

Design of a Testing Tool Based on Fault Injection for Functional Safety

Hang Yan*, Shanshan Li, Jianmei Lei, Tao Yan, Chunpeng Tang

China Automotive Engineering Research Institute Co.,Ltd. Chongqing 401122,China

Abstract. ISO 26262 provides testing requirements for functional safety development and testing to mitigate unacceptable risks arising from system functional failures. Fault injection plays a vital role in assessing system robustness and validating the efficacy of safety mechanisms. This paper explores the fault types and implementation process of fault injection in the context of functional safety confirmation and validation. A fault injection board specifically designed for electrical faults is developed and integrated with Controller Area Network (CAN) messages to verify the effectiveness and correctness of safety mechanisms. The proposed approach offers the advantages of flexible switching and ease of control, making it a valuable tool in ensuring the functional safety of automotive systems.

1. Introduction

The rapid development of automotive electronic and electrical technology has brought convenience, but at the same time, product safety issues have become increasingly prominent. To standardize the safety behaviors involved in product design, research and development, testing, and post-processing of automotive electronics and electrical systems, the International Organization for Standardization released ISO 26262 "Road vehicles -- Functional safety" in 2011[1], aiming to reduce the uncontrollable risks caused by failures in automotive E/E systems. The standard covers the life cycle of automotive systems and provides a basis for product development testing based on the V-model, encompassing the concept phase and system design (software and hardware levels)[2]. Fault injection testing (FIT)[3,4], as a recommended testing method in various stages, injects potential faults into the system under test to detect whether there are failure risks under fault conditions, thereby verifying the effectiveness of the system's safety mechanisms. However, in the actual vehicle validation and verification testing process, there are issues such as complex operations and cumbersome procedures. To reasonably and effectively implement fault injection testing, this paper designs a set of fault injection boards that provide diverse fault types. Compared with manual injection or software simulation, it can achieve precise and controllable fault injection. Furthermore, by integrating CAN (Controller Area Network) message instructions, it simplifies the operation in the actual process.

2. Fault injection

2.1. Types of Fault Injection

The purpose of fault injection testing is to verify the effectiveness of the safety mechanisms or safety measures proposed during the system design and software/hardware design processes, including attributes such as response time and whether the system enters a safe state[5]. The specific implementation methods for fault injection can be broadly categorized into two types: hardware-based faults and software-based fault injection[6,7]. For hardware-based fault injection, the main categories are as follows:

(1) Signal interference: Generating magnetic fields or radio frequency energy using electromagnetic interference (EMI)[8] equipment to affect circuit operation, simulating real-world electromagnetic compatibility issues.

(2) Power faults: Altering the supply voltage, including overvoltage, undervoltage, transient voltage dips or surges, to test the system's adaptability and protection mechanisms against power fluctuations.

(3) Temperature/humidity variations: Subjecting the system to extreme or unstable humidity environments, inducing potential increases in component failure rates.

(4) Structural stress: Applying vibration, shock, or mechanical pressure, which may lead to loose connections, cracked solder joints, or other physical damage.

(5) Short circuits/open circuits: Temporarily short-circuiting or disconnecting a component, pin, or signal line on the circuit board, simulating component failure or electrical connection breakage.

(6) Signal injection: Injecting erroneous signals into circuit nodes, such as changing logic levels or introducing clock signal disturbances.

*yanhang@caeri.com.cn

2.2. Process of Fault Injection

In Part 4 of ISO 26262[9](Table 1), fault injection is recommended at both the software/hardware integration

and system levels. Fault injection serves the following purposes: (1) Demonstrating the diagnostic coverage of safety mechanisms; (2) Proving the correct implementation of safety requirements.

Table 1. Correct implementation of functional safety and technical safety requirements at the system level

Methods	ASIL			
	A	B	C	D
1a Requirement-based test ^a	++	++	++	++
1b Fault injection test ^b	+	+	++	++
1c Back-to-back test ^c	o	+	+	++

- a A requirements-based test denotes a test against functional and non-functional requirements.
- b A fault injection test uses special means to introduce faults into the system. This can be done within the system via a special test interface or specially prepared elements or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.
- c A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

Within the same system, there is traceability between different Automotive Safety Integrity Levels (ASILs), and safety analysis can identify critical elements and hazard propagation paths in the architecture.

