Nuclear Engineering and Design 58 (1980) 349–358

SAFETY ASSESSMENT FOR COMPUTERIZED NUCLEAR REACTOR PROTECTION SYSTEMS: THE MARKOV APPROACH

C.A. CLAROTTI and A. MATTUCCI
CNEN C.S.N. Casaccia, Rome, Italy

In reactor protection systems based on minicomputers a central role is played by the diagnostic capability of selfchecking programs. It is thus of great importance to determine the efficiency that such programs must have with respect to fault detection in order to meet a certain reliability goal. Even though the content of this report is part of the safety study on a particular plant (Tapiro Research Reactor in service at C.S.N. Casaccia) it allows one to reach more general conclusions about the reliability of computerized protection systems. Another major aim of this paper is to point out the methodological difficulties met in the safety qualification of these systems.

1. Introduction

A comfortably low probability of an Anticipated Transient Without Scram (A.T.W.S.) in a nuclear power plant can be obtained on condition that the unavailability on demand of the protection system does not exceed the limit of 10^{-6} (see e.g. ref. [1]).

The present work has been conceived in order to determine whether such an unavailability requirement can be met by using recently designed systems as the computerized ones.

In section 1 of this paper a description is given of a particular system that has been studied for the TAPIRO reactor, in service at the Casaccia Center.

The Markov approach has been chosen to deal with the reliability analysis of the computerized protection system as it allows:

(1) to take into consideration components with more than one failed state,

(2) to treat the statistical dependence among the system states,

(3) to adopt conservative assumptions for those transition-times that in our system are not exponentially distributed.

The Fault Tree Analysis is incapable of describing situations such as those of point 1 and 2; the synchronous Monte Carlo simulation is too expensive in terms of computer time.

By straightforwardly applying the Markov approach to the system to be analyzed, a set of eleven linear differential equations would have to be solved in order to evaluate the accident probability in the plant.

Some conservative assumptions have been introduced (section 2) in order to express an upper bound of the accident probability as a function of the steady state unavailability of the protection system.

In this way, the problem has been simplified, since:

(1) The steady-state distribution probability of a Markov system without absorbing states, can be evaluated by solving a set of algebraic equations.

(2) One is not forced to use numerical methods and it is possible to express explicitly the accident probability (or, better, its upper bound) in terms of the characteristic parameters of the protection system (time to failure, duration of the self-checking program and so on); in this way one can better judge the impact of a parameter variation on plant safety.

In this work, common mode failures are not taken into consideration as their examination in the safety analysis is subordinated to the demonstration that, considering only random failures, the availability goal may be met without too much effort.

1. Description of the protection system

The safety analysis of TAPIRO reactor has indicated that the protection system to be installed in the plant must have an unavailability on demand not greater than 10^{-6}.

As our research aims to verify that digital computers are able to perform safety functions, we have designed and developed a protection system based on a one out of two philosophy, which gives good figures of safety but reduces plant availability. The reduced plant availability does not affect the validity of the work as the major problems concern the safety demonstration: on the other hand the availability problems are not very important for a research reactor as TAPIRO.

The hardware used for this application is constituted by ULP-12 minicomputer and its associated I/O cards. The main characteristics of the ULP-12 are:

(1) 16-bits word (possibility to address bytes),

(2) 32 K maximum amount of memory,

(3) 7 general purpose registers,

(4) 8 addressing modes,

(5) 8 priority levels for interrupts, and

(6) 0.96 μs memory cycle time.

The computerized protection system that will be installed in the TAPIRO reactor is shown in fig. 1.

The signals coming from the plant are sent to the interface of each ULP-12 minicomputer, which carries out safety actions whenever a dangerous condition is detected in the plant.

Software is common to both computers and is organized as shown in fig. 2. A detailed description can be found in [2]; in brief software can be divided in:

(a) Protection Program, and

(b) Self-checking Program.

The protection program is started every 100 ms by the interrupt due to the real-time clock. This program performs three tasks:

(1) execution of integrity tests on the interface and on some important functions of the minicomputers,

(2) acquisition and processing of the signals relevant to safety purposes, and

(3) carrying out the requested safety actions and excitation of the watch-dog.

The self-checking program is run at lower priority and is cyclic; it is activated during the time intervals between the end of the protection program and the next interrupt due to the real-time clock. The task of the self-checking program is to verify the computer integrity.

The philosophy of failure detection and the characteristics of the self-checking program are reported in [3].

Briefly it can be said that if a fault is detected in the hardware the excitation of the watch-dog is forbidden and the safety actions are carried out.

