International Journal of Control and Automation
Vol.8, No.3 (2015), pp.287-296
http://dx.doi.org/10.14257/ijca.2015.8.3.29

Control Strategy of Electric Vehicle Controllers and the Reliability Analysis Based on Dual Computer Hot Stand-by Technology

Guo Yanling[1], Liu Lichen[1], Gao Meng[2] and Wang Meng[3]

[1]*College of Mechanical and Electrical Engineering, Northeast Forestry University, Harbin, China*
[2]*Information and Computer Engineering College, Northeast Forestry University, Harbin, China*
[3]*Traffic College, Northeast Forestry University, Harbin, China*
liulc1983@163.com

Abstract

Aiming at the reliability and security problems existed in stand-alone control mechanism for electric vehicles, a electric vehicle controller control strategy based on dual computer hot stand-by technology was proposed, traditional stand-alone control mechanism was replaced by dual computer hot stand-by control mechanism, when host engine failed, the standby engine would replace the host engine and take over the control tasks, it can ensure the reliable and continuous working of the control unit. Markov model was used to analysis the reliability and security of the dual computer hot stand-by system, and its performance was compared with stand-alone control system on MTBF value, reliability and safety performance curves, the results show that reliability and security level of dual computer hot stand-by system is significantly higher than stand-alone control system, the research has a practical guiding significance for introducing dual computer hot stand-by technology into electric vehicles.

Keywords: *Dual computer hot stand-by; Electric vehicle; Markov model*

1. Introduction

At present, the development trend of electric vehicles is tending to become more systematic, modular and safe, as the drive unit, controller is the core of a control system, its reliability and security is directly related to the whole control system's continuous and stable running [1]. When vehicle controller uses stand-alone control mode, once the controller fails, the whole vehicle system will fall into a dangerous state, therefore, it needs to use a redundant fault-tolerant technology to design the processor's core components and other associated key components of the controller, and this kind of working mode can improve the reliability and security of the vehicle controller. Currently, hardware redundancy techniques mainly have the following ways: single line redundancy, dual computer cold stand-by, dual computer hot stand-by and triple redundancy [2-3]. As the reliability of single line redundancy is limited, control instantaneity of dual computer cold stand-by is poor and system of triple redundancy is too large [4-5], in consideration of the pros and cons of various redundancy mode, combining with the specific engineering achievement condition of electric vehicles, this paper proposes up a safe and reliable control strategy for electric vehicle controllers' development, this strategy is based on a kind of dual computer hot stand-by hardware redundancy design.

ISSN: 2005-4297 IJCA

2. Control Strategy based on Dual Computer Hot Stand-by

Dual computer hot stand-by is a kind of technology to realize the dual engines working mode, it relies on two sets of processor systems, and each of them has the same hardware and software. Under this mode, the one who gains the control right is the host engine (work engine) while this other is the standby engine, host engine's output signal has the output control right, and standby engine's output is invalid at this time. When the two engines are working properly, host engine is responsible for controlling the whole system's stable running as well as monitoring whether the standby engine is working correctly, standby engine is responsible for monitoring the host engine's working situation, but it doesn't output data to peripherals, this mode belongs to hot backup; when host engine is abnormal, its control right will be confiscated through arbitration and switching circuit, standby engine turns to be the host engine, it takes over the control tasks and controls the whole system's running, this kind of control right's seamless transition method can ensure the continuous and reliable working of vehicle controllers; after being repaired, the abnormal controller will re-access to the filed bus control system as the standby engine, it constitutes the dual computer system together with the host engine.

Traditional dual computer host stand-by control mode usually uses independent fault detection unit to detect fault [6], although fault detection unit has a high fault detection rate and low system resources occupancy rate, it needs additional CPU and detection circuitry, which greatly improve the system cost [7], once the fault detection unit is invalid, the system will fall into a dangerous state with unpredicted fault, at this time, system will be judged as fail [8]. The control strategy proposed in this paper removes the independent fault detection circuit based on traditional hot stand-by control mode, and it is replaced by adding heartbeat bus and control signal lines between host engine and standby engine.

3. Controller Implementation based on Dual Computer Hot Stand-by

According to the dual computer hot stand-by control strategy, in consideration of system's functional requirements, reliability requirements and engineering design requirements, design the structure of controller's overall control strategy frame, it is shown in Figure1.

