Study on Design of Fault Injection System Based on Testability Verification

Li Zhiyu
Ordnance Engineering College
Shi Jiazhuang, China
bryantzhi@126.com

Huang Kaoli
Graduate School of Ordnance Technology
Shi Jiazhuang, China

Lian Guangyao
Graduate School of Ordnance Technology
Shi Jiazhuang, China

***Abstract*—Based on testability verification, the paper studies on designing of fault injection system and it is used on designing stage of some auto-driving instrument. The previous design only adapted the designer's request, and ignored testability verification, and it was a large problem to equipment. This paper designs a fault injection system to solve the problem before. The experiment shows that the system can inject faults fast and effectively, and gives quantization results.**

Keywords-testability; testability verification; fault injection; semi-physical simulator

I. INTRODUCTION

With the progress of science and technology, especially the wide application of computer technology and LSI, and they not only improve and enhance the system, weapon and equipment performance, at the same time, but also greatly increased the complexity of the system. This is bound to bring problems such as a long time to a test, fault diagnostic difficulties and using high security costs, which gradually attracted great attention. The researchers conducted a large number of system test and diagnose problems. The requirements are that the system must have self-test during design and development and provide a convenient design features for the diagnosis, this is called testability. As an emerging discipline, it has significant impact to maintenance, reliability and availability of modern weapons and complex systems especially electronic systems and equipment. With a good test, faults of systems and equipments can be quickly detected and isolated, it can also improves the reliability and security tasks, shorten fault detection and isolation time, thereby reducing maintenance time, improving system availability, and reducing system security costs .

Testability verification is an effective means to improve equipment design level. It can assist designers to accelerate the ripening process of the product in the design stage, and prejudge the possible failures and pitfalls in the design and improve or avoid them. The backdrop of a large number of high technology, high performance new weapons and equipment are continually equipping our troops, the validation of the test design is particularly important. That efficient testability analysis technology and test validation method, not only can greatly shorten the test equipment aging cycle, and can achieve the optimal allocation and protection of resources for equipment testing. Therefore, this study has great significance for new equipment "precision" protection, and rapid formation of the support capability.

Key technologies of fault injection of testability verification in this paper face to project needs of testability analysis and verification of the new equipment. A particular model autopilot of the Army weapons as the research object, the target is to increasing new equipment support capacity rapidly, and deeply analysis and study new equipment testability analysis and verification techniques. On this basis, build a technology-based fault injector to achieve testability analysis of the typical combinations equipment.

II. FAULT INJECTION

A. *The concept of fault propagation*

Fault propagation process: when the system is not correct changed caused by a fault (Fault), it is said occurrence error (Error). A failure is confined in the affected code local, but this is a point which can cause a lot of errors and spread throughout the system. When the fault-tolerant systems identify the error, it will trigger some action to deal with failure and error. Recovery）； if these actions are successful, the occurrence recovery (Recovery); otherwise, the system error called failure （Failure）. Figure 1 describes the fault propagation process.

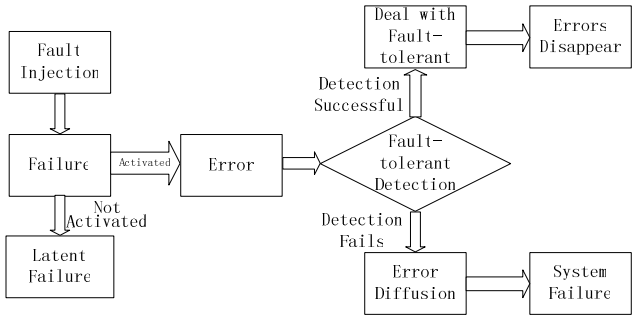

Figure 1. The fault propagation process

B. *Fault injection concept*

Fault injection is in accordance with the selected fault model, which is using artificial means consciously, and imposed on the target system running a specific workload, in order to speed up the system errors and failures occur. Observing and recovering response information, and anglicizing them, to provide testing process about the results. The fault injection technique is an important evaluation means to monitoring and anglicizing system performance. The

evaluation results available on the target system will give reliability and fault-tolerant features, which is shown in Figure 2 by the reaction of the injected fault system.