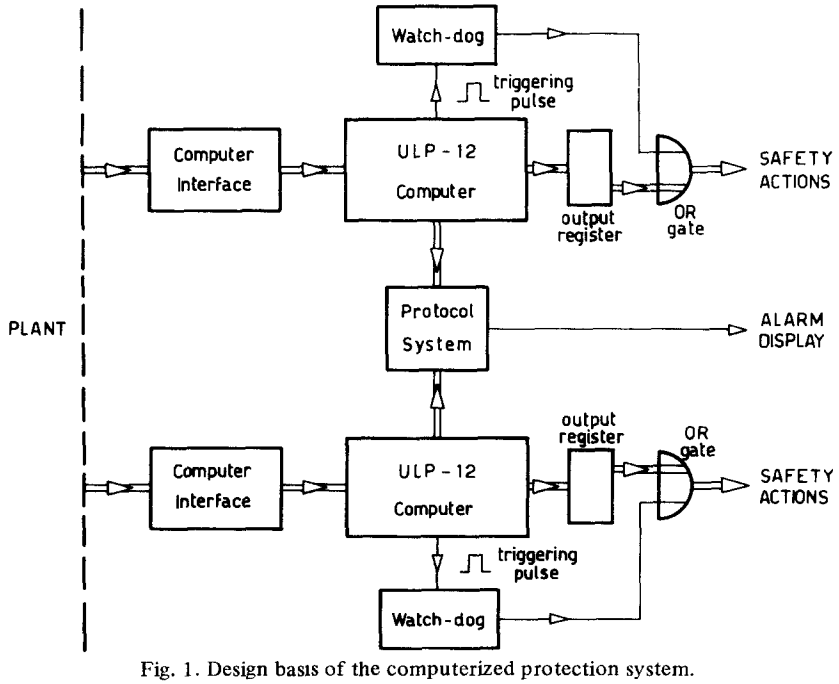

Fig. 1. Design basis of the computerized protection system.

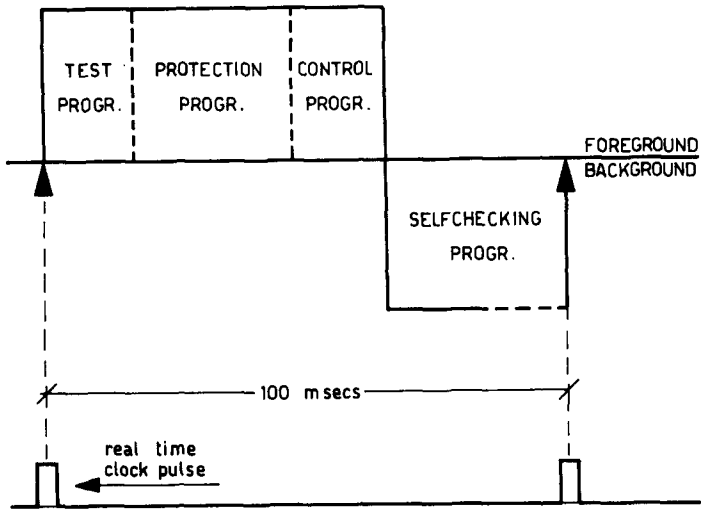

Fig. 2. Software organization in the computerized protection system.

It is evident that, under real-time conditions, the time interval necessary to execute completely the self-checking program is greater than its duration when the program is run without interrupts; in the system analysis the duration under real-time conditions will be taken into account.

Problems of system quality assurance are not the subject of our discussion and are reported in [4].

2. The Markov model

Adopting the homogeneous Markov model for the system whose reliability is to be evaluated, means to admit that the following random variables are exponentially distributed (the related parameter for each distribution, failure or repair rate, is indicated in brackets):

(a) Time to a detectable computer failure (λ_1),

(b) Time to an undetectable computer failure (λ_2),

(c) Time to a detectable computer failure following an undetectable computer failure (λ_{21}),

(d) Time to a plant transient asking for a scram (λ_T),

(e) Time to a reactor start up following a spurious scram (μ_1),

(f) Time to a reactor start up following a scram due to a plant demand (μ_2),

(g) Time to a detectable failure detection (θ).

Hypotheses (a) to (f) are generally adopted in reliability analyses, assumption (g) is a conservative simplification. In fact, as a fixed time T is required for a complete self-checking program run, time to a detectable failure detection is uniformly distributed in $(0, T)$. However it is to be stressed that, choosing $\theta = 1/T$ the event "failure is detected between t and $t + dt$" has probability

$$\exp[-t/T]\,\frac{dt}{T} \leqslant \frac{dt}{T}\,, \qquad \forall t \geqslant 0\,, \tag{1}$$

where the right-hand member of the previous equation represents the probability to be attributed to the same event if a uniform distribution is assumed.

By the way, the mean value of that random variable is doubled assuming an exponential distribution instead of a uniform one.

Let us now turn to listing the possible system states.

The following definitions are referred to a good plant behaviour:

(0) both computers are working correctly,

(1) one computer is working, in the other a detectable failure has occurred,

(2) a scram action has been undertaken, due to the detectable failure detection in one computer (the behaviour of the other computer is unimportant),

(3) one computer is working, in the other an unde-

tectable failure has occurred,

(4) both computers have failed; one in a detectable way, the other in an undetectable one,

(5) both computers have failed in an undetectable way, and

(6) both computers have failed in a detectable way.

In the above definitions is understood that the plant is working correctly; each of these states, with exception of state (2), has a corresponding state, in which the plant asks for a scram action. States characterized by the scram demand of the plant are indicated adding an apex to the label. For the sake of brevity the corresponding definitions are omitted.