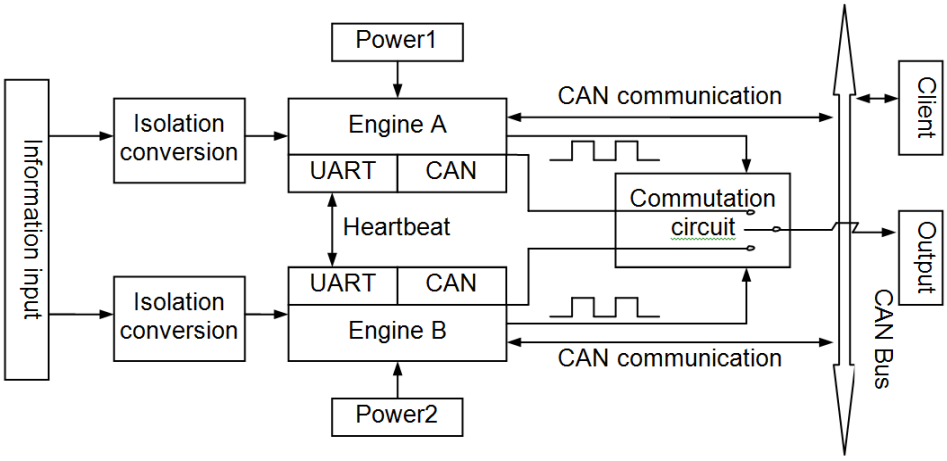

Figure 1. Controller Structure based on Dual Computer Hot Stand-by

It can be seen from the Figure 1 that controller based on dual computer hot stand-by is mainly composed of isolation conversion, dual engines, redundant power supplies, heartbeat communication, commutation circuit and CAN communication bus.

3.1. Information Input and Isolation Conversion

Analog acquisition of information input (switch signal, accelerator pedal input, brake information input, gear information input, etc.) mainly considers the acquisition precision and acquisition converting speed, therefore, choose TI company's TLV320AIC10 as the 16 bit analog-to-digital converting chip in isolation conversion circuit, and in order to improve the anti-jamming capability, choose capacitive coupling analog isolation chip ISO124 and digital isolation chip ADuM1201 and so on.

3.2. Redundant Power

Power supplies the whole controller's power source, it must work reliably, tandem connect the protection diode with the output forward end of power1 and power2 separately, then merge the protection diodes together, on the other hand, connect the two ground electrodes, which can constitute a reliable and redundant supply of dual power.

3.3. Dual Engines

Dual engines consist of two same processors based on TI company's TMS320F28335DSP, after engine A and engine B are contemporarily powering, output dynamic square wave, switch circuit of engine who first outputs square wave will automatically fall to the host side through competition, the host will connect the output circuit and gain the control right, at this time, the dynamic square wave and output of the standby engine are invalid, square wave's period is regarded as the fault detection interval time, if this period is too long, switching time after a fault will become long; if this period is too short (less than a judgment period), it may lead to a false switching, in strategy proposed up in this paper, this period is set to be 200ms. When engine A and engine B are not powering at the same time, the former powering one will be the host engine, the other will be the standby engine.

3.4. Heartbeat Communication

Double engines' communication is a key issue for dual engine system's design, in dual computer hot stand-by system, conversion between double engines is achieved by detecting heartbeat signal, it is the basis of double engines' mutual detection, fault engine isolation and recuperative engine's re-access to dual engine system. The so-called heartbeat signal means that double engines send signals to each other mutually according to the agreed time intervals, in order to show the current working status of each engine.

Independent fault detection unit is replaced by adding heartbeat communication bus and outputted dynamic square wave between dual engines, fault detection work is completed by double engines coordinately, fault detection is divided into testing itself and testing the other engine, the former test is completed by dual engines' internal self-test program, which is used to test the hardware and software fault of itself, once the fault is confirmed, initiatively cut the square wave output; the latter test is completed by communicating with the other engine, which is used to test the fault of the other engine, engines use heartbeat process to send heartbeat signals in order to report their own situations, and monitor whether the opposite engine's heartbeat signal is normal in order to detect whether it fails. If standby engine detects that the host engine fails, then it sends conversion signal to host engine, host engine

start the appropriate wrong judgment mechanism to judge whether the running host engine is failing, if it is true, then stop the square wave output and the switching circuit automatically falls to the side of standby engine, standby engine will gain the control right; if host engine detects that the standby engine fails, host engine sends notification signal to the standby engine, standby engine confirms its fault through self-test program and cuts the square wave output to avoid false switching.

