Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems.

Dr. William M. Goble
exida.com, 42 Short Rd., Perkasie, PA 18944
Eindhoven University of Technology, Eindhoven, the Netherlands
wgoble@exida.com, www.exida.com, +215-896-7170

Prof. Dr. Ir. A. C. Brombacher
Faculty of Mechanical Engineering
Eindhoven University of Technology, Eindhoven, the Netherlands

Abstract

One of the key issues in the quantitative evaluation of programmable electronic systems is the diagnostic capability of the equipment. This is measured by a parameter called the Coverage Factor, C. This factor can vary widely. The range of possible values is often the subject of great debate. Within limits, the diagnostic coverage factor can be calculated by knowing which component failure modes are detected by diagnostics. An extension of the Failure Modes and Effects Analysis (FMEA) can be used to show this information. This extension, called a Failure Modes, Effects and Diagnostic Analysis can serve as a useful design verification tool as well as a means to provide more precise input to reliability and safety modeling.

Introduction

Automatic protection systems are one of the layers being used in many industrial processes to reduce risk. A Programmable Electronic System (PES) offers several advantages for these safety protection applications including graphical application design tools which reduce systematic errors, calculation capability, fast response time, and digital communications capability. A PES is also capable of extensive on-line diagnostics to detect component failures.

These advantages are significant. However, the major disadvantage of PES equipment when compared to specially designed relays is the potential for dangerous failures. Special circuit designs and special architectures are needed to insure safety. Machines built with these special circuits and architectures are called “Safety PLCs.”

The on-line self-diagnostic capability of the system is a critical variable. Good diagnostics improve both safety and availability[1,2]. This has been recognized by fault

Source : Reliability Engineering & System Safety. 66(2):145-148, 1999 Nov.
ELSEVIER SCI LTD, THE BOULEVARD, LANGFORD LANE, KIDLINGTON, OXFORD OX5 1GB, OXON, ENGLAND. URL: http://www.elsevier.nl, ISSN : 0951-8320

tolerant system designers for some time.[3] Although some architectures are more sensitive to diagnostic capability than others[4], all PES architectures are improved when diagnostics are added. Since diagnostics are one of the major advantages of a safety PLC, the ability to measure and evaluate those diagnostics are important. This is done using an extended failure modes and effects analysis (FMEDA)[5,6,7] and fault injection testing[8,9,10]. The measure of diagnostic capability is called the "Coverage Factor." It is defined as the probability (a number from 0 to 1) that a failure will be detected given that a failure has occurred. The symbol for coverage factor is C.

In PES systems it is necessary to distinguish the coverage factor for safe failures from the coverage factor for dangerous failures. The superscript S is used for the safe coverage factor, C^S. The superscript D is used for the dangerous coverage factor, C^D.

Diagnostic Techniques

Detection of component failures is done by two different techniques classified as reference or comparison. Reference diagnostics can be done with a single circuit. The coverage factor of reference diagnostics will vary widely with results ranging from 0.0 to 0.999. Comparison diagnostics require two or more circuits. The coverage factor depends on implementation but results are generally good with most results ranging from 0.9 to 0.999.

Reference diagnostics take advantage of predetermined characteristics of a successfully operating PES. Measurements of voltages, currents, signal timing, signal sequence, and temperature can be utilized to accurately diagnose component failures. Advanced reference diagnostics include digital signatures and frequency domain analysis. Reference diagnostics are performed by a single PES unit. The notation C_1^D is used to designate the dangerous diagnostic coverage factor due to single unit reference diagnostics.

Comparison diagnostic techniques depend on comparing data between two or more PES units. The concept is simple. If a failure occurs in the circuitry, processor or memory of one PES, there will a difference between data tables in that unit when compared to another unit. Comparisons can be made of input scans, calculation results, output readback scans, and other critical data.
The comparison coverage factor will vary since there are tradeoffs between the amount of data compared and the coverage effectiveness. The notation C_2^D is used to designate dangerous coverage due to comparison diagnostics between two units.

Failure Modes and Effects Analysis

An FMEA is a bottom up technique that is very effective in identifying critical component failures in a PES. An FMEA can be described as a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostic techniques. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected) in the safety models.

