KERNFORSCHUNGSZENTRUM

KARLSRUHE

August 1967

KFK 640
EUR 3685 e

Institut für Angewandte Reaktorphysik

# General Criteria to Optimize the Operation of a Power Plant with Special Consideration to its Safety Requirements

L. Caldarola
unter Mitarbeit von G. Weber

GESELLSCHAFT FÜR KERNFORSCHUNG M. B. H.

KARLSRUHE

KERNFORSCHUNGSZENTRUM KARLSRUHE

August 1967 KFK 640
EUR 3685 e

Institut für Angewandte Reaktorphysik

# General criteria to optimize the operation of a power plant with special consideration to its safety requirements*

by

L. Caldarola**
G. Weber

Gesellschaft für Kernforschung m.b.H., Karlsruhe

---

* Work performed within the association in the field of fast reactors between the European Atomic Energy Community and Gesellschaft für Kernforschung m.b.H., Karlsruhe.

** Euratom, Brussels, delegated to the Karlsruhe Fast Breeder Project, Institut für Angewandte Reaktorphysik.

## Abstract

To increase the availability of a power plant means also to invest more money in the plant. A criterion to weigh the improved availability against the increased plant cost is therefore needed. For this reason, the annual loss function of a power plant is introduced: the minimum of this function gives the best balance between improved availability and increased plant cost. The safety requirement is a constraint to the problem of finding the minimum of the function. The mathematical expressions to calculate the annual loss function are derived, and a numerical example is also included. Some general probabilistic considerations on reactor containers are also discussed.

Contents

## 1. Introduction

One of the problems, with which the designer of electric power plants is faced, is that of constructing the plant in such a way that it can function safely and economically. To increase the degree of safety of a plant is paid always by making it to function less economically. In fact the safest plant is that which is always in shut down, which means that it does not function at all.

During normal operation, it can happen that the plant, due to the failure of one of its parts, goes to shut down, and does not produce electricity during the time in which is being repaired. This results in a loss of money for the company which owns the plant. This consideration should drive the designer to design a better plant, in which the failure probability of its parts is reduced. But to design a more reliable plant means also to invest more money in it.

From what we have said, one can already conclude that the designer must weigh the improvement obtained in the plant availability against the increased plant cost. Scope of this report is to give the criteria which allow to find this optimum value of the plant availability, and, at the same time, to satisfy the safety requirements given by the safety committee.

## 2. Fundamental concepts. Different types of failures.

From an operational point of view, we can think that a plant consists of two systems: the "Functional System" and the "Safety System".

The "Functional System" is that part of the plant which performs the function of the plant, that is to produce electricity. The "Functional System" includes those parts of the plant (such as reactor, pumps, heat exchangers, etc.), which all together allow the plant to produce electricity.

The "Safety System" is that part of the plant which protects the "Functional System" against accidents.

For this reason, signals coming from the "Functional System" are continuously detected by the "Safety System" (fig. 1).

If the signals indicate that a dangerous situation exists, the Safety System will shut the plant down.

We shall call "Functional Subsystem" any part of the functional system which, if it fails, does not allow the plant to perform its function at all, or at least in a safe way. To illustrate this definition, we shall make two examples. Let us take the case of a nuclear power plant. The pump of the primary coolant circuit (fig. 13) is driven by an electric motor which is fed from a power supply. If the power supply fails, the pump stops, the coolant flow decreases, and the reactor is not cooled any more. The consequence will be that the heat is not converted into electricity, which means that the functional system does not perform its function any more. In addition, since the reactor is not cooled, the heat produced remains inside it and, if the plant is not shut down, there will be a "disaster" or a "big accident" (core melt down).

The power supply is therefore a functional subsystem, because its failure does not allow the plant to function. Let us suppose now that we have two power supplies, one working and the other in stand-by, connected in such a way that, if the first fails, it is automatically switched off, while the second is automatically switched into operation. In this case the functional subsystem is made of both the power supplies, and each of them will be called "unit". The functional subsystem fails, if both the units fail.

The second example refers also to the primary coolant circuit of a nuclear power plant. The bearings of the primary coolant pump (fig. 13) are cooled with oil, which is maintained in circulation by means of an oil pump. If the

oil pump fails, the functional system can continue still for some time to produce electricity, but not in a safe way. In fact, if the primary coolant pump is not switched off, the bearings will jam and the pump will fail (loss of coolant flow accident). The oil pump is also a functional subsystem and, as for the case of the power supply, we can have an "oil pumps subsystem" which consists of two or more oil pumps, that is of two or more units. The functional subsystems have only one type of failure. This does not mean that they can fail only in one way, but that their failures have only one consequence, namely that they bring the plant in a so dangerous situation, that plant shut down is required.

Let us take, for example, a "power supplies subsystem" consisting of one unit only. The modes of failure of the power supply are many, but the consequence is only one: the motor of the primary coolant pump is not driven any more. The units of the functional subsystems will be characterized by only one average failure rate, $\sigma_F$, which takes into account all the failure modes of the unit. If we indicate with "$h_F(t)$" the total failure probability density distribution of the unit, we have (Appendix 1)

$$\sigma_F = \frac{1}{\text{mean time between two failures}} = \frac{\int_0^{\Theta_F} h_F(t)dt}{\Theta_F \left[1-\int_0^{\Theta_F} h_F(t)dt\right]+\int_0^{\Theta_F} t h_F(t)dt} \qquad (1)$$

where

$t$ = time

$\Theta_F$ = maintenance period, that is time interval between two preventive replacements (or repairs) of the unit.

If no preventive maintenance is planned ($\Theta_F=\infty$), eq. 1 becomes:

$$\sigma_F = \frac{1}{\int_0^{\infty} t h_F(t)dt} \qquad (2)$$

The average failure rate, $\lambda_F$, of a functional subsystem depends upon the characteristics of the units which form the subsystem and upon the way in which these units are connected (strategy). The calculation of "$\lambda_F$" as function of the unit characteristics for different strategies is shown in paragraph 5.4.