In the above model it has been assumed that the computerized protection system can be completely tested and repaired after a reactor scram; therefore the protection system is to be considered "renewed" at the reactor start up.

Another assumption concerns the self-checking program capability to detect a detectable failure, if an undetectable failure takes place after a detectable one; it has been assumed that such capability remains unchanged.

This hypothesis is satisfied when the condition

$$\theta \gg \lambda_2 \tag{2}$$

is verified. In the reality condition (2) is always true; therefore the probability of there being an undetectable failure during the detection phase of a detectable failure is negligible.

Bearing in mind that:

(1) the probability distribution of the time to first system passage into a certain state is obtained considering this state as an absorbing one, and

(2) according to the state definitions, states in which an accident occurs are 4′, 5′ and 6′; in order to evaluate the accident probability in the plant it would be necessary to solve the system of differential equations represented by the Markov graph of fig. 3.

The problem may be simplified by using some results of the "renewal theory", a survey of which may be found in [5].

Let us introduce:

(1) the probability $f_k(t)\,\mathrm{d}t$ that the plant asks for Kth scram in the time interval $(t, t + \mathrm{d}t)$;

(2) the conditional probability $U[t|K(t)]$ that at time t Kth scram demand of the plant is not satisfied.

An upper bound for the probability density function of an accident at time t is

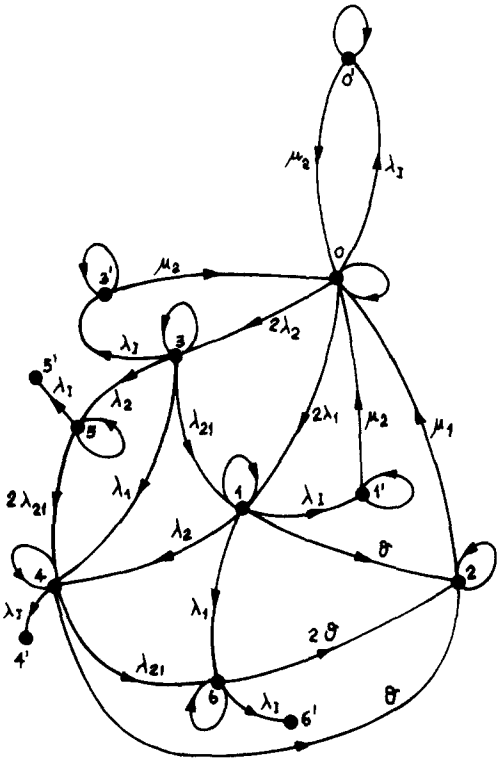

Fig. 3. Markov graph for the protection system and the plant.

$$p(t) \leqslant \sum_{k=1}^{\infty} f_k(t)\, U[t|K(t)] \,. \tag{3}$$

It follows that for the accident probability the following conservative expression holds:

$$P_a(t) = \int_0^t p(x)\,\mathrm{d}x \leqslant \int_0^t \sum_{k=1}^{\infty} f_k(x)\, U[x|K(x)]\,\mathrm{d}x \,. \tag{4a}$$

If U_M is the maximum of $U[t|K(t)]$ with respect to both t and $K(t)$, a fortiori it is:

$$P_a(t) \leqslant U_M \int_0^t \sum_{k=1}^{\infty} f_k(x)\,\mathrm{d}x \leqslant U_M \bar{n}(t) \,, \tag{4b}$$

where

$$\bar{n}(t) = \int_0^t \sum_{k=1}^{\infty} f_k(x)\,\mathrm{d}x \,,$$

is the expected number of scram demands of the plant

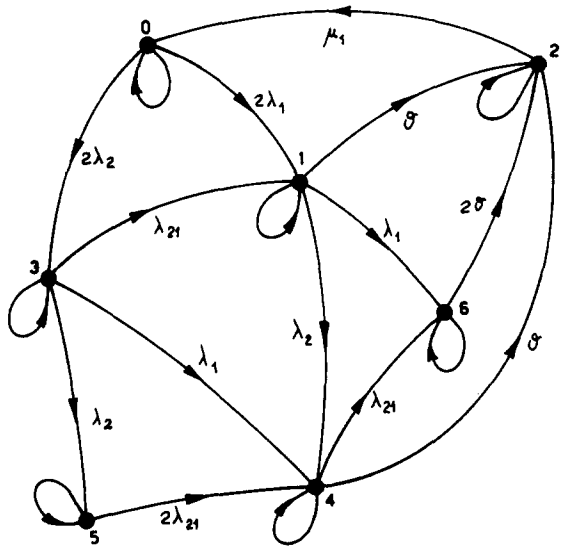

Fig. 4. Markov graph for the protection system operating independently from the plant.

in the time interval $(0, t)$ and is to be estimated performing a probabilistic analysis of the relevant plant transients.

Let us assume that the protection system operates independently of the plant, i.e., the protection system continues to operate when a scram, due to a plant demand, is actuated.

