RC-001

A Study of n-Fault-Tolerant System with Voting Switches
多数決スイッチ回路による n-フォールトトレラントシステムの研究

Hitoshi IWAI
岩井仁司

1. Introduction

In this paper, n-fault-tolerant system with voting switches is proposed to mask any faults in the whole system that includes voters also. The system that has the same plural function modules to work the same processing and majority voting circuit of these outputs is called NMR (N-Modular Redundancy). In the conventional way, multiplication of voting circuits is known as the measures for some failures of voting circuits. However, after all, one more voting circuit for the multiplied voting circuit outputs is needed on their external [4][5]. This problem is caused so that the voting circuit is zero faults tolerant. But we have found a fault-tolerant voter circuit that can mask any faults in it up to the appointed “n”. This circuit consists of switches only. The system with such kind of voters shall be called Voting Switches Redundancy “VSR”. The VSR is more superior to the conventional ways; i.e. NMR, Hybrid redundancy, Self-purging Redundancy and Sift-out modular Redundancy on their reliabilities and system-simplicities.

2. Baseline points for effective solving the problem

Generally a voting circuit consists of some logic gates like AND gates, OR gates and so on. A Sample of a voting circuit is shown in Fig-1. However, a voting circuit can consist of switches only like Fig-2 [11, 12]. Its output must be correct even if any one switch gets one fault while multiplied function units A, B, C have no faults.

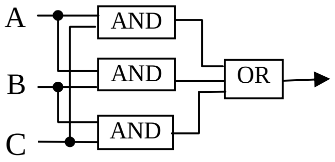


Fig.-1 General Voting Circuit

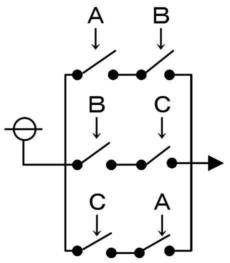


Fig.-2 Voting circuit consisted of Switches only (Voting Switches)

３．One-fault-tolerant case (Triple Modular Redundancy)

First, the system configuration to be proposed is shown in Fig-3 about triple modular redundancy case for one-fault-tolerance. If one function module is out-of-order, it should be invalidated by both of other ones in one period. Then the feature is shown as the below.

1) Each function module has the voting switches like Fig-2 for its own power control. Other function modules can turn them off by sending off-signals at the same time. The voting switches consist of two parallels multiplied by one series switches. Each switch is controlled by different function modules. The capital letter of switch-ID means the function module ID that produces the output. The small letter means the voting switches group-ID.

