A MICROPROCESSOR-BASED HYBRID DUPLEX FAULT-TOLERANT SYSTEM

L. Zhaohui,Y. Luqing and W. Shouping

Department of Electrical Engineering, Huazhong University of Science and Technology, Wuhan, Hubei, China

O.P. Malik, G.S. Hope and G. Hancock

Department of Electrical Engineering, The University of Calgary, Alberta, Canada

Abstract Reliability is one of the fundamental considerations in the design of industrial control equipment. The microprocessor-based Hybrid Duplex fault-tolerant System (HDS) proposed in this paper has high reliability to meet this demand although its hardware structure is simple. The hardware configuration of HDS and the fault tolerance of this system are described. The switching control strategies in HDS are studied in detail. The disputes between two modules are avoided. The reliability estimation methods are also given.

چکیده قابلیت اطمینان، یکی از مهمترین مسائل است. در طراحی یک سیستم کنترل صنعتی سیستم مایکروپروسسوری (HDS) که در این مقاله پیشنهاد شده علیرغم ساختار سخت‌افزاری ساده از قابلیت اطمینان بالائی برای پاسخگوئی به این نیاز برخوردار است. در این مقاله مشخصات سخت‌افزاری و (HDS) نحوهٔ سازگاری آن با خطاهای مختلف شرح داده شده و جزئیات نحوهٔ کنترل سوئیچها در آن بیان گردیده. از تعارض بین دو مدول مختلف پرهیز شده. روش تخمین قابلیت اطمینان نیز عرضه شده است.

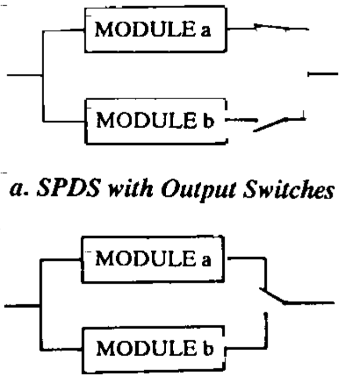
INTRODUCTION

Microprocessor-based systems are widely applied to industrial control. In any such system, reliability is an important consideration. Many kinds of fault-tolerant systems have been proposed and built [1]. Among them, duplicate systems are well known because of their simple hardware and high reliability.

According to their reliability diagrams, the duplicate systems used today are classified into two types:

Series-Parallel Duplex fault-tolerant System (SPDS).

Parallel-Series Duplex fault-tolerant System (PSDS).



a. SPDS with Output Switches

b. SPDS with Select Switches

Figure 1. Hardware configuration of SPDS

SPDS is comprised of two parallel modules with the same function (Figure 1). Although each module is able to perform complete control function independently, control performance of the two modules may be different. One module may possess more sophisticated hardware to support its control tasks than the other so that the system has a high cost effectiveness.When the module with higher performance is normal, it is active and the other module is standby. The switching between two modules is carried out by either output switches or select switches.

The reliability block diagram of SPDS is shown in Figure 2. Let M_a and M_b represent, respectively, the states of module a and module b. Also let S represent the state of the switches. Lastly the state of system is represented by N_s. Using 1 to describe Normal and 0 to describe Fault the follwing Boolean equations are developed.

$$N_s=(M_a+M_b)^*S \qquad (1)$$

If each module has n blocks and B_{xj} stands for the state of block j in module $x\,(x=a$ or $b)$, then:

$$N_s=(B_{a1}{}^*B_{a2}\cdots{}^*B_{an}+B_{b1}{}^*B_{b2}\cdots{}^*B_{bn})^*S \qquad (2)$$

In contrast with SPDS, PSDS is composed of a group of fault-tolerant units and each unit consists of two parallel blocks with the same function. The reliability diagram is shown in Figure 3. If S_j stands for the state of switches and B_{xj} stands for the state of block x in unit j, then normal system condition can be represented as:

$$N_p=(B_{a1}+B_{b1})\cdots{}^*(B_{an}+B_{bn})^*S_1{}^*S_2\cdots{}^*S_n \; (3)$$

The hardware configuration of SPDS is simpler and development cost is lower. However, its reliability cannot meet the demand of industrial control in some cases.

If switches were absolutely reliable, PSDS would have higher reliability than SPDS. Unfortunately, the failure rate of switches cannot be ignored and it is much higher in PSDS than in SPDS. The reliability of PSDS is deeply influenced by switches. It is even lower than the reliability of SPDS. So PSDS is generally not suitable for most industrial controllers.

