功能安全浮筒液位计的研究与实现

李倩如 杨振荣 王 鑫
(上海自动化仪表有限公司 上海 200072)

摘 要：随着工业自动化的不断发展，安全仪表系统技术越来越受到关注，而我国对功能安全仪表系统的研究尚在起步阶段。提出了功能安全浮筒液位计的安全构架，主要研究了浮筒液位计的功能安全技术、FMEDA技术、软件自诊断技术、V&V技术及软件测试技术，并将其应用于浮筒液位计的设计开发中。最终实现了浮筒液位计的SIL2功能安全认证，是国内首个获得莱茵TUV颁发SIL2证书的功能安全浮筒液位计产品，打破了国外对安全仪表及系统的长期技术垄断。

关键词：功能安全；液位计；SIL2；FMEDA
中图分类号：TH816 **文献标识码**：A **国家标准学科分类代码**：510.8040

Research and design of safety-related digital level transmitter

Li Qianru Yang Zhenrong Wang Xin
(Shanghai Automation Instrumentation Co., Ltd., Shanghai 200072, China)

Abstract: With the development of industrial automation, the technology of safety instrument & system is paid more and more attention, while the research on safety instrument & system in our country is still in its infancy. This paper put forward to the safety structure of the Digital Level Transmitter, mainly studies the functional safety of the digital level transmitter, FMEDA analysis, software self-diagnosis technology, V&V and software testing, and achieved SIL2 certification of the digital level transmitter. It is the first digital level transmitter in the domestic that achieved the SIL2 certificate by Rhine TUV, which break the technological monopoly of long-term safety instruments and systems by foreign countries.

Keywords: functional-safety; level transmitter; SIL2; FMEDA

0 引 言

随着我国工业的不断发展，工业自动化仪表作为过程工业自动化中的一个重要组成部分，其安全问题越来越受到人们的重视。安全仪表系统(SIS)，在危险事件发生之前正确地执行其安全功能，可以有效的避免或减少事故的发生[1]。2000年，国际电工委员会(IEC)发布了IEC61508标准，明确的提出了安全相关系统的功能安全[2]。仪表及系统的功能安全标准、评估、产品研究和开发、认证等问题逐渐成为国内外研究的热点。

在我国，功能安全仪表及系统的研究和开发尚在起步阶段[3-4]。功能安全浮筒液位计作为安全仪表系统的重要组成部分，使用在重要的安全和控制领域，为确保生产过程的安全可靠运行发挥非常重要的作用[5]。对浮筒液位计实施功能安全认证，能够对液位计的安全功能进行科学的分析，对产品的失效进行有效的控制，从而减少事故发生的概率，从而从根本上保证工业生产过程的本质安全，实现保障国家经济安全的目的[6]。

1 主要工作原理及系统概述

功能安全浮筒液位计主要包含功能安全液位变送器、浮筒室组件、浮筒组件、杠杆组件、扭力管。主要实现对液位的测量[7]。其主要工作原理如图1所示，浮筒浸没在被测液体中，与扭力管系统刚性连接。当被测液体的液位l发生变化，则悬挂在液体中的浮筒受到的浮力也随之发生变化，从而改变了扭力管的扭矩，从而导致扭力管角度的变化。这种扭力管的旋转运动传递到液位计的摆动组件上，从而导致摆动组件上的磁钢随之发生移动，从而导致了磁场的变化。液位变送器中的霍尔传感器可以感应到这种磁场的变化，并将磁信号转变为电信号，通过A/D转换电路对该电信号进行采样得到电压值之后传输至CPU模块进行数据处理，通过数据处理之后，将物位信号变送成标准的

收稿日期：2017-05

4～20 mA 信号远程传输,完成整个液位计的基本功能;HART 通信的信号以 4～20 mA 电路为物理层,耦合符合 FSK 标准的 HART 总线信号,以达到电浮筒物位计与 HART 主机间的信息交互功能。通过对液位计的传感器故障诊断、硬件故障诊断、FEMDA 分析及计算、软件 V&V 认证及测试等,并在产品的整个生命周期(需求、设计、测试、生产、质量)中遵循 IEC61508,从而开发出满足 SIL2 要求的功能安全浮筒液位计。