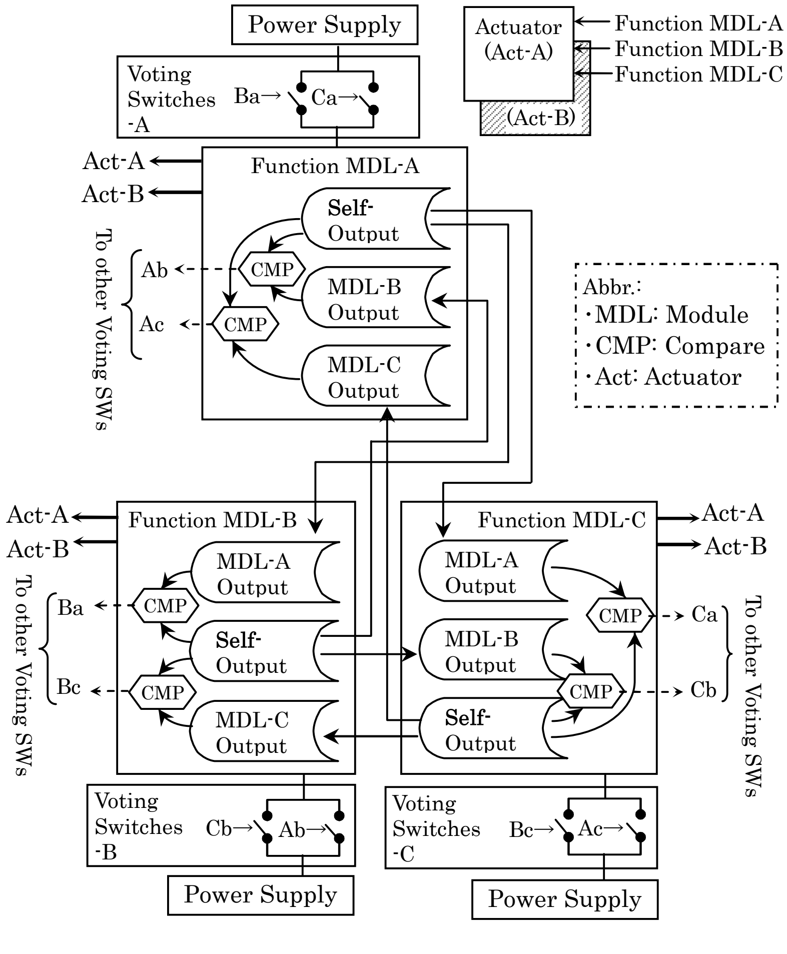


Fig.-3 Configuration of 1FT by Triple Module Redundancy

2) All function modules are connected with data communication lines to each other and they can exchange data.
3) The synchronization mechanism among the function modules is needed. (ex. Mutual Feedback [6,pp.126] [10])

In this configuration, the action is shown as the below.

1) Each function module performs the same process at the same period.
2) Each function module exchanges its output data with other ones, and compares its own data with the other's data.
3) If a function module finds any differences between its data and the others, it sends switch-off signal to the voting switches of the function module. When the voting switches receive switch-off signals from other two function modules, it will be powered off.
4) The function module outputs the own processed data to the external, like an actuator.
5）It goes to step 1) and performs periodically.

4. Two or more fault-tolerant case on the assumption that two or more faults must not happen in one control period. (Quadruple or more modular Redundancy)

The assumption that two or more faults do not happen in one control period must be adequate when the fault rate is very small. On this assumption two-fault-tolerant system can be configured from four function modules at least. Because after the first failed module is invalidated, voting of the rest three modules can mask the second fault.

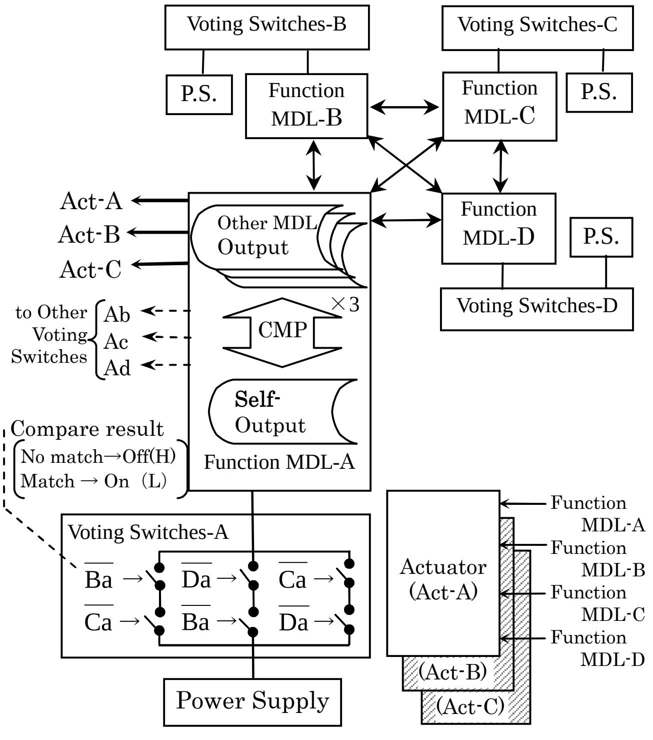


Fig.4 Configuration of 2FT by Quadruple Module Redundancy [2]

