Vehicle Redundant Power with High Safety and Reliability

Xi CHEN\textsuperscript{1,a}, Tong WANG\textsuperscript{1,b} and Xiao-Min LIAN\textsuperscript{1,c,*}

\textsuperscript{1}State key Laboratory of Automotive Safety and Energy, Department of Automotive Engineering, Tsinghua University, China
\textsuperscript{a}chenxi14@mails.tsinghua.edu.cn, \textsuperscript{b}wangtong19929@foxmail.com, \textsuperscript{c}lianxm@tsinghua.edu.cn
\textsuperscript{*}Xiao-Min LIAN

Keywords: Power Electronic, Redundant, Safety and Reliability, Failure Management Strategy.

Abstract. Power module is one of the most important modules for automotive safety-critical electronic systems (ASCES) such as electronic steering and braking system. The paper proposes vehicle redundant power (RP) and focuses on improving the safety and reliability of power module for redundant ASCES (RASCES). The proposed vehicle RP adopts isolated strong and weak power based on redundancy theory, which not only has the ability of failure tolerance, but also provides clean and stable electricity to RASCES controllers. Analyzing the safety and reliability of vehicle RP using Fault Tree Analysis method, the failure rate can meet the automotive safety integrity level (ASIL) D random hardware failure target value demand in automotive functional safety standard ISO26262. Failure injection test results show vehicle RP can reach “failure/operation/warning” high safety and reliability.

Introduction

Compared with traditional mechanical systems, automotive electronic systems are lightweight, flexible control and quickly respond. There exists a tendency that more and more traditional mechanical systems are replaced by automotive electronic systems [1], such as steer-by-wire (SBW) system and brake-by-wire (BBW) system. However, electronic systems have many safety and reliability problems, such as unreliable stability in electrical signal transmission, and no omen before breakdown. To solve these problems, redundancy systems which named RASCES are used to improve the safety and reliability of the electronic system. [2, 3, 4, 5]. However, RASCES power module’s safety and reliability has been less considered. Once the power module of RASCES malfunctioned, it would lead to serious automotive safety problems. Thus, how to ensure safety and reliability of RASCES power module is becoming more and more important. Jones III, J. L. [6] proposes a system and method for providing power redundancy to certain devices with critical functions in vehicle. However, the proposed system needs external controller and switching delay to choose the power path, which has possibility of systematic failure.

This paper proposes a new structure of vehicle redundant power (RP) using isolated strong and weak power based on redundancy theory. The RASCES’s power module using this structure can reach “failure/operation/warning” safety mechanism and meet the automotive safety integrity level (ASIL) D random hardware failure target value demand in ISO26262.

This paper is organized as follows. Section 2 introduces the structure of the proposed vehicle RP and its working mechanism. The theoretical analysis of vehicle RP’s safety and reliability will be presented in section 3. In section 4, tests will be given to validate this structure of the proposed vehicle RP. Finally, it will conclude this paper in Summary.

Vehicle RP

Vehicle RP adopts dual modules hot spare architecture. The two single power modules provide electric energy in parallel to RASCES in automotive. In addition, vehicle RP has comprehensive and effective redundant management strategy to ensure its safety and reliability.
Vehicle RP’s Function and Structure

Vehicle RP consists of two same modules and each module consists of strong and weak power path. In normal working state, the dual modules provide electric energy together. Once any path or any module malfunctioned, the faulted path or module would be cut off automatically and vehicle RP works continually relying on another normal single power path. Vehicle RP detector checks vehicle RP’s working state and transforms state message to vehicle CAN bus continuously. In addition, vehicle RP adopts isolated strong and weak power structure. The structure not only provides power to high-power loads like motors, but also provides stable, reliable and clean power to controllers, which avoids voltage fluctuation influence caused by high power loads switched-on and switched-off.

The schematic diagram of vehicle RP architecture is shown in Fig.1.

![Figure 1. Schematic diagram of vehicle RP architecture.](image)

vehicle RP architecture P can be expressed as

\[ P = \{S, C, I, R, O\} \]  \hspace{1cm} (1)

S means RP supply set including battery and alternator; C means RP control switch set including ACC start and ON start. I means RP redundant input path set including \(I_{B}\) and \(I_{G}\). R means RP structure set including the first power module RPA, the second power module RPB and failure detection module RPE. O means RP redundant output path set including redundant strong power output path \(U_{p1}, U_{p2}\) and redundant weak power output path \(U_{d1}, U_{d2}\). All sets made up of vehicle RP architecture P are redundant structures.

