2011 International Conference on Computer and Automation Engineering (ICCAE 2011)
IPCSIT vol. 44 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V44.11

Reliability Analysis and Safety Evaluation of an Analog Output Module Based on FMEA and FTA

Yi Zhang [1+] and Yan Bai [2]

School of Control and Computer Engineering, North China Electric Power University, Beijing, China

Abstract. Based on FMEA (Failure Mode and Effects Analysis) and FTA (Fault Tree Analysis), the reliability of an analog output module is analyzed and its safety integrity level is evaluated in this paper. Firstly, two of the reliability analysis methods, FMEA and FTA, are introduced. Secondly, the two methods are employed to analyze an analog output module. The failure modes and failure data of the electronic components in the module are presented by FMEA. Then, based on the schematic diagram of the module and the information given by FMEA, the fault tree of the module is built and its PFD (Probability of Failure on Demand) is calculated, by which the SIL (Safety Integrity Level) of the module can be determined. Finally, conclusions are given and future research directions are also pointed out.

Keywords: reliability, safety, SIL, FMEA,FTA

1. Introduction

Reliability and safety engineering is built on the basis of probability and statistical theory. There are a large number of quantitative analysis techniques, including Reliability Block Diagrams (RBD), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Markov Model. These methods are used to evaluate failure probability of the system with the combinatorial probability [1][2].

The key point of RBD, which provides a simple mathematics to quantify the reliability, is to convert the physical system into a reliability block diagram. However, it is only suitable for an overview of the reliability of a system and the result is somewhat conservative. FMEA, which provides the detailed information for the further reliability analysis and safety evaluation, is usually used to identify system failure modes, and it is primarily performed on electrical components [3-5]. FTA can be employed for qualitative analysis to search all the failure modes those result in the system failures. It is also frequently used for quantitatively analysis to measure the reliability of a system according to the probability of the bottom events [6-9]. The main advantage of Markov Model is flexibility since a variety of features can be included in one model. However, Markov Model is very difficult to build and is easily susceptible to model errors. In addition, it is also quite a time-consuming task [10][11]. Generally, FTA produces similar results as Markov Model, but it is much easier to model large and complex systems using FTA than Markov Model [12]. Thus, FEMA and FTA are two commonly used methods in reliability and safety engineering. Reference [7], [13] and [14] presented the procedure of reliability analysis on a transmitter, an actuator and a special protection system using the methods of FMEA and FTA. In this paper, these two methods are employed to analyze the reliability of an analog output module and evaluate its safety integrity level. The module is decomposed into sub-modules to simplify the modeling procedure. In order to make the analysis more comprehensive, some other practical factors such as self-diagnostic capability, repair time, common cause failure are considered.

The analysis of the reliability and safety of an analog output module is presented in this paper and it is arranged as follows. In section 2 the general reliability analysis procedure and the analysis methods used in this paper are introduced. The specific reliability analysis and safety evaluation of an analog module is described in details in section 3. Finally, conclusion is given in section 4.

[+] Email: [1] evazyi@sina.com.cn, [2] by@ncepu.edu.cn

2. Reliability Analysis Methods

The key point of reliability analysis and safety evaluation is that, no matter what kind of reliability model is used, the reliability modeling procedure has to follow systematic approach steps:

- Identify the involved components. Find out which components should be considered in the reliability model and which should be excluded.
- Obtain the components' failure data and failure modes. Establish a checklist including all components and their failure modes.
- Completely make clear how the system works and how each failure mode affects the whole system. These works can be done through Failure Modes and Effects Analysis (FMEA).
- Build the reliability model. Ensure that all components and their associated failure modes have been included in the model.

As the most frequently used reliability analysis methods, FMEA and FTA are employed in this paper to analyze an analog output module.

2.1. Failure Mode and Effects Analysis(FEMA)

FMEA is a systematic bottom-up inductive method of analyzing reliability and safety problems in a system or process in order to avoid hazards or consequences. It essentially consists of identifying and listing all potential failure modes, accessing effects on the overall system for each failure mode, and then identifying all potential causes which may lead to each system failure mode.

Failure modes can be divided into safe failures, as well as dangerous failures. When considering self-diagnostic function, the failure modes can also be divided into detected and undetected failures. In addition, the common cause failures should be considered for systems with redundant architecture.