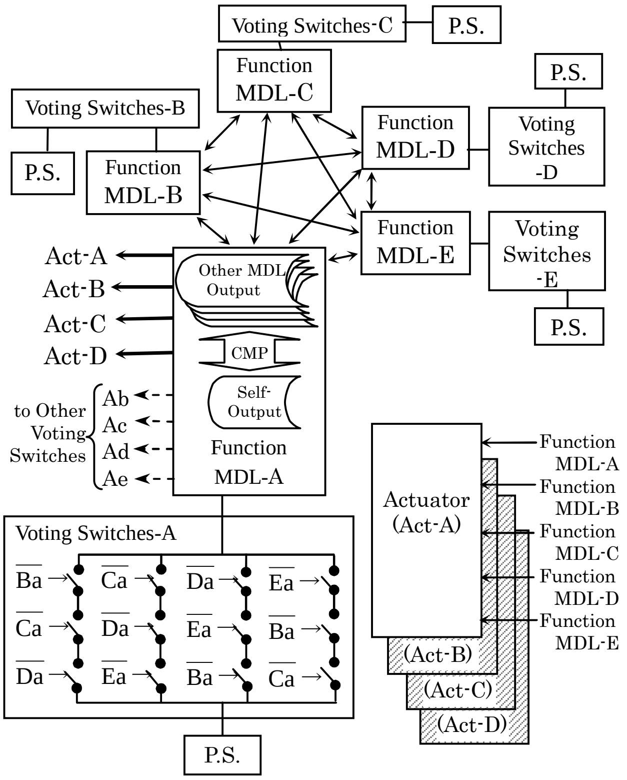


Fig.5 Configuration of 3FT by Quintuple Module Redundancy [2]

The configuration of 2FT system by Quadruple Modular Redundancy is shown in Fig.4. Each group of voting switches consists of six switches (=three parallel multiplied by two series) and is controlled by other three function modules without the self-function module. The capital letter of switch-ID means the function module ID that outputs the switch control signal. The small letter means the voting switches group-ID that is controlled. The box of voting switches in the figure has two same switch-IDs and these are from same function module.

When two or more other function modules of three know the difference between their each output data and one's of a function modules, they are going to powered off the function modules.

In order to invalidate switch control signals from a powered-off function module, the high level should mean to turn switch-off and the low level should mean to turn switch-on, because the signal from a powered-off module must be low and the status low does not influence to the voting switches. The bar of switch-ID in the figure means the inverse of logic status.

Next, the configuration of 3FT system by Quintuple Modular Redundancy is shown in Fig.5. Quintuple Modular Redundancy can reach three-fault-tolerance.

Finally, the configuration of n-FT system by (n+2) Modular Redundancy is shown in Fig.6. This configuration needs n+2 function modules. These system should be called (n+2)MR for our argument.

The series number of voting switches in this configuration must be "n" or more. Because if less than "n" the function module cannot be invalidated when all switches in a series have stuck-on-faults and the connected function module has some failures, "n" or more switches are needed for n-fault-tolerant.

Next the parallel number of voting switches must be the number of combinations of a population of the majority voting taken the series number. The number of function modules is n+2. But the connected module to the voting switches group can be omitted from the population of the majority voting, because the module cannot fairly judge to its own data. Then the population of majority voting can be (n+1) and the combination number is $_{n+1}C_n$ (= n+1).

And the switch control line from a function module must have some branch lines to different voting switches, the number of braches is equal to (Series number)×(Parallel number) ／ (Population of majority voting) = n×(n+1)／(n+1) = n.

In order to invalidate powered-off function modules, the signal-high of the switch control lines from the modules should mean to turn the switches off and the signal-low should mean to turn the switches on. This rule invalidates powered-off function modules from voting automatically.