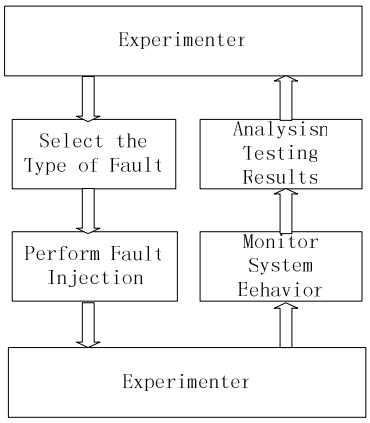

Figure 2. Fault Injection schematic

III. SEMI-PHYSICAL SIMULATION TESTING TECHNOLOGY

Practical embodiment of the weapons and equipment design for testability is including several aspects, such as the design of the test points, BIT design and test and diagnostic process design. Test design level validation is generally only after the completion of the design and manufacture, so that it is difficult to discover test questions and to improve the design process. The paper designs a universal semi-physical simulation test environment. Through a combination of hardware and software simulation, it can simulate equipment design level, and using the universal automatic test system to test the model of semi-real weapons and equipment, in order to achieve its level of design for testability validation. The semi-physical simulation test environment is equipped with semi-physical test simulator, test modeling, fault injection software, and the composition of the universal automatic test and diagnostic system. The working principle is shown in Figure 3.

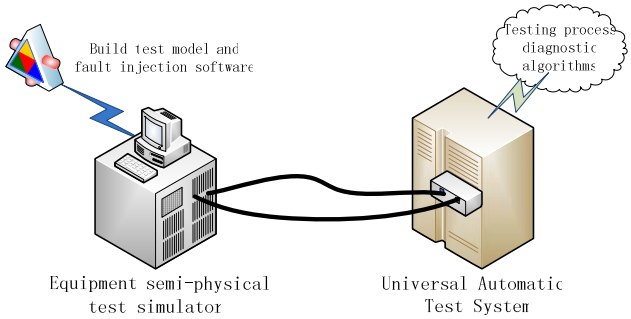

Figure 3. Semi-kind test simulation environment of block diagram

Its workflow is shown in Figure 4.

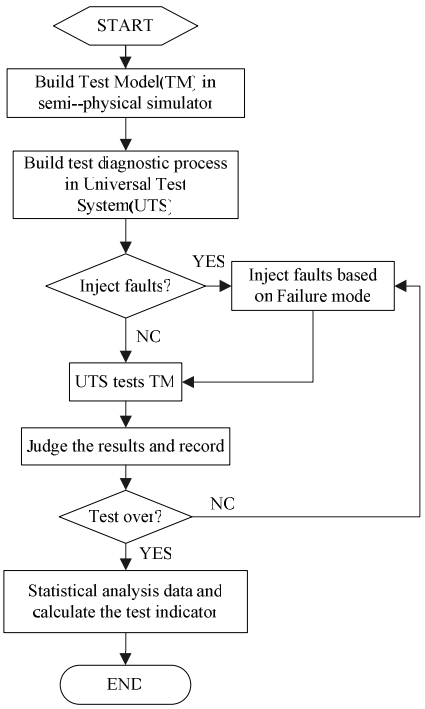

Figure 4. Semi-physical testability validation flow chart

IV. TEST AND ANALYSIS TECHNIQUES

With the change of the technical requirements of equipment design, testability measure is also faced with new challenges, and also proposed new requirements to it:

1) The test measure shall be oriented to equipment maintenance

Testability design for metrics is consistent with the diagnosis and maintenance goals in the whole process, not only as an independent, abstract design rules. Therefore, it needs to considerate both testability design specifications and equipment real fault diagnostic capabilities.

2) Test measure should weigh several aspects

This design, in aspect of test indicators measure, is focusing on reference to the IEEE Std 1522-2004. The indicators are more standard in the IEEE Std 1522-2004, and taking into account the testability and diagnostic, and making objectives of the test design clear. Based on the standard, the paper builds six commonly specification used in testability design metric, namely:

a) FDR Fault detection rate (FDR)

FDR is generally defined the ratio of as within the time prescribed by the BIT and (or) external test equipment (ETE) correctly detect faults number and the total faults number.

Non-weighted fault detection rate is calculated as follows:

$$FDR = \frac{N_D}{N_T} \times 100\%$$

Which, N_T-system total failures number during work;

N_D-number of faults can be detected.

The weighted fault detection rate calculated as follows:

$$FDR_W = \left(\sum_{i=1}^{L_D} \lambda_i \Big/ \sum_{i=1}^{M-1} \lambda_i \right) \times 100\%$$

b) FIR Fault isolation rate (FIR)

The FIR is generally defined as the ratio of the number of detected faults within the time prescribed by the BIT and (or) ETE correct isolation not greater than replaceable unit number and the specified number of failures at the same time, expressed as a percentage.