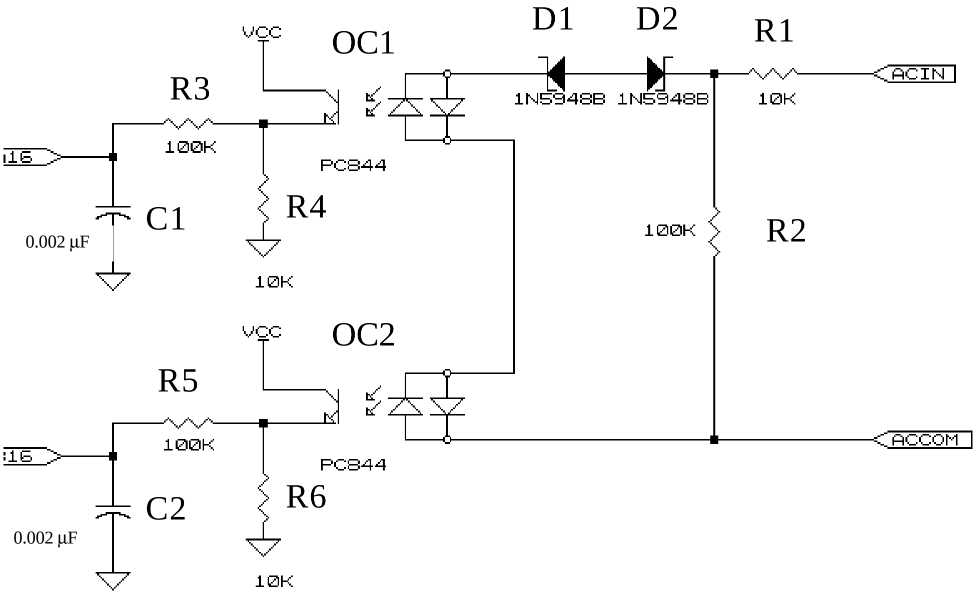

Figure 1 - High diagnostic PLC AC input circuit.

Figure 1 shows a PES input circuit specially designed to detect potentially dangerous failures using reference diagnostics and local comparison between two circuits. The FMEDA for this circuit is from Reference 5 and is shown in Table 1. The format for the FMEDA is an extension of the standard from MIL STD 1629A[11], Failure Modes and Effects Analysis. The first nine columns are identical.

Columns 10 through 16 are added to show diagnostic capability and resulting failure rate categories. The tenth column identifies that the component failure is detectable by on-line diagnostics. A number "1" is entered to indicate detectability. A number "0" is entered if the failure mode is not detectable. Column eleven is used to identify the diagnostic. Column twelve is used to numerically identify failure mode. A "1" is entered for safe failure modes. A "0" is entered for dangerous failure modes. The number is used in spreadsheets to calculate the various failure rate categories.

The safe detected failure rate is listed in column thirteen. This number can be calculated using the previously entered values if a spreadsheet is used for table. It is obtained by multiplying the failure rate (Column 8) by the failure mode number

(Column 12) and the detectability (Column 10). The safe undetected failure rate is shown in column fourteen. This number is calculated by multiplying the failure rate (Column 8) by the failure mode number (Column 12) and one minus the detectability (Column 10). Column 15 lists the dangerous detected failure rate. It is obtained by multiplying the failure rate (Column 8) by one minus the failure mode number (Column 12) and the detectability (Column 10). Column sixteen shows the calculated failure rate of dangerous undetected failures. It is obtained by multiplying the failure rate (Column 8) by one minus the failure mode number (Column 12) and one minus the detectability (Column 10).

TABLE 1 - FMEDA for High diagnostic PLC AC input circuit.