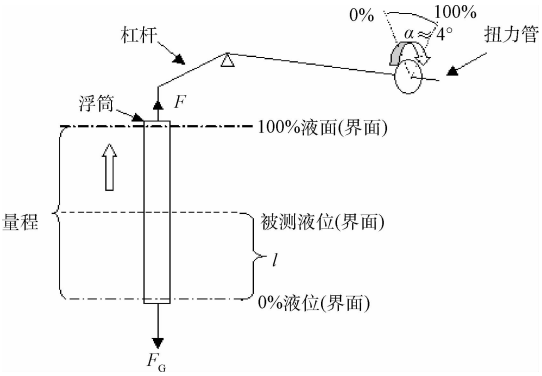

图 1 液位传感器物理原理

2 安全系统架构

根据 IEC61508 标准,一套完整的安全仪表系统由传感变送器、逻辑运算器和最终执行元件构成[8]。逻辑运算器作为核心部件,负责按照设定的逻辑进行控制。功能安全浮筒液位计作为传感变送器,主要对液位信号进行采集,并输出给逻辑运算器。

2.1 硬件安全架构

功能安全浮筒液位计的安全构架如图 2 所示:主要包括霍尔传感器、RTD 传感器、测量 A/D、诊断 A/D、MCU 模块、按键、LCD、HART 模块、电源模块、D/A 输出模块、时钟诊断模块、电源及输出诊断模块。

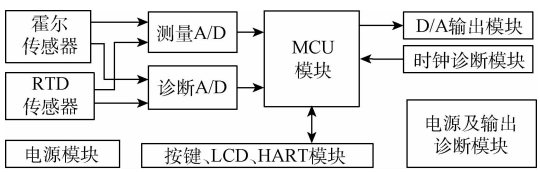

图 2 功能安全浮筒液位计的安全构架

其中霍尔传感器、RTD 传感器、测量 A/D、MCU、电源及 D/A 输出模块为安全相关的部分,其任何故障均需要进行诊断和 FMEDA 分析;其中诊断 A/D、时钟诊断模块、电源及输出诊断模块为诊断部分,其功能是对安全相关部分电路进行诊断;按键、LCD、HART 模块为非安全相关的部分,其失效不会影响到仪表的安全功能。

测量 A/D 采样模块主要采集霍尔传感器及 RTD 的温度信号并实现与 MCU 模块的通信,诊断 A/D 则实现对测量 A/D 模块的诊断。MCU 模块的主要对 A/D 模块采样的数字量进行运算处理并输出数字量给 D/A 从而控制 4～20 mA的电流输出。同时,MCU 还可实现对电源、环境温度、激励电流、及 MCU 内部的诊断。电源提供系统所需要的+3.3 V 及+5 V 电源。D/A 输出模块根据 MCU 提供的数字量输出 4～20 mA 电流。电源及输出诊断模块实现对系统电源、通讯故障和回路电流诊断。时钟诊断模块主要实现对 MCU 时序的故障诊断。按键可实现对仪表的功能配置,LCD 具有显示功能,HART 模块具有 HART 通信功能。

2.2 软件系统架构

功能安全浮筒液位计软件遵从 V&V(verification and validation)过程,通过检查、分析、评估评审、评价、测试的方法为软件产品和过程提供置信度证明[9-10]。功能安全浮筒液位计的安全功能是通过传感器采集液位信号,转变成数字信号实现 4～20 mA 模拟量输出,同时可通过 LCD 进行显示,并通过按键进行参数设置,通过上位机 Hart 协议进行通信,实现监视和出厂标定。

MCU 的软件功能总体设计如图 3 所示。

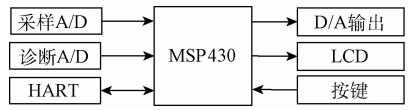

图 3 软件总体设计图

MSP430 通过 SPI 接口实现对模拟信号的采样;通过 SPI 接口实现 D/A 的模拟量输出;通过 UART 接口以完成产品的标定功能;另外,MCU 通过 I2C 接口控制液晶显示,通过按键设置量程范围。

功能安全浮筒液位计软件从功能上分为运行模块及诊断模块。运行模块负责信号的采集处理、LCD 显示、键盘设置及 HART 通信等仪表基本功能的实现。诊断模块则是仪表安全的重要保障。其运行模块流程如图 4 所示。