3.5. Fault Alert

Under the situation that CAN communication is normal while other units fail, double engines can send fault points to the client via CAN bus, and client can switch engines and test program manually, which can achieve the interaction between human and computers.

4. Reliability Analysis of Dual Computer Hot Stand-by Control System

4.1. Reliability Analysis Method

Dual computer hot stand-by system's failure is a random and dynamic process [9], before researching on its reliability and security, it needs to analyze the failure mode of the system, and then contrast the mathematical model. This paper mainly studies 3 factors' influence on system's reliability and security, the factors are failure rate, fault detection rate and fault detection rate, assume that failure rate is λ, scale factor that unit failure causes dangerous output is α, fault detection rate is c, common cause failure factor is β, divide failure modes combining with these 3 factors above, 8 division results can be obtained, they are shown as follows:

$$\text{Safe-Detected-Normal-Failure-Rate } \lambda_{sdn} = (1-\beta)\lambda_{sd} = (1-\beta)c(1-\alpha)\lambda \quad (1)$$

$$\text{Safe-Detected-Common-Cause-Failure-Rate } \lambda_{sdc} = \beta\lambda_{sd} = \beta c(1-\alpha)\lambda \quad (2)$$

$$\text{Safe-Undetected- Normal -Failure-Rate } \lambda_{sun} = (1-\beta)\lambda_{su} = (1-\beta)(1-c)(1-\alpha)\lambda \quad (3)$$

$$\text{Safe-Undetected-Common-Cause-Failure-Rate } \lambda_{suc} = \beta\lambda_{su} = \beta(1-c)(1-\alpha)\lambda \quad (4)$$

$$\text{Dangerous-Detected- Normal -Failure-Rate } \lambda_{ddn} = (1-\beta)\lambda_{dd} = (1-\beta)c\alpha\lambda \quad (5)$$

$$\text{Dangerous-Detected-Common-Cause-Failure-Rate } \lambda_{ddc} = \beta\lambda_{dd} = \beta c\alpha\lambda \quad (6)$$

$$\text{Dangerous -Undetected- Normal -Failure-Rate } \lambda_{dun} = (1-\beta)\lambda_{du} = (1-\beta)(1-c)\alpha\lambda \quad (7)$$

$$\text{Dangerous -Undetected-Common-Cause-Failure-Rate } \lambda_{duc} = \beta\lambda_{du} = \beta(1-c)\alpha\lambda \quad (8)$$

4.2. Reliability Analysis Model

Currently, Markov process is the most appropriate analytical method in conducting reliability modeling analysis [10-11], using this method for modeling and analysis needs to be based on the following assumptions, namely:

(1) The model does not consider the maintenance, namely that there is no maintenance during system's running, only carry out repair or regular maintenance before system's running.

(2) The host and standby engine have the same failure rate.

(3) System is in a fault-safety state when failing, the dangerous failure state does no exist.

Based on the above assumptions, define the states of dual computer hot stand-by system as follows:

State 0: host and standby engine are all working properly, system is working properly;

State 1: single engine working state 1, host or standby engine appears the detected normal failure.

State 2: single engine working state 2, standby engine appears the undetected normal failure.

State 3: System's fault - safety state;

State 4: System's fault - danger state.

When dual computer hot stand-by system appears different kinds of failures, system state transfers from among the 5 states above, the Markov state transition diagram is shown in Figure 2.