The plant will be shut down from time to time to carry out the maintenance of the

big components. This maintenance is called "routine plant maintenance".

The maintenance period "$\theta_F$" of a unit belonging to a functional subsystem can be shorter than that of the "routine plant maintenance", if the functional subsystem consists at least of two units. In fact, in the case in which the functional subsystem consists of one unit only, in order to carry out the preventive maintenance of the unit, it is necessary to shut the plant down.

The safety system too can be divided in "Safety Subsystems". For a better understanding, we shall illustrate a particular case. Fig. 2 shows a schematic block diagram of some safety subsystems, which protect the reactor of a nuclear power plant against accidents. In a safety system we can distinguish three types of subsystems and exactly

> Subsystems S11, S12, S13. They measure some parameters (such as power, temperatures, pressures, etc.) of the functional system, and, on the basis of these measurements, decide wether or not to shut the plant down.
>
> Subsystem S14. It is an intermediate relays network, which receives the dicision taken by the previous subsystems, and transmit it to the following subsystem.
>
> Subsystem S15. It is a structure of actuators. The actuators are the organs, which carry out the decision received from the relays network. In the case of a nuclear reactor, the actuators would be the safety rods and its associated mechanisms. In the case of a pump, the actuators would be the electric switches which connect the pump motor to the power supply.

With reference to fig. 2, let us suppose that the power supplies subsystem (which feeds the motor of the primary coolant pump) fails. The loss of voltage to the motor will be measured by the "$n_{S11}$" measuring channels which are connected in such a way that, if at least "$k_{S11}$" out of the "$n_{S11}$" units measure the loss of voltage correctly, the decision to shut the reactor down will be given to S14. This means that at least "$k_{S11}$" units, at the time of the loss of voltage accident, must not have already failed in such a way that they cannot detect the accident any more. We shall call with failure type "a" that type of failure which makes the unit (of a safety subsystem) unable to function correctly when the accident occurs. The subsystem S14 operates in a similar way. When S14 receives the shut down decision from S11 (or S12 or S13), if "$k_{S14}$" out of the "$n_{S14}$" units (relays)

operate correctly, it will transmit this decision to subsystem S15. Finally, if "$k_{S15}$" control rods will drop inside the reactor, no big accident will take place and the reactor will be shut down. If instead, at the time of the loss of voltage accident,

$$m_{S11} = n_{S11} + 1 - k_{S11} \qquad (3)$$

out of the "$n_{S11}$" units don't measure the loss of voltage correctly, no decision to shut the reactor down is given to subsystem S14. In this case, since the primary coolant pump will stop, the primary coolant flow will decrease, and this will be detected by the measuring channels of subsystem S12, which operates in a way similar to S11. If also subsystem S12 fails to shut the reactor down, the reactor outlet coolant temperature will increase, and this will be detected by the measuring channels of subsystem S13, which operates in a way similar to S11 and S12. If also subsystem S13 fails to shut the reactor down, there will be a big accident (core melt down).

The big accident (or "disaster") will take place also in the cases in which subsystems S14 and S15 fail to operate correctly, when they are required to shut the reactor down.

It can also happen that "$k_{S11}$" out of the "$n_{S11}$" units detect the loss of voltage to the pump motor, when no loss of voltage exists (failure type b). In this case the reactor would be erroneously shut down (false trip).

From what we have said above, we can conclude that the units of a safety subsystem can have two types of failures: failure type "a" and failure type "b".

Failure type "a" is that type of failure, which makes the unit unable to operate when it is asked to operate.

Failure type "b" is that type of failure, which makes the unit to operate, when it is not asked to operate.

For a relay mounted in such a way, that its contacts are asked to open when there is a danger, the failure type "a" would occur if the relay becomes unable to open its contacts when it is asked to do it. The failure type "b" would instead take place, if the relay contacts open without being asked to open.

The units of the safety subsystems will be therefore characterized by two average failure rates one, $\rho_S$, related to failure type "a" and the other, $\sigma_S$, to failure type "b".

In order to find out that a unit of a safety subsystem is failed with failure type "a", it is necessary to test it from time to time. Let us indicate with "$\tau_S$" the checking period (that is the time interval between two tests), with $h'_S(t)$ the failure type "a" probability density distribution of the unit and with $h''_S(t)$ the failure type "b" probability density distribution of the unit. We have (Appendix 2)

$$\rho_S = \frac{\int_0^{\Theta_S(1+\delta'_S/\tau_S)} h'_S(t) \left[1 - \int_0^{t(1+\delta''_S/\tau_S)} h''_S(t)dt\right] dt}{\Theta_S\left[1 - \int_0^{\Theta_S} \bar{h}_S(t)dt\right] + \int_0^{\Theta_S} t\,\bar{h}_S(t)dt} \qquad (4)$$

and

$$\sigma_S = \frac{\int_0^{\Theta_S(1+\delta''_S/\tau_S)} h''_S(t) \left[1 - \int_0^{t(1+\delta'_S/\tau_S)} h'_S(t)dt\right] dt}{\Theta_S\left[1 - \int_0^{\Theta_S} \bar{h}_S(t)dt\right] + \int_0^{\Theta_S} t\,\bar{h}_S(t)dt} \qquad (5)$$

where

$\Theta_S$ = maintenance period, that is time interval between two preventive replacements (or repairs).

$\delta'_S$ = const.

$\delta''_S$ = const.

$\bar{h}(t)$= total failure probability density distribution given by eq. 5 in Appendix 2.

Fig. 3 shows the qualitative behaviour of $\rho_S$ and $\sigma_S$ as functions of "$\Theta_S$" and "$\tau_S$". It is understandable that the shorter is $\Theta_S$ and the longer is $\tau_S$, the smaller are $\sigma_S$ and $\rho_S$.

