Study and Design on Self-diagnostic Based Safety Pressure Transmitter

Yan Song[1], Jinli Li[2], Aidong Xu[1], Tianran Wang[1], Kai Wang[1], Zhijia Yang[1]
[1]Shenyang Institute of Automation, Chinese Academy of Sciences. Shenyang, 110016,China
[2]Liaoning Electric Power Central Hospital, Shenyang, 110015,China

***Abstract*—A functional safety pressure transmitter (SPPT) which was based on self-diagnostic is introduced. Challenge in safe communication is discussed, too. SPPT's hardware design, software design and diagnostic design is given. Furthermore, the safety communication design of SPPT is introduced, too. At last, a FIT test and FMEDA analysis of SPPT is introduced, and a markov model is established. According test, analysis and modelling, the SPPT can achieve SIL2 level.**

Keywords-functional safety; SIS; pressure transmitter; self-diagnostic.

I. INTRODUCTION

Functional safety[1][2] popular concept, there are safe PLC, safe communication, safe projects, and so on[3][4]. Under this background, safety Instrument Systems(SIS) are rapidly booming in the industrial field, meanwhile, more and more new safety related requirements are under considering. The most perspective one is safety communication in SIS. As is well known, data transfer is not always correct in real world, its quite different from mathematic model. Lots of data corruption event occurred during data exchange in plant field. The mainly sources of data destroy are effects of EMC events, random hardware failures and system failures, while the first and second one introduce transient effects meanwhile the third one may introduce both transient or long term effect. According to IEC 61508[5] most part of normal communication which not designed for safety application are named black channel, such as stack software in transmitter, media access control chip and firmware, communication chip and driver chip, physical media, network switch devices, and so forth. And, for some safety critical application, the communication's residual failure rate must be restricted under certain value. So, main manufacture of transmitter and PLC propose their own safety communication requirements and safety communication solution. Main fieldbuses have their own corresponding safety communication verson. PROFISafe[6][7] is proposed by Siemens, which as a safety patch of both PROFIBus and PROFINet.

PROFISafe has some interest feature, such as invisible sequence number, full crc check data protection and so on. Design of a safety pressure transmitter with profisafe features will be introduced, including firmware and hardware.

II. DESIGN OF SAFETY PRESSURE TRANSMITTER

A. Hardware structure design

The Safety PA pressure transmitter (SPPT) device is mainly including two parts: acquire board and communication board. Original pressure data is acquired from sensor by acquire board, meanwhile the pressure value is recalculated and packs into a PROFIsafe safety PDU by communication board. The whole structure of the SPPT is shown in figure 1.

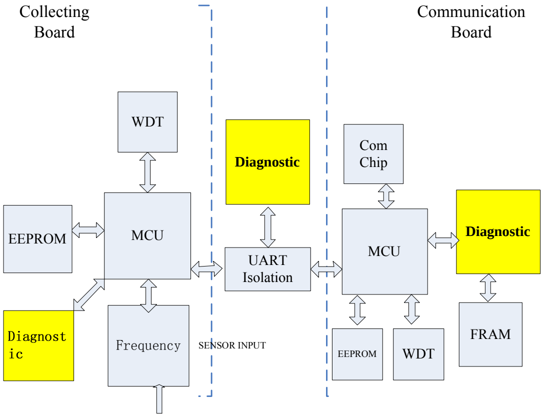

Figure 1. SPPT principle diagram

As figure 1 shown, two boards are connected by UART and power supply pin, original pressure data is transferred by UART link, meanwhile, the control commands generated in communication board are delivered through UART link.

Communication board is mainly composed by six parts, MCU controller chip, EEPROM chip, WDT chip, FRAM , communication chip and Diagnostics channel part. MCU controller executes the recalculation work and profibus stack, the MCU chip is ATMEL. The EEPROM chip is used to store static data, such as range, user configuration, etc., EEPROM can be serial or parallel, either one is ok. The WDT chip is mainly to monitor the footsteps of program, to determine if the program is work right or not. Communication chip is used to communicate on fieldbus network. The communication chip should following all requirements of Differential Manchester encoding which was physical layer coding standard of PROFIBus PA devices. The PROFISafe PDU will send by this chip to the network. The Diagnostic part is used to diagnose if FRAM work correct or not. According to IEC

61508, RAM must be test well which not locates in MCU chip.