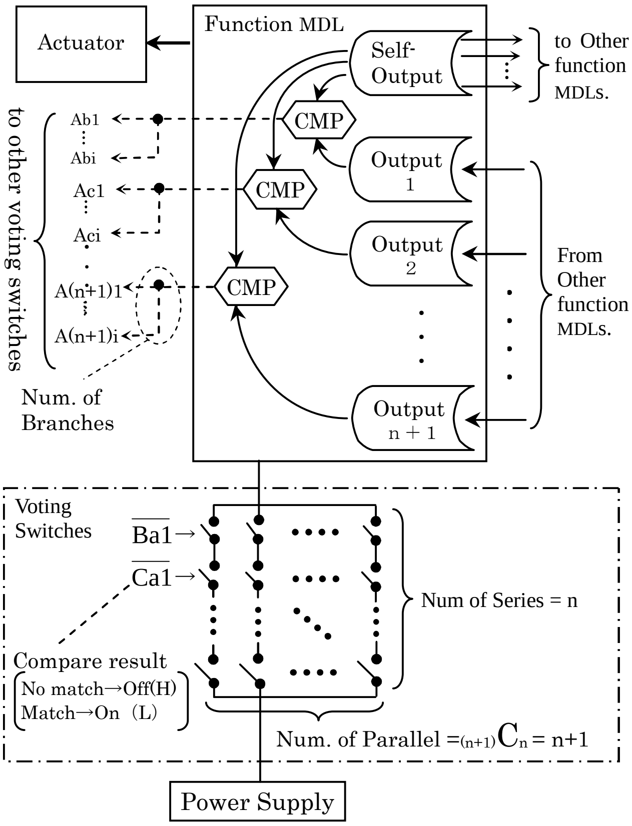


Fig.6 Configuration sample of a function module for n-FT on the assumption that two or more faults must not happen in the same control period.[1][2]

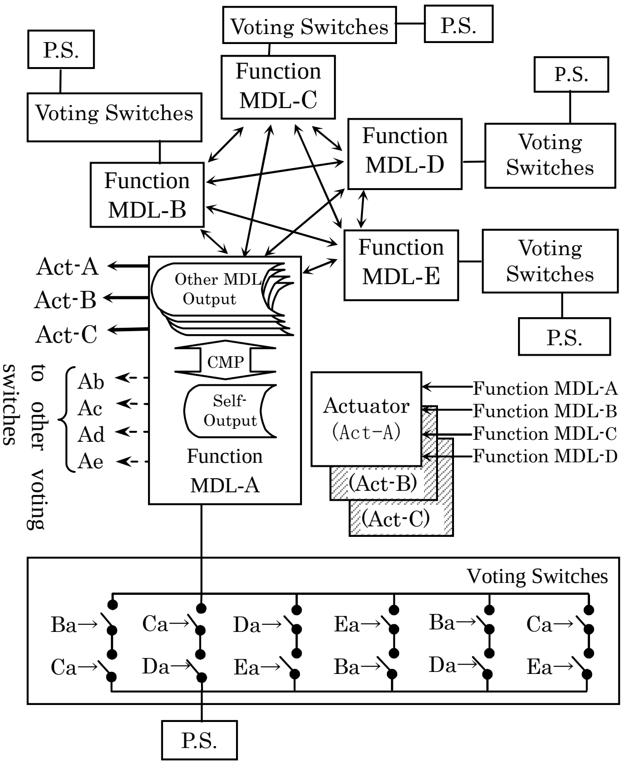
5. Two or more fault-tolerant case on the assumption that majority voting must be correct. (Quintuple or more modular Redundancy)

Next, we assume that two or more faults may happen in one control period. For example, the configuration of 2FT system by Quintuple Modular Redundancy is shown in Fig-7. Two-fault-tolerant system needed five function modules.

Generally in order to tolerate n-faults, (2n+1) function modules are needed. If a function module get some faults, “n” serial inhibits are needed for n-fault-tolerance. And $_{2n}C_n$ parallel switches are needed for majority voting but not $_{2n+1}C_{n+1}$, because the self function module can be exceptive. Then in fig-7 each voting-switches-group have two serial and six parallel swithes. These system should be called (2n+1)MR for our argument.