A safety subsystem is characterized by two parameters

(i) the reduction coefficient "$K_S$" for failure type "a"

and (ii) the average failure rate "$\lambda_S$" for failure type "b".

If a functional subsystem fails (for example the power supplies subsystem), there is a certain probability that one of the safety subsystems which should cooperate to shut the reactor down (for example S14) has already failed with failure type "a". This would happen if "$m_S$" out of the "$n_S$" units (belonging to the safety subsystem) have failed with failure type "a". If "$\lambda_F$" is the failure rate of the functional subsystem, the rate of occurrence "$\upsilon$" of the event, that, the safety subsystem fails before the functional subsystem does, is given by (Appendix 3)

$$\upsilon = K_S \lambda_F \tag{6}$$

where

$$K_S = \frac{(n_S)!(\rho_S \tau_S)^{m_S}}{(m_S+1)!(n_S-m_S)!} \tag{7}$$

and

$\rho_S$ = unit average failure rate for failure type "a" given by eq. 4

$n_S$ = number of the units belonging to the safety subsystem

$m_S$ = number of the units which must fail in order to make the safety subsystem to fail (failure type "a")

$\tau_S$ = checking period.

Figs. 4, 5 and 6 show the reduction coefficient "$K_S$" as function of "$\rho_S \tau_S$" for different values of "$n_S$" and "$m_S$".

If we now ask for the rate of occurrence "$\upsilon$", of the event that two safety subsystems (i and j) fail before the functional subsystem fail, we have (Appendix 3)

$$\upsilon = H_{Si;Sj} K_{Si} K_{Sj} \lambda_F \tag{8}$$

where

$K_{Si}$ = reduction coefficient of the safety subsystem "i"

$K_{Sj}$ = reduction coefficient of the safety subsystem "j"

$H_{Si;Sj}$ = coupling coefficient

$H_{Si;Sj}$ is given by

$$H_{Si;Sj} = \frac{(m_{Si}+1)(m_{Sj}+1)}{(m_{Si}+m_{Sj}+1)} \tag{9}$$

For the case of "N" safety subsystems we have

$$\upsilon = \lambda_F \left[ \prod_{i=1}^{N} K_{Si} \right] H_{S1;S2...SN} \tag{10}$$

where

$$H_{S1;S2;...;SN} = \frac{\prod_{i=1}^{N} (m_{Si}+1)}{1 + \sum_{i=1}^{N} m_{Si}} \tag{11}$$

The failure rate "$\lambda_S$" for failure type "b" of a safety subsystem is given by (Appendix 4)

$$\lambda_S = \frac{\sigma_S}{\sum_{i=o}^{\ell_S-1} \left[ \left(\frac{\mu_S}{\sigma_S}\right)^i \sum_{q=n_S-\ell_S+1+i}^{n_S} \frac{(q-1-i)!}{q!} \right]} \tag{12}$$

where

$\sigma_S$ = unit average failure rate for failure type "b" given by eq. 5

$\ell_S$ = number of units which must fail (failure type "b") in order to make the safety subsystem to fail.

$\mu_S$ = average repair rate of a unit, equal to the reciprocal of the mean time needed to repair the unit. (defined by eq. 13)

$$\mu_S = \frac{1}{\int_o^\infty t\, g_S(t)dt} \tag{13}$$

where $g_S(t)$ is the repair probability density distribution of a unit.

Since $\mu_S/\sigma_S$ is usually extremely large, eq. 12 can be written as follows

$$\lambda_S \simeq \frac{n_S!}{(n_S-\ell_S)!} \frac{\sigma_S^{\ell_S}}{\mu_S^{(\ell_S-1)}} \tag{14}$$

For safety subsystems like structures of measuring channels or relays networks, we have always

$$\ell_S = k_S = n_S+1-m_S \tag{15}$$

For the safety actuators subsystems, we can have either eq. 15 or

$$\ell_S \neq k_S \tag{16}$$

In the case of the reactor actuators subsystem (S15 in fig. 2), if one control rod alone is sufficient to reduce the reactor power to a low value, we have

$$\ell_{S15} = 1 \tag{17}$$

and therefore from eq. 12

$$\lambda_{S15} = n_{S15}\ \sigma_{S15} \tag{18}$$

## 3. A simple model. The annual loss function "Z".

In order to understand the type of problem which we intend to solve, let us start to consider a very simplified model of the electric plant.

At a given time the plant can be only in one of the following states

| | |
|---|---|
| State "0" "Normal Operation" | The plant is in "normal operation" which means that it is producing electric power. |
| State "1" "Shut Down" | The plant is in "shut down", which means that it is not producing electric power, but that it can be repaired and started up again. |
| State "2" "Disaster" | The plant is in the "disaster" state which means that it is so heavily damaged (as a consequence of a big accident), that it cannot be repaired any more. |

Fig. 7 shows a schematic flow diagram of the various states of the plant. The plant, as seen in paragraph 2, consists of the "functional system" and of the "safety system". A failure of the "functional system" leads to a "big accident", if the safety system does not shut the plant down.

The plant goes from state "0" to state "1" in the two following cases:

a) failure of the "functional system" followed by a correct action of the safety system.

b) false trip, due to a failure of the safety system. This means that the safety system shuts the plant down while the functional system is operating correctly. We have called this type of failure of the safety system failure type "b".

The plant goes from state "0" to state "2" (disaster) when the functional system fails and the safety system does not shut the plant down. We have called this type of the failure of the safety system failure type "a".

We introduce now the following symbols

$Q_0(t)$ = probability that the system is in state "0" at time "t"

$Q_1(t)$ = probability that the system is in state "1" at time "t"

$Q_2(t)$ = probability that the system is in state "2" at time "t"

$\lambda_F$ = failure rate of the functional system

$K_S$ = reduction coefficient of the safety system

$\Psi$ = plant repair rate, that is the reciprocal of the mean time needed to repair the plant

$\lambda_S$ = rate of occurrence of a false trip.