2.2. Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is mainly used to discover design problems in the system. It is a structured top-down deductive analysis technique, which involves two steps: deriving the fault tree and analyzing the fault tree. It can systematically identify and evaluate all possible events that could lead to a given hazard. The basic principle of deriving a fault tree is that setting the most unwanted failure as the goal and starting point of the failure analysis. Firstly, find out the direct reasons of this initial failure as the first layer of causing events. Then, setting each causing event of this layer as a starting point to identify the factors that led directly to this reason, and these factors are the second layer of causing events .The procedure is finished until the original factors are found, of which the failure mechanism or the probability distribution are known.

3. Reliability Analysis and Safety Assessment of an Analog Output Module

The analog output module (which is called AO module in the following for short) to be analyzed has 4 analog output channels which are isolated from each other and from the SCM(Single Chip Microcomputer).The AO module has two CAN-bus transceivers for redundancy. Data are delivered through CAN-bus transceiver into the SCM. Then, they are sent through the optical isolators to the D/A converter. Finally, the data are output as current or voltage signals selected by jumpers. The schematic diagram of the AO module is shown in Fig. 1.

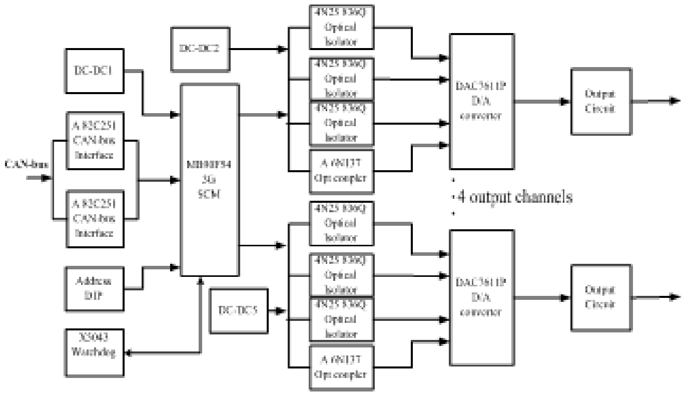

Fig. 1: Schematic diagram of the AO module

3.1. FMEA of the AO Module

With FMEA, every single electronic component in the AO module is listed to identify all the potential failure modes which result in the failure of the module. The results of FMEA provide important information for FTA and ensure no component and failure mode is missed in FTA. Failure modes and related failure data of electronic components can be obtained from many industrial reliability databases. But in these databases, the failure modes and data are only sketchily recorded. According to safety verify calculation and conservative estimate, the dangerous failure ratio is generally around 50% and diagnostic coverage of the processor-based equipment can be conservatively estimated at 50%.

3.2. FTA of the AO Module

Fault Tree Analysis of the analog output module is based on the schematic diagram of the module and the results of FMEA. Since the module consists of numerous electronic components, the module is decomposed. As a result, three fault trees are built to reduce the size of the fault tree of the AO module.

First of all, according to the schematic diagram, the AO module is decomposed to the CAN-bus interface block, the output channel block and the other components including SCM, DC-DC convert and so on. Then, the fault tree of an output channel block is built as shown in Fig.2.

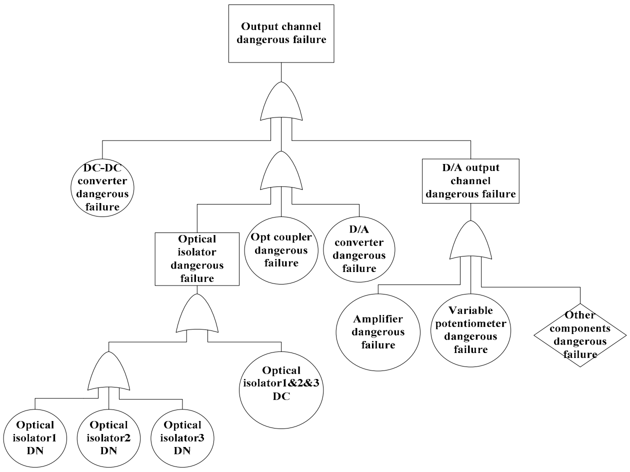
Output channel dangerous failure
DC-DC converter dangerous failure
D/A output channel dangerous failure
Optical isolator dangerous failure
Opt coupler dangerous failure
D/A converter dangerous failure
Amplifier dangerous failure
Variable potentiometer dangerous failure
Other components dangerous failure
Optical isolator1&2&3 DC
Optical isolator1 DN
Optical isolator2 DN
Optical isolator3 DN

