功能安全温度变送器设计和可靠性分析

Design and Reliability Analysis of the Functional Safety Temperature Transmitter

周　亚[1,2]　徐晓东[1,2]　白书元[2]　王　锴[1,2]　刘梁梁[1,2]

(中国科学院研究生院[1],北京　100039;中国科学院沈阳自动化研究所[2],辽宁 沈阳　110016)

摘　要：为发展我国自主知识产权的安全控制技术,开发国内首个经第三方认证的安全相关产品,给出了功能安全温度变送器的设计方法和可靠性分析方法。依据 IEC 61508 功能安全标准,结合安全温度变送器 1oo1D 的结构特点,研究了变送器自诊断的实现方法,同时建立了 Markov 模型,并对变送器的可靠性进行了定量评估。分析结果表明,安全温度变送器满足功能安全要求和安全完整性等级要求。

关键词：功能安全　温度变送器　IEC 61508　自诊断　Markov 模型　安全完整性等级(SIL)

中图分类号：X937　　**文献标志码**：A

Abstract: To develop the safety control technology with our own intellectual property, and develop the first safety related product authenticated by the third-party certification, the design and reliability analysis methods of the functional safety temperature transmitter are given. In accordance with the IEC 61508 functional safety standard, and combining the features of functional safety temperature transmitter with 1oo1D architecture, the implementing method of self-diagnostics for the transmitter is researched. In addition, the Markov model is established to quantitatively assess the reliability of transmitter. The results of analysis show that the temperature transmitter meets the requirements of functional safety and safety integration level.

Keywords: Functional safety　Temperature transmitter　IEC 61508　Self-diagnostic　Markov model　Safety integrity level(SIL)

0　引言

在石油、化工、冶金和核电等领域,对生产过程的安全性要求非常严格,对环境的检测和控制显得越发重要。安全控制系统[1]能够行使一项或多项安全功能,是保障安全生产的重要装备。作为安全控制系统的重要组成部分,安全仪表变送器能够检测生产环境的关键性输入,为确保生产过程的安全可靠运行发挥非常重要的作用。随着现场总线技术在工业应用中的普及,温度变送器能对现场的环境因素实现远程监测,对工业现场数字信息进行实时采集和监控,突显其便利性与实时性。由于采用了一系列行之有效的降低风险、提高安全性的手段,安全温度变送器能够可靠地采集信息和监控工业现场,保障了工业现场的安全。

为了确保安全温度变送器可靠地运行,需对变送器进行周期性诊断[2]。即在变送器开发的过程中,采取一系列有效的诊断方法,提高诊断覆盖率,使变送器达到所要求的安全完整性等级[3-4]。

国家高技术发展计划(863)基金资助项目(编号:2012AA041103);
国家自然科学基金资助项目(编号:61004068)。
修改稿收到日期:2012-10-07。

第一作者周亚(1986-),男,现为中国科学院沈阳自动化研究所模式识别与智能系统专业在读硕士研究生;主要从事安全仪表技术方面的研究。

1　温度变送器的功能安全

安全功能是针对某个具体潜在危险事件的保护措施,而功能安全表征了仪表的安全功能是否能够有效地得到执行,它取决于安全相关系统和外部风险降低设施的正确功能。通过降低安全相关系统和外部的风险以降低设施覆盖的部分风险,从而达到特定可容忍风险。温度变送器的安全功能有:① 测得温度与通信模块的实际输出一致,变送器测温过程中没有失效产生,测温功能得到执行;② 若诊断出错误,产生报警,若变送器测温过程中诊断出失效,则输出报警。

影响温度变送器安全功能的主要因素有失效模式和自诊断。温度变送器的失效模式分为危险失效、安全失效和无影响失效。为确定部件的失效模式对整个变送器的影响,需对变送器进行失效分析。温度变送器的自诊断功能可以检测变送器状态,在变送器出现失效时发出警告,把危险失效转换为安全失效,使变送器能够尽快得到修复。诊断覆盖率表示了变送器自动检测失效的能力,若诊断覆盖率达不到安全功能要求和安全完整性要求,则需要对硬件和软件设计进行修改,直至达到安全要求为止。