The rate of occurrence "$\upsilon_d$" that a big accident occurs (safety system fails with failure type "a" before the functional system fails) will be given by

$$\upsilon_d = K_S \lambda_F \tag{1}$$

The rate of occurrence "$\upsilon$", that the plant goes to shut down as a consequence of the failure of the functional system, is

$$\upsilon = (1-K_S)\lambda_F \tag{2}$$

Since "$K_S$" is very small ($<10^{-5}$), eq. 2 can be written

$$\upsilon \simeq \lambda_F \tag{3}$$

Typical values for $\lambda_F$, $\lambda_S$, $\Psi$ and $K_S$ are the following

$$\lambda_F = 0.1 \div 1/\text{year} \tag{4}$$

$$\lambda_S = 0.01 \div 0.05/\text{year} \tag{5}$$

$$\Psi = 10 \div 100/\text{years} \tag{6}$$

$$K_S < 10^{-5} \tag{7}$$

From 4 to 7, we get the expression 8 which holds in the practical cases

$$\Psi > \lambda_F + \lambda_S \gg K_S \lambda_F \tag{8}$$

In the following analytical treatment, we suppose that $\lambda_F$, $\lambda_S$ and $\Psi$ are constant. This means that failure and repair probability density distributions are supposed to be exponential.

The following equations can be written (fig. 7)

$$\frac{dQ_o}{dt} = -(\lambda_F+\lambda_S+K_S\lambda_F)Q_o+\Psi Q_1 \tag{9}$$

$$\frac{dQ_1}{dt} = (\lambda_F+\lambda_S)Q_o - \Psi Q_1 \qquad (10)$$

$$\frac{dQ_2}{dt} = K_S\lambda_F Q_o \qquad (11)$$

$$1 = Q_o + Q_1 + Q_2 \qquad (12)$$

where "t" indicates the time.

Only three of the four equations 9, 10, 11 and 12 are independent. For instance, eq. 11 can be easily obtained from eqs. 9, 10 and 12.

The solution of the system of eqs. 9, 10 and 12 is described in Appendix 5.

Here we write the approximate expression of "$Q_o$" under the condition that the expression 8 is satisfied

$$Q_o \simeq \left[\frac{\Psi}{\Psi+\lambda_F+\lambda_S} + \frac{\lambda_F+\lambda_S}{\Psi+\lambda_F+\lambda_S}\exp\{-(\Psi+\lambda_F+\lambda_S)t\}\right]\exp(-K_S\lambda_F t) \qquad (13)$$

Eq. 13 can be written as follows

$$Q_o \simeq A \cdot R \qquad (14)$$

where

$$A = \frac{\Psi}{\Psi+\lambda_F+\lambda_S} + \frac{\lambda_F+\lambda_S}{\Psi+\lambda_F+\lambda_S}\exp\{-(\Psi+\lambda_F+\lambda_S)t\} \qquad (15)$$

and

$$R = \exp(-K_S\lambda_F t) \qquad (16)$$

"A" is a function which has the following characteristics

$$[A]_{t=o} = 1 \qquad (17)$$

and

$$\lim_{t\to\infty} A = \frac{\Psi}{\Psi+\lambda_F+\lambda_S} = A_\infty \qquad (18)$$

Due to the large values of "$\Psi$" (eq. 6), "A" reaches $A_\infty$ in a very short period of time.

For "R" we have instead

$$[R]_{t=o} = 1 \tag{19}$$

and

$$\lim_{t\to\infty} R = 0 \tag{20}$$

Due to the very small values of $K_S\lambda_F$, "R" is practically equal to "1" for the all plant lifetime. We have therefore that the average plant availability "$\bar{A}$" during the time interval "t" is given by

$$\bar{A} = \frac{1}{t}\int_o^t Q_o dt \simeq \frac{1}{t}\int_o^t A\, dt = A_\infty + (1-A_\infty)\,\frac{1}{\Psi+\lambda_F+\lambda_S}\,\frac{1}{t}\left[1-\exp\{-(\Psi+\lambda_F+\lambda_S)t\}\right] \tag{21}$$

For a time interval

$$t \gg \frac{1}{\Psi+\lambda_F+\lambda_S} \tag{22}$$

eq. 21 becomes

$$\bar{A} \simeq A_\infty = \frac{\Psi}{\Psi+\lambda_F+\lambda_S} \tag{23}$$

"A" is called point availability and $A_\infty$ asymptotic availability. "$A_\infty$" can also be expressed as follows

$$A_\infty = \frac{\text{operation time}}{\text{operation time + repair time}} \tag{24}$$

It is very interesting to notice that the point availability "A", given by eq. 15, would be the exact solution of the system of eqs. 9 to 12 in the particular case $K_S=0$, that is when we suppose that the probability of the plant to be in the absorbing state (disaster) is equal to zero.

Appendix 6 shows that eq. 23 is valid also in the case in which failure and repair probability density distributions are not exponential. In this case $\Psi$, $\lambda_F$, $\lambda_S$ are only average values.

"$1-A_\infty$" is called "unavailability" and we shall indicate it with the symbol "U"

$$U = 1-A_\infty = \frac{\lambda_F+\lambda_S}{\Psi+\lambda_F+\lambda_S} \tag{25}$$

We shall now introduce the annual loss function "Z".

When the plant is in shut down, it does not produce electricity. The expected amount of money lost in a year because of the unavailability of the plant is

$$P\,T\,\gamma\,U \tag{26}$$

where

P = power of the plant (kW)

T = number of hours in a year, during which the plant is planned to be in operation (hrs)

$\gamma$ = price of the kWh minus price of the fuel which produces a kWh.

We shall call the quantity given by eq. 26: annual unavailability cost. The value of "$\gamma$" is very difficult to estimate. It depends upon many factors such as the possibility to increase the load of other plants, or to buy the energy from another electricity producer. The price of the kWh, due to the "unavailability" of the plant occurred during the day, will be different from that due to the "unavailability" occurred during the night.