Acquire board is composed by five parts, MCU is MSP430, which used to acquire the original pressure data and calculating the real pressure value. WDT is a special designed chip, and use to monitor the footstep of program, to make sure the program is correct at a given test time point. The EEPROM is used to store user data and calibration data, both serial and parallel are ok. The frequency part is mainly a RC oscillation circuit, and pressure sensor contains an capacitance which value changed following the pressure trend. If the RC oscillation circuit's frequency is defined, the pressure value should be unique and can be deduced. Diagnostic circuit is used to monitor if the main part of acquire board including RC oscillation circuit work correctly.

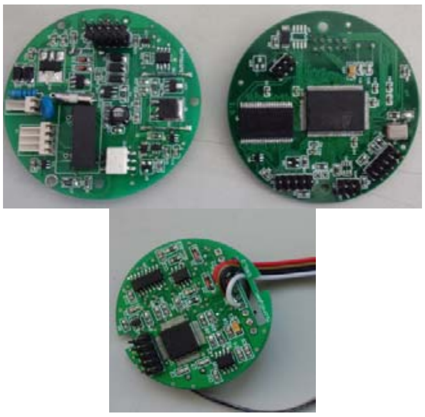

Figure 2. Port board, Communication board and acquire board

As figure 2 shown, we have developed the port board, communication board and acquire board, from left to right in figure3, they are port board, which mainly provides connector interface and power supply, communication board which provide the ability of access to fieldbus, acquire board which acquires original pressure data and sends to communication board.

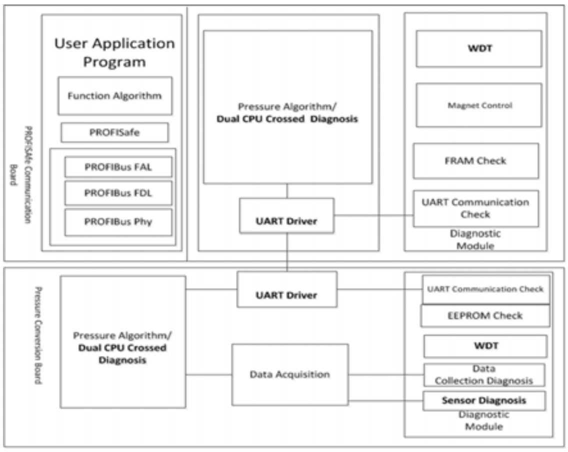

Figure 3. SPPT software structure

B. Firmware structure Design

The SPPT's firmware can be cataloged into two types, safety-related program and non-safety program. Safety-related program is including three parts: PROFISafe communication module, pressure acquire module, diagnostic module. For the communication stack, its belong to black channel, not safety-related. Because the huge cost of safety-related software development and certification, the manufacture hope there are not very much safety-related software code in a device. As mentioned above, SPPT's communication is complies with profisafe, so the profisafe layer its self must be safe one. Because the communication via balck channel between the control network peers should be secured by profisafe. And profisafe must make sure safety capabilities is enough.

The firmware architecture of whole SPPT is shown as following figure 3. Figure 3 shows us that there are two board mainly in logical, the port board have no program, so it should be ignored in this part. The two boards are communication board and conversion board. The first one is responsible for communication with the other PA devices or profisafe devices on network. And, its deal with the safety calculation of final pressure value, which is the core safety function of SPPT.

C. Diagnostic Function Design

According to figure 3, diagnostic functions are located in communication board as well as in conversion board. The diagnostic functions can be catalogued into followings:

i) Intelligent components, including CPU, RAM, FPGA, and so forth;

ii) Non-intelligent components, such as resistances, capacitors, amplifiers, etc.

The policy to deal with these two vary types of components are quite different. To the intelligent components, there are not well defined failure modes, we can only make use of indirect ways to diagnostic this type of components. For the non-intelligent components, there are usually well defined failure modes exist, so we can design special approach for most failure modes, only if its necessary. In SPPT device, we design the following diagnostic approach. They are RAM diagnostic, ROM diagnostic, CPU including resisters group and program counter diagnostic, by indirect way; The AD/DA channel, internal communication bus and external communication bus. For the purpose of making sure the final pressure value is right or safety output, the two channel comparison is used in SPPT. In most diagnostic functions, if failures are detected, a predefined safety handle program will be launched in a certain time restriction, and SPPT will turn into safe state and work no longer. The diagnostic function its self will not be check, because if we do it, may be the diagnostic for diagnostic function should be checked, too. Then it will be endless.

D. PROIFISafe Communication Design

SPPT has a special designed data structure which named F-Structure. F-Structure includes safe address, watching dog timer, SIL level, Communication version, F-Parameter, etc. Safe_address describes the local F-application's address, not Profibus PA or DP address. Watching dog timer describes the local WDT's trigger time limit. SIL level describes the safety integrity level of this device. Communication version describes the safety communication's version and profile. PROFISafe is a state machine based protocol layer, its including several important states which are the base of PROFISafe.