Fig. 2: Fault Tree of an output channel block

As shown in the schematic diagram, each channel has three identical optical isolators, so the common cause failures are considered in this fault tree. The PFD of the output channel (PFD_{OC}) can be calculated by (1).

$$PFD_{oc}=(5\times\lambda_{DC-DC}^{D}+\lambda_{OI1\cup OI2\cup OI3}^{DN}+\lambda_{OI}^{DC}+\lambda_{OC}^{D}+\lambda_{D/A}^{D}+\lambda_{A}^{D}+\lambda_{R}^{D}+\lambda_{Other}^{D})\times TI \quad =\{5\times\lambda_{DC-DC}^{D}+3\times(1-\beta_{OI})\times\lambda_{OI}^{D}-C_{3}^{2}[(1-\beta_{OI})\times\lambda_{OI}^{D}]+[(1-\beta_{OI})\times\lambda_{OI}^{D}]^{3} +\beta_{OI}\times\lambda_{OI}^{D}+\lambda_{OC}^{D}+\lambda_{D/A}^{D}+\lambda_{A}^{D}+\lambda_{RW}^{D}+\lambda_{Other}^{D}\}\times TI \qquad (1)$$

In the equation, $\lambda_{DC-DC}^{D}, \lambda_{OI}^{D}, \lambda_{OC}^{D}$, $\lambda_{D/A}^{D}, \lambda_{A}^{D}, \lambda_{R}^{D}, \lambda_{Other}^{D}$ represent the dangerous failure rates of DC-DC converter, optical isolator, opt coupler, D/A converter, isolation amplifier, variable potentiometer and other components, respectively. λ_{OI}^{DC} is the common failure rate of the optical isolator and $\lambda_{OI1\cup OI2\cup OI3}^{DN}$ means the non-common failure rate of optical isolator1 or optical isolator2 or optical isolator3. β_{OI} is the common failure factor of the optical isolator.

Fig.3 is the fault tree of the CAN-bus interface block. Because the AO module has two CAN-bus transceivers for redundancy, in this fault tree, common cause failure is considered.

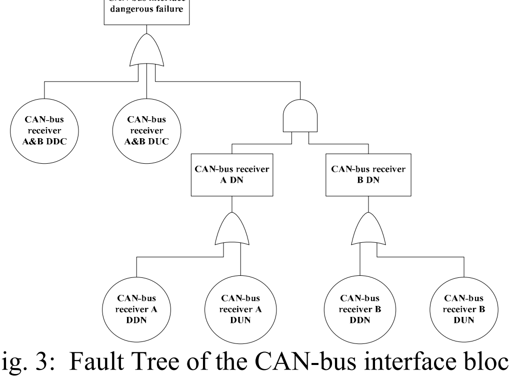

Fig. 3: Fault Tree of the CAN-bus interface block

The PFD of the CAN-bus interface block ($\mathrm{PFD_{CI}}$) can be calculated by (2).

$$PFD_{CI} = \lambda_{CTA\&B}^{DDC} \times RT + \lambda_{CTA\&B}^{DUC} \times TI + (\lambda_{CTA}^{DDN} \times RT + \lambda_{CTA}^{DUN} \times TI) \times (\lambda_{CTB}^{DDN} \times RT + \lambda_{CTB}^{DUN} \times TI) = \beta_{CT} \times C_{CT} \times \lambda_{CT}^{D} \times RT + \beta_{CT} \times (1 - C_{CT}) \times \lambda_{CT}^{D} \times TI + (1 - \beta_{CT})^2 \times [C_{CT} \times \lambda_{CT}^{D} \times RT + (1 - C_{CT}) \times \lambda_{CT}^{D} \times TI)]^2 \tag{2}$$

In the equation, $\lambda_{CTA\&B}^{DDC}$, $\lambda_{CTA\&B}^{DUC}$ are denoted by the detected and undetected common dangerous failure rates of CAN-bus transceiver A and B, respectively. λ_{CTA}^{DDN} , λ_{CTB}^{DDN} , λ_{CTA}^{DUN} , λ_{CTB}^{DUN} represent the detected and undetected non-common dangerous failure rates of CAN-bus transceiver A and B, respectively. λ_{CT}^{D}, β_{CT} and C_{CT} are dangerous failure rate, common failure factor and self-diagnostic coverage of the CAN-bus transceiver, respectively. RT is the repair time.