The evaluation of "$\gamma$" is by itself a big problem which exceeds the limits of this report. We shall suppose that $\gamma$ has been elsewhere already evaluated.

Some money will be lost, to repair and start the plant up after a failure is occurred. We shall indicate this amount of money with "ß". The expected total amount of money lost in a year for repair and start-up will be

$$ß(\lambda_F+\lambda_S) \tag{27}$$

We shall call the quantity given by eq. 27: annual shut down cost.
We shall indicate with "C" the annual subsystems cost, that is the cost per year of all those parts of the plant which contribute to its "unavailability". This cost will include the capital costs per year for design, construction and installation, the operation costs, and the maintenance costs.

We can now calculate the expected amount of money lost in a year "Z" (annual loss function). Taking into account eqs. 26 and 27, and the definition of "C", we can write

$$Z = P\,T\,\gamma\,U + ß(\lambda_F+\lambda_S) + C \tag{28}$$

From eqs. 25 and 28 we get finally

$$Z = \left( \frac{P\ T\ \gamma}{\Psi+\lambda_F+\lambda_S} + \beta \right) (\lambda_F+\lambda_S) + C \qquad (29)$$

We notice that the first term (on the right side of eq. 29) is a function which increases with "$\lambda_F+\lambda_S$". The term "C" will instead decrease with "$\lambda_F+\lambda_S$", for the simple reason that the less the parts of the plant will fail, the more they will cost.

The function "Z", being the sum of two terms, one increasing and the other decreasing with "$\lambda_F+\lambda_S$", will have a minimum. We shall indicate with

$$(\lambda_F)_{opt} \quad \text{and} \quad (\lambda_S)_{opt}$$

respectively the values of $\lambda_F$ and $\lambda_S$ which give the minimum value of "Z" ($Z_{min}$).

The problem, which the designer must solve, is to find $(\lambda_F)_{opt}$, $(\lambda_S)_{opt}$ and $Z_{min}$. Let us suppose that we have already found these values.

We can now define a second problem. The safety committee requires that, for safety reasons, the rate of occurrence of a big accident ($K_S\lambda_F$) should not exceed a value "$\upsilon_{max}$" which is fixed by the safety regulations. We can write therefore

$$\upsilon_d = K_S\lambda_F < \upsilon_{max} \qquad (30)$$

For $(\lambda_F)_{opt}$, eq. 30 will become

$$K_S < \frac{\upsilon_{max}}{(\lambda_F)_{opt}} \qquad (31)$$

The safety system must be designed in such a way, that its reduction coefficient "$K_S$" does not exceed the limit value given by the expression 31. In effect, the fullfillment of 31 will have a feedback to the evaluation of $Z_{min}$ because "$\lambda_S$" depends too on the characteristics of the safety system. Condition 31 must therefore be regarded as a constraint to the problem to minimize "Z". This will become clearer with the numerical example which will be shown in the following paragraph.

## 4. A numerical example

We shall suppose that all the functional subsystems are 100 % reliable with the exception of the power supply subsystem, which feeds the motor of the pump in the primary coolant circuit of a nuclear reactor plant.

We shall also suppose that only the measuring channels of the voltage to the pump motor can fail, while the other safety subsystems cannot fail.

If the power supply subsystem fails, the pump stops and the reactor is not cooled any more. If, in addition, the safety subsystem fails to shut the reactor down (failure type "a"), there will be a big accident (core melt down).

The plant can go from state "0" (fig. 7) to state "1" in the two following cases

(i) failure of the power supply subsystem followed by a correct action of the voltage measuring channels

(ii) failure type "b" (false trip) of the voltage measuring channels.

We shall suppose that the mean time "$1/\Psi$" and the shut down cost "$\beta$" to repair the plant will be the same for both the cases.

The annual loss function "Z" will be

$$Z = \left( \frac{P\ T\ \gamma}{\Psi+\lambda_F+\lambda_S} + \beta \right) (\lambda_F+\lambda_S) + C_F + C_S \qquad (1)$$

where

$\lambda_F$ = failure rate of the power supply subsystem

$\lambda_S$ = failure rate of the motor voltage measuring channels (failure type "b").

$C_F$ = annual cost of the power supply subsystem

$C_S$ = annual cost of the motor voltage measuring channels.

Since we have

$$\Psi \gg \lambda_F+\lambda_S \qquad (2)$$

eq. 1 can be simplified as follows

$$Z = \left( \frac{P\ T\ \gamma}{\Psi} + \beta \right) (\lambda_F+\lambda_S) + C_F + C_S \qquad (3)$$

Eq. 3 can still be written in a different way

$$Z = Z_F + Z_S \tag{4}$$

where

$$Z_F = \left[\frac{P\ T\ \gamma}{\psi} + \beta\right] \lambda_F + C_F \tag{5}$$

and

$$Z_S = \left[\frac{P\ T\ \gamma}{\psi} + \beta\right] \lambda_S + C_S \tag{6}$$

Let us suppose that the constraint given by the safety committee is

$$\upsilon_d = K_S \lambda_F < \upsilon_{max} = 10^{-9}/\text{year} \tag{7}$$

The "power supply subsystem" consists of "$n_F$" units, one of which is working and the others are in stand-by. When the working unit fails, it is automatically switched off, while one of the stand-by units is switched into operation. The power supply subsystem will fail if all the "$n_F$" units fail before the repair of the first has been completed. We shall suppose in our example that the automatic switch cannot fail. We have (eq. 20 of para 5.4 and Appendix 7 para A7.2)

$$\lambda_F \simeq \frac{\sigma_F^{n_F}}{\mu_F^{(n_F-1)}} \tag{8}$$

where

$\sigma_F$ = average failure rate of a power supply unit (9)

$\mu_F$ = average repair rate of a power supply unit (10)

We have also

$$C_F = n_F c_F \tag{11}$$

where

$c_F$ = annual cost of a power supply unit (12)