Failure Modes, Effects and Diagnostic Analysis

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Name	Code	Function	Mode	Cause	Effect	Criticality	λ	Remarks	Det.	Diagnostics	Mode	SD	SU	DD	DU
R1-10K	4555-10	Input threshold	short		Threshold shift	Safe	0.125		0		1	0	0.13	0	0
			open	solder open	open circuit	Safe	0.5		1	lose input pulse	1	0.5	0	0	0
			drift low			Safe	0.01	none until too low	0		1	0	0.01	0	0
			drift high			Safe	0.01	none until too high	1	lose input pulse	1	0.01	0	0	0
R2100K	4555-100	current limit	short		short input	Safe	0.125		1		1	0.13	0	0	0
			open	solder open		Safe	0.5		1	lose input pulse		0	0	0.5	0
			drift low			Safe	0.01	none until too low	0		1	0	0.01	0	0
			drift high			Safe	0.01	none until too high	1	lose input pulse	1	0.01	0	0	0
D1	4200-7	voltage drop	short	surge	overvoltage	Safe	2		1	lose input pulse	1	2	0	0	0
			open		open circuit	Safe	5		1	lose input pulse	1	5	0	0	0
D2	4200-7	voltage drop	short	surge	overvoltage	Safe	2		1	lose input pulse	1	2	0	0	0
			open		open circuit	Safe	5		1	lose input pulse	1	5	0	0	0
OC1	4805-25	isolate	led dim	wear	no light	Safe	28		1	Comp. mismatch	1	28	0	0	0
			tran. short	internal short	read logic 1	Dang.	10		1	Comp. mismatch	0	0	0	10	0
			tran. open		read logic 0	Safe	6		1	Comp. mismatch	1	6	0	0	0
OC2	4805-25	isolate	led dim	wear	no light	Safe	28		1	Comp. mismatch	1	28	0	0	0
			tran. short	internal short	read logic 1	Dang.	10		1	Comp. mismatch	0	0	0	10	0
			tran. open		read logic 0	Safe	6		1	Comp. mismatch	1	6	0	0	0
OC1/OC2			cross channel short		same signal	Dang.	0.01		0		0	0	0	0	0.01
R3-100K	4555-100	filter	short		lose filter	Safe	0.125		0		1	0	0.13	0	0
			open		input float high	Dang.	0.5		1	Comp. mismatch	0	0	0	0.5	0
R4-10K	4555-10	voltage divider	short		read logic 0	Safe	0.125		1	Comp. mismatch	1	0.13	0	0	0
			open		read logic 1	Dang.	0.5		1	Comp. mismatch	0	0	0	0.5	0
R5-100K	4555-100	filter	short		lose filter	Safe	0.125		0		1	0	0.13	0	0
			open		input float high	Dang.	0.5		1	Comp. mismatch	0	0	0	0.5	0
R6-10K	4555-10	voltage divider	short		read logic 0	Safe	0.125		1	Comp. mismatch	1	0.13	0	0	0
			open		read logic 1	Dang.	0.5		1	Comp. mismatch	0	0	0	0.5	0
C1	4350-32	filter	short		read logic 0	Safe	2		1	Comp. mismatch	1	2	0	0	0
			open		lose filter	Safe	0.5		0		1	0	0.5	0	0
C2	4350-32	filter	short		read logic 0	Safe	2		1	Comp. mismatch	1	2	0	0	0
			open		lose filter	Safe	0.5		0		1	0	0.5	0	0
							110.8					86.9	1.4	22.5	0.01

Total Failure Rate	110.8	Safe Coverage	0.9839
Total Safe Failure Rate	88.29	Dang. Coverage	0.9996
Total Dangerous Failure Rate	22.51		
Safe Detected Failure Rate	86.895		
Safe Undetected Failure Rate	1.395		
Dangerous Detected Failure Rate	22.5		
Dangerous Undetected Failure Rate	0.01		

Failures per Billion Hours

The safe coverage factor for the circuit is calculated by taking the total safe detected failure rate and dividing by the total safe failure rate.

$$C^{S} = \frac{\sum\limits_{all\ components} l^{SD}_{component\ i}}{\sum\limits_{all\ components} l^{SD}_{component\ i} + \sum\limits_{all\ components} l^{SU}_{component\ i}}$$

The dangerous coverage factor is calculated in similar way.

$$C^D = \frac{\sum_{allcomponents} l^{DD}_{componenti}}{\sum_{allcomponents} l^{DD}_{componenti} + \sum_{allcomponents} l^{DU}_{componenti}}$$

The analysis indicates that for this circuit, the safe diagnostic coverage factor is 0.96 and the dangerous coverage factor is 0.9996.