The behaviour of the protection system under the above assumptions is represented by the Markov graph of fig. 4 where the states are labelled according to the definitions already used for the graph of fig. 3.

Let $U(t)$ be the probability that the protection system is incapable of satisfying a scram demand of the plant (from now on $U(t)$ will be referred to as protection system unavailability).

In such a context the following inequality holds:

$$U(t) \geqslant U[t|K(t)] \,, \qquad \forall K, t \,. \tag{6}$$

In reality indeed, after each scram (spurious or not) a time interval follows in which the protection system is completely tested; therefore it can be reasonably assumed that the protection system has been renewed when the plant is started up again. This fact entails that the probability of no intervention of the protection system is reset to zero.

In the simplified model one considers the system completely renewed only after a spurious scram.

A qualitative behaviour of the functions U(t) and U[t|K(t)] is shown in fig. 5.

The set of differential equations corresponding to

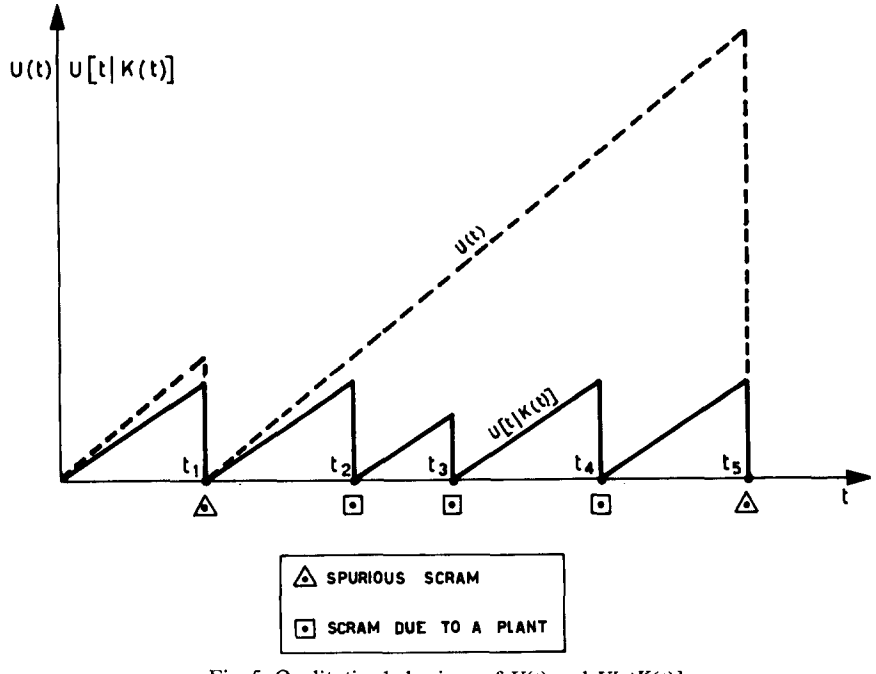

Fig. 5. Qualitative behaviour of $U(t)$ and $U[t|K(t)]$.

the graph of fig. 4 is

$$\frac{\mathrm{d}}{\mathrm{d}t}\boldsymbol{P}(t) = A \cdot \boldsymbol{P}(t)\,, \tag{7}$$

where

$$\boldsymbol{P}(t) = \begin{bmatrix} p_0(t) \\ p_1(t) \\ - \\ - \\ - \\ - \\ p_0(t) \end{bmatrix}, \qquad \boldsymbol{P}(0) = \begin{bmatrix} 1 \\ 0 \\ - \\ - \\ - \\ - \\ 0 \end{bmatrix} \tag{8}$$

$$A = \begin{bmatrix} -2(\lambda_1+\lambda_2) & 0 & \mu_1 & 0 & 0 & 0 & 0 \\ 2\lambda_1 & -(\lambda_1+\lambda_2+\theta) & 0 & \lambda_{21} & 0 & 0 & 0 \\ 0 & \theta & -\mu_1 & 0 & \theta & 0 & 2\theta \\ 2\lambda_2 & 0 & 0 & -(\lambda_1+\lambda_2+\lambda_{21}) & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & \lambda_1 & -(\theta+\lambda_{21}) & 2\lambda_{21} & 0 \\ 0 & 0 & 0 & \lambda_2 & 0 & -2\lambda_{21} & 0 \\ 0 & \lambda_1 & 0 & 0 & \lambda_{21} & 0 & -2\theta \end{bmatrix} \tag{9}$$

According to the state definitions

$$U(t) = P_4(t) + P_5(t) + P_6(t)\,. \tag{10}$$

If one could demonstrate that the steady-state unavailability U_∞ satisfies the inequality

$$U_\infty = \lim_{t\to\infty} U(t) \geqslant U(t)\,, \qquad \forall t\,, \tag{11}$$

it would hold also

$$U_\infty \geqslant U_{\mathrm{M}}\,. \tag{12}$$

The statement (11), even though it is reasonable, is difficult to be proved analytically. In order to determine what values of parameters appearing in $\boldsymbol{A}$ meet our safety requirements, condition (11) has been assumed true.