The isolated strong and weak power structure of RPA is shown in Fig.2.

![Figure 2. Schematic diagram of RPA.](image)
RPA consists of two strong power paths and two weak power paths. Strong power path 1 consists of Over-current Protection Module 1, while strong power path 2 consists of Over-current Protection Module 2 and strong power path from RPB through Parallel Connection Interface Module P_{Up1}. Weak power path 1 consists of DC-DC Module and Over-current Protection Module 3, while weak power path 2 consists of Over-current Protection Module 4 and weak power path from RPB through Parallel Connection Interface Module P_{Up2}. Over-current Protection Module 1 and Module 3 are working in Over-current Protection for strong power path 1 and weak power path 1 respectively. Over-current Protection Module 2 and Module 4 are working in over-current isolation protection for strong power path 2 and weak power path 2 respectively, which can prevent over-current failure from interacting between RPA and RPB.

The schematic diagram of failure detection module RPE is shown in Fig.3.

The Micro-processing Unit is used for failure confirmation and failure warning. Signal Conditioning Module 1 and 2 can receive state signals from RPA and RPB through Status Interface Module 1 and 2. And then Signal Conditioning Modules condition the state signals to appropriate voltage signals which can be received by Micro-processing Unit. CAN Bus Communication Module is used for transforming message between vehicle RP and vehicle CAN bus. It’s worth mentioning that RPE power supply is both from RPA through Status Interface Module 1 PD1 and RPB through Status Interface Module 2 PD2. So, once RPA or RPB malfunctioned, RPE could work continuously.

**Vehicle RP Failure Detection and Failure Warning**

Vehicle RP redundant management strategy consists of failure detection, failure warning, failure protection and failure isolation. The management strategy can provide effective and comprehensive monitoring to vehicle RP’s working state. As illustrated in Fig.4, the framework of this flow chart consists of 3 steps including failure detection (step 1), failure confirmation (step 2) and failure warning (step 3), in which failure confirmation is to prevent false warning.

Vehicle RP power path state set V can be expressed as \( V = \{ v_{ik}, i=1,2; k=1,...,4 \} \), and \( v_{ik} \) represents power path state sensing signals \( S_{o1} - S_{o4} \) from RPA and \( v_{ik} \) represents power path state sensing signals \( S_{o5} - S_{o8} \) from RPB as shown in Fig.3. Power path failure analysis set A can be expressed as \( A = \{ a_{ik}, i=1,2; k=1,2 \} \), where \( a_{11}, a_{12} \) are working states of strong power path 1, 2 and \( a_{21}, a_{22} \) are working states of weak power path 1, 2. Vehicle RP power path state Message set M can be expressed as \( M = \{ m_{ik}, i=1,2; k=1,2 \} \), where \( m_{11}, m_{12} \) are attached to strong power path 1, 2 and \( m_{21}, m_{22} \) are attached to weak power path 1 and 2 respectively.
Safety and Reliability of Vehicle RP

Automotive functional safety standard ISO26262 is the global standard to meet such demands for a more structured and systematic approach to functional safety design. According to ISO26262, the failure of vehicle RP will lead to the failure of key components, such as SBW and BBW system.

ASIL Analysis of Vehicle RP

The first step in risk assessment is to prescribe ASIL levels for the vehicle RP under various situations. ASIL is categorized into four levels, A, B, C and D, where A has the lowest risk and D has the highest risk. The ASIL levels are composed of Severity (S0–S3), Exposure (E1–E4), and Controllability (C0–C3). The harm of vehicle PR is that it can’t afford power. When we are driving the vehicle equipped with SBW or BBW system, the vehicle cannot steer or brake if vehicle RP power supply failure occurs. The risk assessment table is as Table 1.

Table 1. ASIL assignment for various driving situations of vehicle RP.

| Hazard | Driving Situation | Controllability Sort Description | Severity Sort Description | Posure Sort Description | ASIL |
|--------|-------------------|----------------------------------|---------------------------|-------------------------|------|
|        |                   | driver can’t control the vehicle without electrical power | cause serious/fatal injury to driver | Driving scenario accounted for > 10% of vehicle’s whole driving life | D    |
|        |                   | Classification C3 | Classification S3 | Classification E4 |      |
Thus, the functional safety target is ‘to prevent vehicle RP from not providing power’, and the safety level is ASIL D. According to ISO26262, to achieve the safety level ASILD, random hardware failure target value should be $< 10^{-8} h^{-1}$.

