“功能安全产品实现技术”系列讲座

第 6 讲　安全相关产品的硬件实现(三)

Chapter Ⅵ　Implementation of the Hardware for Safety-related Products:Part 3

谢亚莲[1,2]　郭　栋[1,2]

(上海工业自动化仪表研究院[1],上海　200233;上海仪器仪表自控检验测试所功能安全中心[2],上海　200233)

摘　要:判断安全相关产品的硬件设计是否达到硬件安全完整性等级的要求,就需要量化随机失效的影响。为了达到量化随机失效影响的目的,介绍了针对安全相关产品的失效率预计和 PFD/PFH 的计算方法。

关键词:安全相关产品　硬件安全完整性　可靠性预计　共因失效　PFD

中图分类号:TP202　　**文献标志码**:A

Abstract: To determine the hardware design of safety-related product meets the requirements of hardware safety integrity level, we need to quantify the impact of random failures. In order to achieve the purpose of quantifying the impact of random failures, introduced the reliability prediction metbod and PFD / PFH calculation method for safety-related products.

Keywords: Safety-related products　Hardware safety integrity　Reliability prediction　Common cause failure　Probability of dangerous failure on demand

0　引言

安全相关产品的硬件实现过程已在上两讲中作了部分描述,这个过程从编制产品设计要求规范开始,然后进入安全相关产品的硬件设计。该设计过程包含满足硬件安全完整性要求、系统安全完整性要求以及检测到故障时对系统(产品)的行为的要求的硬件设计。完整的安全相关产品的硬件实现还包括安全确认计划的编制、安全确认试验、功能安全评估以及每一阶段的验证,这部分内容本讲不作讲述。

在这一讲中,我们主要细化量化随机失效的影响这一过程,详细讲述元器件的失效率预计和 PFD/PFH(要求时的平均危险失效概率/每小时危险失效概率)的计算。

1　失效率预计

对元器件进行失效率预计就是可靠性预计。要计算安全相关产品要求时危险失效概率(PFD)或平均危险失效频度(PFH),则首先需获得组成安全相关产品并参与执行安全功能的所有元器件的失效率。然后将功能模块的失效率按失效对所执行的安全功能的影响划分为安全失效、可诊断的危险失效和不可诊断的危险失效。

失效率预计基于电子元器件的失效概率分布为指数分布,用以估算元器件在产品有效寿命期间的失效率。

我们可采用以下方法进行失效率预计:

① 分析产品结构;

② 选择合适的可靠性预计手册;

③ 确定各种环境应力条件。

目前在国际、国内获得公认并广泛采用的可靠性预计手册以及每种可靠性预计手册采用的可靠性预计模型及各模型的特点、适用范围如表 1 所示。

功能安全最早兴起于欧洲,在功能安全领域通常采用西门子公司的元器件预计手册 SN29500。SN29500 给出各元器件在基础温度、功率、电压、电流等基础应力条件下的基础失效率 λ_b,然后根据规定的工作和负载条件计算该元器件的失效率 λ:$\lambda=\lambda_b\times\pi_T\times\pi_Q\times\pi_U\cdots$,所以元器件的失效率与质量等级、温度应力、电压、电流、功率等有关。

修改稿收到日期:2013-10-14。

第一作者谢亚莲(1966-),女,1991 年毕业于上海机械学院可靠性技术专业,获硕士学位,高级工程师;主要从事可靠性技术和功能安全技术的研究。

表 1　各种可靠性预计方法特征的比较

Tab. 1　Comparison of the features of various prediction methods for reliability

可靠性预计手册	应　用	说　明	适用产品
MIL-HDBK-217F	提供了元器件计数和元器件应力预计法的失效率数据和应力模型,预计的环境温度范围为 0 ~ 125 ℃	1995 年版本的数据手册。一些元器件的预计失效率比实际效果差。 2006 版以软件方式面世。	军品
Telcordia SR332 Bellcore TR332	提供了三种预计方法,这三种方法组合了元器件计数法、试验室测试数据和现场数据跟踪。	最新 SR332 Issue 2 为 2006 年版本,预计的环境温度范围限制在 30 ~ 65 ℃	民品
British Telecom HRD4 and HRD5	与 Telcordia SR332 相似	1995 年版本。预计的环境温度范围限制在 0 ~ 55 ℃。	民品
Siemens SN29500	提供了元器件计数和元器件应力预计法的失效率数据和应力模型。采用的参考条件是典型的元器件在设备中的应用。	2005 年版本。现场失效率数据是由使用在西门子产品中的元器件确定,同时也考虑了来源于外部的试验结果。	民品
IIEC-62380	提供可元器件应力预计法的失效率数据和应力模型,强调了温度变化对元器件封装的影响。	2004 年版本	民品
GJB/Z 299C	与 MIL-HDBK-217F 相似,提供了元器件计数和元器件应力预计法的失效率数据和应力模型	2006 年版本	军品/民品

