Advanced Materials Research Vol. 716 (2013) pp 521-526
Online available since 2013/Jul/15 at www.scientific.net
© (2013) Trans Tech Publications, Switzerland
doi:10.4028/www.scientific.net/AMR.716.521

Design of Functional Safety Temperature Transmitter and Reliability Analysis

Aidong Xu[1,a], Ya Zhou[2,b], Zhanyuan Bai[1,c], Kai Wang[1,d], Liangliang Liu[2,e]

[1]Shenyang Institute of Automation, Chinese Academy of Sciences, China
[2]University of the Chinese Academy of Sciences, China

[a]xad@sia.cn,[b]zhouya@sia.cn, [c]breezyon@sia.cn, [d]wangkai@sia.cn, [e]liuliangliang@sia.cn

Keywords: Functional safety;Temperature transmitter; 1oo1D; Self-diagnostic; Markov model

Abstract. This paper presents the design of the functional safety temperature transmitter and reliability analysis to develop the certified safety related product with independent intellectual property rights. According to the functional safety standard IEC61508 and the 1-out-of-1 and Diagnosis (1oo1D) architecture of the temperature transmitter, self-diagnostic methods are proposed. At the same time a Markov model is established to assess the reliability of the transmitter quantitatively. Analysis results show that safety integrity level(SIL) is SIL2 and safety temperature transmitter complies with functional safety requirements and safety integrity level requirements.

Introduction

SIS(Safety Instrumented System)[1] is an important system which performs one or more safety functions to make production process into safe state when the process runs into abnormal condition. As one of important devices of SIS, safety transmitter can detect key inputs of the production environment. Because a series of effective means to reduce risks are adopted, safety temperature transmitter can reliably collect information and monitor production process to ensure the safety of the industrial field.

Although safety related equipments have been used in high safety fields for many years, development details of safety related equipment are rarely mentioned due to technical confidentiality. This paper presents the most important two aspects about the development of functional safety temperature transmitter :design and reliability analysis. The functional safety temperature transmitter is the first safety related product certified by TÜV in China..

To realize safety and reliability at required SIL(Safety Integrity Level), safety temperature transmitter uses the self-diagnostic mechanism[2] in single channel. Various measures have been taken in order to control random hardware failures that are the most important factor for achieving high SIL[3,4,5].

Functional Safety of Temperature Transmitter

Functional safety represents how safety functions can be implemented effectively, it depends on the correct function execution of the safety related system and external risk reduction facilities to reduce its risk in order to achieve fault tolerance. If temperature value measured and output of the communication module are consistent, this means there is no fault in transmitter, The function of temperature measuring is implemented effectively. Otherwise, safety temperature transmitter outputs alarming signals when faults are detected.

The main factors that have effects on safety functions of temperature transmitter are failure modes and self-diagnosis. Failure analysis is necessary to determine how failure modes have effects on the entire transmitter. Self-diagnostic functions can detect transmitter's condition when a fault occurs.

Design of Functional Safety Temperature Transmitter

System Design

The 1oo1D(1-out-of-1 and Diagnosis) architecture is used in functional safety temperature transmitter with a data acquisition channel and a diagnostic channel as shown in Fig. 1.

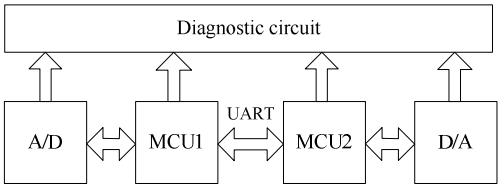

Fig.1 1oo1D system structure of safety temperature transmitter

Data acquisition channel provides functions of temperature data collection, calculation and communication. Two microcontrollers (MCU) communicate with each other through the serial port. A/D, D/A and MCUs are diagnosed one by one in diagnostic channel. If any fault is detected by diagnosis channel, MCU will obtain a fault alarming signal[6] which is pre-defined different types of faults. The transmitter begins to collect data when there is no error. Digital signal will be converted to the standard current signal through D/A.

Diagnostic Methods

Fig.2 shows the diagnosis logic diagram of safety temperature transmitter.