In order to avoid the influence of powered-off function modules, on the opposite side of (n+2)MR, the signal-high of the switch control lines from the modules should mean to turn the switches on and the signal-low should mean to turn the switches off.

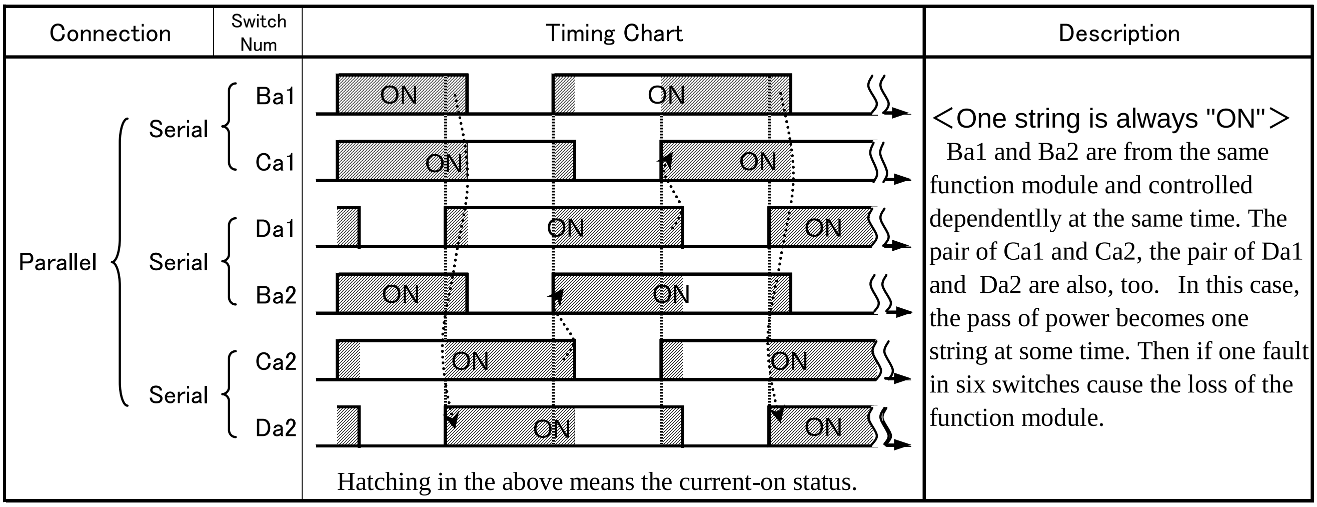
To summarize the above discussion, Table-1 is shown.



Fig−7 Configuration of 2FT by Quadruple Module Redundancy on the assumption that majority voting must be correct [2]

Table-1 Voting Switches Parameters on the case that a single fault in one period and the case that majority voting must be correct [1][2]

		On the assumption that two or more faults must not happen in one control period.	On the assumption that majority voting must be correct
Minimum number of Function Modules		n+2	2n+1
Voting switches	Series Num.	n	n
	Parallel Num.	n+1	$_{2n}C_n$
	Branch Num.	n	$_{2n-1}C_{n-1}$



<One string is always "ON">
Ba1 and Ba2 are from the same function module and controlled dependentlly at the same time. The pair of Ca1 and Ca2, the pair of Da1 and Da2 are also, too. In this case, the pass of power becomes one string at some time. Then if one fault in six switches cause the loss of the function module.

