A short study on rebooting safe computers and the impact on safety

E.N. Rosenberg,

H. Schäbe,

I.B. Shubinsky

1. Introduction

Safe computers are mainly constructed using several subsystems and complex diagnostic procedures. They consist at least of two independent sub-systems (channels), where selftests and cross-checking of the channels is used to detect failures, also safety relevant ones. Not each failure can be detected, even with the best diagnostics. This also holds for safety critical failures.

In the following paper we will discuss the rebooting of systems consisting of two identical channels. There, a safety relevant failure can only occur if it occurs simultaneously and in the same manner in both channels. Hence, in these systems comparison between the channels is used as a main diagnostic measure to detect safety relevant failures.

There exists an approach to reboot a computer system upon occurrence of a failure. This is done assuming that the failure that has occurred has been a transient one and that after reboot either the failure is gone or will be revealed again by the diagnostics. In the latter case, the system would not come up again and needs to undergo repair. However, this practice might lead to a situation, where failures are accumulated in the computer system. This holds, if a certain failure shows up only under specific circumstance. Then, a failure might be detected by crosscheck in a specific situation. After reboot, the computer system has still the sleeping fault in one channel. If then, after some time the same fault occurs in the other channel this would not be detected at once. It would only be detected, if the specific situation would occur again. However, then it would be too late, because both channels would give the same result.

In this paper we will use a simple model to investigate the influence of rebooting during the time to dangerous failures of a safe computer system. In section two, we will define and present the model and derive the main mathematical results. Moreover, a special case will be discussed. Section three is dedicated to the discussion of an example, whereas conclusions will be drawn in the fifth section.

2. The model

2.1 General formulation

We assume that the safe computer consists of two identical sub-systems, i.e. the channels. Both channels are crosschecked, so that the safe computer would allow a less restrictive state only, if both channels give the same result. If the results from both channels differ, the less restrictive state would not be allowed, but a failure message would be issued. A less restrictive state could e.g. be a railway sign showing a green aspect.

Each of the channels consists of further components. We will not model them directly, but assume that each channel can have m different, disjunctive failure modes. For simplicity, we will assume that they all are dangerous. If now the same dangerous failure would occur in both channels, the safe computer would admit an unsafe state and we would observe a dangerous situation. Moreover, the failures we consider are only those that cannot be detected permanently in a short time cycle.

Thus, we will neglect

- all safe failures
- all dangerous failures that can be diagnosed within a short time using permanent diagnostics or crosschecking.

These failures usually do not play a great role for safety because they can be mitigated by the methods shown above.

The remaining failures (dangerous undetectable, if the single channel is considered) are those that can only be detected when the special request has to be fulfilled by the computer system and both channels give different results. In the sequel, we will relate to this kind of failure, when using the term "fault". With "failure" we will denote a system failure caused by two coinciding faults, i.e. there are two faults of the same mode in both channels.

Let us now assume:

- The distribution function until occurrence of the fault of the k-th mode is Fk(t).
- The probability that a fault of the k-th mode is detected at reboot (e.g. by self-diagnostics), is Ck.

Then the system can be modelled in the following manner. The distribution function of the Gk(t) time of occurrence of a fault of the k-th mode in one channel can be derived as

$$Gk(t) = (1-Ck) \sum_{i=1}^{\infty} C_k^{\,i-1} \bullet F_k^{*(i)}(t),$$

where $Fk^{*(i)}(t)$ denotes the i-fold convolution of Fk(t) with itself. The distribution has the following properties:

The mean mGk of Gk is

mGk = mFk/(1-Ck),

where mFk is the mean of Fk.

If Fk admits the NBUE, NWUE, HNBUE or HNWUE property, the same holds for Gk, for details see Schäbe (1986)).

Now, the system would fail, if two faults of the same mode would occur in both channels simultaneously. Since there are m different failure modes, we can model the system as a parallel - series system, in which the faults of the same kind in different channels are connected in parallel and all different failure modes are connected in series.

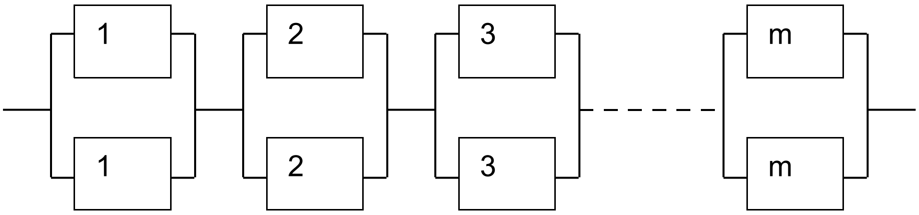

Fig. 1 Block Diagram of the system

The derivation of the distribution of the time until failure is straightforward and gives

F(t) = $1 - \prod_{k=1}^{m} (1 - G_k(t))^2$.