Fault Tree Analysis (FTA) [7] method is a common used method for evaluating system’s safety and reliability. It is a top down, deductive failure analysis in which an undesired state of a system is analyzed using boolean logic to combine a series of lower-level events. For vehicle RP, the top event is ‘vehicle RP can’t supply power’, the cause of the top event is likely to be:

1) RPA and RPB breakdown at the same time. If just RPA fails, due to the fault isolation, RPB can still work.

2) Vehicle power supply battery and alternator breakdown at the same time. If just battery fails, alternator can still supply power, the same to alternator. So the fault tree of vehicle RP is in Fig.5.

![Fault tree of vehicle RP](image)

The code names’ meanings in Fig.5 are listed in Table 2:

| Code name | Meaning                  |
|-----------|--------------------------|
| E         | Vehicle RP can’t supply power |
| X1        | Battery fails            |
| X2        | Alternator fails         |
| X3        | RPA fails                |
| X4        | RPB fails                |

The Failure Rate of Vehicle RP

Referring to GJB/Z 299C-2006 [8] and components counting method, we can get the failure rates of RPA and RPB are:

$$\lambda_{X3} = \lambda_{X4} = \lambda_{RPA} = \lambda_{RPB} = 1.43 \times 10^{-5} h^{-1}$$  (2)

In the same way, the failure rate of battery and alternator is:

$$\lambda_{X1} = \lambda_{p_B} = 2.43 \times 10^{-6} h^{-1}$$  (3)

$$\lambda_{X2} = \lambda_{p_A} = 1.04 \times 10^{-5} h^{-1}$$  (4)

The probability of occurrence of top event E is:

$$E = X_1X_2 + X_3X_4$$  (5)

The system’s reliability is:
\[
R_E = R_{X1X2} + R_{X3X4} \quad (6)
\]

\[
R_{X1X2} = R_{X1} R_{X2} + R_{X1} (1 - R_{X2}) + R_{X2} (1 - R_{X1})
\]

\[
= R_{X1} + R_{X2} - R_{X1} R_{X2} \quad (7)
\]

Assuming \( R \) is subject to exponential function and \( t = 1h \).

\[
R = e^{-\lambda t} \quad (8)
\]

So, we can calculate the failure rate of vehicle RP is:

\[
R_{X1X2} = e^{-\lambda_X t} + e^{-\lambda_X t} - e^{-\lambda_X t} \cdot e^{-\lambda_X t} \quad (9)
\]

\[
R_{X3X4} = e^{-\lambda_X t} + e^{-\lambda_X t} - e^{-\lambda_X t} \cdot e^{-\lambda_X t} \quad (10)
\]

\[
\lambda_E = \frac{-R'_E(t)}{R_E(t)} = \frac{R'_{X1X2} + R'_{X3X4}}{R_{X1X2} + R_{X3X4}}
\]

\[
= 4.1 \times 10^{-10} h^{-1} \quad (11)
\]

Thus, the failure rate of vehicle RP \( \lambda_E \) can meet the random hardware failure target value demand of ASIL D.

**Vehicle RP Failure Test Results**

Vehicle RP failure test platform consists of vehicle RP principle prototype and other devices as shown in Fig.6.

Vehicle bus analysis device CANoe is used for simulating vehicle bus network environment. Several 50W high power halogen lamps and controllers are used for RASCES loads. NI voltage acquisition system and labview software are used for power path output voltage acquisition.

The ability and validity of redundant management strategy can be tested roundly by using the test platform. We adopt failure injection method to verify vehicle RP, and the failure refers mainly to open-circuit failure. Vehicle RP failure test positions are marked in Fig.7, and 5 failure test points \( P_{b1} \sim P_{b5} \) are set in RPA.
Figure 7. Vehicle RP failure test position.

The 5 test points simulate strong power path, weak power path and parallel power path failure respectively. What we concern most is the fluctuation of power path output voltage when failure occurs. Vehicle RP failure test results are in Fig.8.

![Vehicle RP failure test results](image)

Figure 8. Vehicle RP failure test results.