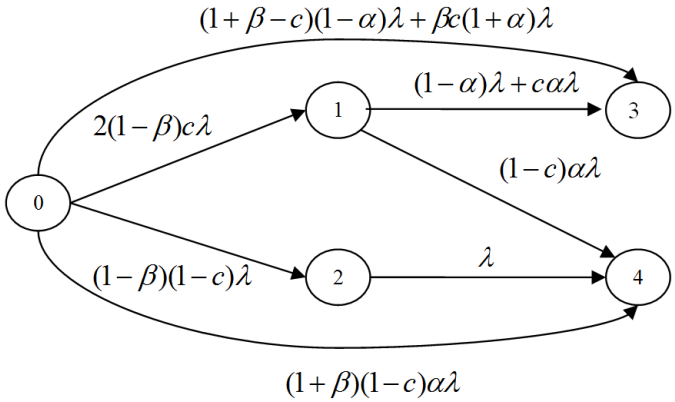

Figure 2. State Transition Diagram of Dual Computer Hot Stand-by System

State 0 $\rightarrow$ State 1: host engine or standby engine appears the detected normal failure, failure engine is been switched, the other engine works properly, and the system is in the single engine working state 1.

State 0 $\rightarrow$ State 2: standby engine appears the undetected normal failure, the system does not switch, host engine works properly, and the system is in the single engine working state 2.

State 0 $\rightarrow$ State 3: host engine and standby engine appear the detected common cause failure, safe undetected common cause failure or dangerous detected common cause failure, two engines are all invalid, the system will be in failure state3; when host engine appears the safe undetected common cause failure, the system will be also in failure state3.

State 0 $\rightarrow$ State 4: host engine and standby engine appear the dangerous undetected common cause failure, the system will be in failure state4; when standby engine appears the dangerous undetected normal failure, the system will be also in failure state4.

State 1 $\rightarrow$ State 3: when the system is in state1, only one engine is working, it will not appear the common cause failure. If engine appears the safe detected failure, safe undetected failure or dangerous detected failure at this time, the system will be in failure state3.

State 1 $\rightarrow$ State 4: when the system is in state2, as standby engine has already appeared the undetected fault, therefore, no matter what kind of failure that host engine appears, the system will be in failure state4;

4.3. Reliability Analysis

According to the Markov state transition diagram of dual computer hot stand-by system, use total probability formula to calculate the system's state transition equation [12], they are shown as follows:

$$\begin{cases} P_0(t+\Delta t) = (1-2\lambda)P_0(t) \\ P_1(t+\Delta t) = 2(1-\beta)c\lambda P_0(t) + (1-\lambda)P_1(t) \\ P_2(t+\Delta t) = (1-\beta)(1-c)\lambda P_0(t) + (1-\lambda)P_2(t) \\ P_3(t+\Delta t) = \left[(1+\beta-c)(1-\alpha)\lambda + \beta c(1+\alpha)\lambda\right]P_0(t) + \left[(1-\alpha)\lambda + c\alpha\lambda\right]P_1(t) + P_3(t) \\ P_4(t+\Delta t) = \left[(1+\beta)(1-c)\alpha\lambda\right]P_0(t) + (1-c)\alpha\lambda P_1(t) + \lambda P_2(t) + P_4(t) \end{cases} \quad (9)$$

in which, $P_i(t)(i = 0,1,2,3,4)$ is the probability that system is in state i at the moment t; $P_i(t+\Delta t)(i = 0,1,2,3,4)$ is the system's state transition probability after Δt interval at the moment t.

Derivate based on the system state transition equations, and obtain the differential equations as follows:

$$\begin{cases} P_0'(t) = -2\lambda P_0(t) \\ P_1'(t) = 2(1-\beta)c\lambda P_0(t) - \lambda P_1(t) \\ P_2'(t) = (1-\beta)(1-c)\lambda P_0(t) - \lambda P_2(t) \\ P_3'(t) = \left[(1+\beta-c)(1-\alpha)\lambda + \beta c(1+\alpha)\lambda\right]P_0(t) + \left[(1-\alpha)\lambda + c\alpha\lambda\right]P_1(t) \\ P_4'(t) = \left[(1+\beta)(1-c)\alpha\lambda\right]P_0(t) + (1-c)\alpha\lambda P_1(t) + \lambda P_2(t) \end{cases} \quad (10)$$

At the initial moment, host and standby engine are all working properly, the system is in state0, therefore, $P_0(0) = 1, P_1(0) = 0, P_2(0) = 0, P_3(0) = 0, P_4(0) = 0$, use MATLAB to solve differential equations in formula(10), obtain the function expressions of $P_i(t)$, as these functions are complex, this paper does not elaborate them.