Let us suppose that only three types of power supplies are available on the market and that they lie on the following curve (fig. 8)

$$c_F = A' + \frac{A''}{\sigma_F} = (10^4 + \frac{100}{\sigma_F}) \text{ D.M./year} \qquad (13)$$

Fig. 9 shows "$Z_F$" as function of "$\sigma_F$" for different values of "$n_F$". To calculate the curves of fig. 9 we have used the following numerical values for the known parameters

$$\mu_F = 10^2/\text{years} \qquad (14)$$

$$\frac{P\ T\ Y}{\Psi} + \beta = 2 \cdot 10^6 \text{ D.M.} \qquad (15)$$

The "Safety subsystem" (measuring channels) consists of "$n_S$" units all in active redundancy. The network is built in such a way that, if the voltage to the stator fails, and "$m_S$" out of the "$n_S$" units also fail (failure type "a"), the safety system will not shut the reactor down and there will be a big accident (reactor melt down).

For the "safety subsystem" we have the following expressions (para. 2 eqs. 7, 13)

$$K_S = \frac{(n_S)!(\rho_S \tau_S)^{m_S}}{(m_S+1)!(n_S-m_S)!} \qquad (16)$$

$$\lambda_S = \frac{(n_S)!}{(n_S-\ell_S)!} \frac{\sigma_S^{\ell_S}}{\mu_S^{(\ell_S-1)}} \qquad (17)$$

Since we have (eq. 14 of para. 2)

$$\ell_S = n_S + 1 - m_S \qquad (18)$$

eq. 17 becomes

$$\lambda_S = \frac{(n_S)!}{(m_S-1)!} \frac{\sigma_S^{(n_S+1-m_S)}}{\mu_S^{(n_S-m_S)}} \qquad (19)$$

The symbols of eqs. 16 to 19 have the following meaning

$\rho_S$ = unit failure rate for failure type "a"

$\tau_S$ = checking period

$\sigma_S$ = unit failure rate for failure type "b"

$\mu_S$ = unit repair rate, that is reciprocal of the mean time to repair a unit after a failure type "b"

$\ell_S$ = number of units which must fail in order to make the subsystem to fail (failure type "b")

The cost "$C_S$" of the safety subsystem is given by

$$C_S = n_S \, c_S \tag{20}$$

where

$c_S$ = annual cost of a unit

Taking into account eq. 16, the constraint 7 becomes

$$K_S = \frac{(n_S)!(\rho_S \tau_S)^{m_S}}{(m_S+1)!(n_S-m_S)!} < \frac{\upsilon_{max}}{\lambda_F} = \frac{10^{-9}}{\lambda_F} \tag{21}$$

For the sake of simplicity, we shall suppose that only one type of measuring channel is available on the market and that "$\tau_S$" has already been chosen.

For the designer therefore, the following values will be fixed

$$\sigma_S = 1/\text{year} \tag{22}$$

$$\rho_S \tau_S = 10^{-3} \tag{23}$$

$$\mu_S = 10^4/\text{year} \tag{24}$$

$$c_S = 10^2 \text{ D.M./year} \tag{25}$$

Fig. 10 shows the limit curve

$$K_{max} = \frac{10^{-9}}{\lambda_F} \tag{26}$$

as function of "$\lambda_F$".

The following two tables give "$\lambda_S$" (eq. 19); $Z_S$ (eq. 6) and $K_S$ (eq. 16) as functions of "$m_S$" and "$n_S$"

Table 1

| $m_S = 2$ | | | |
|---|---|---|---|
| $n_S$ | $\lambda_S$ (years$^{-1}$) | $Z_S$ (D.M./year) | $K_S$ |
| 3 | $6 \cdot 10^{-4}$ | $1.5 \cdot 10^{3}$ | $10^{-6}$ |
| 4 | $2.4 \cdot 10^{-7}$ | $4 \cdot 10^{2}$ | $2 \cdot 10^{-6}$ |
| 5 | $1.2 \cdot 10^{-10}$ | $5 \cdot 10^{2}$ | $3.33 \cdot 10^{-6}$ |
| 6 | $7.2 \cdot 10^{-14}$ | $6 \cdot 10^{2}$ | $5 \cdot 10^{-6}$ |

Table 2

| $m_S = 1$ | | | |
|---|---|---|---|
| $n_S$ | $\lambda_S$ (year$^{-1}$) | $Z_S$ (D.M./year) | $K_S$ |
| 2 | $10^{-4}$ | $2 \cdot 10^{2}$ | $10^{-3}$ |
| 3 | $6 \cdot 10^{-8}$ | $3 \cdot 10^{2}$ | $1.5 \cdot 10^{-3}$ |
| 4 | $2.4 \cdot 10^{-11}$ | $4 \cdot 10^{2}$ | $2 \cdot 10^{-3}$ |
| 5 | $1.2 \cdot 10^{-14}$ | $5 \cdot 10^{2}$ | $2.5 \cdot 10^{-3}$ |

From the analysis of figs. 9 and 10 and of the tables 1 and 2, we can easily conclude that the designer will obtain the minimal annual loss "$Z_{min}$", and at the same time will satisfy the constraint given by the safety committee, if he will take the following decisions:

(i) he chooses, among all the types of power supply units available on the market, the type No. 2 which is characterized by

$$\sigma_F = 0.1/\text{years} \tag{27}$$

and

$$c_F = 11{\cdot}000 \text{ D.M./year} \tag{28}$$

(ii) he decides to have one power supply unit working and the other in stand-by, that is

$$n_F = 2 \tag{29}$$

(iii) he decides to have 4 measuring channels so connected that "3" of them must fail (failure type "b") in order to give a false trip.

$$n_S = 4 \tag{30}$$

$$m_S = 2 \tag{31}$$

With the numerical values 27, 28, 29, 30 and 31, we get

$$\lambda_F = 10^{-4}/\text{year} \tag{32}$$

$$Z_F = 22'000 \text{ D.M./year} \tag{33}$$

$$Z_S = 400 \text{ D.M./year} \tag{34}$$

$$Z = Z_F + Z_S = 22'400 \text{ D.M./year} \tag{35}$$

and

$$K_S \lambda_F = 2 \cdot 10^{-10}/\text{year} < 10^{-9}/\text{year} \tag{36}$$

It is very interesting to notice from eqs. 33 and 34 that

$$Z_S << Z_F \tag{37}$$

which means that the minimum of the partial annual loss "$Z_S$" of a safety subsystem is much smaller than that of the partial annual loss "$Z_F$" of a functional subsystem.