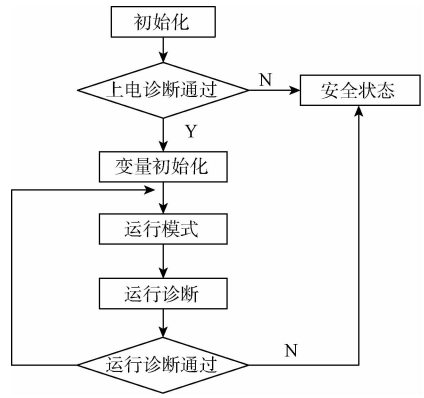

图 4 运行模块流程

首先,仪表完成上电初始化,同时进行上电诊断。如果诊断通过,则进行变量初始化,进入运行模式;若诊断出安全相关错误,则进入安全状态。仪表在运行模式中也要进

行运行自诊断，如果自诊断出错则进入安全状态(输出安全电流)。

运行模块首先判断仪表的所处模式。如在正常运行模式，仪表需完成 A/D 采样，AD 线性化处理，计算出物位值，D/A 输出转换，显示输出，诊断功能，同时若有上位机通信，完成上位机监测(注：标定对用户是不开放的功能，是安全相关的)功能。如果扫描按键输入，LCD 显示输入的密码正确，完成按键处理，实现按键设置功能。如果仪表处于安全模式，则输出安全电流。

运行模块分为 8 个子模块：按键处理模块、显示模块、主采样模块、诊断采样模块、D/A 转换模块、控制模块、中断处理模块、配置模块。

2.3　功能安全浮筒液位计诊断模块的设计

功能安全浮筒液位计在基本检测仪表的基础上增加诊断功能，实现对仪表状态的实时监控。因此诊断功能模块的设计决定着产品的安全功能，是至关重要的。功能安全浮筒液位计的诊断包括上电诊断和运行中诊断。上电诊断主要对 CPU 内部性能进行诊断，包括中断错误诊断、RAM 上电诊断、ROM 上电诊断、EEPROM 上电诊断、堆栈上电诊断、寄存器上电诊断、指令上电诊断。运行中的诊断除了包括 CPU 诊断，还包括外部器件的诊断，如：采样 AD 诊断、DA 诊断、电源诊断等。

3　安全完整性等级的评估

3.1　安全完整性等级

功能安全完整性评估方法[11-12]是综合考虑系统或设备的每小时失效概率密度(probability of failure per hour，PFH)，危险损害严重程度，暴露在危险中的时间，避免危险损害的可能性等因素进行的评估。安全性是安全相关系统的一种固有属性，并且以安全完整性等级(SIL)的形式来表征。安全完整性等级表示能成功完成安全功能的概率。根据 IEC61508 的规定，SIL 分为 4 个等级，SIL1 为最低，SIL4 为最高，等级越高代表发生故障的概率越低，安全性越高。SIL 等级与发生故障概率的关系如表 1 所示。

表 1　功能安全完整性等级与危险失效概率的关系

SIL	风险降低	低要求模式下 PFD_{Avg}(平均失效概率)	高要求或连续操作模式下 PFH(每小时危险失效概率)
1	10～100	$\geqslant 10^{-2}$至$<10^{-1}$	$\geqslant 10^{-6}$至$<10^{-5}$
2	100～1 000	$\geqslant 10^{-3}$至$<10^{-2}$	$\geqslant 10^{-7}$至$<10^{-6}$
3	1 000～10 000	$\geqslant 10^{-4}$至$<10^{-3}$	$\geqslant 10^{-8}$至$<10^{-7}$
4	10 000～1 000 000	$\geqslant 10^{-5}$至$<10^{-4}$	$\geqslant 10^{-9}$至$<10^{-8}$

3.2　安全相关系统的诊断及 SIL 等级验证

为了确定功能安全液位变送器的 SIL 等级，必须对液位计进行模块划分和模块独立诊断，对诊断方案进行分析，从而确定功能安全液位变送器诊断技术的有效性及诊断覆盖率。本文采用 FMEDA 的分析方法，可以定性和定量的对功能安全液位计的各个安全相关的模块进行有效的分析、研究和改进，从而实现安全仪表系统的高安全性、高可靠性以及高可用性[13]。

FMEDA 方法是指通过分析元器件(或部件)所有可能的故障模式[14]，根据电路的原理进行科学的分析，确定所有元器件的所有失效模式对液位计安全功能的影响，并确定和区分所有的安全失效和危险失效。所有的危险失效必须有对应的诊断电路进行诊断，从而达到 SIL2 要求的 90%以上的诊断覆盖率和 90%以上的安全失效分数(SFF)。针对功能安全浮筒液位计的硬件电路的各个模块进行 FMEDA 分析和计算可以得出表 2 的结论，从而满足了功能安全 SIL2 的等级要求。

表 2　功能安全浮筒液位计的 FMEDA 分析结果

(FIT)