It has been verified numerically [6] that condition (11) holds for those values of parameters of $\boldsymbol{A}$ which fit our problem.

We can evaluate U_∞ by means of the limiting theorem of the Laplace transforms.

Transforming eqs. (7) we get

$$(s\boldsymbol{I} - \boldsymbol{A}) \cdot \boldsymbol{P}^*(s) = \boldsymbol{P}(0)\,, \tag{13}$$

where $\boldsymbol{I}$ is the identity matrix of the same order of $\boldsymbol{A}$ and $\boldsymbol{P}^*(s)$ is the Laplace transform of $\boldsymbol{P}(t)$

As

$$U_\infty = \lim_{t\to\infty} U(t) = \lim_{s\to 0} sU^*(s)\,, \tag{14}$$

it follows

$$U_\infty = \lim_{s\to 0} s[P_4^*(s) + P_5^*(s) + P_6^*(s)]\,. \tag{15}$$

Solving eqs. (13) and substituting in (15) we get

$$U_\infty = \Delta'/\Delta\,, \tag{16}$$

where

$$\begin{aligned}\Delta' = {} & 4\mu_1\lambda\lambda_{21}\{(2\theta+\lambda_{21})(\lambda+\theta)(\lambda+\lambda_{21}) \\ & - \theta[\lambda(1-\alpha)+\lambda_{21}][2\theta+\lambda_{21}+\lambda(1-\alpha)]\} \\ & + 4\alpha^2\lambda^2\theta\mu_1(\lambda+\theta)(\theta+\lambda_{21})\,,\end{aligned} \tag{17}$$

and

$$\begin{aligned}\Delta = {} & 4\lambda(\lambda+\theta)(\theta+\lambda_{21})\{\lambda_{21}(\lambda+\lambda_{21})(2\theta+\mu_1) \\ & + \alpha^2\lambda\theta\mu_1\} + 4\lambda_{21}\mu_1\theta\{[\lambda(1-\alpha)+\lambda_{21}] \\ & \times[2\lambda\lambda_{21} + \lambda\theta + \theta^2 + \lambda_{21}\theta - \lambda^2(1-\alpha)] \\ & + \lambda(\lambda+\theta)[\lambda+\lambda_{21}+3\alpha(\theta+\lambda_{21})]\}\,.\end{aligned} \tag{18}$$

3. Result analysis

A parametric study has been carried out, assuming

$$\lambda_1 = (1-\alpha)\lambda\,, \qquad \lambda_2 = \alpha\lambda \tag{19}$$

where λ is the failure rate of each channel (computer and its interface) and α is the fraction of the failures which are not detected by the computer self-checking program.

The parameters have been chosen as follows:

$\mu_1 = 0.0416\ \mathrm{h}^{-1}$,

$10^{-4}\ \mathrm{h}^{-1} \leqslant \lambda \leqslant 5\times 10^{-3}\ \mathrm{h}^{-1}$,

$0 \leqslant \alpha \leqslant 1$,

$0.5\ \mathrm{h}^{-1} \leqslant \theta \leqslant 6\ \mathrm{h}^{-1}$,

$0 \leqslant \lambda_{21} \leqslant (1-\alpha)\lambda$.

For parameter μ_1 it has to be recalled that a detected failure causes a reactor scram. From the operation data of the nuclear power plants it may be seen that an average value of one day for the time to reactor start-up after a spurious scram is suitable. This time

interval is sufficient to repair the protection system if spares are stocked in the plant. Therefore the inverse of one day has been adopted for μ_1.

For the parameter λ a reliability study [7] has been executed on the ULP-12 and its interface cards which has derived a value of 10^{-3} h^{-1} for the failure rate of each channel. However, a parametric study has been done, especially to verify in what manner the use of Large Scale Integrated (LSI) chips (microcomputers), which have lower failure rates, weights on the system unavailability.

The whole definition interval of the parameter α has been examined to determine the values of the undetected failure fractions which can satisfy the availability requirements for the protection system. It is clear that the values which may be achieved in practice constitute a subset of the previous interval.

The range assumed for θ insures that the self-checking program duration is consistent with fractions of detected failures very close to unity.

The major problem concerns the value to be attributed to λ_{21}. Indeed we know that λ_{21} lies in the interval $0 - (1 - \alpha)\lambda$, but there are no criteria for the choice of a suitable value for λ_{21}.

A sensitivity analysis has been performed, and the behaviour of the protection system has been investigated, assuming:

(1) $\lambda_{21} = 0$, i.e., the self-checking program capability to detect failures is lost;

(2) $\lambda_{21} = (1 - \alpha)\lambda$, i.e. the self-checking program capability to detect failures remains unchanged;

(3) $\lambda_{21} = \frac{1}{2}(1 - \alpha)\lambda$, i.e., the detectable failure may or may not be detected with the same probability.