The fault injection process[10] typically involves the following steps: (1) Defining the fault model; (2) Fault activation; (3) Analysis of experimental results and evaluation of safety measures. Fault models can be extracted from potential failure causes, critical components, or safety analyses of critical paths[11]. The fault injection strategy is based on verifying the identified failure models against the implemented safety mechanisms, such as the failure modes in a Failure Mode and Effects Analysis (FMEA)[12]. To meet the technical requirements for functional safety verification testing, a system analysis of the object under test is necessary, including its functional logic and implementation methods. Then, considering the ASIL levels required for the system and its components, an analysis of fault points that directly violate safety objectives is conducted, enabling targeted fault injection testing (Figure 1).

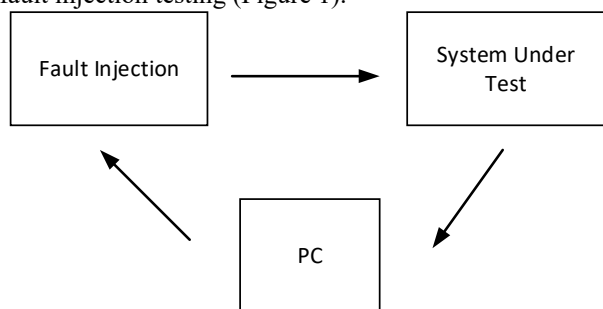


Figure 1. Fault injection test process

2.3. Theory and Implementation of Fault Injection

Combining the actual testing requirements and the ASIL level requirements specified in ISO 26262, this paper focuses on developing designs for several types of electrical faults, including power short circuits, ground short circuits, open circuits, and short circuits to other pins.

The main principle is illustrated in Figure 2. It primarily utilizes cascaded control of multiple I/O (Input/Output) lines, combined with an MPU (Micro Processor Unit) to enable control of the I/O chain by sending a single command. This allows for the selection of different fault injection methods and provides the advantage of flexible switching between multiple integrated fault types.

Since the CAN bus is widely used in automotive communications, to minimize operational steps during actual testing, the fault injection commands are integrated with CAN messages. Specific CAN messages are sent to trigger fault injection. The fault injection command index and values are shown in Table 2. The physical picture is shown in Figure 3 and 4.

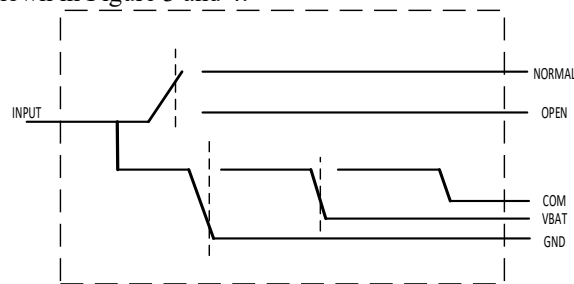


Figure 2. Theory of fault injection

Table 2. Control protocol

Index	Value	Remarks
0	02	Starting bit
1	01	Control mode
2	1~10	Channels
3	1~5	Fault types
4	03	End Bit

Where fault types, 1-normal; 2-open circuit; 3-short circuit to power; 4-short circuit to ground; 5-COM terminal. Reset message: 02 01 00 00 03.