2　安全温度变送器设计

2.1　系统设计

本文设计的安全温度变送器采用 1oo1D(即 1-out-

of-1 diagnosis)系统结构,具有一个数据采集通道和一个诊断通道,两通道相互独立,不存在冗余。安全温度变送器的1oo1D体系结构如图1所示。

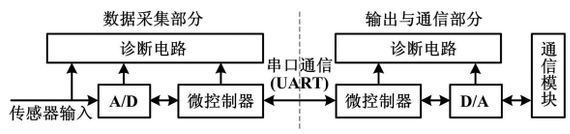

图1　安全温度变送器1oo1D体系结构

Fig. 1　Safety temperature transmitter with 1oo1D architecture

安全变送器由两大部分组成,分别为数据采集部分和输出与通信部分。数据采集部分完成温度数据的采集并计算,然后通过串口发送给通信部分。输出与通信部分完成温度数据的计算、通信、模拟量数据输出等功能。两部分配合使用完成安全变送器的全部功能。

安全温度变送器包括A/D、D/A、微控制器、诊断电路、通信(包括串口通信(UART))等模块。A/D模块负责模拟量采集;D/A模块负责最后的4~20 mA模拟输出;微控制器实现数据采集功能和安全功能的数据处理;诊断电路用于对变送器各组成部分进行诊断;通信模块采用HART总线通信,HART芯片用于将HART输出叠加到D/A上;串口通信(UART)模块负责数据采集部分和输出与通信部分的数据交换。由于开发的变送器中HART总线不涉及安全功能,因此并没有为通信模块添加诊断。

变送器上电后首先对微控制器进行诊断,微控制器通过自检后,依次对传感器模块、A/D模块、D/A模块、信号输出模块进行诊断。当诊断出错误时,变送器发出报警信号[5],通知控制器有失效产生;当没有错误产生时,则变送器开始采集数据。对于HART总线,则由D/A转换为标准的电流信号,与HART调制解调器的FSK信号一起叠加到4~20 mA电流环路上。

2.2　诊断方法

安全温度变送器具有两个微控制器,分别完成数据采集功能和通信功能。针对该特点,将冗余结构常用的数据对比方法[6]引入到变送器之中,进一步保证了数据可靠地采集和发送。对于其他模块也需进行周期性诊断,确保变送器安全运行。安全温度变送器诊断逻辑如图2所示。

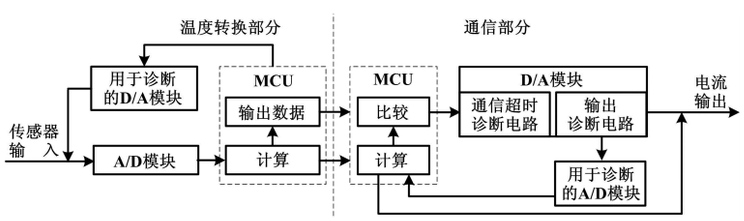

图2　安全温度变送器诊断逻辑图

Fig. 2　Diagnosis logic of the safety temperature transmitter

在A/D模块采集数据之前,对A/D模块和D/A模块进行诊断,确保A/D数据采集通道和D/A数据输出通道没有失效产生,A/D模块和D/A模块都有相应的D/A和A/D用于对数据进行采集。诊断内容主要包括以下3个方面的内容。

① A/D模块的诊断。诊断A/D模块时,由微控制器产生一个设定值,经过A/D芯片采样、离散化之后,通过用于诊断的D/A模块将数据采回。判断设定值和采回值是否相同,如果设定值和采回值相同,则认为A/D数据采集通道没有问题;如果不同,则认为失效产生。

② D/A模块的诊断。D/A模块的诊断方法与A/D模块类似,也是产生一个设定值,并与采回值进行比较,如果检测出失效,D/A输出报警电流到电流环路上。除此之外,D/A还具有监视环路电流和通信计时等安全功能,当环路电流超出一定范围以及微控制器与D/A通信超时,则进行报警输出。