In order to achieve results of general validity the expected number of relevant plant transients $\overline{n}(t_M)$ at mission time t_M (5000 h) has been chosen

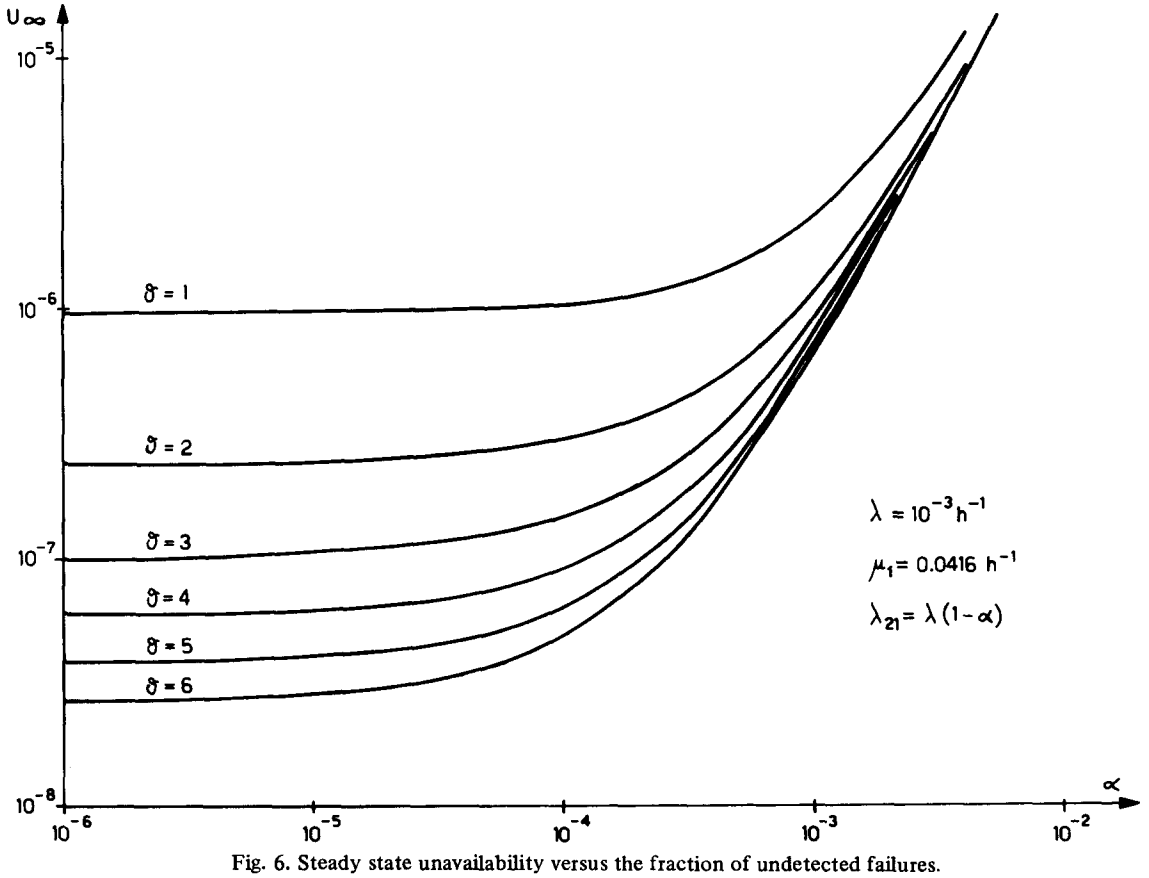

Fig. 6. Steady state unavailability versus the fraction of undetected failures.

equal to 1 [1]; this value agrees with the ones determined for nuclear power plants and is greater than the one stated in the safety analysis of TAPIRO reactor [8].

In fig. 6 U_∞ is plotted against the undected fraction of failures α for different values of θ, assuming $\lambda_{21} = \lambda$.

Let θ^* be the minimum value of θ which guarantees that the unavailability limit of 10^{-6} is not exceeded; in fig. 7 θ^* is represented versus α, for different λ's and $\lambda_{21} = \lambda_1$.

It can be seen that values of α greater than 10^{-3} make it impossible to meet the unavailability requirements.

For this value of the undetected failure fraction an investigation has been made of the dependence on parameters θ and λ_{21}, as such a value of α may be achieved with the least difficulty in practice.

In fig. 8 time diagrams of the unavailability $U(t)$ for $\lambda = 10^{-3}\ h^{-1}$, $\alpha = 10^{-3}$ are given, assuming λ_{21} as a parameter; the monotone character of the curves enhances the validity of inequality (11).

The accident probability has been also calculated by solving numerically the equation system corresponding to the graph of fig. 3, using as parameters θ and assigning to the other variables the values used in the simplified model.

These calculations have been performed in order to ensure that the hypotheses made to simplify the reliability model of the system are conservative.