To improve the overall reliability of the system, a hybrid Duplicate fault-tolerant System (HDS) is proposed. HDS combines the advantages of both SPDS and PSDS. It implements the fault tolerance techniques used in the PSDS on the basis of the hardware type configuration of SPDS.

HARDWARE CONFIGURATION OF HDS

The hardware configuration of HDS (Figure 4) is quite similar to SPDS. It includes two parallel modules with the same function and communication interfaces between the two microprocessors. Each module can complete the

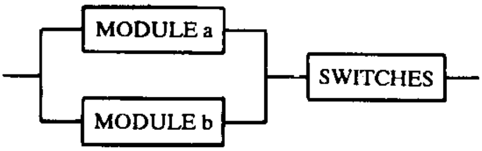


Figure 2. Reliability block diagram of SPDS

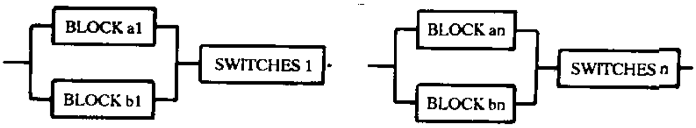


Figure 3. Reliability block diagram of PSDS

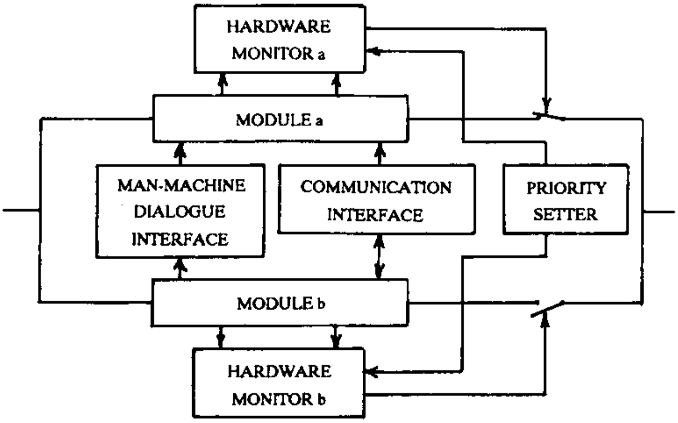


Figure 4. Hardware configuration of HDS

control tasks of the system independently. Two modules share a man-machine dialogue interface.

Output switching between the two modules is carried out by the output switches. The two relevant outputs from different modules are joined together after their output switches as the output of the system. Only one of these two output switches may be closed at any one time, i.e:

1. If both outputs are normal, the switch with higher priority will be closed.
2. If one output is normal and the other is faulty, the switch on the module with normal output will be closed.
3. If both outputs are faulty, both switches will be opened.

The output switches are operated separately. As an example, suppose that the system has three outputs A, B and C. It is possible that A and C are from one module and B is from another.

Each module has a hardware monitor. This monitor is used to supervise the execution of the programs in the module according to the sequences appointed and to operate output switches according to the test results of both software and hardware. Priority exists between two monitors to ensure that only one of the two relevant switches is closed when both outputs are normal. The priority is set by the operator and can be changed during operation.

Some extra hardware such as output feedback may be added for some applications.

It is considered good to design input, processing and output hardware on different boards.

FAULT TOLERANCE PRINCIPLE IN HDS

Information flow in each module of HDS is divided into three levels: input, processing and output instead of the division of hardware as in PSDS. Input level and output level can be further divided into blocks. Each block inputs or outputs a single message or a group of messages. Processing level can also be further divided into blocks. Each block produces a control strategy or a series of control strategies according to corresponding input(s).

In addition to the three levels mentioned above, a hardware block is defined as an executive block in each module. This block is crucial for the module because it makes the information "flow." The executive block includes all the hardware which is necessary for programs to be executed in normal sequence such as microprocessor, data bus and control bus, etc. The module will fail if its executive block breaks down.

Two modules run in parallel. In case the communication between the two modules is normal, the system information will flow as described below:

1. The inputs of one module are all transferred to the other module as well as entering their own processing level. So each module has two inputs for the same message. They are compared and tested in each module. When both inputs in the module are normal, any one of them or the average of them enters the processing level. If one is faulty and the other normal, the normal one enters the processing level and if both are faulty, the relevant processing block(s) cannot produce correct results. Procedure to test whether a module is normal or faulty is described later.
2. All processed results of the two modules are exchanged via communication. They are treated in a similar way as inputs.
3. If both relevant output blocks have normal output, the output switch with higher priority is closed. If both relevant output blocks do not have normal output, the system fails. Otherwise the output switch connected to the block which has normal output is closed.