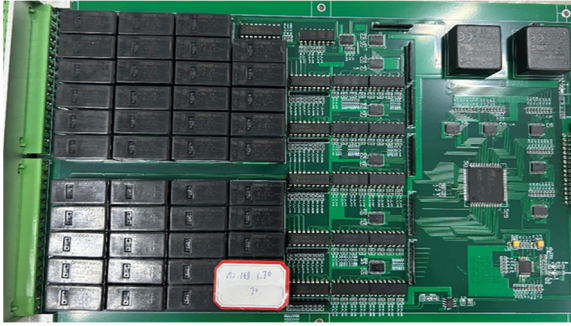


Figure 3. Fault Injection Board

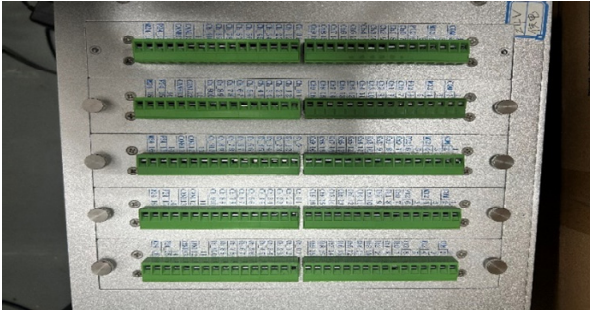


Figure 4. Multi-board integration

3. Solution Validation and Comparison

In a certain project test, targeting the functional safety requirement (Table 3) "The headlight controller should avoid erroneous control causing unintended extinguishing of the low beam headlights, leading to loss of forward illumination for the vehicle." During fault injection testing at the full vehicle level, a short circuit test needed to be performed on the control signal for the front left low beam headlight. According to the pin definition interface list for the headlight controller, the signal wire for the front left illumination lamp was connected to the fault injection board. Utilizing the self-defined protocol and with the assistance of the CANoe software, a message with the content "02 01 01 04 03" was transmitted (Fig. 5), and the change in the fault signal was observed in the Graphic window.

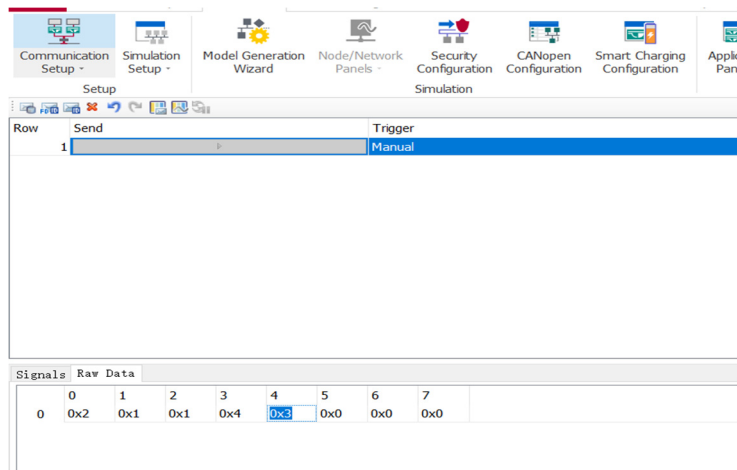


Figure 5. Fault injection message

Table 3. Functional safety requirement

Requirement Description	Testing Category	Test Description
The headlight controller should avoid erroneous control causing unintended extinguishing of the low beam headlights, leading to loss of forward illumination for the vehicle	Fault Injection	1.vehicle powered on and the low beam headlights remaining illuminated; 2. a short-circuit to ground was applied to the LDM_FR signal. LDM_FR transmitted LCU_ xxxFlt as 0x2: Fault

As demonstrated in Figure 6, after sending custom fault messages, the observed value of the "LCU_ xxxFlt" signal jumps, changing from "no fault" to "fault". In actual testing processes, there are situations where various faults are combined for testing. If signal and harness changes are made one by one, it would result in a significant waste of time and resources. To realize the combination of multi-

signal and multi-fault, a host computer was developed. As shown in Figure 7, the host computer can implement different types and quantities of test combinations, and it supports the import and export of test results. This not only simplifies the operation process but also enhances testing efficiency.