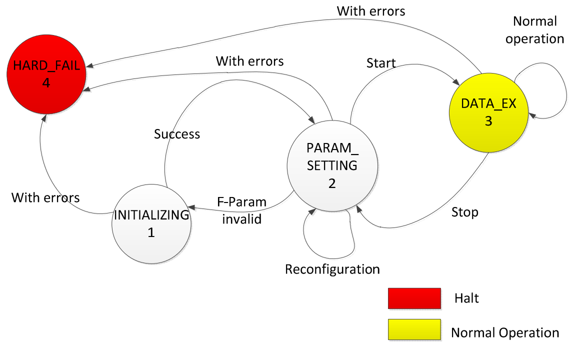

Figure 4. State machine of PROFISafe[8]

As figure 4 shown, there are four major state of PROFISafe sate machine. Hard_Fail means some thing wrong within profisate program, such as wrong CRC, wrong SN, or wrong visual sn, etc. Once the program is in Hard_Fail, which means there are something wrong in communication, and the SPPT should be halt or shutdown until the failure is figured out and removed. Init state is the very first sate after power on. In Init state, the F-Structure including F-Parameter[2] and local sate communication variables are initialized. In this step the safe communication layer is ready for receiving the configuration data. In state 2, an important phase parameterization is carried out, and if it is successful, which means the configuration software gives right value to SPPT, the state machine can make a progress to next step by invoking the Start() primitive. After that, the state machine turns into Data_EX state, normal safety data exchange is carried out periodically in this state. If any error occurs during this three phase, the state machine turn into HARD_FAIL state immediately.

III. Test and Analysis

A. Interpolation function

The SPPT need careful test and analysis to prove it is safe enough. The most important thing is fault insertion test (FIT), the significant FIT is to hardware, but software need FIT, too. Main purpose of FIT is to prove if the device is robust enough and have enough diagnose to intelligent component or non-intelligent component. For example, if a resister is important to the system, then all the possible failure mode of this resister should be simulated, such as open circuit, short circuit, drift, etc. The following figure shows the FIT hardware platform.

SPPT's FIT specification mainly including 20 items, there several test case in every items, its cover most failure mode of all important non-intelligent components. And for intelligent components, cause the failure modes not well defined, so this type components should be test indirectly. For SPPT firmware test, the program flow, WDT are tested. All FITs are carried out correctly and successfully. FIT test can tell which component is important meanwhile others not.

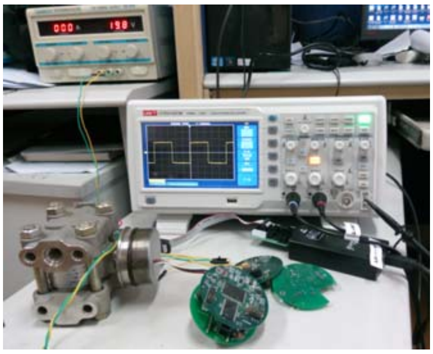

Figure 5. SPPT FIT platform

Analysis of SPPT is crucial to classify the SIL class, the famous failure mode and effect analysis (FMEA) and failure mode and effect diagnose analysis (FMEDA) are used widely. In our project, FMEDA is major analysis approach. There are three type of failure: safe failure, dangerous failure, no effect. Safe failure can be cataloged into safe failure detected and safe failure undetected. Dangerous failure can be cataloged into detected and undetected, too. Because SPPT has well defined diagnostic approaches, so most failures can be detected, and there are always some failures hard be found, to the safe failure, its not important being detected or not, but to the dangerous failure, if it was detected, it possibly turn into safe failure, so the true critical is dangerous failures not detected.

According to FIT test and FMEDA analysis, the safe failure fraction SFF of SPPT can be calculated.

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} \tag{1}$$

λ_S is safe failure rate and λ_{Dd} is detected dangerous failure rate which can be turn into safe failure by technologies. λ_{Du} is undetected dangerous failure rate, which will cause dangerous things happen, such as explosion, leak of poison materials, etc. SFF is an important factor of a safety device. According to FIT test and FMEDA, SPPT's failure rates are shown as following.

TABLE I. FAILURE RATE OF SPPT

Failure rate\value	Value (FITS, 1FIT = 10E-9)	How to Get
$\sum\lambda_S$	5400.51	FIT, FMEDA
$\sum\lambda_{Dd}$	120.26	FIT, FMEDA
$\sum\lambda_{Du}$	118.25	FIT, FMEDA

According to table 3 and formula (1), the SFF value can be calculated easily: $SFF = 97.90\%$ Other important of SPPT's safety indexes are probability failure on demand (PFD), and mean time between failure (MTTF). Both of them can be calculated by MARKOV model[9]. Cause the SPPT is 1oo1D structure, the corresponding MARKOV model's state transfer diagram is shown as following.