   The paths of information flow are shown in Figure 5.

If the communication breaks down, HDS downgrades as SPDS. The reliability diagram of HDS is shown in Figure 6. Let B_{xi}, and E_x represent respectively the state of block i and the executive block in module x (x=a,b; i=1, 2, ... m) and C,S represent, respectively, the

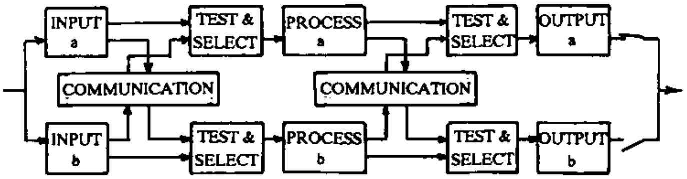


Figure 5. Information flow paths in HDS

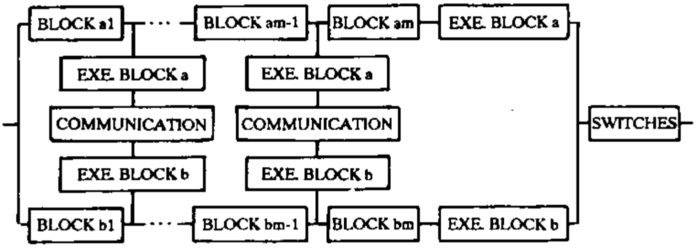


Figure 6. Reliability block diagram of HDS

states of communication and output switches. Generally failure rate of software for industrial control is far smaller than that of hardware so it is ignored. If N_h stands for the state of system, the following boolean equation is obtained.

$$\begin{aligned}N_h=S^{*}(C^{*}(B_{a1}{}^{*}E_a+B_{b1}{}^{*}E_b)\cdots{}^{*}\\ (B_{am}{}^{*}E_a+B_{bm}{}^{*}E_b)\\ +C^{*}(B_{a1}{}^{*}\cdots{}^{*}B_{am}{}^{*}E_a+B_{b1}{}^{*}\quad{}^{*}B_{bm}{}^{*}E_b))\end{aligned}\tag{4}$$

After suitable transformation, equation (4) can be expressed as:

$$\begin{aligned}N_h=S^{*}(M_a+M_b)+S^{*}C^{*}\\ E_a{}^{*}E_b{}^{*}((B_{a1}+B_{b1})^{*}(B_{a2}+B_{b2})\cdots{}^{*}\\ (B_{am}+B_{bm})-B_{a1}{}^{*}\cdots{}^{*}B_{am}-B_{b1}{}^{*}\cdots{}^{*}B_{bm})\end{aligned}\tag{5}$$

Comparing equation (5) with equation (1), it can be seen that the reliability of HDS is always higher than that of SPDS. If equation (3) is transformed to a form similar to that of equation (4), then:

$$\begin{aligned}N_p=S_1{}^{*}\cdots{}^{*}S_a{}^{*}(M_a+M_b)\\ +S_1{}^{*}\cdots{}^{*}S_n((B_{a1}+B_{b1})\cdots{}^{*}(B_{an}+B_{bn})\\ -B_{a1}{}^{*}\cdots{}^{*}B_{an}-B_{b1}{}^{*}\cdots{}^{*}B_{bn})\end{aligned}\tag{6}$$

Suppose that $n=m+k$ and $B_{x1}\cdots B_{xk}$ in PSDS are equivalent to the executive block in HDS. Also, let

$C_p=S_1\cdots{}^{*}S_n{}^{*}(B_{a1}+B_{b2})\cdots{}^{*}(B_{ak}+B_{bk})$ and $C_h=S^{*}C^{*}E_a{}^{*}E_b$. Then the reliability of HDS is higher than that of PSDS in case the probability of $C_h=1$ is larger than the probability of $C_p=1$.

In PSDS, the division of blocks is implemented by hardware. With the further division of blocks, the hardware for switching (includes switches, block test and switching control hardware) increases very fast. Practically always, n is kept smaller than m. Even so, the failure rate of switches in PSDS is much higher than in HDS for most industrial controllers. So HDS is more suitable for industrial control than PSDS and SPDS.