A/D module and D/A module should be diagnosed to ensure there are no faults in data acquisition channel and data output channel before A/D module collects data. A/D module and D/A module have a corresponding D/A and A/D[7,8] for writing data back. Diagnoses are described as follows:

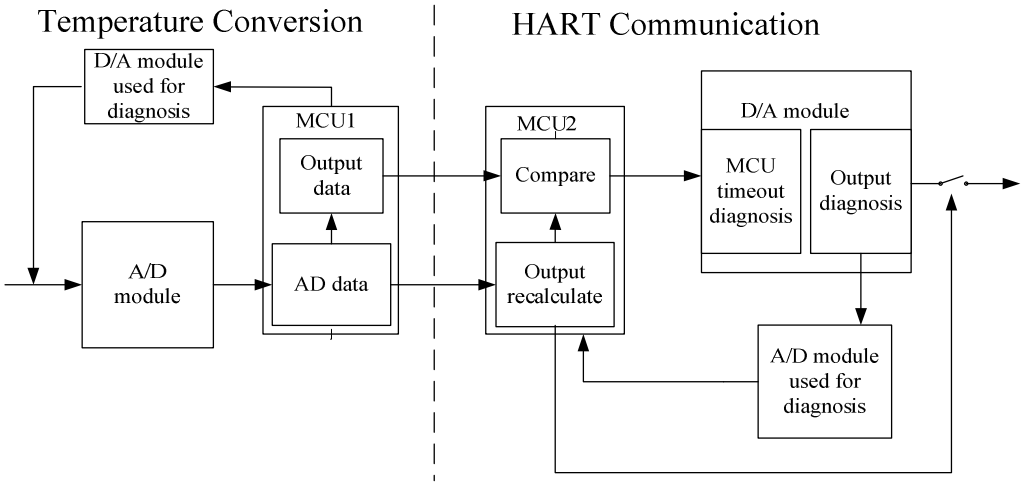

Fig.2 Diagnosis logic diagram of the safety temperature transmitter

(1) A/D module diagnosis

A voltage value is set by MCU1 and converted to analog value through D/A used for diagnosis. MCU1 reads the setting value back after sampling and discrimination of A/D chip. A conclusion can be made that there is no fault in data acquisition channel if setting value is equal to value that MCU1 reads back and there is fault if they are not equivalent after the comparison of two values.

(2) D/A module diagnosis

The approach of D/A module diagnosis is similar to that of A/D module. MCU2 also sets a value and reads the value back for comparison. If any fault is detected, D/A will output alarming signal to the current loop of HART bus. Besides, D/A also provides safety functions such as monitoring loop current and communication timer. Alarm output will be activated when the loop current is beyond a certain range or communication time between MCU2 and D/A module is out.

(3) MCU diagnosis

Two microcontrollers of temperature transmitter can be used for data comparison. After mining of temperature sensor signals, two MCUs perform the same computation of data conversion, Their results are compared to make sure that all fault in activated function of MCU can be detected.

Setting of Deviation Value Used for Diagnosis

Deviation Value

The essence of A/D diagnosis is to judge if setting voltage value is identical with measured value that MCU reads back. Comparison of two values determines whether there is a fault in data acquisition channel. Accuracy loss is inevitable in the process of data conversion. A/D chip is vulnerable to temperature drift and noise. So it is not practical to claim that two values are equal strictly. Judgment can be made through setting value equals to measured value if the deviation of two values is in the permitted range.

Setting of Deviation Value

A random voltage value in a certain range is able to be set by MCU and can be read back through A/D chip. Calculation of the deviation can be easily performed between setting value and measured value. Analysis of calculation results should be made to get the appropriate value as deviation used for diagnosis.

D/A used for diagnosis outputs 0 ~ 0.8V voltage, it is corresponding to random number between 0 and 4095. Random number between 400 and 600 is selected and voltage value is in the range from 78mv to 118mv correspondingly. A set of deviation value can be acquired after calculation and comparison of different setting value and measured value. Calculation results are shown in Table 1.

Table 1 Calculation results of Deviation value

Random number	Setting value [mV]	Measured value [mV]	Deviation [%]
410	80.724	80.339	— 0.477
420	82.693	82.148	— 0.658
430	84.661	83.967	— 0.819
……	……	……	……
510	100.413	100.491	0.0008
520	102.382	103.3604	0.950
530	104.350	104.136	— 0.206
……	……	……	……

Absolute values of deviation distribute in the range from 0.0008% to 0.966%. Special random numbers out of the range are tested many times to be close to the exact value. It is also considered that probability of undetected fault will increase when fault appears if deviation value is too large, The deviation value is set to 1% for diagnosis in this paper. Measured values distribute in the setting point nearby randomly while the setting values are linear. This conclusion can be confirmed in Fig.3, it shows setting value and measured value contrast diagram.