Fig-8 Timing Chart of check-out for any stuck-on-faults in Fig-4.[1]

6. Counting internal faults

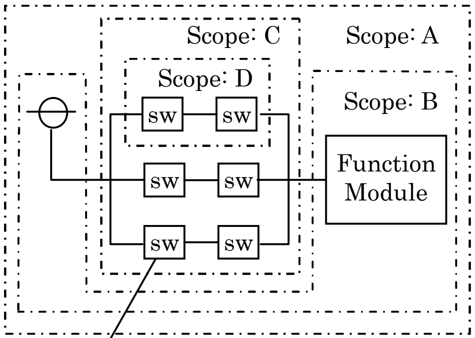
If any faults can not be detected in a system, they increase there internally and the service may fall down suddenly. Then it is necessary that any faults can be detectable and countable.

In order to detect any faults in voting switches, switch status monitors are needed for all the switches. Then any stuck-OFF-faults can be detected.

However, some stuck-ON-faults cannot be detected, because usually all switches stay “ON”. Then a parallel circuit in voting switches is turned On/Off alternatively while always power on to check out any stuck-ON faults. Fig-8 is the timing chart of check-out for the configuration of 2FT by Quadruple Module Redundancy, Fig-4.

7. Reliability of voting switches group

Finally we study the reliability of the proposed n-fault-tolerant system. For the first step of the study, the fig-9 is shown as one function module, voting switches group and power supply that belong to the function module.



Reliability of Scope A : R_A
Reliability of Scope B : R_B
Reliability of Scope C : R_C
∴ $R_A = R_B \times R_C$
Reliability of one switch : s

Fig-9 Reliability of one function module, voting switches and power supply.

Switch has two fail modes: Stuck-On fault and Stuck-Off fault. And one appears and the other does not appear according to some situation. To simplify an argument we assume any faults must cause some errors from the argument here.

The reliability of scope-A is shown as the below.

- Fail Probability of scope-D: $1-s^2$
  (=the Complement of Reliability)
- Fail Probability of all three parallel scope-D’s: $(1-s^2)^3$
- Reliability of scope-C: $1-(1-s^2)^3 = 3s^2 - 3s^4 + s^6$

∴ $R_A = R_B \times (3 \times s^2 - 3s^4 + s^6)$ ··· EQ (1)

The factor of EQ (1) is drawn as fig-10. If the reliability of one switch is greater than about 0.4, the reliability of the group becomes better than it.

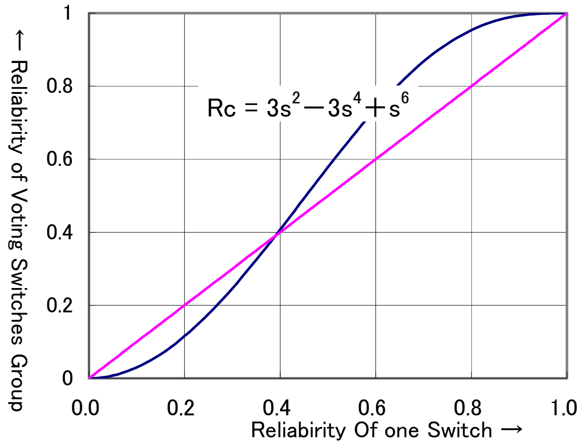


Fig-10 Reliability of one Voting Switches Group

8. Comparison of reliabilities between (n+2)MR and (2n+1)MR

Then the reliability of 2FT system by Quadruple Modular Redundancy like fig-4 is shown as the below.

$$R = R_A^4 + 4\times R_A^3\,(1-RA) + 6\times R_A^2\,(1-R_A)^2$$
$$= 3\,R_A^4 - 8\,R_A^3 + 6\,R_A^2$$

Generally the reliability of an n-fault-tolerant system that consists of (n+2) function modules on the assumption that two or more faults must not happen in one control period is shown as the EQ (2). And the graph of EQ (2) is drawn as fig-11. This system shall be called (n+2)MR for our argument now.

$$R_{(n+2)MR} = \sum_{i=0}^{n} {}_{n+2}C_i \times R_A^{\,n+2-i} \times (1-R_A)^i \quad \cdots \text{EQ (2)}$$