Each module in HDS can be removed for repair and be put back after repair without interrupting the work of another module. The module repaired starts its work from the present state of the system. If the input, processing and output hardware are designed on different boards, the input and/or output can be removed for repair without interrupting the work of the rest of the blocks on that module.

SWITCHING CONTROL IN HDS

Switching control is a key problem for duplicate systems because of the existence of dispute between two modules [2].

Switching control is carried out in different ways according to switch types. Output select switches are controlled by two blocks or two modules together. Output switches are controlled only by their own block or module. In both cases, switching control must be performed on the basis of test results.

The main idea of the first method may be described as follows: Let M_{aa} and M_{bb} represent respectively the self test result of module a and module b. Let $M_{xy}(x,y=a,b\ x\neq y)$ represent the test results of module x to module y. Then, M_{aa}, M_{ab}, M_{ba} and M_{bb} have sixteen combinations and only four of them are concordant between the two modules. If the switches connected to module x are controlled simply according to M_{ax} and M_{bx}, it is evidently unreasonable.

After analyzing the test results, a set of rules can be obtained to minimize the dispute between the two modules. For example:

1. If module x thinks that is faulty, it is faulty.
2. If module x is faulty and module y thinks that module x is normal, module y is faulty.

According to the above rules, only one case of dispute exists between the two modules. It is (1 0 0 1). If this case is considered as both modules being faulty, the control strategy for the switches connected to module x is:

$$CS_x = M_{xx}^{*}\,(\,M_{yx}^{*}\,M_{yy} + M_{yx}^{*}\,M_{xy} + M_{xy}^{*}\,M_{yy}\,) \quad (7)$$

Here $x,y=a,b$ and $x\neq y$. The output switches connected to module x are closed as $CS_x=1$ and opened as $CS_x=0$.

This control strategy is available for the blocks or modules which possess the ability to do self tests such as the modules in SPDS. However, the dispute is still not fully resolved and wrong switching may occur.

The HDS, the second way of switching control mentioned above is preferred. Control strategies of switching at input, processing and output levels are described below.

1. Switching control at input level and at processing level.

Input(s) of each input block and processing result(s) of each processing block are in two modules. They are tested by the use of software in two modules at the same time. The software judges the states of blocks by analyzing their results.

Each input has some laws to follow. These laws can be found off-line and be stored in memory. They can also be accumulated on-line by the use of artificial intelligent techniques.

Processing procedure is defined by the designer. So the processing results under certain inputs can be estimated in a simple way.

For block i in module $z(z=a,b)$, there are two test results B_{zia} and B_{zib} produced by module a and by module b respectively. The test results are also exchanged between the two modules via communication. The results exchanged are labeled in B'_{zib} and $|B'_{zia}$. So in module $x(x=a,b)$, whether the results of this bolck can enter the next level is determined by the following conditions:

i). If $B_{zix}=B'_{ziy}=1$, they can enter the next level. And if $B_{zix}=B'_{ziy}=0$, they cannot.

ii). When $B_{zix}=B'_{ziy}$, this block will be tested again in module x. If the result this time is 1, they can enter the next level. Otherwise, they cannot.

Here, $y=a,b\ \ y\neq x$.

2. Switching control at output level.

Output blocks can be tested in two ways:

i). For the closed-loop control system, output blocks can be tested according to the feedback from the controlled system, i.e. the inputs of the controller. This method is not suitable for systems with large inertia because some accidents may have occurred before the controller gets feedback information.

ii). Adding hardware to feed back information from suitable places into module.

Let B_{xj} stand for the state of output block j in module x. B_{xi} and B'_{yi} represent, respectively, the states of relevant processing blocks in module x and module y. Following boolean equation can be developed:

$$CS_{xj}=E_x^{*}\,B_{xj}^{*}\,(\,B_{xi}+B'_{yi}\,) \quad (8)$$

Here, $x,y=a,\ b\ \ x\neq y$. When $CS_{xj}=1$, the output switch connected to this channel may be closed. Otherwise, it must be opened.

It can be seen that in HDS all switches are controlled only according to the test results of their own module. The test results made by the other module are only used as reference. In this way, disputes between two modules are avoided.

RELIABILITY ANALYSES OF HDS

The following three hypotheses are given to simplify the reliability estimates of HDS:

1. Reliability of each part (such as blocks, communication interface and switches) follows the exponential distribution.
2. Failure of each part is independent from the other parts.
3. Blocks with same function have same failure rate.