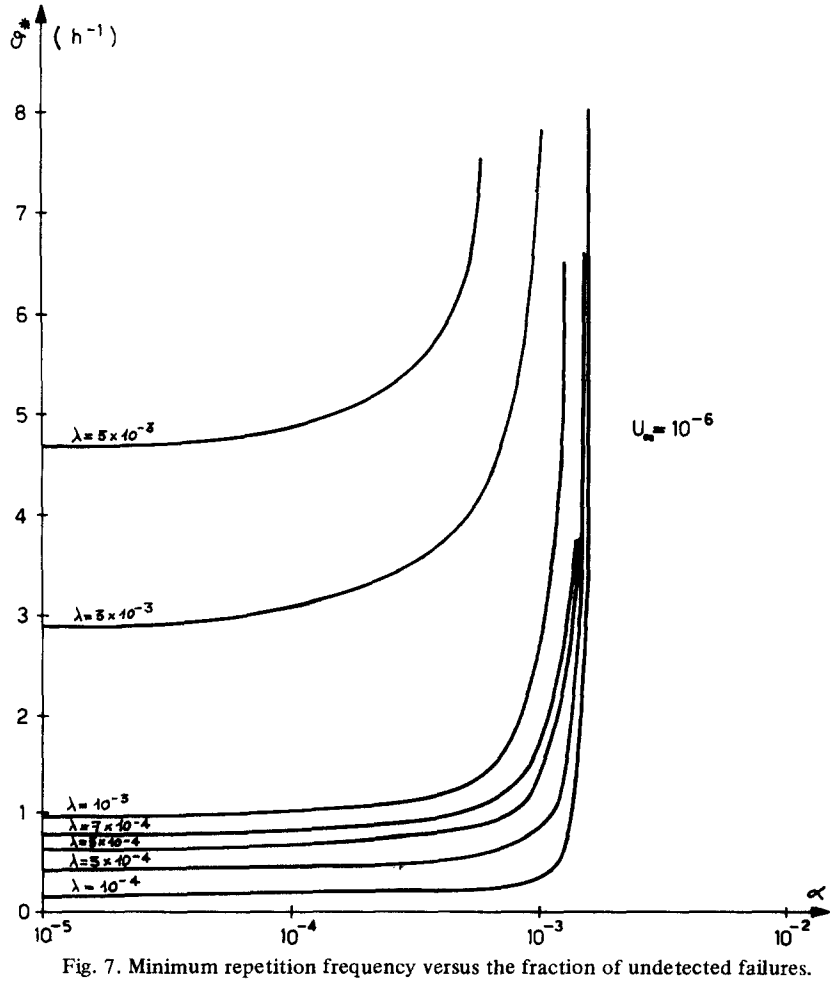

Fig. 7. Minimum repetition frequency versus the fraction of undetected failures.

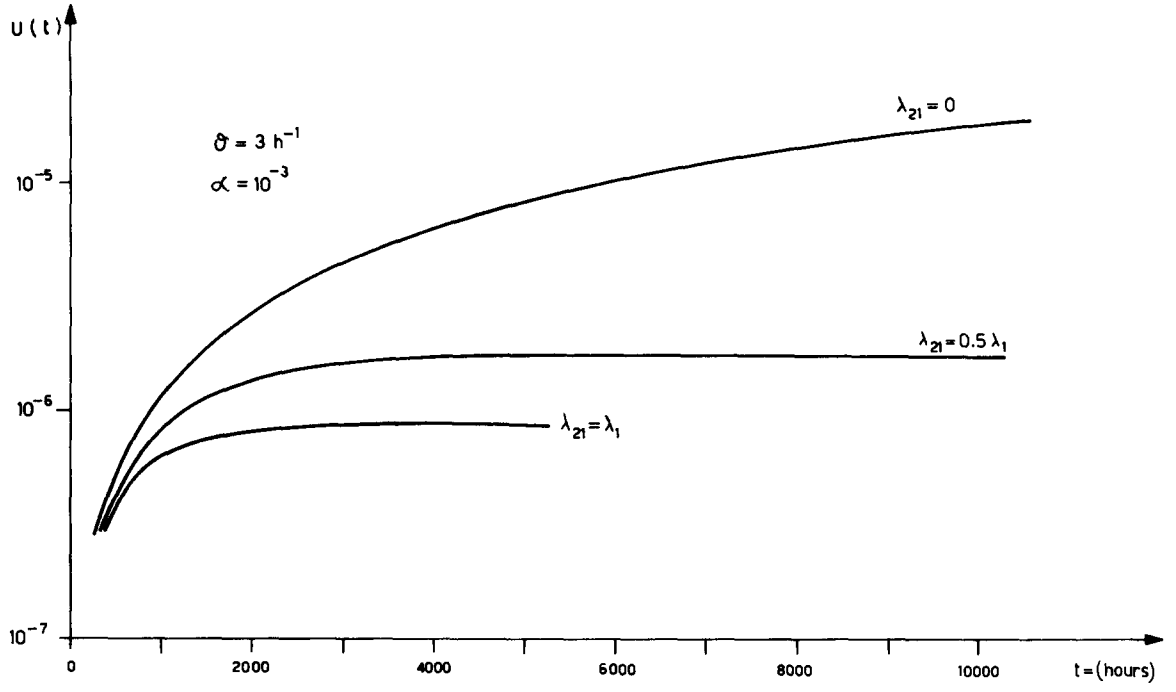

Fig. 8. Time behaviour of the protection system unavailability.

