frac{1}{579} + \frac{1}{579} = \frac{2}{579}$$

由上式得出，通道的 $\mathrm{MTTF_d}$ = 289.5，对照 ISO 13849-1：2006，通道的 MTTFD 为“高”。根据图 6，不考虑故障诊断率 DCavg 和共因失效 CCF，确定 PL 为“c”，即 PL = PLr。

5. 结论

控制系统有关安全部件(SRP/CS)作为提供安全功能的机械控制系统部件，其安全性能关系到整个机器的安全。本文阐述了 SRP/CS 性能评估流程，确定了采用基于危险的方法确定 SRP/CS“要求的性能等级”(PLr)，介绍了 SRP/CS 控制回路的类别、平均危险失效时间(MTTFd)、平均危险失效的诊断覆盖率(DCavg)及共因失效(CCF)四个参数的确定方法，并对数控车床可移动式防护门控制系统进行了性能评估。

参考文献 (References)

[1] 崔正斌. 机械安全技术[M]. 北京: 化学工业出版社, 2009.

[2] ISO 13849-1 (2006) Safety of Machinery—Safety-Related Parts of Control Systems—Part1: General Principles for Design.

[3] 刘治永, 张晓飞, 程红兵, 等. 安全控制系统的性能等级与计算案例[J]. 标准科学, 2013(2): 30-33.

[4] 郭有儒. 机电设备安全性的研究[D]: [硕士学位论文]. 上海: 上海交通大学, 2012.