2　PFD/PFH 计算

安全相关产品的硬件能达到的安全完整性等级能力是采用架构约束条件和安全完整性等级目标失效量值来衡量的,安全完整性等级目标失效量值为在要求模式下的要求时平均危险失效概率(PFD)和在连续模式下的平均每小时危险失效概率(PFH),结构约束和控制故障措施的效用也是由安全相关参数 PFD/PFH 描述。

安全相关产品有别于安全相关系统,通常安全相关产品在安全相关系统中作为一个组件存在。安全相关产品内部的功能模块的冗余为 1(即 $HFT=1$),常选用 1oo2 结构(1 out of 2),当其中一个功能模块/通道发生故障时,安全相关产品或因不能执行失效安全功能而常采用输出报警功能。故障修复是针对安全相关产品而不存在单个功能模块的修复,故安全相关产品执行其安全功能的 PFD/PFH 值与平均修理时间(mean repair time, MRT)及平均恢复时间(mean time to restoration,MTTR)无关。在标准 IEC 61508-6 (GB/T 20438-6) 中给出了一种计算 PFD/PFH 的方法,适用于安全相关系统的计算,例如安全功能是由分布控制系统 DCS 执行,其中冗余的 AI 功能分别由二或三个独立的卡件实现,对其安全功能的 PFD/PFH 计算可采用标准提供的方法。这里我们给出了 TUV 提供的一种计算方法,它更适用于安全相关产品的 PFD/PFH 计算。

与 PFD/PFH 相关的因子具体如下。

① 不可检测的危险失效 λ_{Du}:诊断测试不能检测到的危险故障。

② 可检测的危险失效 λ_{Dd}:诊断测试能检测到的危险故障,在这里诊断测试间隔 T_D 大于过程安全时间(PST)。

③ 共同原因失效(CCF):在冗余系统中,由一个或多个事件导致的,引起两个或多个分离通道同时失效,从而导致系统失效;共因失效的影响用共因失效因子 β 和 β_D 描述。β 定义为不可诊断危险失效(λ_{Du})的共因失效因子;β_D 定义为可诊断危险失效(λ_{Dd})的共因失效因子,在一个诊断测试时间间隔 T_D 内,在两个通道中同时或先后发生的失效。

对 PFD/PFH 的计算分为四种情况:无诊断功能的单通道结构、带诊断功能的单通道结构、无诊断功能的双通道结构、带诊断功能的双通道结构。

这四种情况具体介绍如下。

① 无诊断功能的单通道结构(1oo1)

无诊断功能的单通道结构框图如图 1 所示。

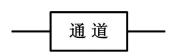

图 1　1oo1 结构图

Fig. 1　Structure of 1oo1

因只考虑危险失效概率,故要求时的失效概率为:

$$PFD(t)=1-e^{-\lambda_D t} \tag{1}$$

由于 $\lambda_D t<<1$,故式(1)可以简化为:$PFD(t)=\lambda_D t$

在时间间隔 T 内,$PFD(t)$ 的平均值由下式给出:

$$PFD_{AV}(T)=\frac{1}{T}\int_0^T PFD(t)\,dt=\frac{1}{2}\lambda_D T \tag{2}$$

$$PFH=\frac{PFD(T)}{T}=\lambda_D \tag{3}$$

② 带诊断功能的单通道结构(1oo1)

1oo1 结构具有在线诊断功能,且故障检测时间小

于过程安全时间(*PST*),即在故障可能产生危险之前,这些故障已被检测出。对于该单通道结构,危险失效概率只与不可诊断的危险失效 λ_{Du} 有关。

在时间间隔 T 内,$PFD(t)$ 的平均值由下式给出:

$$PFD_{AV}(T)=\frac{1}{2}\lambda_{Du}T \tag{4}$$

PFH 由下式给出:

$$PFH=\lambda_{Du} \tag{5}$$

③ 无诊断功能的双通道结构(1oo2)

双通道结构的结构框图如图 2 所示。在每个单通道中无诊断功能,即 $\lambda_{Dd}=0$、$\lambda_{Du}=\lambda_D$。该双通道结构的可靠性框图如图 3 所示,CCF 为共因失效。

