Reliability Analysis of Brake-by-wire Systems on Fault Tree

Ce Zhang*, Yu Han, Yier Lin*, Dan Wang

College of Mechanical Engineering Tianjin University of Science & Technology
Tianjin, China
aZhangce@tust.edu.cn
* yier.lin@tust.edu.cn

Abstract—Brake-by-wire (BBW) system is the key system to ensure the safety and stability control of intelligent vehicle chassis. How to evaluate the BBW systems to meet the safety design requirements is one of the important links of system design. This article takes the BBW system as an example to illustrate the basic process of the safety assessment of intelligent vehicle. The fault tree analysis (FTA) method is used to quantitatively evaluate the failure status of the complete loss of the main brake function, and the fault tree analysis process is detailed. The results show that FTA plays an important role in guiding the design of system architecture. With the help of the importance index, we can quickly find out the weaknesses in the system architecture, when the probability of the failure state of the automobile brake-by-wire system cannot meet the ASIL requirements. Furthermore, effective countermeasures can be taken to optimize the design of the system architecture. Finally, the failure probability corresponding to the failure state of the car's brake-by-wire system is reduced to $7 \times 10^{-14}$.

1. INTRODUCTION

Automobile electrification, networking, intelligence and sharing are one of the strategic opportunities for development of Chinese automobile industry. It is not only a carrier of artificial intelligence, Internet of Things, cloud computing, big data and other new technologies, but also it will promote deep integration of new technologies and traditional automobile industry and reshape the ecosystem of automobile industry. Sensing, control decision and implementation technologies are necessary for intelligent vehicles. New brake-by-wire chassis is a key technology for intelligent vehicles. Among them, brake-by-wire (BBW) system decides chassis safety and control stability of intelligent vehicles. Faults of BBW system, especially under severe road and meteorological conditions, will increase drivers' working load greatly and affect traffic safety. Therefore, study on the safety design of BBW system is of great significance to the functional safety of intelligent vehicles.

Automobile industry has established its own functional safety standard - ISO26262 to ensure functional safety of various vehicle components and subsystems. In this standard, functional safety is defined as "there is no unreasonable risk that is related to every hazardous event caused by E/E system faults" [1]. Furthermore, functional safety is guaranteed by preventing or eliminating potential hazards. Sinha [2] performed detailed system architecture design and analysis for BBW system based on the method in ISO26262, and proved the effectiveness of this operational architecture. Cheon [3] discussed another conceptual design process of functional safety of BBW system. Leu [4] designed and analyzed a BBW system based on ISO26262, and demonstrated how to achieve a real safety critical system with the functional safety concept in ISO26262. In addition, there are more studies that focus on fault diagnosis and fault tolerant control algorithm to ensure system fault operation in case of faults. For
example, Huang [5] discussed transient fault tolerant control issue of BBW system based on transient fault propagation characteristics. However, discussions on risk management and mitigation in such studies are quite qualitative without giving out the way to realizing functional safety objectives by designing and implementing fault mitigation strategies. Meanwhile, a systematic design and assessment system is necessary to implement safety analysis and assessment of a highly complex and comprehensive intelligent vehicle efficiently, thoroughly and completely. Current aerospace industry has a mature safety design and assessment system. This paper puts forward a quantitative method for implementing vehicle functional safety requirements based on FTA method by referring to the safety design and assessment method [6] of civil aircraft system. This method is not only able to define functional safety requirements quantitatively, but also able to improve and optimize the biggest contributor of top event faults, meeting functional safety requirements.

This paper takes BBW system as an example, and conducts study on how to optimize system architecture, etc. when fault tree modeling process, probability calculation and safety requirements cannot be met, which provides reference for the safety analysis and system design of the BBW system of intelligent vehicles. The organization of this paper is as follows. Section 1 puts forward safety assessment methods. Sections 2 introduces FTA method. Section 3 introduces a general BBW system. Section 4 performs failure state analysis of BBW system, draws up a system chart and FTA, and makes optimization analysis on the biggest contributor of top event faults. Section 5 summarizes the future work that is discussed in this paper.