Non-weighted fault isolation rate is calculated as follows:

$$FIR = \frac{N_L}{N_D} \times 100\%$$

N_L-unit faults can be replaceable which is correctly isolated less than or equal to L under specified conditions;

N_D-The number of failures can be detected.

Weighted fault isolation rate calculated as follows:

$$FIR_W = \left(\sum_{i=1}^{L_I} \lambda_i \Big/ \sum_{i=1}^{L_D} \lambda_i \right) \times 100\%$$

c) The average failure detection time (AFDT)

AFDT means that when a failure occurs, the average of the time required by BIT / ETE detects and indicates failure. The mathematical model can be expressed as follows:

$$FIR_W = \left(\sum_{i=1}^{L_I} \lambda_i \Big/ \sum_{i=1}^{L_D} \lambda_i \right) \times 100\%$$

Where t_{Di}-the time required when BIT/ETE detects and indicates the ith failure;

N_D -the faults number BIT / ETE detected.

d) Average fault detection costs (AFDC)

AFDC means that when a failure occurs, the average of the money required by BIT / ETE detects and indicates failure. The mathematical model can be expressed as:

$$MFDT = \frac{\sum C_{Di}}{N_D}$$

Where C_{Di} -the money required when BIT/ETE detects and indicates the ith failure;

N_D- the faults number BIT / ETE detected.

e) Fault isolation effectiveness (IE)

IE means the extent of the given fault diagnosis model can achieve the maximum fault isolation (isolated to a single failure source), the reasoning calculated formula as follows:

$$IE = 1 - \frac{\sum_{j=1}^{m} MFIR_j(k_j) \cdot (k_j - 1)}{\sum_{j=1}^{m} MFIR_j(k_j) \cdot k_j}$$

Where, MFIRj (k_j)-the average fault isolation rate of fuzzy group which size is k_j.

Obviously, if the system only has one kind of fault fuzzy group which size is 1, then IE = 1.

f) RTOK Retest OK rate RTOK

$$\text{RTOK} = \sum_{n-1}^{\text{nmax}} (1 - \frac{1}{n}) PA_n$$

PA_n-the cumulative probability of every fuzzy group.

V. FAULT INJECTION SYSTEM HARDWARE DESIGN

A. The composition and function

The fault injector is composed by two parts of the hardware and software systems. The hardware system includes the core control board, the signal conversion board, and communication cable. The control circuit consists of analog circuits and digital circuits. It is used for the realization of the signal conditioning, storage, computing, work status conversion and control signal output.

B. Fault Injection hardware design

The fault injection system consists of the core control board and four fault injection board. The core control board combines FPGA chip and RS422, and achieve the host computer controls the signal conversion board. The system in accordance with the functions can be divided into a host, the self-test circuit, the information collection circuit and the fault injection unit shown in Figure 5.

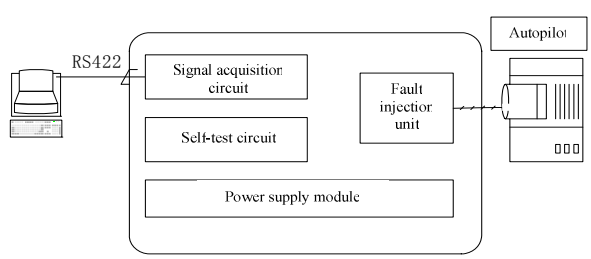

Figure 5. System hardware modules

VI. FAULT INJECTION SYSTEM SOFTWARE DESIGN

The system structure is shown in Figure 6. The system includes controller, fault Library, fault injector, data collector and analyzer, etc. modules.

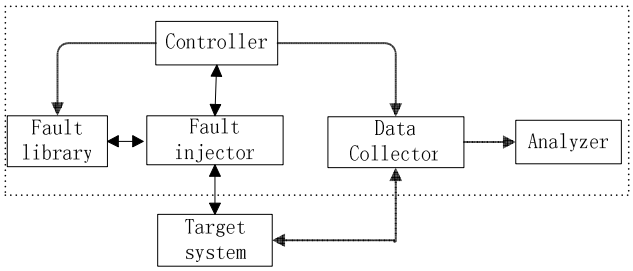

Figure 6. Software fault injection system test connection diagram

Each module has different function. They complete fault injection experiment on the target system through their coordination, and then gives the evaluation of fault-tolerant properties. The fault injection system needs to do the following functions: accord to a certain failure model to generate faults; inject a fault to the target system; collect affected information of the target system; analyze the results. The above-mentioned functions are achieved by all modules complement each other.