Generally, it is complicated to obtain the distribution F(t) in explicit form, since already Gk consists of convolutions, which can be calculated explicitly only for the gamma, normal and Cauchy distribution families. Therefore, we will consider a special case to derive some results.

2.2 Special case

Let us consider the following special case:

a) All Fk(t) are the same exponential distribution with parameter □ (failure rate)

b) All Ck are equal to C.

Then,

Gk(t) = 1- exp(-(1-C)□t),

F(t) = 1- [1-(1- exp(-(1-C)□t))^2]^m.

The mean of F can be computed as follows.

$$m_F = \int_0^\infty (1 - F(t))dt = \int_0^\infty [2\exp(-(1-C)\lambda t) - \exp(-2(1-C)\lambda t)]^m dt .$$

This gives

mF = $\frac{2^m}{\lambda(1-C)} \sum_{j=0}^{m} \binom{m}{j} (-1)^j 2^{-j} \frac{1}{m+j}$

We will now consider an additional result. This is the probability, that the n-th fault occurring in a system, being the i-th fault in the coinciding channel, will cause a dangerous system failure.

Since all distributions are identical, the probabilities that the fault occurs with a certain mode in a certain channel are equal and not depending on the particular component or channel. Then, the problem is a combinatorial one.

Considering to put i white balls and n-i black balls in m cells, where only one ball of the same colour is allowed to be in the same cell.

Then there are

$$\binom{m}{i}$$

possibilities to distribute the white balls and

$$\binom{m}{n-i}$$

possibilities to distribute the black balls, giving an overall number of

$$N0 = \binom{m}{i} \square \binom{m}{n-i}$$

possibilities of distributing the balls into the cells. Obviously, this is equivalent to the possible states with i and n failures in the both channels of the system.

Now, we must compute the number of possibilities, where precise one cell contains two balls of different colours. This is just the situation, when upon occurrence of the n-th fault the system fails, but has not failed before.

There are

$$NF = \frac{m!}{(i-1)!(n-i-1)!(m-n+1)!}$$

possibilities for this distribution.

Therefore, the probability that the n-th failure leads to system failure is

$$NF/N0 = \frac{m!i!(m-i)!(n-i)!(m-n+i)!}{(i-1)!(n-i-1)!(m-n+1)!m!m!}$$

$$= \frac{i(n-i)(m-i)!(m-n+i)!}{(m-n+1)!m!}$$

The probability is symmetric in i and n-i. Further, if i=0 or n=i, i.e. all faults are in the same channel, it turns to zero.

Note that, the probabilities for fixed m and all n and i do not exactly add up to one. This is caused by the fact that these events are not independent. The event that the system fails is under the condition that the system has not failed with n-1 faults.

Also, we can compute the probability that n faults with i faults occurring in the same channel do not lead to system failure.

The number of combinations, say NUF, of faults such that the system is unfailed can be computed as

$$\binom{m}{n}.$$

This is just the number of combinations to distribute n balls into m cells with one ball per cell. That means, all faults are distributed in such a manner that there is no matching pair of faults in both channels. Therefore,

$$\text{NUF/N0} = \binom{m}{n} \;/\; [\binom{m}{i} \;\square\; \binom{m}{n-i}]$$

is the probability that n faults, with i faults in the same channel, do not lead to system failure.

3. Example

In order to study the influence of rebooting a safe computer we will use the simplified model with exponentially distributed lifetimes as described in section two.

We assume:

All distribution functions Fk are identical exponential distributions. This is motivated by the fact that failure times of electronic equipment are exponentially distributed in most cases. In addition, we distributed the different failure modes equally, i.e. all probabilities are equal for the different failure modes, i.e. failures of the components of a channel. This is modelled by the same exponential distribution.

We assume that there are m different failure modes per channel. If then the failure rate of one entire channel is □, then each failure mode occurs with a rate □/m.

For sake of simplicity we set C=0 and let □ denote the rate of failures, uncovered during tests at reboot.

The following figure shows the probability of a failure for a time of 10000 hours and different failure rates. The curves are computed for different numbers of components and failure modes of one channel.