2. SAFETY ASSESSMENT METHODS

Safety work is an important part in the research & development process of intelligent vehicles. As shown in Figure 1, system research & development and safety analysis process constitute the research & development process of intelligent vehicles, and there are close combination and mutual feedback between them. As shown in the figure, main safety assessments include Vehicle Functional Hazard Assessment (VFHA), System Functional Hazard Assessment (SFHA), Preliminary System Safety Assessment (PSSA) and System Safety Assessment (SSA) [7].

Figure 1 Safety assessment process in the development process

VFHA is able to analyze vehicle functions systematically and identify failure states that are related to vehicle functions. It is classified based on severity of failure impact. Safety requirements for all functions can be distributed to all systems on the basis of VFHA analysis results through PASA. SFHA will be performed by all systems based on distribution results to identify failure states and impact levels...
that are related to system-level functions. SFHA analysis results will be output to PSSA, and then, PSSA will determine how SFHA identification function hazard is caused by system faults, and how to meet the identification safety requirements in SFHA through systematic inspection of the proposed system architecture. SSA will perform systemic analysis based on the realized system design and determine that a system is able to meet related safety requirements based on analysis results.

To improve the operability of measuring safety objectives, severity of failure state is determined qualitatively in ISO 26262 and GB T34590 standards based on overall consideration of vehicle impact as well as driver and occupant impact from failure state. Automotive Safety Integration Level (ASIL) is the risk level of the hazard that may be caused by functional failures of road vehicles. ASIL can be classified into Level A, Level B, Level C and Level D. Among them, Level A is the lowest level, and Level D is the highest level, as shown in Table 1. The higher the ASIL, the much geometric growth of system design complexity, development cycle and development cost, which means higher cost for safety, including more strict development process, greater hardware diagnostic coverage and higher technical requirements.

| ASIL level | Random hardware failure target value(/h) | Severity level |
|------------|----------------------------------------|---------------|
| ASIL A     | <1.00x10^-6                            | Slight        |
| ASIL B     | <1.00x10^-7                            | Considerable  |
| ASIL C     | <1.00x10^-7                            | Dangerous     |
| ASIL D     | <1.00x10^-8                            | Catastrophic  |

3. FAULT TREE ANALYSIS
As a graphic deductive analysis method from top to bottom, fault tree analysis (FTA) method is used to assess whether a system architecture is able to meet the probability requirements that are corresponding to the failure state defined in system risk assessment. It is widely applied in PSSA and SSA under safety assessment [7]. It takes the events that are undesirable in a system as the topmost failure event, analyzes all possible factors (such as hardware, software, environment and human factor) leading to such events from top to bottom as well as the logical relationship among them, and makes in-depth analysis on this basis until finding out the basic causes of such events, or meeting the analysis requirements for top events.

3.1. Basic Symbols and Definitions of Fault Tree
A fault tree consists of logical symbols and event symbols. Generally, the simpler the symbols used, the easier they can be reviewed and understood by fault tree. Logical symbols are used to connect all branches of a fault tree. Logical symbols cannot be connected directly, and their input and output shall be an event. Logical gates and event symbols used in this paper are listed in Table 2.

| Symbol | Name      | Definition                                      |
|--------|-----------|-------------------------------------------------|
| ∩      | AND-Gate  | Event can occur when all the next lower conditions are true |
| ∪      | OR-Gate   | Event can occur if any one or more of the next lower conditions are true |
3.2. Fault Tree Qualitative Analysis

The purpose of fault tree qualitative analysis is to figure out the possibility of certain top event in a system based on fault tree. Minimum cut sets of a system shall be determined before qualitative analysis.

Cut set is the set of several fault bottom events that lead to a system fault. One cut set represents one possibility or one fault mode of system fault. Minimum cut set refers to the cut set that contains the minimum number of the most necessary bottom events. The complete set of all minimum cut sets represent all given faults. Therefore, the significance of minimum cut set is that it gives out the fault modes that are necessary to be repaired in a system in fault state.

3.3. Fault Tree Quantitative Analysis

The main purpose of fault tree quantitative analysis is to analyze the probability of occurrence of a system fault and the degree of importance of each bottom event. The impact on the occurrence of a top event from each bottom event (or each minimum cut set) of a fault tree is known as the degree of importance of bottom event (or minimum cut set). Event research is of great significance for improving system design and reliability or determining fault monitoring locations, preparing system fault diagnosis schemes, reducing fault elimination time, etc. A fault tree usually contains multiple bottom events. To compare their degrees of importance in a fault tree, structural importance, probability importance and critical importance are calculated in fault tree quantitative analysis in general.