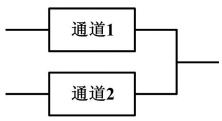

图 2　1oo2 结构图

Fig. 2　Structure of 1oo2

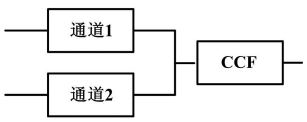

图 3　1oo2 可靠性框图

Fig. 3　1oo2 reliability block diagram

无诊断的双通道结构的危险失效概率函数 $PFD(t)$ 的表达式为:

$$PFD(t)=f(\lambda_{Dch1},\lambda_{Dch2}t,\beta) \tag{6}$$

无诊断的双通道的危险失效概率 $PFD(t)$ 为:

$$PFD(t)=[(1-\beta)\lambda_{Dch1}t]\times[(1-\beta)\lambda_{Dch2}t]+\beta\times\frac{\lambda_{Dch1}+\lambda_{Dch2}}{2}\times t \tag{7}$$

式中:"+"左边为两个通道同时都发生危险失效的概率;"+"右边为因危险共因失效引起的失效概率。

要求时平均危险失效概率为:

$$PFD_{AV}(T)=\frac{1}{3}(1-\beta)^2\lambda_{Dch1}\times\lambda_{Dch2}\times T^2+\frac{1}{4}\beta\times(\lambda_{Dch1}+\lambda_{Dch2})\times T \tag{8}$$

每小时危险失效概率为:

$$PFH(T)=(1-\beta)^2\lambda_{Dch1}\times\lambda_{Dch2}\times T+\frac{1}{2}\beta\times(\lambda_{Dch1}+\lambda_{Dch2}) \tag{9}$$

④ 带诊断功能的双通道结构(1oo2)

我们知道在功能安全中是考虑引起系统安全功能发生危险失效的那部分失效的概率,所以我们只考虑引起危险失效的 λ_D。

当在单通道中具有诊断功能时,危险失效 λ_D 又可分为可诊断的危险失效 λ_{Dd} 和不可诊断的危险失效 λ_{Du}。诊断测试时间间隔 T_D 小于过程安全时间的这部分可诊断的危险失效不会引起安全功能的危险失效发生,所以只有不可诊断的危险失效 λ_{Du} 和诊断测试时间间隔大于过程安全时间的那部分不可诊断的危险失效 λ_{Du} 被考虑。

带诊断的双通道结构的危险失效概率函数为:

$$PFD(t)=f(\lambda_{Duch1},\lambda_{Duch2},\lambda_{Ddch1},\lambda_{Ddch2},T_D,\beta,\beta_D) \tag{10}$$

带诊断的双通道结构的 *PFD* 计算公式为:

$$PFD(t)=[(1-\beta)\lambda_{Duch1}t]\times[(1-\beta)\lambda_{Duch2}\times t]+\beta\times\frac{\lambda_{Duch1}+\lambda_{Duch2}}{2}\times t+[(1-\beta_D)\lambda_{Ddch1}\times t_D]\times[(1-\beta_D)\lambda_{Ddch2}\times t_D]+\beta_D\times\frac{\lambda_{Ddch1}+\lambda_{Ddch2}}{2}\times t_D$$

需要计算 $PFD(t)$ 的平均值,因为 $PFD(t)$ 的平均值与安全完整性等级(SIL)相关,所以:

$$PFD_{AV}(T)=\frac{1}{T}\int_0^T PFD(t)\,dt \tag{11}$$

要求时的平均危险失效概率为:

$$PFD_{AV}(T)=\frac{1}{3}(1-\beta)^2\lambda_{Duch1}\times\lambda_{Duch2}\times T^2)+\frac{1}{4}\beta\times(\lambda_{Duch1}+\lambda_{Duch2})\times T+\frac{1}{3}(1-\beta_D)^2\lambda_{Ddch1}\times\lambda_{Ddch2}\times T_D^2)+\frac{1}{4}\beta_D\times(\lambda_{Ddch1}+\lambda_{Ddch2})\times T_D$$

每小时危险失效概率为:

$$PFH(T)=(1-\beta)^2\lambda_{Duch1}\times\lambda_{Duch2}\times T+\frac{1}{2}\beta\times(\lambda_{Duch1}+\lambda_{Duch2})+(1-\beta_D)^2\lambda_{Ddch1}\times\lambda_{Ddch2}\times\frac{T_D^2}{T}+\frac{1}{2}\beta_D\times(\lambda_{Ddch1}+\lambda_{Ddch2})\times\frac{T_D}{T}$$

由上式可以看出,当诊断测试时间间隔 T_D 小于验证测试时间间隔 T 时,关于 T_D 的两项失效概率可以忽略不计。

3　结束语

关于安全相关产品的安全相关参数 PFD/PFH 值的计算是判断安全相关产品的硬件安全完整性是否达到要求的安全完整性目标值和安全完整性等级的重要因素,也是量化随机失效影响这一过程的最终结果;而量化随机失效的影响这一整个过程是一项复杂繁琐的工作,需要功能安全评估人员熟练掌握电子电路知识、可靠性知识、功能安全知识。