Let λ_x present the failure rate of part$x(x=i$ for block i, c for communication interface, s for switches and e for executive block). The reliability of HDS without repair can be presented as below:

$$R_h = 2^* e^{-\lambda t} - e^{-2\lambda t} + e^{-\lambda_\sigma t} * \left[\prod_{i=1}^{m} (2 * e^{-\lambda_i t} - e^{-2\lambda_i t}) - (2^* e^{-\sum_{i=1}^{m} \lambda_i t} + e^{-2\sum_{i=1}^{m} \lambda_i t}) \right] \tag{9}$$

Here, $\lambda = \sum_{i=1}^{m} \lambda_i + \lambda_e$, $\lambda_\sigma = 2^* \lambda_e + \lambda_s$.

The reliability of HDS with repair is difficult to obtain directly according to Markov stochastic process. Depending on equation (5), HDS can be divided into three subsystems as shown in Figure 7 and the reliability of HDS is the algebraic sum of the reliability of these three subsystems.

So the reliability of HDS with repair can be presented as below:

$$R_{hr} = R_{1r} + R_{2r} - R_{3r}$$

Here R_{1r}, R_{2r} and R_{3r} represent, respectively, the reliability of subsystem 1,2 and 3 under repairing condition. R_{2r} can be further presented as:

$$R_{2r} = \prod_{i=1}^{m} R_{bir} {}^* e^{-\lambda_\sigma t}$$

Here R_{bir} is the reliability of i^{th} small SPDS in subsystem 2.

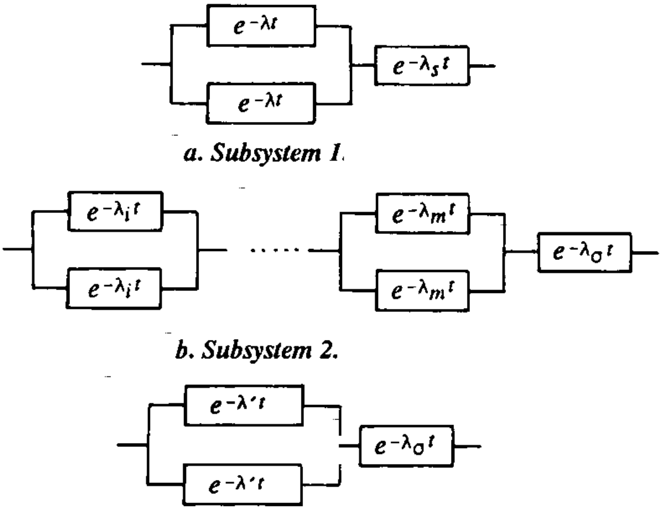
Note: 1. The repair rate of subsystem 1 is the weighted average of the repair rates of m+1 parts (block 1–block m and executive block).

2. The repair rate of subsystem 3 is the weighted average of the repair rates of m blocks (block 1–block m).

3. If each block is designed on different board, subsystem 2 can be considered as series of m small SPDSs ans the total failure rate of switches is λ_σ.

Furthermore, the MTBF (mean time between failure) and the availability of HDS can be treated in a similar way.

The reliability comparisons among SPDS, PSDS and HDS for a specific application are developed in [3].



a. Subsystem 1.

b. Subsystem 2.

c. Subsystem 3.

Figure 7. Reliability block diagram of HDS subsystems

CONCLUSIONS

Microprocessor-based hybrid duplicate fault-tolerant system proposed in this paper has the following features:

1. Its hardware configuration is simple and flexible.
2. It has high reliability due to its fault tolerance at block level, low failure rate of switches and repairable construction.
3. Software development cost (especially for test and fault tolerance software) is higher than that in SPDS. Both software and hardware development costs are lower than that in PSDS.
4. Successful switching control must depend on correct test results.

HDS is suitable for industrial control.

The fault tolerance and switching control strategies proposed for HDS in this paper can be applied to other multi-processor based fault-tolerant systems.

HDS has been successfully applied to governor for water turbine [3].

REFERENCES

1. W.C. Carter, and W.G. Bouricius. *Computing*, 4, 9 (1971).
2. B. Randell. IEE Trans on S.E. SE-1, 2 (1975).
3. Y. Luquing, W. Shouping and L.Zhaohui. "Repairable Hybrid Duplicating Fault Tolerant Microprocessor-Based Governor and Its Reliability Analysis." Proceedings, Mini and Microcomputer and Their Applications, Sant Feliu de Guixols, Spain (1988).