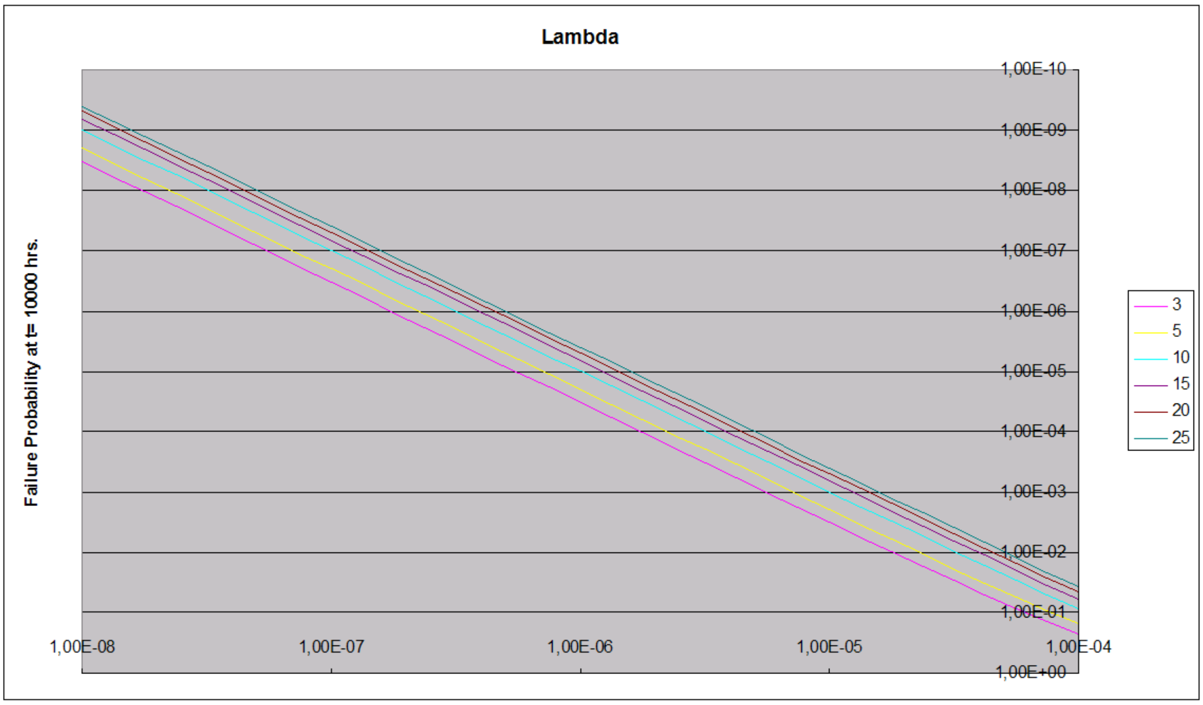

Fig. 2 Failure probability at 10000 hours.

It can be seen that the failure probability is decreasing with a growing number of components or failure modes of a channel. This is clear, since the probability to have two matching faults in both channels decreases with an increasing number of components.

Interlockings have typically a rate of undetected failures not exceeding a value of 10^{-6}/h per channel. This reflects a failure rate of 10^{-5}/h for electronic equipment and a coverage of 90% during start-up. In many cases, the coverage may even reach values of 95%, 99% or higher.

Then, depending on the number of components, the probability of a dangerous failure is between 3.32□10^{-5} (for m=3) and 4□10^{-6} (for m=25). This is for a time interval of 10000 hours. This implies that approximately once per year the interlocking is tested so that there are no sleeping failures left.

Computing the coinciding rate of dangerous failures we obtain values between

3.32□10^{-9} (for m=3) and 4□10^{-10} (for m=25).

This is below the value of 10^{-8}/h for dangerous failures, which is required to reach a SIL 4. For realistic systems, the data would even be much better caused by smaller failure rates and better coverages.

The computation shows that

a) It is important to have a good coverage of failures at start-up of the system.

b) It is important to have a large number of components or failure modes. Note that, this number can be increased with an improved diagnostics distinguishing a larger number of failure types and having different sub-functions in one channel, i.e. with growing complexity.

c) If the channels are diverse, then the probability of having the same failure in both channels can be further reduced.

4. Conclusions

In this paper we have discussed the use of reboot of safe computers consisting of two identical channels. The general model is complicated. However, with a simplified model we were able to demonstrate that under some not very optimistic assumption reboot of a safe computer would not corrupt its performance.

However, specific investigation has to be carried out on particular systems.

5. References

H. Schäbe, Ein Erneuerungsprozess mit Informationsverlusten, Elektron. Informationsverarbeitung Kybern., 22 (1986), No. 7/8, S.423-428.

R. Barlow, F. Proschan, Statistical Theory of Reliability, Holt, Rinehart, Winston, 1975

EN 50126, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), May 2001

EN 50129, Railway applications - Communication, signalling and processing systems -Safety related electronic systems for signalling, February 2003,

E.N. Rozenberg, I.B. Shubinsky, Functional Safety of Railway Automation Systems: Methods and Models, Moscow, 2005