## 5. The annual loss "Z" as function of the characteristics of the units of the plant

### 5.1 Generals

The annual loss function "Z" is given by the sum of three terms

$$Z = PT\gamma U + B + C \qquad (1)$$

"$PT\gamma U$" is the "annual unavailability cost", and represents the expected amount of money lost each year, because of the unavailability of the plant.

"B" is the "annual shut down cost", and represents the expected amount of money needed each year to repair the plant any time shut down occurs and to bring it back into normal operation.

"C" is the "annual subsystems cost", and represents the total cost per year of all the subsystems which contribute to the plant unavailability. This cost includes the capital, operation and maintenance costs per year of the subsystems.

In the next paragraphs we shall express "Z" as function of the characteristics of the units of the plant.

### 5.2 The "plant unavailability", U, as function of the characteristics of the functional and safety subsystems

In paragraph 3 we have defined three possible states of the plant: normal operation, shut down, and disaster.

In reality the "shut down" state is not only one state, but a collection of different states which have in common the two following properties

(i) when the plant is in one of these states, no electric power is produced

(ii) it is possible to repair the plant and to bring it to "normal operation".

Fig. 11 shows a schematic flow diagram of the various states. They are

State 0 = normal operation
States 1 to N = shut down
State D = disaster

Each state "i" of the "N" shut down states is characterized by the failure rate "$\upsilon_i$", the repair rate "$\Psi_i$" and the shut down cost "$\beta_i$", which is the cost to repair the plant and to bring it back into normal operation.

As seen in paragraph 3, the probability "$Q_o$" that the plant at time "t" is in state "0" is given by

$$Q_o \simeq AR \tag{1}$$

where

$$R \simeq \exp(-\upsilon_d t) \tag{2}$$

and "A" is the point availability, which is calculated by supposing that the probability of the plant to be in the absorbing state (disaster state) is equal to zero.

If we neglect the absorbing state and indicate with "$S_i$" the probability that the plant at time "t" is in state "i" (i=1;2...N), we can write the following equations (fig. 11)

$$\frac{dA}{dt} = - A \sum_{i=1}^{N} \upsilon_i + \sum_{i=1}^{N} \Psi_i S_i \tag{4}$$

$$\frac{dS_i}{dt} = \upsilon_i A - \Psi_i S_i \qquad (i=1;2;...N) \tag{5}$$

and

$$\sum_{i=1}^{N} S_i = 1 - A \tag{6}$$

The above "N+2" equations are not all independent: one of them can be obtained from the others "N+1". Since we are interested in the asymptotic availability "$A_\infty$", we can solve the equations 4 to 6 by putting all the derivatives equal to 0.

From the equations 5 we get

$$S_{i\infty} = \frac{\upsilon_i}{\Psi_i} A_\infty \qquad (i=1;2;...N) \tag{7}$$

where

$$S_{i\infty} = S_i(\infty) \tag{8}$$

Putting the eqs. 7 in 6, we obtain

$$1-A_\infty = A_\infty \sum_{i=1}^{N} \frac{\upsilon_i}{\Psi_i} \tag{9}$$

and finally

$$A_\infty = \frac{1}{1 + \sum_{i=1}^{N} \frac{\upsilon_i}{\Psi_i}} \tag{10}$$

We shall now introduce the symbol "$A_{i\infty}$" so defined

$$A_{i\infty} = \frac{\Psi_i}{\upsilon_i + \Psi_i} \tag{11}$$

"$A_{i\infty}$" would be equal to the asymptotic plant availability "$A_\infty$" in the particular case in which the state "i" is the only possible shut down state, that is when

$$\upsilon_j = 0 \qquad (j \neq i) \tag{12}$$

and

$$\upsilon_i \neq 0 \tag{13}$$

Taking into account eq. 11, eq. 10 becomes

$$A_\infty = \frac{1}{1 + \sum_{i=1}^{N} \frac{1-A_{i\infty}}{A_{i\infty}}} \tag{14}$$

Introducing the "plant unavailability" U, we get finally from eq. 14

$$U = \frac{\sum_{i=1}^{N} \frac{\bar{U}_i}{1-\bar{U}_i}}{1 + \sum_{i=1}^{N} \frac{\bar{U}_i}{1-\bar{U}_i}} \tag{15}$$

where $\bar{U}_i$ is called "partial unavailability" and it is given by

$$\bar{U}_i = 1 - A_{i\infty} = \frac{\upsilon_i}{\upsilon_i + \Psi_i} \tag{16}$$

Eqs. 15 and 16 have been obtained for constant values of $\upsilon_i$ and $\Psi_i$. This corresponds to the case in which the failure probability density distribution "$f_i(t)$" and the repair probability density distribution "$w_i(t)$" are both exponential. However, due to the conclusions reached in Appendix 6, these two equations are also valid in the case in which "$f_i(t)$" and "$w_i(t)$" are not exponential. In this last case "$\upsilon_i$" and "$\Psi_i$" are average values given respectively by eqs. 5 and 4 of para A6.7.

If one thinks to all the possible combinations of failures among functional and safety subsystems, he would conclude that the number of shut down states in a plant is tremendously high. For this reason it is convenient to divide the shut down states in groups which are chosen with a criterion explained below.