Reliability and security of dual computer hot stand-by system are separately calculated as follows:

$$R_1(t) = P_0(t) + P_1(t) + P_2(t) \quad (11)$$

$$S_1(t) = R_1(t) + P_3(t) \quad (12)$$

Reliability and security of stand-alone system are separately calculated as follows:

$$R_2(t) = e^{-\lambda t} \quad (13)$$

$$S_2(t) = e^{-\lambda t} + c(1-e^{-\lambda t}) \quad (14)$$

In order to make the result have an universal meaning, the parameter values are set as: $\lambda = 1.39\times10^{-5}$, $\beta = 0.085$, $c = 0.85$, $\alpha = 0.2$, and set the system's running time to be ranging from 0h to 3×10^4 h, use MATLAB to do the simulation experiments, the comparison curves are shown as Figure 3. and Figure 4.

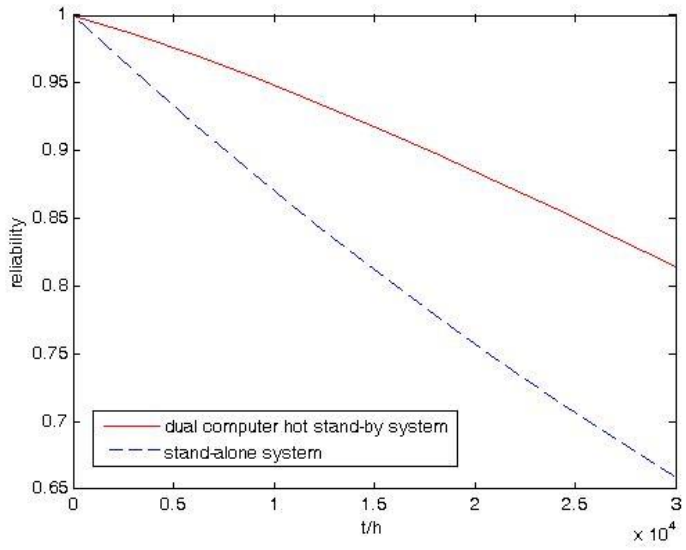

Figure 3. Reliability Comparison Curves

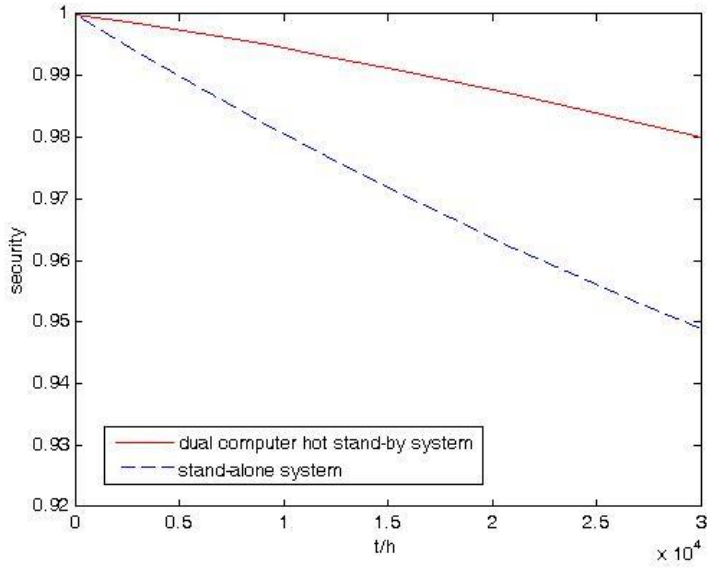

Figure 4. Security Comparison Curves

It can be seen from the figures above that dual computer hot standby system has obvious advantages comparing with stand-alone system on reliability and security. However, as the extension of the device service time, two kinds of systems' reliability and security are all decreasing, but the decreasing rate of dual computer hot stand-by system is lower than stand-alone system.

In order to reflect the dual computer hot stand-by system's reliability more intuitively, this paper uses MTBF (mean time between failures) to examine it, use MATLAB to integrating the two systems' reliability, and obtain the MTBF values of dual computer hot stand-by system and stand-alone system as follows:

$$MTBF_1 = \int_0^\infty R_1(t) = 93570h \quad (15)$$

$$MTBF_2 = \int_0^\infty R_2(t) = 74074h \quad (16)$$

Namely, expected time from running to first failure of electric vehicle controller based on dual computer hot stand-by system is 93570h, which can extend about 19496h comparing with stand-alone system, therefore, electric vehicle controller control strategy based on dual computer hot stand-by system is feasible and it has a higher reliability and security.