The results obtained are summarized respectively in table 1 and table 2; as the expected number of transients in 5000 h is 1, the data of the tables are directly comparable.

It can be seen that in every case the simplified model gives a pessimistic estimate of the accident probability.

The behaviour of the protection system is strongly dependent on the values of λ_{21}; in fact, keeping θ constant, the importance of λ_{21} on the unavailability is relevant. If λ_{21} is equal to 0, the accident probability increases drastically and is not affected by the self-checking program duration.

4. Conclusions

For what concerns random failures it follows that, given a hardware failure rate $\lambda = 10^{-3}\ h^{-1}$ and in the assumption that every failure is by itself (intrinsically) unsafe, the availability target is achieved only if the self-checking program is able to detect a percentage of failure greater than 99.9.

This goal is hard to meet; in fact, a minicomputer being made up by a very large number of components, which interact in a complicated way, it is very difficult to perform an exhaustive failure mode and effect analysis on the C.P.U. and its associated cards. On the other hand the lack of detailed failure data forces the analyst to keep the conservative hypothesis that every

Table 1
Steady-state unavailability of the protection system

λ_{21}	$0.0\ h^{-1}$	$0.5 \times 10^{-3}\ h^{-1}$	$10^{-3}\ h^{-1}$
θ			
$1\ h^{-1}$	1.996×10^{-5}	3.49×10^{-6}	2.378×10^{-6}
$3\ h^{-1}$	1.788×10^{-5}	1.8×10^{-6}	0.900×10^{-6}
$6\ h^{-1}$	1.769×10^{-5}	1.51×10^{-6}	0.662×10^{-6}

Table 2
Accident probability at t = 5000 hs

λ_{21}	$0.0\ h^{-1}$	$0.5 \times 10^{-3}\ h^{-1}$	$10^{-3}\ h^{-1}$
θ			
$1\ h^{-1}$	4.371×10^{-6}	2.56×10^{-6}	2.021×10^{-6}
$3\ h^{-1}$	2.68×10^{-6}	1.086×10^{-6}	0.678×10^{-6}
$6\ h^{-1}$	2.378×10^{-6}	0.846×10^{-6}	0.472×10^{-6}

failure is intrinsically unsafe. It is then impossible to demonstrate the achievement of the required degree of safety for protection systems based on minicomputers even considering only random failures. Any further refinement of the analysis, as for instance taking into consideration common mode failures, is then of no importance in such context.

As the minicomputer cost is rather high, any protection system based on minicomputer logic must be characterized by a low degree of redundance; the requested level of safety must be necessarily achieved by a sophisticated self-checking capability. The main result of the previous analysis is to have shown the inadequacy of such a philosophy in the nuclear field. Anyway, the commercial availability of cheap L.S.I. circuits, whose failure rates are lower than those of minicomputers, makes possible solutions previously too expensive to be adopted. In particular the protective functions may be shared on more units and the degree of redundance may be increased in order that the self-checking programs play a less important role.

For the analysis of such systems, if the number of states is not high, the use of the Markov method may be convenient providing that common mode failures are also considered.

To treat some kinds of common mode failures two models are available in the literature and more precisely: the first model "treats chance failures and also common mode failures of catastrophic nature", while the second one "assumes that the common mode mechanism could increase the failure rate of components over an exponentially distributed time" [9].

In particular much effort will be spent on the analysis of common mode failures due to errors in software.

Acknowledgement

The authors would like to thank Prof. G. Volta for valuable comments and discussions covering several aspects of the present analysis.

References

[1] WASH 1270 Technical Report on A.T.W.S. for Water Cooled Power Reactors, Washington (Sept. 1973).
[2] P. Monaci and M.G. Putignani, Design of reliable software for a computerized protection system, EMPG Meeting, Fredrikstad, 6–10 June, 1977.
[3] S. Babiloni, F. Fioretta, G. Grazioli and C. Santucci, Hardware structure and self-checking features of a computerized protection system, EMPG Meeting, Fredrikstad, 6–10 June, 1977.
[4] S. Bologna, E. de Agostino, D. Manzo, A. Mattucci, P. Monaci, M.G. Putignani, C. Santucci and N.M. Stephanos, Implementation and validation of a computerized reactor protection system EMPG Meeting, Loen, 4–9 June, 1978.
[5] R.E. Barlow and F. Proshan, Mathematical Theory of Reliability (Wiley, New York, 1965).
[6] L. Menga, FIDO– A computer code to solve differential equations, AGIP Nucleare (1977).
[7] F. Zambardi, Preventive failure rate evaluation for an ULP-12 protective channel, RIT/TECN-AUCOIMP (78) 6, In Italian.
[8] L. Musso and N. Santangelo, Safety report of TAPIRO reactor, CNEN Report-347, in Italian.
[9] B.B. Chu and D.B. Gaver, Stochastic models for repairable systems susceptible to common mode failures, in: Nuclear System Reliability Engineering and Risk Assesment, Eds.: J.B. Fussel and G.R. Bursick (1977).