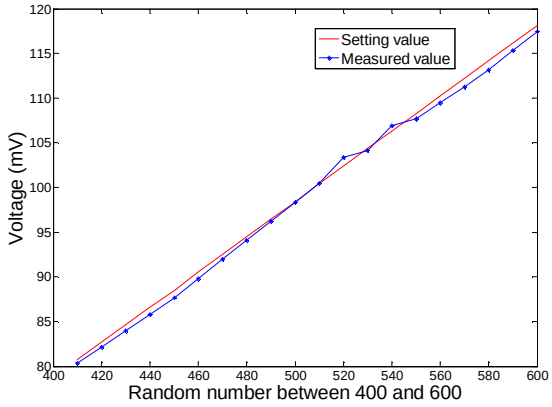

Fig.3 Setting value and measured value contrast diagram

Different gain value of the chip should be selected when measured values are in different range. Probability of output alarming signals increases obviously if deviation value is appropriately reduced to 0.9%. The test results show that setting deviation value confirms to the requirements of the diagnosis.

Reliability Analysis

Safety integrity level(SIL) is the probability of correct execution of safety functions under certain conditions. The identification of SIL value is essentially to choose the order of magnitude of probability of failure on demand (PFD). At the same time, selection of SIL is related to safety failure fraction(SFF). Therefore, quantitative value of PFD and SFF will be the ultimate goal of establishing reliability model.

Markov model of safety temperature transmitter

Temperature transmitter uses 1oo1D system structure. Dangerous failure and safety failure are considered in the Markov model. Safety transmitter can be repaired after failure occurs and the restoration rate is constant. Another assumption is that safety transmitter can perform normally after restarting. All assumptions that may occur in the process of establishing reliability model are detailedly described in IEC61508-6.

Fig.4 shows the Markov state transition diagram of safety temperature transmitter. State 0(OK) means safety transmitter performs in normal state, there is safety failure in state 1 and undetected dangerous failure in state 2.

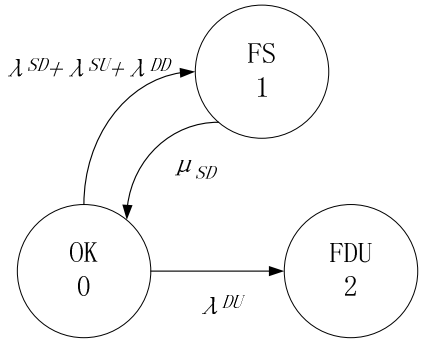

Fig.4 Markov state transition diagram

Dangerous failure will be turned into safety failure if diagnosis detects a fault in common function of data acquisition channel and state 0 switches to state 1. Safety transmitter performs normally after restarting, its state will be OK. State 0 will switch to state 2 if faults are not detected although faults occur in data acquisition channel. Abbreviations mentioned in this model are as follows. SD: safety failure detected, SU: safety failure undetected, DD:dangerous failure detected, DU: dangerous failure undetected. λ^{SD}, λ^{SU}, λ^{DD}, λ^{DU} is the corresponding failure rate. State transition matrix can be got according to Fig.4:

$$\boldsymbol{P}=\begin{bmatrix} 1-(\lambda^{S}+\lambda^{D}) & \lambda^{SD}+\lambda^{SU}+\lambda^{DD} & \lambda^{DU} \\ \mu_{SD} & 1-\mu_{SD} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

PFDavg (Average Probability of Failure on Demand) is the probability of the average undetected dangerous failure[9] which is corresponding to state 2 of the transition diagram. PFDavg calculation method is simplified to calculate the residual risk probability which is equal to the probability of the average undetected dangerous failure. The average value of the last element calculated in the matrix in different time will be PFDavg. SIL of the safety transmitter can be identified in the table whose value is corresponding to PFDavg.

Assessment of safety integrity level

FMEDA (Failure Modes Effects and Diagnostic Analysis) is accomplished to analyze every failure mode[10] and corresponding impact on the transmitter, it is used for calculation for the failure rate of each failure mode, safety failure and dangerous failure proportion. IEC61508-2 has listed the failure modes and diagnostic coverage which should be considered for complex and intelligent device. Failure data used in the analysis process come from Siemens internal reliability prediction document SN29500, failure modes and distribution data are obtained from mechanical safety standards IEC62061. The analysis process of FMEDA is so complex that this paper only gives the final analysis results as listed in Table 2.