5. Conclusions

(1) This paper proposes up an electric vehicle controller control strategy based on dual computer hot stand-by system, and use heartbeat communication mode to replace the independent fault detection unit, it can solve that whole system will fail once the host engine is invalid.

(2) Dual computer hot stand-by system has a higher reliability than single computer system, dual computer hot stand-by system's MTBF value is 93570h, while stand-alone system is about 74070h.

(3) The two systems' security curves show that they all have a high security, but dual computer hot stand-by system is higher than stand-alone system.

(4) The electric vehicle controller control strategy based on the dual computer hot stand-by system proposed in this paper is better than stand-alone system both in reliability and security, and as the extension of the device service time, this advantage is reflected more obvious, therefore, the control strategy can be applied to practical applications.

Acknowledgements

This work is supported by The National 948 Project (2011-4-11) and The Fundamental Research Funds for the Central Universities (2572014AB23).

References

[1] M. Yu and Z.-y. He, "Reliability analysis of repairable hot stand-by redundant system based on Markov model", Computer Engineering and Design, vol. 8, (**2009)**, pp. 2040-2046.
[2] F. Liu and H.-f. Wang, "Performance comparison between two-by-two takes two and the hot stand-by computer interlocking system, RAILWAY SIGNALLING & COMMUNICATION, vol. 2, (**2008**), pp. 26-29.
[3] C. E. Wells, "Reliability analysis of a single warm-standby system subject to repairable and non-repairable failures", European Journal of Operational Research, vol. 5, (**2014**), pp. 180-186.
[4] K. Wang, T. Yen and Y. Fang, "Comparison of availability between two systems with warm standby units and different imperfect coverage", Quality Technology & Quantitative Management", vol. 9, (2**012**), pp. 265-282.
[5] J. E. Ruiz-Castro and G. Fernandez-Villodre, "A complex discrete warm standby system with loss of units", European Journal of Operational Research, vol. 4, (**2012**), pp. 456-469.
[6] Y. Li and X.-y. Meng, "Reliability analysis of warm standby repairable system with priority in use", Applied Mathematical Modeling, vol. 9, (**2011**), pp. 4295-4303.
[7] W. Y. Yun and J. H. Cha, "Optimal design of a general warm standby system", Reliability Engineering & System Safety, vol. 8, (**2010**), pp. 880-886.
[8] R. Moghaddass, M. J. Zuo and M. Pandey, "Optimal design and maintenance of a repairable multi-state system with standby components", Journal of Statistical Planning and Inference, vol. 8, (**2012**), pp. 2409-2420.
[9] B. Çekyay and S. Özekici, "Mean time to failure and availability of semi-Markov missions with maximal repair", European Journal of Operational Research, vol. 8, (**2010**), pp. 1442-1454.
[10] S. Malefaki, N. Limnios and P. Dersin, "Reliability of maintained systems under a semi-Markov setting", Reliability Engineering & System Safety, vol. 11, (**2014**), pp. 282-290.

[11] F. Barsotti, Y. De Castro and P. Rochet, "Estimating the transition matrix of a Markov chain observed at random times", Statistics & Probability Letters, vol. 11, **(2014)**,pp. 98-105.
[12] Q. Zhang, "Explicit solutions for an optimal stock selling problem under a Markov chain model", Journal of Mathematical Analysis and Applications, vol. 12, **(2014),** pp. 1210-1227.

Authors

Guo Yan-ling, Female, she was born in 1962, supervisor, working in College of Mechanical and Electrical Engineering of Northeast Forestry University, mainly engaged in electromechanical integration technology, Agriculture and forestry picking machine and robot technology.

Liu Li-chen, Male, he was born in 1983, Ph.D., studying in College of Mechanical and Electrical Engineering of Northeast Forestry University, mainly engaged in electromechanical integration technology , vehicle control.

Gao Meng, Female, she was born in 1989, Ph.D., studying in Information and Computer Engineering College of Northeast Forestry University, mainly engaged in forestry informatization, system security.

Wang Meng, Male, he was born in 1990, Post Graduate, studying in Traffic College of Northeast Forestry University, mainly engaged in System controller technology for electric power steering.