The FMEDA can also be used as a guide when selecting manual fault injection test cases. If 100% testing is not done, the tests should be done on components with the highest failure rate first. These contribute the most to the coverage factor.

Limitations of FMEDA

The FMEDA can be very effective but there are limitations. The method shows diagnostics only for known component failure modes. While an extensive body of knowledge exists in databases around the world, new electronic components present a risk in that all failure modes may not be known. This can be included in the FMEDA by adding an additional undetected component labeled “unknown” and assigning a failure rate.

As stated above, the technique requires that all failure modes of a component are known. This is all but impossible in complex VLSI integrated circuits like microprocessors. For these circuits an estimate can be made of various failure modes based on manufacturers life test data or failure mode handbooks. For complex devices with safety critical functionality, more extensive analysis is required. A new technique called Random Intelligent Failure Injection Technique[12] (RIFIT) can provide diagnostic coverage via computer simulation of the complex circuit. Internal faults can be simulated and diagnostics can be measured. The results of a RIFIT analysis can be incorporated into the FMEDA.

Conclusions

Regardless of architecture, the diagnostic ability of a PES is one of the critical parameters that affect the safety rating of the system. Specially designed safety PLCs have circuit designs optimized to achieve high diagnostic coverage. While perfect diagnostics are arguably not achievable, priority can be given to potentially dangerous failures. Within limits the coverage factor can be analyzed using an FMEDA. This analysis can be verified with fault injection testing for discrete circuit elements. The FMEDA is also useful to determine fault injection test priorities.

References

[1] Smith, S. E., "Fault Coverage in Plant Protection Systems," *ISA Transactions*, Vol. 30, Number 1, 1991.

[2] Goble, W. M., and Speader, W. J., "1oo1D - Diagnostics Make Programmable Safety Systems Safer", *Proceedings of the ISA92 Conference and Exhibit*, Toronto, ISA, 1992.

[3] Bouricius, W. G.; Carter, W. C.; and Schneider, P. R., "Reliability Modeling Techniques for Self-Repairing Systems," *Proceedings of ACM Annual Conference*, 1969; Reprinted *in Tutorial -- Fault-Tolerant Computing*, Nelson, V. P., and Carroll, B. N., eds., Washington, DC: IEEE Computer Society Press, 1987.

[4] Bukowski, J. V., and Lele, A., “The Case for Architecture-Specific Common Cause Failure Rates and How They Affect System Performance,” *1997 Proceedings of the Annual Reliability and Maintainabiltiy Symposium,* NY: New York, IEEE, 1997.

[5] Goble, W. M*., Evaluating Control Systems Reliability - Techniques and Applications,* NC: Raleigh, ISA 1992.

[6] Amer, H. H., and McCluskey, E. J., "Weighted Coverage in Fault Tolerant Systems*," 1987 Proceedings of the Annual Reliability and Maintainability Symposium*, NY: New York, IEEE, 1987.

[7] Luthra, P., "FMECA: An Integrated Approach," *1991 Proceedings of the Annual Reliability and Maintainability Symposium*, NY: New York, IEEE, 1991.

[8] Lasher, R. J., "Integrity Testing of Control Systems," *Control Engineering*, February 1990.

[9] Hummel, R. A., "Automatic Fault Injection for Digital Systems*," 1988 Proceedings of the Annual Reliability and Maintainability Symposium*, NY: New York, IEEE, 1988.

[10] Johnson, D. A., “Automatic Fault Insertion,” *INTECH*, NC: Raleigh, ISA, November 1994.

[11] *US MIL-STD-1629: Failure Mode and Effects Analysis*, National Technical Information Service, VA: Springfield, MIL1629

[12] Brombacher, A. C., Van der Wal, J., Rouvroye, J. L. and Spiker, R. Th. E., “RIFIT: a technique to analyse safety of Programmable Safety Systems,” *Proceedings of TECH97*, Raliegh, N. C., ISA, 1997.