Next the reliability of an n-fault-tolerant system that consists of (2n+1) function modules on the assumption that majority voting must be correct is shown as the EQ (3). And the graph of EQ (3) is drawn as fig-12. This system shall be called (2n+1)MR for our argument now.

$$R_{(2n+1)MR} = \sum_{i=0}^{n} {}_{2n+1}C_i \times R_A^{\,2n+1-i} \times (1\text{-}R_A)^i \quad \cdots \text{EQ (3)}$$

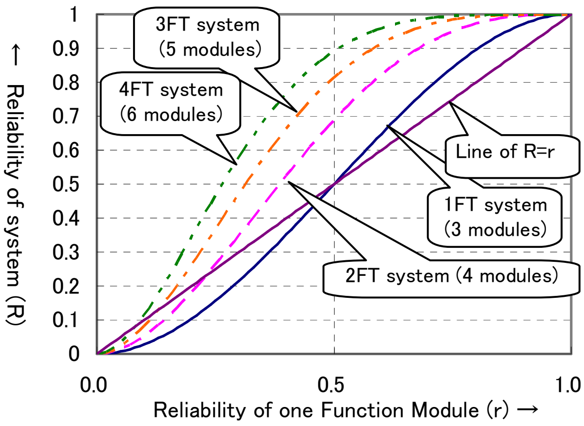


Fig-11 Reliability of (n+2)MR for 2FT

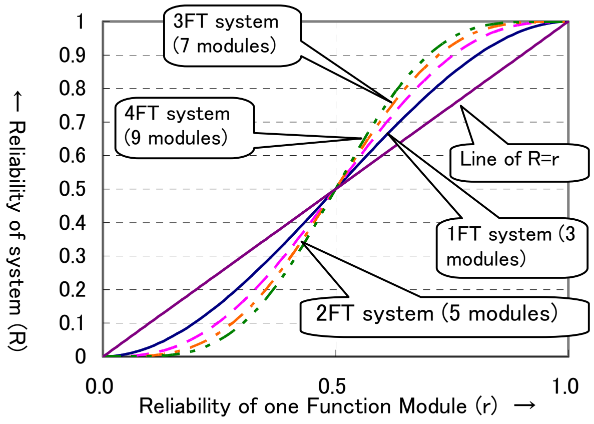


Fig-12 Reliability of (2n+1)MR for 2FT

In (2n+1)MR system, if the reliability of one function module is greater than 0.5, the reliability of the system becomes better than it. But if that is less than 0.5, this becomes worse than it. This reliability curve is equal to that of conventional NMR without the voter. On the other hand in (n+2)MR system, even if the reliability of one module is less than 0.5, the reliability of system may be improved.

Then how much is the probability of two or more faults in one control period? How does such the phenomenon drop the reliability of (n+2)MR system? We shall evaluate reliability drop of 4MR on the assumption that two or more faults must not happen for 2FT. The reliability drop is shown as the below.

$$R_{drop} = \sum_{k}^{life} \left(P_{\text{no faults until k}} \times P_{\text{two faults in one period}}\right) \cdot\cdot \;\text{EQ (4)}$$

Where, $P_{\text{no faults until k}}$ = ＜Probability of no faults out of four modules until k-th control period＞
$P_{\text{two faults in one period}}$ = ＜Probability of two faults in one control period＞

Here, the parameters as the below shall be determined.

R: Reliability of one function module for life
r: Reliability of one function module in one control period (constant)
m: Cycle count of control period for life

Then the equation R = r ^{m} is possible. And EQ (4) can be transformed as the EQ (5).

$$R_{drop} = \sum_{k}^{m} r^{4k} \times {}_4C_2 \times r^2 (1-r)^2$$
$$= 6\times r^2 (1-r)^2 \times \left(\frac{r^4 - r^{4(m+1)}}{1-r^4}\right) \quad \cdots \text{EQ(5)}$$

For example, if a system designed life shall be 1 year and one control period shall 1 second, the graph of reliability according to the reliability of one function module is shown as Fig-13. There is a singular point near zero in Fig-13. Most of reliability drop is negligible without the neighborhood of the singular point.