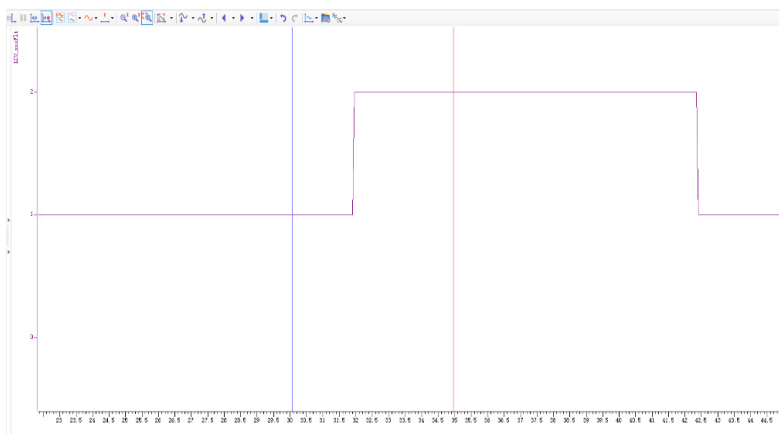


Figure 6. Fault message response

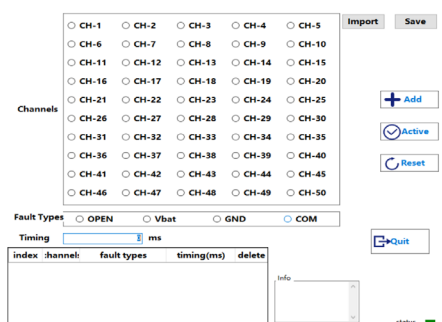


Figure 7. Multi-channels fault combination injection

4. Conclusion

In this paper, an analysis of the fault injection methodology was conducted in accordance with the ISO 26262 "Road Vehicles – Functional Safety" standard. Building upon this analysis, a fault injection board was designed to meet the requirements for electrical fault injection in the context of functional safety. This board enables fault injection through the selection of fault types via CAN messages, a solution that was subsequently validated. The integration with CAN messages streamlines the operation process. The versatility of multiple fault injection boards allows their application across various testing levels, such as hardware-in-the-loop (HIL) testing and vehicle validation testing.

References

1. ISO 26262:2011 Road Vehicles—Functional safety.
2. Luo, Y., Saberi, A. K., & den Brand, M. V. (2019). Safety-driven development and ISO 26262. *Automotive Systems and Software Engineering: State of the Art and Future Trends*, 225-254.
3. Da Silva, F. A., Bagbaba, A. C., Hamdioui, S., & Sauer, C. (2019, December). Combining fault analysis technologies for ISO26262 functional safety verification. In *2019 IEEE 28th Asian Test Symposium (ATS)* (pp. 129-1295). IEEE.
4. Kongjian, Q., Tong, Z., Kuiyuan, G., Hongwei, Z., Yu, W., & Haoxin, C. (2020, September). The Method of Functional Safety Validation Test of

AEBS Based on Fault Injection. In *2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)* (pp. 377-381). IEEE.

5. Breier, Jakub, and Xiaolu Hou. "How practical are fault injection attacks, really?" *IEEE Access* 10 (2022): 113122-113130.
6. Juez, G., Amparan, E., Lattarulo, R., Rastelli, J. P., Ruiz, A., & Espinoza, H. (2017, June). Safety assessment of automated vehicle functions by simulation-based fault injection. In *2017 IEEE International Conference on Vehicular Electronics and Safety (ICVES)* (pp. 214-219). IEEE.
7. Given-Wilson, T., Jafri, N., & Legay, A. (2020). Combined software and hardware fault injection vulnerability detection. *Innovations in Systems and Software Engineering*, 16(2), 101-120.
8. Dumont, M., Lisart, M., & Maurine, P. (2020). Modeling and simulating electromagnetic fault injection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(4), 680-693.
9. ISO 26262-4:2011 Road vehicles--Functional safety—Part 4: Product development at the system level.
10. Ziade, H., Ayoubi, R. A., & Velazco, R. (2004). A survey on fault injection techniques. *Int. Arab J. Inf. Technol.*, 1(2), 171-186.
11. Schmid, T., Schraufstetter, S., Wagner, S., & Hellhake, D. (2019, November). A safety argumentation for fail-operational automotive systems in compliance with iso 26262. In *2019 4th International Conference on System Reliability and Safety (ICSRS)* (pp. 484-493). IEEE.
12. Sulaman, S. M., Beer, A., Felderer, M., & Höst, M. (2019). Comparison of the FMEA and STPA safety analysis methods—a case study. *Software quality journal*, 27, 349-387.