③ 微控制器的诊断。温度变送器的两个微控制器完成各自功能后也可以用于数据对比,实现对整个数据采集通道和CPU的间接诊断。温度传感器信号经A/D采集后,两个微控制器对原始温度数据进行计算,然后对比计算结果,若不同则输出报警电流,相同则通过通信模块输出。

3　可靠性分析

在开发安全温度变送器的过程中,将安全完整性等级(safety integrity level,SIL)作为总体设计的依据和衡量整个变送器安全性能的标准。安全完整性等级是一定条件下安全功能得到正确执行的概率,其数值代表着风险降低的数量级。为降低一定的风险,需要将诊断方法等安全措施引入安全变送器,以提高诊断覆盖率,保证安全变送器达到所要求的安全完整性等级。基于此,本文依据可靠性模型,通过计算结果给出安全变送器所能达到的安全完整性等级,作为评价功能安

全水平的指标。

评价安全功能的可靠性能是通过一些统计指标[2]来完成的,这些指标有平均无故障时间、要求时失效概率(probability of failure on demand,PFD)等。对于低要求操作模式,安全完整性等级的选择实质上是选择要求时失效概率的数量级,同时,安全完整性等级的确定还与安全失效分数(safety failure fraction, SFF)有关。因此,将定量要求时平均危险失效概率和安全失效分数作为建立可靠性模型的最终目标。

3.1　温度变送器的 Markov 模型

Markov 模型将系统归于不同的安全状态,通过描述不同状态之间的转换来分析系统的安全性,它不仅可以用于简单模型,也可以为更复杂的模型提供精确的结果。温度变送器采用 1oo1D 系统结构,诊断通道将被检测到的危险失效转换为安全失效。模型考虑了危险失效和安全失效这两种失效模式,还考虑了变送器出现故障后可以进行修复且修复率为常数,变送器重启后可正常工作。建模过程中的假设在 IEC 61508-6 中有详细描述。

1oo1D 体系结构温度变送器的 Markov 状态转移图如图 3 所示。转移过程共有 3 个状态,其中,OK(状态 0)表示初始正常状态,FS(状态 1)表示安全失效状态,FDU(状态 2)表示未检测到的危险失效状态;SD 表示检测到的安全失效,SU 表示未检测到的安全失效,DD 表示检测到的危险失效,DU 表示未检测到的危险失效。λ_{SD}、λ_{SU}、λ_{DD}、λ_{DU}则为相对应的失效率。

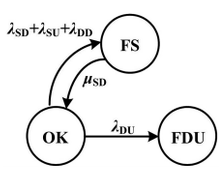

图 3　Markov 状态转移图

Fig. 3　Markov state transition diagram

当诊断通道检测到数据采集通道发生失效时,则将危险失效转换为安全失效,变送器由状态 0 转换为状态 1,变送器重启后正常工作,由状态 1 转换为状态 0;当没有检测到失效时,由状态 0 变为状态 2。

在有诊断的情况下,需要计算的 PFD_{avg} 为要求时的平均未检测到的危险失效概率[7],对应状态转移图中最后一个状态的情况。对 PFD_{avg} 的计算方法作了如下简化:所要计算的残余错误概率,即要求时失效概率 PFD,也就是图 3 中状态 2 时的未检测到的危险失效的概率,对这 n 个不同时间间隔得到的矩阵的最后一个元素(即最后一个状态)的值取平均值,即可得到 PFD_{avg},再从 SIL 等级表中查出相对应的 SIL 等级。

3.2　安全完整性评估

诊断覆盖率和失效率由失效模式影响及其诊断分析(failure modes effects and diagnostic analysis,FMEDA)确定。FMEDA 是一种对设备的不同失效模式和诊断能力进行详细分析的方法,它需要的信息包括:① 所有部件的定量的失效数据(失效率和失效模式分布);② 通过诊断发现内部失效的能力。详细的失效模式影响和诊断分析方法能够提供相对准确的失效模式和诊断覆盖评估信息。当这些信息由现场失效报告组成时,就会得到失效率和失效模式的合理评估;依据这些信息,可以计算诊断覆盖率和安全失效分数等参数,实现对所开发的变送器的安全评价。