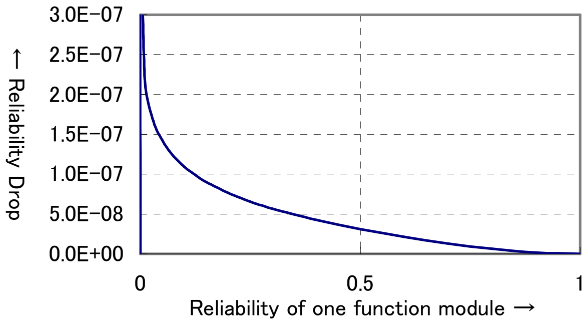


Fig-13 Reliability Drop of 4MR for 2FT

The reliability of (n+2)MR is equal to that of hybrid redundancy, self-purging redundancy and sift-out modular redundancy[6][7][8][9] without the voter. These systems need complex and high reliability voters. On the other hand, our proposed (n+2)MR system needs some switches only and these do not need so high reliability because the redundancy of voting switches group increase its reliability.

9. Conclusion

Our proposed system has perfect n-fault-tolerance, because the system can mask any faults not only in function modules but also in voters, and the number of faults is countable up to the required "n" before a failure appears.

The conventional NMR, hybrid redundancy, self-purging redundancy and sift-out redundancy have some weak points in their voters, which need complex circuits and high reliability (that is high cost). And the conventional NMR decreases the reliability if the reliability of one function module is less low than 0.5.

On the other hand, our fault-tolerant voter doesn't need any complex circuits and high reliability. And (n+2) modular redundancy system that applied with our voters for n-fault-tolerant on the assumption that two or more faults must not happen in one control period can increase the reliability even if the reliability of one function module is less low than 0.5.

Reference

[1] H. Iwai: "A Construction Method of a Fault Tolerant Voter for N-Modular Redundancy", FIT2010 C-018, (Sept. 2010)

[2] H. Iwai: "Fail-safe control equipment", Publication of patent applications Japan 2011-198038

[3] E. J. McCluskey: "Fault Tolerant System", Information Processing Society of Japan", Uehara Trans. to Japanese, Vol.23 No4, (Apr. 1982).

[4] T. Nanya: "Fault Tolerant Computer", Ch.4, Ohmsha, 1991

[5] J. Von Neumann: "Probabilistic Logics and the synthesis of reliable organisms from unreliable components," *Automata Studies, Ann. of Math. Studies*, no. 34, C. E. Shannon and J. McCarthy, Eds., Princeton University Press, pp. 43-98, 1956.

[6] University of Houston-Clear Lake: "Fault Tolerant Computing", Lectures and research projects, CENG5334, 2008.

[7] A. D. Ingle and D. P. Siewiorek: "A reliability model for various switch designs in hybrid redundancy", IEEE Trans. Compt., Vol.C-25, No.2, pp.115-133 (Feb. 1976).

[8] J. Losq: "A highly efficient redundancy scheme: self-purging redundancy", IEEE Trans. Compt., Vol.C-25, No.6, pp.569-578 (June 1976).

[9] De Sousa, Paulo T.; Mathur, Francis P., "Sift-Out Modular Redundancy," *Computers, IEEE Transactions on*, vol.C-27, no.7, pp.624, 627, July 1978

[10] D. Davies and J.F. Wakerly: "Synchronization and matching in redundant systems", Trans. Compt., Vol.C-27, No.6, pp531-539 (June 1978).

[11] Komazaki, Ikeda, Inada: "Fail-safe output equipment", Publication of patent applications Japan H10-340101

[12] Makino, Ebana, Noda, Kanamori, Sasaki: "Failure detection equipment", Publication of patent applications Japan S58-169079