3.3.1. Probability importance (\(PI\))

The probability importance of Event A is the difference between the probability of occurrence of top event when Event A happens and the probability of occurrence of top event when Event A does not happen, which is expressed as follows.

\[
PI = P_t(TOP/A=1) - P_t(TOP/A=0)
\]  \hspace{1cm} (1)

Probability importance measures the changes in the probability of occurrence of the top event caused by Event A rather than taking the actual probability of occurrence of Event A into account directly.
3.3.2. Critical importance (CI)
A critical importance analysis method for correcting probability importance is needed to take the events that not only play a key role in the occurrence of top events, but also whose probability of occurrence is very high or can be improved into account. Critical importance of Event A is defined as follows:

$$\text{CI} = [P_r(\text{TOP} \mid A = 1) - P_r(\text{TOP} \mid A = 0)] \cdot \frac{P(A)}{P(\text{TOP})}$$  \hspace{1cm} (2)$$

Critical importance of Event A refers to the impact on the probability of occurrence of top events from Critical Event A that happens as per certain probability. Compared with probability importance, critical importance also considers the probability of occurrence of Event A.

3.3.3. Structural importance (SI)
The calculation of structural importance is very different from that of probability importance or critical importance. It is composed of minimum cut sets, and used to measure the importance of Event A by dividing the probability of occurrence of top events by the joint probability of all minimum cut sets that contain Event A. It is expressed as follows.

$$\text{SI} = \frac{P_r(\text{TOP}) - P_r(\text{TOP} \mid A = 0)}{P_r(\text{TOP})}$$  \hspace{1cm} (3)$$

If analysis purpose is to minimize the contribution to top events from primary events, the primary events that need to be improved can be chosen with this importance analysis method.

4. DESCRIPTION OF BBW SYSTEM
BBW technology is the most difficult and the most critical technology in intelligent BBW chassis technologies. BBW system decides chassis safety and control stability of intelligent vehicles. Only when good brake performance (including high response speed and good ride comfort) is provided can good safety be guaranteed. Current BBW systems can be classified into Electro-Hydraulic Brake (EHB) system and Electro-Mechanical Brake (EMB) system based on realization forms of BBW system [8].

EHB system is a brake system that integrates electronic system and hydraulic system. A complete EHB system consists of 4 major parts, i.e. wheel brake control unit (WBCU), hydraulic pump, brake pedal-interface unit (BPIU) and electronic control unit (ECU) as well as auxiliary systems like power supply [9], as shown in Fig. 2. EHB system is driven electrically with high response speed, which is convenient to control four-wheel braking respectively. Moreover, it has pedal decoupling function, so that active braking and energy recovery can be realized.

![Figure 2 Structure of EHB System](image)

Compared with EHB, EMB is more concise, and the biggest difference is that it cancels brake fluid and hydraulic components, so that vehicle mass is reduced. Brake pedal sensor signal, speed and other vehicle state signals are able to control actuator motors distributed in 4 wheels via ECU directly to generate required braking force. Fig. 3 is the schematic diagram of EMB system.
5. FTA of BBW System

5.1. Failure State of BBW System

Assume the failure states regarding BBW system that are identified in System Functional Hazard Assessment (SFHA) are shown in Table 3, and this table lists out failure states and their No., application stage, failure impact, classification and probability requirements. The probability corresponding to the impact level of “major” is $1.00 \times 10^{-8}$ [1].

5.2. Block Diagram of BBW System

General electronic BBW system is shown as Fig. 4 [10]. Generally, it consists of BPIU, EBCM, four-wheel WBCU and communication network. Among them, BPIU contains multiple sets of sensing sensors, each of them work independently to detect force and speed of brake pedal. WBCU consists of actuator, electronic control unit (ECU) and sensor. EBCM is electronic controller or micro controller that receives signals regarding vehicle motion and stability from BPIU, such as brake, steering, speed and wheel speed signals, calculates braking force of actuator based on the signals received, and sends braking torque to WBCU for brake control. Meanwhile, wheel sensors provide wheel brake controllers with wheel state feedback.