本文通过 FMEDA 分析变送器的每一种失效模式[8]及对整个变送器造成的影响,确定每种失效模式的失效率、安全失效和危险失效的比例。对于复杂器件,IEC 61508-2 列举了针对复杂器件必须予以考虑的失效模式的诊断覆盖率。分析过程中用到的失效数据来源于西门子内部可靠性预计文档 SN29500,失效模式及分布数据来源于机械安全标准 IEC 62061。由于 FMEDA 的分析过程繁琐且复杂,篇幅所限,本文只给出最终分析结果。分析结果如表 1 所示。

表 1　FMEDA 分析结果

Tab. 1　Analyzing results of FMEDA

λ_S/h	λ_D/h	λ_{SD}/h	λ_{DD}/h
1.58×10^{-6}	2.84×10^{-7}	1.47×10^{-6}	2.60×10^{-7}

表 1 中:λ_S为安全失效率;λ_D为危险失效率;λ_{SD}为检测到的安全失效率;λ_{DD}为检测到的危险失效率。

IEC 61508-6 给出的相关公式如下:

$$\lambda_{DU}=(1-C_D)\lambda_D \quad C_S=\lambda_{SD}/\lambda_S \quad C_D=\lambda_{DD}/\lambda_D \tag{1}$$

$$SFF=(\lambda_S+\lambda_{DD})/(\lambda_S+\lambda_D) \tag{2}$$

式中:λ_{DU}为未检测到的危险失效率;C_S为安全失效诊断覆盖率;C_D为危险失效诊断覆盖率;SFF 为安全失效分数;μ_{SD}可以通过将节点平均重启时间取倒数得到。平均重启时间为 24 h,各失效率单位为每小时(/h)。

由式(1)~式(2)可得其他变量的值,如表 2 所示。

表 2　计算结果

Tab. 2　Calculation results

λ_{DU}/h	C_S/%	C_D/%	SFF/%	μ_{SD}/h
0.24×10^{-7}	93	91.5	98.7	0.041 667

将计算所得数据代入状态转移矩阵,得:

$$\boldsymbol{P}=\begin{bmatrix}0.999\ 998 & 0.000\ 001\ 835 & 0.000\ 000\ 024\\ 0.041\ 667 & 0.958\ 333 & 0\\ 0 & 0 & 1\end{bmatrix}$$

初始时变送器正常工作,用数字 1 表示,因此初始状态 S = [1　0　0],则极限状态转移和初始矩阵满足:

$$\boldsymbol{S}_{\mathrm{L}}=\boldsymbol{S}\times\boldsymbol{P}^{n} \tag{3}$$

式中:$\boldsymbol{S}_{\mathrm{L}}$ 为极限状态矩阵;$\boldsymbol{S}$ 为初始状态矩阵。由式(3)可得 n 个时间间隔后各状态的概率情况。本文取 10 个功能测试周期即 n 为 876 00 h 后的结果如表 3 所示。

表 3　功能测试后的状态概率

Tab. 3　State probability after functional test

时间/h	状态 0	状态 1	状态 2
1	0.999 998 00	1.835 000 00e-06	2.400 000 00e-08
2	0.999 996 08	3.593 537 38e-06	4.799 995 20e-08
3	0.999 994 23	5.278 798 26e-06	7.199 985 78e-08
4	0.999 992 45	6.893 835 98e-06	9.599 971 92e-08
…	…	…	…
87 597	0.985 607 66	4.340 598 62e-05	0.002 087 12
87 598	0.985 607 50	4.340 597 91e-05	0.002 087 14
87 599	0.985 607 34	4.340 597 19e-05	0.002 087 16
87 600	0.985 607 18	4.340 596 47e-05	0.002 087 19