To ensure the accuracy of the test results, we conduct 50 times repeated experiments on every test point, and calculate the average value of voltage fluctuation. The final test results are listed in Table 3.
Table 3. Vehicle RP failure test final results.

| No. | Test Point | Vehicle RP average value of voltage fluctuation /V |
|-----|------------|---------------------------------------------------|
|     |            | \(\Delta U_{\rho_1}\) | \(\Delta U_{d1}\) |
| 1   | \(P_{b1}\) | 0.62 | 0 |
| 2   | \(P_{b2}\) | 0.58 | 0 |
| 3   | \(P_{b3}\) | 0   | 0.59 |
| 4   | \(P_{b4}\) | 0.12 | 0 |
| 5   | \(P_{b5}\) | 0   | 0 |

It can be found in Table 3 that vehicle RP power paths output voltage exist minor fluctuation when failure occurs in \(P_{b1}\), \(P_{b2}\) and \(P_{b3}\). The minor voltage fluctuation is caused by switching disturbance and has no influence to RASCES. Furthermore, we can know that the 0.6V voltage fluctuation belongs to inherent errors. Because RPA and RPB adopts the smart high-side power switch BTS555 and BTS6143D, and its internal structure is shown in Fig.9.

![Figure 9. Smart high-side power switch internal structure.](image)

When current reverses in strong power path 2 through Over-current Protection Module 2 and in weak power path 2 through Over-current Protection Module 4 is shown in Fig.2. It exists drain-source diode voltage = 0.6V if \(V_{out} > V_{bb}\) in Over-current Protection Module 2 and 4. So this is the reason where is the minor voltage fluctuation from. Failure test position \(P_{b4}\) and \(P_{b5}\) are in parallel power path, and there is no current in normal condition. So there is no inherent error but other random minor fluctuation when failure occurs in \(P_{b4}\) and \(P_{b5}\).

At the same time, during in long-running test, we monitor the voltage fluctuation of strong power path and weak power path. Comparison of power path output voltage fluctuation is shown in Fig.10.

![Figure 10. Comparison of output voltage fluctuation.](image)
Test results in Fig.10 indicate that the proposed isolated structure of vehicle RP can reduce the voltage fluctuation influence caused by high power loads greatly. Weak power path voltage has small voltage fluctuation while Strong power path voltage fluctuates greatly. So, the proposed structure can provide clean and stable electricity to RASCES controllers.

Summary

In this paper, firstly, the structure of vehicle RP using isolated strong and weak power based on redundancy theory is proposed and designed for RASCES in vehicle. The proposed structure of vehicle RP not only satisfies the safety and reliability of RASCES power supply, but also provides clean and stable electricity to RASCES controllers. Secondly, analyzing the safety and reliability of vehicle RP using FTA method, and the failure rate of proposed vehicle RP is \( \lambda = 4.1 \times 10^{-10} \text{h}^{-1} \), which satisfies the random hardware failure target value demand of ASIL D in ISO26262. Lastly, failure injection tests show that vehicle RP can reach “failure/operation/warning” high safety and reliability and satisfy the safety and reliability requirements of RASCES power supply.

Acknowledgement

This research was financially supported by the State key Laboratory of Automotive Safety and Energy, Tsinghua University.

References

[1] Rivero, A. A. L., from complex mechanical system to complex electronic system: the case of automobiles, International Journal of Automotive Technology & Management, 14(1): 65-81, 2014.
[2] Baleani, M., Ferrari, A., Mangeruca, L., Sangiovannivincentelli, A. et al., Fault-tolerant platforms for automotive safety-critical applications, Compilers, Architecture, and Synthesis for Embedded Systems, 2003.
[3] Gang, X., Jun, W., Da, Q. T. et al., Research on Two-Machine Fault-Tolerant of Automotive Electric Power Steering System Controller. Automotive Technology, 2006 (6): 11-14.
[4] Xiao, Y. P., Xiao, D. D., Jing, Z., A Research on the Reliability Analysis and Fault-tolerant Technology of Vehicle BBW System. Automotive Engineering, 2009, 31(7): 624-628.
[5] Feng, M., Xiao, M. L., Congruent duplex redundant central coordinators in automotive electric and electronic networks. Journal of Tsinghua University (Science and Technology), 2016, 56(10): 1091-1096.
[6] Jones III, J. L., Russel, K. J., Shoshiev, A., & Sheng, Y., U.S. Patent No. 7,235,898, 2007.
[7] Hiraoka. Y., Yamamoto. K., Murakami. T., Furukawa. Y., et al, Method of Computer-Aided FTA in Reliability Design and Development -Using Knowledge Management based on Quantity Dimension Indexing and Block Diagrams, SAE Technical Paper 2012-01-0203, Journal of Commercial Vehicles, 5(1), 72-82, 2012.
[8] GJB/Z299C-2006. Reliability prediction handbook for electronic equipment, 2006.