5.3. Fault Tree Analysis (FTA)

Next, a fault tree is derived based on the block diagram of the general BBW system above. For this purpose, top event is defined as “brake function is completely lost”. The fault tree displays logical groups of the basic element faults that may lead to this event. A top event may be caused by faults of any of the four subsystems below: wheel node fault, EBCM fault, BPIU fault and communication system fault. Among them, in case of faults of 4 WBCUs, wheel node fault happens; in case of faults of
3 groups of BPIUs, BPIU fault happens; in case of any fault of sub-configured sensor, processor and transmitter, sub-configuration fault happens. The detailed FTA process for the failure state of “brake function is completely lost” is shown in Fig. 5.

We briefly discussed some fault modes of these key components. But it should be noted that not all fault modes will lead to top event. For example, the pedal sensor in BPIU may have zoom or calibration error, so that there may be transient noise or input short circuit, open circuit or other faults. Such faults may lead to missing or excessive brake, but may not necessarily cause BPIU faults. In our analysis, BPIU fault refers to the state that the brake pedal unit doesn't work at all. Similarly, signal conversion design error or calibration error of

\[ \text{Figure 5 Fault Tree Analysis of System Architecture} \]

WBCU sensor will not lead to top event. Instead, the fact that the sensor doesn't work at all will lead to this top event.

5.4. Reliability Analysis Results of System Architecture

Next, reliability analysis of the general BBW system structure in Section 4.3 is made. Failure rates \([2]\) of all basic events involved in the entire FTA process are shown in Table 4.

### TABLE 4. FAILURE RATE OF DIFFERENT COMPONENTS

| ID | Subsystem | Component | Failure rate \( \lambda \) (/h) |
|----|-----------|-----------|-----------------------|
| 1  | Communication | Serial bus | 1x10^-7 |
| 3  | WBCU | Control module | 1x10^-7 |
| 4  | WBCU | Sensor | 2x10^-7 |
| 5  | WBCU | Actuator | 7x10^-7 |
| 6  | EBCM | Electronic controller/micro-controller | 1x10^-7 |
| 7  | WBCU | Sensor | 1x10^-7 |
| 8  | BPIU | Processor | 5x10^-7 |
| 9  | BPIU | Voter | 1x10^-7 |

According to calculation with FTA tool based on the fault rates in Table 4, the result shows that: The probability of occurrence of complete loss of main braking function is 2x10^-7, which does not meet the probability requirement of 1.00x10^-8. Quantitative analysis of the probability of occurrence of top event is shown in Table 5, which lists out the probability value, probability importance, critical importance and structural importance of each subsystem. It can be learn from the table that the probability importance of communication fault, EBCM fault, BPIU fault and wheel node fault is 1, so that such
four subsystems have the same importance, and occurrence of any event can lead to complete loss of main braking function. Among them, critical importance and structural importance of communication fault and EBCM fault are the same and far greater than other faults, so they are both regarded as the biggest contributor. To make the probability of occurrence of top event meet the requirement of $1.00 \times 10^{-8}$, it is necessary to make further optimization and improvement centering on the biggest contributors - communication fault and EBCM fault.

| Subsystem   | Unreliability | Probability importance | Critical importance | Structural importance |
|-------------|---------------|------------------------|---------------------|----------------------|
| Communication | 1x10^{-7}     | 1                      | 5x10^{-6}           | 0.50                 |
| EBCM        | 1x10^{-7}     | 1                      | 5x10^{-6}           | 0.50                 |
| BPIU        | 3.43x10^{-19} | 1                      | 1.72x10^{-38}       | 1.72x10^{-12}        |
| Wheel Node  | 6.56x10^{-25} | 1                      | 3.28x10^{-18}       | 3.28x10^{-18}        |

5.5. Optimization and Analysis

5.5.1. Optimization Measures
Specific optimization measures are put forward focusing on communication and EBCM to meet the probability requirement of $1.00 \times 10^{-8}$.