VII. EXPERIMENTS

The fault injection system is tested on an autopilot of some type equip in the design phase, which is shown in Figure 7. The results show that the faults can be tested by the system. And the detection by BIT and ATE can locate faults to the replaceable unit. Finally, the experiments analyze 65 kinds of failure modes. The analysis results of testability indicators are shown in TABLE.1. It can be known, from the table, that the actual test results are more accurate than the experiment. So system designing is successful and has certain advantages.

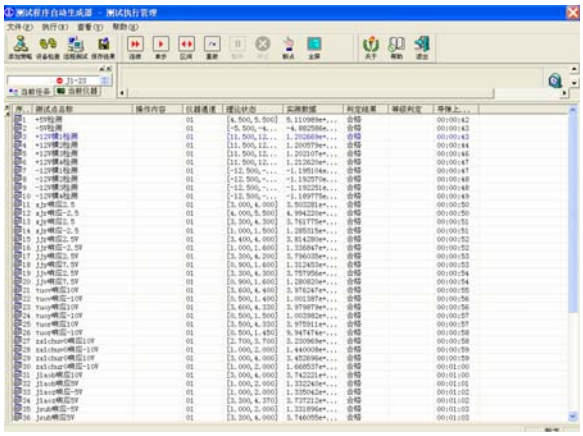

Figure 7. Test results

TABLE I. THE FAULT INJECTION SYSTEM ANALYSIS AND MEASURED COMPARATIVE TABLE

	Analysis Results	Actual Results
FDR	97.4%	98%
FIR	89.2%	92.3%
FAR	<5%	4.83%

In the table, FAR means False alarm rate.

VIII. CONCLUSION

The paper designs a fault injection system based on testability analysis and verification. The design stage of autopilot equipment is for the verification, greatly improving the testability and reliability. The designed fault injection system has more efficient and better testability. It can greatly increase the efficiency of the army's equipment design and produce huge military and economic benefits. The system has the design ideas of integrated, modular, combination and scalability, with the increasing of the number or change of the equipment, just simple improvements and adjustments, the system will be able to complete the testing and validation tasks, and its military and economic benefits will be more obvious.

REFERENCES

[1] Sosnowski J, Gawkowski P. Enhancing fault injection test bench [A].In: DepCos2RELCOMEX’ 06 [C]. 2006: 76-83.

[2] Moraes R L O,Martins E,MendesN V. Fault injection app roach based on dependence analysis[A]. In: Computer Software and Applications Conference[C]. 2005: 181-188.

[3] Fidalgo A V, Alves G R. Real time fault injection using enhanced OCD2A performance analysis[A]. In: DFT’06 [C]. 2006: 254 - 264.

[4] Little wood B. Dependability assessment of software2based systems: state of the art, software engineering [A]. ICSE 2005, Proceedings of 27th In2 ternational Conference[C]. 2005: 6-7.

[5] Kwang Ik Seo, Eun Man Choi. Comparison of five black2box testing methods for object2oriented software [A]. Software Engineering Research, Management and App lications, 2006, Fourth International Conference[C]. 2006: 213-220.

[6] Zhao Q C, Krogh B H. Generating test inputs for embedded control systems[J]. IEEE, Control Systems Magazine, 2003, 23 (4): 49-57.

[7] J. Karlsson, J. Arlat. App lication of Three Physical Fault Injection Techniques to the Experimental Assessment of theMARS Architecture [A]. / / Pro. Fifth Ann. IEEE int. Working Conf. Dependable Computing for Critical Application[C]. IEEE, CS press, 1995, 150-16.

[8] Gwan S. Choi, Ravishankar K. Iye, Victor A. Carreno. Simulated Fault Injection: A Methodology to Evaluate Fault Tolerant Microp rocessor Architecture [J] , IEEE Transactions On Reliability, 1990. 39 (4): 486 - 491.

[9] R. Chandra, R. M. Lefever, K. R. Joshi, et al. A Global-state-triggered Fault Injector for Distributed System Evaluation. IEEE Transactions on Parallel and Distributed Systems. 2004, 15(7):593–605.

[10] W. Hoarau, S. Tixeuil. A Language-driven Tool for Fault Injection in Distributed Applications. Proceedings of the IEEE/ACM Workshop GRID 2005. Seattle,USA, 2005:194–201.

[11] Z. Lin, B. Mao, L. Xie. A Practical Framework for Dynamically Immunizing Software Security Vulnerabilities. The First International Conference on Avail-ability, Reliability and Security (ARES2006). 2006:348–357.