模块	λ_S	λ_D	λ_{DD}	λ_{DU}	SFF
信号调理模块	4.43	8.71	8.63	0.09	0.99
测量 A/D 模块	8.3	8.3	8.22	0.08	0.99
MCU 模块	23.65	22.41	21.04	1.37	0.97
时钟	9.98	9.98	8.98	0.998	0.95
电源及 D/A 模块	45.19	42.28	41.72	0.56	0.99
总计	91.55	91.68	88.59	3.10	

3.3　软件安全完整性分析

要达到功能安全液位计 SIL2 的要求，软件则须满足 SIL3 的等级要求，在软件的开发过程中遵循 V&V(verification and validation)的要求，从而减少软件开发过程中所带来失效。同时需要对软件设计中的设计方法、技术路线、测试方法等采取一系列的故障避免措施，并对这些故障避免措施的有效性根据 IEC61508 进行分析和确认[15]。

3.4　软件测试及验证

软件验证主要包括软件静态测试、动态测试和集成测试。静态测试采用了人工审查分析和软件工具自动分析两种方法相结合的方式对软件源代码进行了静态测试分析。测试结果表明，软件源代码符合 MISRA—C：2004 编程规范。浮筒液位计动态测试同时采用了黑盒测试和白盒测试两种方法。

集成测试则主要是产品的功能测试。不同于常规产品，功能安全浮筒液位计还需要做故障插入测试，以检验 FMEDA 分析的有效性，对液位计各部分的故障进行人为的模拟注入测试，并验证输出结果是否导致安全的失效。

4　结　　论

“功能安全浮筒液位计”是我国首个具有自主知识产权

的安全级智能液位仪表,本项目的实施打破了国外对功能安全仪表技术的垄断,实现了对其关键零部件的自主创新,掌握了产品的关键工艺技术,提升了我国对安全级仪表工业的技术、工艺水平。

国内对于功能安全浮筒液位计的研发和生产起步较晚,这是我公司完全独立自主研发、国内首个通过功能安全完整性 SIL2 认证的浮筒液位计,达到了国内外先进水平。

参考文献

[1] 靳江红,吴宗之,赵寿堂,胡玢. 安全仪表系统的功能安全国内外发展综述[J]. 化工自动化及仪表,2010,37(5):1-5.

[2] 靳江红,吴宗之,胡玢. 对功能安全基础标准 IEC61508 的研究[J]. 中国安全生产科学技术,2009,5(2):71-75.

[3] 黄文君,何伟挺,边俊. 安全仪表系统的功能安全设计[J]. 自动化仪表,2010,31(7):75-78.

[4] 陈锐,韩亮,潘剑. 浅谈火电厂安全仪表系统[J]. 仪器仪表用户,2017,24(4):91-94.

[5] 兰羽,汪晓鸿. 基于 AT89C52 的超声波液位测量系统设计[J]. 国外电子测量技术,2013,32(10):30-33.

[6] 赵林,王雪,刘佑达. 基于突变理论设冷水泵转轴功能安全完整性评估[J]. 仪器仪表学报,2016,37(12):2728-2734.

[7] 韩健君,杨振荣,王鑫. 基于 HART 协议的浮筒液位计的改进和应用[J]. 电子测量技术,2010,33(4):137-140.

[8] 彭瑜. 工业控制软件功能安全的实现方法和评估[J]. 石油化工自动化,2011,24(1):1-7.

[9] 张杰颖. V&V 活动中对自诊断的关注和执行方法研究[J]. 自动化仪表,2016,37(7):71-75.

[10] 刘真,江国进,孙永滨. 核电安全级仪控系统软件 V&V 活动及其方法研究[J]. 核科学与工程,31(2):45-50.

[11] 张艳丽,刘友英,朱大胜. 过程装备控制系统安全完整性研究[J]. 化工自动化仪表,2013,40(6):783-786.

[12] 沈学强,白焰. 安全仪表系统的功能安全评估方法性能分析[J]. 化工自动化仪表,2012,39(6): 703-706.

[13] 白丹. 基于 FMEA 的安全仪表系统安全完整性研究[J]. 机电产品开发与创新,2016,29(5):32-35.

[14] 陆妹,蔡福全,孙京诰. FMEDA 在功能安全温度变送器验证中的应用[J]. 自动化仪表,2015, 36(4):37-40.

[15] 袁宜峰,凌志浩. 基于 IEC61508 的嵌入式软件可靠性设计与验证[J]. 南京工业大学学报:自然科学版,2011,33(6):82-86.

作者简介

李倩如,工学硕士,主要研究方向为工业仪表及系统的产品开发。

E-mail:liqianru2001@163.com