Table 2 Analysis Results of FMEDA

λ^{S}	λ^{D}	λ^{SD}	λ^{DD}
1.58×10-6/h	2.84×10-7/h	1.47×10-6/h	2.60×10-7/h
λ^{S} : safety failure rate , λ^{D} : dangerous failure rate, λ^{SD}:detected safety failure rate, λ^{DD}:detected dangerous failure rate			

Calculation results of other variables are listed in Table 3 according to formulas of IEC61508-6 as follows.

$$\lambda^{DU} = (1 - C^{D})\lambda^{D}. \quad (1)$$

$$C^{S} = \lambda^{SD}/\lambda^{S}. \quad (2)$$

$$C^{D} = \lambda^{DD}/\lambda^{D}. \quad (3)$$

$$SFF = (\lambda^{S} + \lambda^{DD})/(\lambda^{S} + \lambda^{D}). \quad (4)$$

Table 3 Calculation Results

λ^{DU}	C^{S}	C^{D}	SFF
0.24×10-7/h	93%	91.5%	98.7%
λ^{DU} : undetected dangerous failure rate, C^{S}: diagnostic coverage of safety failure, C^{D} :diagnostic coverage of dangerous failure			

μ_{SD} is the reciprocal of average restoration time and the value of average restoration time is constant to 24h in this paper.

So we can get Markov state transition matrix:

$$\boldsymbol{P} = \begin{bmatrix} 0.999998 & 0.000001835 & 0.000000024 \\ 0.041667 & 0.958333 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Initial state matrix **S**=[1 0 0], every state probability can be determined in each hour after computation:

$$S\_n = S\_\{n-1\} \times P = S\_0 \times P\_n. \quad (5)$$

Final results are listed in Table 4 after 10 functional test cycles(87600hours)

Table 4 State probability after Ten Functional Test Cycles

Time[h]	State 0	State 1	State 2
1	0.999998	1.835000e-06	2.400000e-08
2	0.999996	3.593537e-06	4.799995e-08
3	0.999994	5.278798e-06	7.199986e-08
4	0.999992	6.893836e-06	9.599972e-08
……			
87597	0.985607	4.340598e-05	0.002087
87598	0.985607	4.340597e-05	0.002087
87599	0.985607	4.340597e-05	0.002087
87600	0.985607	4.340596e-05	0.002087

Values of the last state are continuously increasing as time goes by. Average all values of the last state and PFDavg is 0.00104. Safety integrity level is SIL2 when we make the easy contrast $10^{-3}<0.00104<10^{-2}$ according to the table of safety integrity levels in low demand mode of operation. Safety failure fraction should meet the requirement 99% > *SFF* > 90% if safety transmitter obtains safety integrity level SIL2, its hardware fault margin is 0. SFF of safety transmitter is 98.7%, conclusions can be made that the whole design of safety transmitter confirms to safety integrity requirements.

Conclusion

1oo1D structure is used in the safety temperature transmitter. Considering the structural characteristics of two MCUs, contrast methods are applied and diagnostic methods are proposed. Self-diagnostic measures are used in analog data acquisition module, data processing module and analog signal output module to obtain a certain amount of risk reduction. Setting deviation value has

been accomplished in order to make sure diagnoses are available. Test results show that diagnoses are capable of controlling the system failure and random failure effectively. FMEDA is accomplished to analyze every failure mode and corresponding impact on the transmitter in the process of establishing Markov model. Final analysis results are Reliable and accurate.

Acknowledgment

This work is supported by the National High Technology Development Plan (863): Research and Development of Safety Instrumented Technology under contract 2012AA041103 and Natural Science Foundation of China under contract 61004068. I'd like to express my sincere thanks to all those who give me pertinent suggestions to finish this paper.

References

[1] Fang Laihua,Wu Zongzhi: Development and requirements of safety instrumented system. China Safety Science Journal, 2009,Vol. 19(4).(in chinese)

[2] Yang Xianhui,Guo Haitao: *Functional safety of safety instrumented system*. BeiJing：Tsinghua university press, 2007, p. 36-59. (in chinese)

[3] IEC61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General requirements, 2010.

[4] IEC61508:Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 2: Requirements for electrical/electronic/programmable electronic safety related Systems, 2010, pp. 47-88.

[5] IEC61508: Functional safety of electrical/electronic/programmable electronic safety-Related systems, Part 3: Software requirements, 2010, p.13-45.

[6] Ryotaro Shishiba: Implementation of a safety instrumented system. SICE Annual Conference , 2007, p. 17-20.

[7] William M.Goble, Harry Cheddie: Safety instrumented systems verification:practical probabilistic calculations. ISA, 2005, p. 28-343.

[8] J.L.Rouvroye.Comparing : *Safety analysis techniques.Reliability Engineering and System Safety,* 2002, Vol. 75, p. 289-294.

[9] J.Borksok: Estimation and evaluation of common cause failures. Proceedings of the Second International Conference , Apr. 2007.

[10] IEC61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, 2010, p. 76-80.

Materials Science and Technology II
10.4028/www.scientific.net/AMR.716

Design of Functional Safety Temperature Transmitter and Reliability Analysis
10.4028/www.scientific.net/AMR.716.521