Finally, the fault tree of the AO module can be built as shown in Fig.4, in which the output channels block dangerous failure and the CAN-bus interface block dangerous failure are basic events since their PFD can be calculated by (1) and (2).

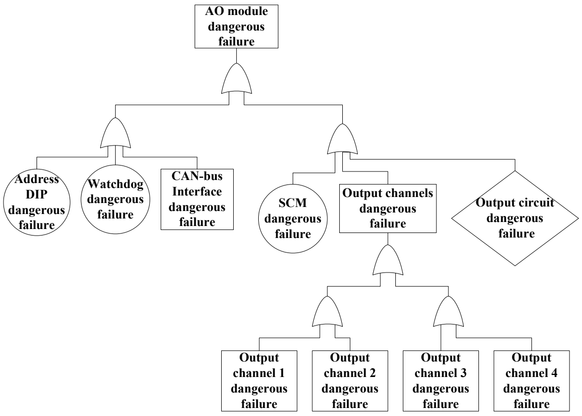
AO module dangerous failure
Address DIP dangerous failure
Watchdog dangerous failure
CAN-bus Interface dangerous failure
SCM dangerous failure
Output channels dangerous failure
Output circuit dangerous failure
Output channel 1 dangerous failure
Output channel 2 dangerous failure
Output channel 3 dangerous failure
Output channel 4 dangerous failure

Fig. 4: Fault Tree of the AO module

Because the channels of the AO module are isolated from each other and from the SCM as well, the basic events in this fault tree can be seen as mutually exclusive events. According to probability and statistics theory, the PFD of the AO module ($\mathrm{PFD_{AO}}$) can be calculated by (3).

$$PFD_{AO} = (\lambda_{DIP}^{D} + \lambda_{WD}^{D} + \lambda_{SCM}^{D} + \lambda_{O}^{D}) \times TI + PFD_{CI} + 4 \times PFD_{OC} \tag{3}$$

In the equation, λ_{DIP}^{D} , λ_{WD}^{D} , λ_{SCM}^{D} , λ_{O}^{D} represent failure rate of the address DIP, watchdog, BCM and the output circuit, respectively.

According to the four safety integrity levels defined in IEC61508, as shown in Table 1[1], the safety integrity level of the AO module can be determined since its PFD is calculated.

Table 1: Four SILs in IEC61508

Safety Integrity Level (SIL)	**Probability of Failure on Demand (PFD)**	**Risk Reduction Factor (RRF)**
4	<0.0001	>10,000
3	0.001~0.0001	1,000~10,000
2	0.01~0.001	100~1,000
1	0.1~0.01	10~100

4. Conclusion

This paper presents the reliability analysis and safety evaluation of an analog output module with the combination of two methods: Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). Based on the results of FMEA and the analysis on the fault trees of the module, both the PFD and SIL of the

AO module are calculated.

However, this paper only focused on the analysis of the AO module using FMEA and FTA, and it merely analyzed the dangerous failure of the module. In fact, analog output module is only a small part of a complex control system, and there are far more types of failure modes in a system. Thus, the future work will put emphasis on the reliability analysis and safety evaluation of a more complex system with the combination of FEMA, FTA and Markov Model. Furthermore, taking more reliability indices into account is also one of the further research directions.

5. References

[1] Edward M. Marszal, Eric W. Scharpf, “Safety Integrity Level Selection,” The Instrumentation, Systems,and Automation Society, 2002, pp. 2-10.

[2] William M. Goble, Harry Cheddie, “Safety Instrumented Systems Verification: Practical Probabilistic Calculations,” The Instrumentation, Systems,and Automation Society, 2005, pp.61-78, pp. 83-86.