由表 3 可知,最后状态的值随时间的增长不断增大。对状态 2 的值取平均值,可得 PFD_{avg}为 0.001 04。低要求操作模式的安全完整性等级表如表 4 所示。

表 4　低要求操作模式的 SIL

Tab. 4　SIL in low demand operation mode

SIL	PFD_{avg}	风险降低因子
4	$10^{-4}\sim10^{-5}$	100 00 ~ 100 000
3	$10^{-3}\sim10^{-4}$	10 00 ~ 10 000
2	$10^{-2}\sim10^{-3}$	100 ~ 1 000
1	$10^{-1}\sim10^{-2}$	10 ~ 100

对照低要求操作模式的安全完整性等级表,由于 $10^{-3}<0.001\ 04<10^{-2}$,因此,可知此时变送器的安全完整性等级是 SIL2。1oo1D 体系结构的硬件故障裕度为 0,安全完整性等级达 SIL2,需满足 90% <*SFF*< 99%,而 *SFF* 为 98.7%。因此,应用上述诊断方法的安全变送器总体设计方案满足安全完整性要求。

4　结束语

安全温度变送器采用 1oo1D 体系结构,结合变送器两个微控制器的结构特点,将冗余结构的对比方法引入安全温度变送器之中;对模拟量采集模块、数据处理模块和模拟信号输出模块进行诊断,实现了切实可行的诊断方法,有效控制了系统失效和随机失效;应用 FMEDA 分析失效模式和各模式对变送器的影响,使建立马尔可夫模型的结果可靠精确。

参考文献

[1] 方来华,吴宗之. 安全仪表系统的开发与要求[J]. 中国安全科学学报, 2009,19(4):159-168.

[2] 阳宪惠,郭海涛. 安全仪表系统的功能安全[M]. 北京:清华大学出版社,2007:36-59,68-95.

[3] 国家质量监督检验检疫总局. GB/T 20438.1-2006 电气/电子/可编程电子安全相关系统的功能安全　第 1 部分:一般要求[S]. 北京:中国标准出版社,2006:1-39.

[4] 国家质量监督检验检疫总局. GB/T 20438.2-2006 电气/电子/可编程电子安全相关系统功能安全　第 2 部分:电气/电子/可编程电子安全相关系统的要求[S]. 北京:中国标准出版社,2006:28-51.

[5] Shishiba R. Implementation of a safety instrumented system[C]//SICE Annual Conference 2007, Society of Instrument and Control Engineers, 2007:2493-2496.

[6] Goble W M, Cheddie H. Safety instrumented systems verification: practical probabilistic calculations[M]. ISA, 2005:28-343.

[7] Borcsok J, Schaefer P S, Ugljesa E. Estimation and evaluation of common cause failures[C]//Second International Conference on Systems, Proceedings of the Second International Conference, 2007: 1-41.

[8] 国家质量监督检验检疫总局. GB/T20438.6-2006 电气/电子/可编程电子安全相关系统的功能安全第 6 部分:GB/T 20438.2 和 GB/T 20438.3 的应用指南[S]. 北京:中国标准出版社,2006:44-46.

(上接第 69 页)

性能要求外,还要满足在设计、制造、试验、鉴定等过程中的核电产品的特殊规范要求,并用一套科学的体系来保证这些特殊要求的实现,实现产品生命周期全过程的可控管理和可追溯,确保电磁阀对核电站正常、高效、安全地运行发挥保驾护航的作用。

参考文献

[1] ASME. BPVC-Ⅲ核设施部件建造规则[S]. 上海:上海科学技术文献出版社,2007.

[2] JB/T 7352-2010 工业过程控制系统用电磁阀[S]. 北京:机械工业出版社,2010.

[3] 林诚格. 非能动安全先进核电厂 AP1000[M]. 北京:原子能出版社,2008.

[4] AFCEN. RCC-M 法国压水堆核岛机械设备设计建造规则[S]. 上海:上海科学技术文献出版社,2010.

[5] AFCEN. RCC-E 法国压水堆核岛电气设备设计建造规则[S]. 上海:上海科学技术文献出版社,2012.