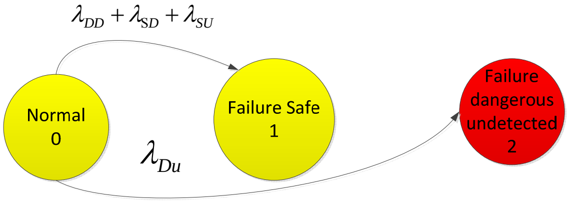

Figure 6. SPPT FIT platform

The MARKOV model is shown in figure 6, and the state 0 means normal state, has no failure occurs. State 1 means detected safe failure or un detected safe failure or detected dangerous failure occurred in SPPT. In state 1, the SPPT should halt until the failure is removed successfully, in SPPT any failure occurs should launch a halt event for safe reason. In state 2, which means dangerous failure undetected lead a system failure dangerous, may lead dangerous accident occurs. According the MARKOV model, a MARKOV transfer matrix can be got easily, shown as following.

$$P = \begin{bmatrix} 1-\lambda_{DD}+\lambda_{SD}+\lambda_{SU}, & \lambda_{DD}+\lambda_{SD}+\lambda_{SU}, & \lambda_{DU} \\ 0 \quad , & 1 \quad , & 0 \\ 0 \quad , & 0 \quad , & 1 \end{bmatrix} \qquad (2)$$

As a typical value, the test interval is set to 8760 hours which are a year. In the first hour, the SPPT's transfer matrix is P, and in second hour, the probability transfer matrix is P*P,

$$P_2 = P * P$$
$$P_3 = P * P * P$$

For an hour, the probability transfer matrix is

$$P_n = P^n$$

So in one year later, the probability transfer matrix is P^{8760}。 According to SPPT's MARKOV model and the safety index calculation theory described in [5][9], the MTTF value's analytical solution is as following.

$$MTTF = \frac{1}{\lambda_S + \lambda_D} \qquad (3)$$

And the PFD is appreciatively as following.

$$PFD_{SPPT} = \lambda_{DU} \times TI \qquad (4)$$

According table 3 and (2),(3),(4), we got the MTTF and PFD value of SPPT:

$$\begin{cases} MTTF = 180472 \\ PFD = 0.0010359 \end{cases}$$

According to IEC 61508, the SPPT can achieve SIL2 level.

IV. CONCLUSIONS

A safety pressure transmitter is designed in this paper, the hardware structure is proposed in detail, as well as software structure. Safe communication is study and safe communication function is designed, too. FIT, FMEDA of SPPT are introduced and a MARKOV model of SPPT is established, too. According to the FIT test, FMEDA analysis, serials of failure rates of SPPT are given. Finally, according to failure rates and MARKOV model, the MTTF and PFD are calculated. The results shows the SPPT is fulfill the requirements of SIL2, which defined in IEC 61508.

ACKNOWLEDGEMENTS

This work is supported by the National High Technology Development Plan (863): Large-scale PLC key technologies research and products' development & application under contract 2013AA040301.

REFERENCES

[1] Stirgwolt, P. Effective management of functional safety for ISO 26262 standard, *Reliability and Maintainability Symposium (RAMS)*, 2013 Proceedings – Annual.

[2] Suwoong Lee, Safety-Function Design for the Control System of a Human-Cooperative Robot Based on Functional Safety of Hardware and Software, *Mechatronics, IEEE/ASME Transactions on* Volume:19 , Issue: 2, 2014.

[3] Walkington, J., One approach to functional safety assurance and safety lifecycle compliance, *System Safety Conference incorporating the Cyber Security Conference 2013*,8th IET.

[4] Iden, J., Functional safety aspects of pattern detection algorithms, *Automation Science and Engineering (CASE), 2012 IEEE International Conference on*, 2012.

[5] IEC, IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems, ver 2, *IEC*, 2010.

[6] IEC Technical Committee SC 65C, IEC61784 Digital data communications for measurement and control –Part 3: Profiles for functional safety communications in industrial networks, *IEC*, 2005.

[7] IEC, PROFIsafe-Profile for safety technology on PROFINET IO, *IEC*, 2008.

[8] Simatic, PROFIsafe driver V2.1 for F-Slaves, ver 1, 2009.

[9] Y. Bai, L. Dong and W. M. Goble, Control systems safety and reliability: techniques and applications, China Electric Power Press, Beijing, 2008.