[3] Karsten Pickard, Peter Muller, Bernd Bertsche, “Multiple Failure Mode and Effect Analysis-An Approach to Risk Assessment of Multiple Failure with FMEA,” Proc. IEEE Symp. Reliability and Maintainability Symposium(RAMS 05), IEEE Press, Jan. 2005, pp.457-462, doi:10.1109/RAMS.2005.1408405.

[4] Akio Cofuku, Seiji Koide, Norikazu Shimada, “Fault Tress Analysis and Failure Mode Effects Analysis Based on Multi-level Flow Modeling and Causality Estimation,” Proc. IEEE Symp. International Joint Conference(SICE-ICASE 06), IEEE Press, Oct. 2006, pp.497-500, doi:10.1109/SICE.2006.315478.

[5] Rajiv Kumar Sharma, Pooja Sharma, “System failure behavior and maintenance decision making using, RAC,FEMA and FM,” Quality in Maintenance Engineering, vol. 16, 2010, pp. 64-85, doi:10.1108/13552511011030336.

[6] Song Hua, Zhang Hongyue, Wang Xingren, “Fuzzy Fault Tree Analysis Based on T-S Model,” Control and Decision, vol . 20, Aug. 2005, pp. 854-859, doi:cnki:ISSN:1001-0920.0.2005-08-002(In Chinese).

[7] Xu Yujuan, Yang Xianhui, “Application of Fault Tree Analysis Technique for Calculation of Transmitter's Failure Probability,” Automation in Petro-Chemical Industry , vol. 3, March. 2007, pp. 1-5, doi:.cnki:ISSN:1007-7324.0.2007-03-000(In Chinese).

[8] S.P. Sharma, N. Sukavanam, Naveen Kumar and Ajay Kumar, “Reliability analysis of complex robotic system using Petri nets and fuzzy lambda-tau methodology,” Engineering Computations, vol. 27, 2010, pp. 354-362, doi:10.1108/02644401011029925.

[9] Milena Krasich, “Use of Fault Tree Analysis for Evaluation of System-Reliability Improvements in Design Phase,” Proc. IEEE Symp. Reliability and Maintainability Symposium(RAMS 00), IEEE Press, Jan. 2000, pp. 1-7, doi:10.1109/RAMS.2000.816275.

[10] Abbas Karimi, Faraneh Zarafshan, Adznan b. Jantan, Abdul Raham b. Ramli, M. Iabal b. Saripan, “Accurate and Efficient Reliability Markov Model Analysis of Predictive Hybrid M-out-N Systems,” Proc. IEEE Symp. Computer Science and Information Technology (ICCSIT 10), IEEE Press, July. 2010, pp. 130-134, doi:10.1109/ICCSIT.2010.5564803.

[11] Peng Xiangyu, Jiang Letian, Xu Guozhi, “Reliability Modeling Method Based on State Truncation and Error Bound Analysis,” Proc. IEEE Symp. Communications, Circuits and Systems Proceedings (ICCCAS 05), IEEE Press, July. 2006, pp. 2791-2795, doi: 10.1109/ICCCAS.2006.285247.

[12] Tsun-Yu Hsiao, Chan-Nan Lu, “Reliability Evaluation of a Taipower System,” Proc. IEEE Symp. Power Systems Conference and Exposition (PSCE 04), IEEE Press, Oct. 2004, pp. 157-162, doi: 10.1109/PSCE.2004.1397510.

[13] Tao Jianfeng, Wang Shaoping, Yao Yiping, Li Peiqiong, “Relaiblity analysis on combination of FMECA and FTA for Redundant Actuator System,” Proc. IEEE Symp. Digital Avionics Systems Conference (DASC 99), IEEE Press, Nov. 1999, pp. 3.B.2-1-3.B.2-7,doi: 10.1109/DASC.1999.863708.

[14] Tsun-Yu Hsiao, Chan-Nan Lu, “Special Protection System Reliability Assessment,” Proc. IEEE Symp. Industrial & Commercial Power Systems Technical Conference(ICPS 07), IEEE Press, May. 2007, pp. 1-7, doi:10.1109/ICPS.2007.4292105.