Add a standby EBCM module to connect with BPIU. If a fault is detected in normal EBCM, it will be keep silent, and the standby EBCM will be converted to active mode, so as to take over and implement expected functions. Upon optimization, the fault rate of the EBCM subsystem was reduced to $1x10^{-14}$, and the biggest contributor of top event fault was changed to communication fault from EBCM fault. The following optimization measures are taken for communication: A star connector is introduced to the interconnection between EBCM and WBCU, and double hybrid topology mode is used for connection [11]. This connection form is simple and easy to realize, which is flexible to add or remove nodes, so that faults of individual nodes will not affect normal work of other nodes in the network. Star connector fault rate [12] is $2x10^{-7}$, then, the optimized communication fault rate is $6x10^{-14}$. The block diagram of the optimized BBW system is shown in Fig. 6.

FTA has been performed for the block diagram of the optimized BBW system, and the resultant fault tree is shown in Fig. 7.

![Figure 6 Block Diagram of The Optimized BBW System](image)
5.5.2. Comparative Analysis

Comparison between the result of the original scheme and that of the optimization measures scheme is shown in Table 6, and the required probability is $1.00 \times 10^{-8}$.

**TABLE 6. SUMMARY OF FAULT-TREE ANALYSIS BBW SYSTEM**

| System     | Unreliability | Acceptable | Optimization measures |
|------------|---------------|------------|-----------------------|
| Before     | $2 \times 10^{-7}$ | No         | None                  |
| Optimized  | $7 \times 10^{-14}$ | Yes        | 1. Add an alternate EBCM; 2. Introduce the star connector in the interconnection between the dual EBCM and WBCU, and use the dual hybrid topology for connection; |

6. CONCLUSIONS

Along with the development of electrification, networking, intelligence and sharing of automobile industry, BBW chassis technology will play a key role in the development of intelligent vehicles, so that study of BBW chassis technology is beneficial to functional safety and reliability development. This paper put forward a quantitative method for implementing vehicle functional safety requirements by referring to the safety design and assessment method of civil aircraft system. FTA was performed for electronic BBW system. When safety probability requirements cannot be met, redundancy design was added focusing on the biggest contributor, and system hierarchy for BBW system optimization was proposed to further reduce the failure rate of the biggest contributor, so as to meet safety probability requirements. However, the result obtained was approximate evaluation based on fault rate, and data needs to be deduced and reviewed carefully in actual system analysis. The concepts and methods discussed in this paper can be taken as reference methods at the preliminary system security assessment stage, but the feasibility of the optimized structure needs to be proved at the system safety assessment stage through experiments.
REFERENCES

[1] Road vehicles - functional safety - part 2: management of functional safety, 2018b.
[2] Purnendu Sinha, “Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives,” J. Reliability Engineering and System Safety, 2011, 96(10).
[3] J. Cheon, Jongsun Kim, Jaehan Jeon and S. Lee, Brake by wire functional safety concept design for ISO/DIS 26262. SAE 2011 annual brake colloquium and engineering display. SAE International, 2011.
[4] Leu K, Huang H and Chen Y, 2015 International conference on connected vehicles and expo (ICCVE). 2015, pp. 150-6.
[5] Shuang Huang, Chunjie Zhou, Lili Yang, Yuanqing Qin, Xiongfeng Huang and Bowen Hu, “Transient fault tolerant control for vehicle brake-by-wire systems,” J. Reliability Engineering and System Safety, 2016, 149.
[6] S International, “Guidelines And Methods For Conduction The Safety Assessment Process On Civil Airborne Systems And Equipment,” J. 1996.
[7] Zhongxin Xiu , Introduction to Civil Aircraft System Safety Design and Evaluation Technology. Shanghai Jiao Tong University Press, 2013.
[8] Wenlong Sun, Research on characteristics analysis and braking force control of compound braking system based on EHB and EMB. Changchun: Jilin University, 2016.
[9] Hongyu Zheng, Changfu Zong, Tianjun Zhu, Chengwei Tian, Yan Qiao and Fengyue Juan, Stability analysis of automobile wire-controlled hydraulic brake system. Transactions of the Chinese Society of Agricultural Machinery, 2008, pp. 180-184.
[10] Weidong Xiang, P. Richardson, Chenming Zhao and S. Mohammad, “Automobile Brake-by-Wire Control System Design and Analysis,” J. IEEE Transactions on Vehicular Technology, 2008.
[11] EASIS, General architecture framework, deliverable 0.2.4, EASIS consortium, August 2004.
[12] Hammett R C and Babcock P S, Achieving 10-9 Dependability with Drive-by-Wire Systems.SAE TECHNICAL, 2003.