Eq. 15 can be written as follows

$$\frac{U}{1-U} = \sum_{i=1}^{N} \frac{\bar{U}_i}{1-\bar{U}_i} \qquad (17)$$

Eq. 17 suggests the idea that, to get the unavailability "$U_j$" of a group of "partial unavailabilities", one has to sum the partial unavailabilities in the following way

$$\frac{U_j}{1-U_j} = \sum_{i=1}^{N_j} \frac{\bar{U}_{ji}}{1-\bar{U}_{ji}} \qquad (18)$$

where

"j" indicates group "j"

"ji" indicates shut down state "ji" belonging to group "j"

$\bar{U}_{ji}$ = partial not availability due to shut down state "ji"

$N_j$ = number of the shut down states belonging to group "j".

Fig. 12 shows a schematic diagram of the major components of a nuclear power plant. A major component, with associated auxiliary parts to make it to function and safety subsystems to protect it against accidents, will be called "block". A "block" is therefore a group of subsystems. A "block" will be said unavailable, when it does not perform the function for which it has been built. For instance, the primary coolant pump (block No. 2) will be not available, if it does not maintain the primary coolant in circulation. All the partial unavailabilities, which contribute to the unavailability of a block, will be grouped together to give the unavailability of the block.

With reference to fig. 12, we can define the following nine blocks

Block No. 1 Reactor
Block No. 2 Primary Coolant Pump
Block No. 3 Steam Generator
Block No. 4 Primary Circuit

Block No. 5 Turbine
Block No. 6 Electric Generator
Block No. 7 Condenser
Block No. 8 Water Pump
Block No. 9 Secondary Circuit

The division of the plant in blocks is a matter of convenience and is somewhat arbitrary. The designer may find more convenient to divide the plant in blocks different from those listed above.

The plant unavailability "U" will be given by:

$$\frac{U}{1-U} = \sum_{j=1}^{M} \frac{U_j}{1-U_j} \qquad (19)$$

where "M" is the total number of the blocks. In the case of fig. 12 we have M=9.

One can also divide the blocks in sub-blocks and these in subsystems.

The "block unavailability" "$U_j$" will be a function of the "partial unavailabilities" "$U_{ji}$" according to eq. 18. We shall now analyse an example to show how to calculate "$U_j$".

Fig. 13 shows a schematic diagram of the primary coolant pump /Block No. 2/.

The primary coolant pump is driven by an electric motor, which is fed from the power supplies subsystem. The pump bearings are cooled with oil, which is maintained in circulation by means of the oil pumps subsystem. It is important to point out that this example is made purposely simple, because we intend to illustrate the principles and not to solve a practical case. Let us now continue with our example. The safety system has the purpose to save the major components (reactor, primary coolant pump) against accidents. It is clear that, from safety point of view, the reactor will have first priority. This means that, if a choice must be done between reactor and pump, we shall choose to save the reactor first and after the pump. If the oil pressure decreases, (which is dangerous for the bearings), it will be detected by the "oil pressure measuring channels" (S21), which will first shut the reactor down (through the intermediate relays network S14 and the reactor actuators S15) and after will switch the pump drive motor off (through the intermediate relays network S22 and the pump actuators S23). This sequence of actions is obtained through a feedback from the reactor actuators (S15) to the input of the intermediate relays network (S22).

If the voltage to the pump drive motor fails, the pump will stop and this will produce a big reactor accident (loss of coolant flow accident). For this reason the voltage is measured by the "voltage measuring channels" (S11), which will shut the reactor down through S14 and S15.

The safety system includes also two other trips: one for low coolant flow (S12) and the other for high reactor outlet coolant temperature (S13).

We shall call "initial event" any failure of a functional subsystem or of a safety subsystem, which brings the plant to a failed state (shut down or disaster). For the sake of simplicity, we shall suppose that only some of the functional subsystems belonging to the block No. 2 (primary coolant pump) can fail. They are

Functional Subsystem No. F21 = Oil pumps subsystem
Functional Subsystem No. F22 = Oil circuit subsystem (oil leakage)
Functional Subsystem No. F23 = Power supplies subsystem

A functional subsystem will be indicated with the letter "F" followed by two or more figures, the first figure being the number of the block to which the functional subsystem belongs.

The safety subsystems, which belong to the block No. 2, are those which protect the primary coolant pump and exactly

Safety Subsystem S21 = measuring channels of oil pressure
Safety Subsystem S22 = pump intermediate relays network
Safety Subsystem S23 = pump actuators

A safety subsystem will be indicated with the letter "S" followed by two or more figures, the first figure being the number of the block to which the safety subsystem belongs.

The safety subsystem S21 acts on the intermediate relays network S14 and S22, and protects both primary coolant pump and reactor against accidents. The safety subsystem S21 can therefore be assigned either to the block No. 2 (primary coolant pump) or to the block No. 1 that is the reactor.

We have thought to assigne the structure of the oil pressure measuring channels (S21) to the block of the primary coolant pump (No. 2), because the oil pressure is strictly related to the good operation of the pump bearings. In this case the unavailability of the reactor is a consequence of the not availability of the primary coolant pump, because the pump is not allowed to function with

too low oil pressure at the bearings.

The assignement of a safety subsystem to a block instead of another may be a matter of personal judgement of the designer. But the designer must be very careful, when he makes the division of the plant in blocks, that he does not assigne the same shut down state to two different blocks. In order to avoid this error, he must check that the list of the shut down states grouped in a block contains only those having as "initial events" the failures of the functional and safety subsystems which he has assigned to the block.

The safety subsystems

S11 (measuring channels of stator voltage)
S12 (measuring channels of primary coolant flow)
S13 (measuring channels of reactor outlet temperature)
S14 (reactor intermediate relays network)
S15 (reactor actuators)

belong to the reactor block (No. 1) because they protect only the reactor against accidents.

Now we can illustrate the procedure to calculate the not availability $U_2$ of block No. 2. The initial events which must be considered are only those linked to failures of the subsystems belonging to block No. 2 and exactly: F21, F22, F23, S21, S22, S23. For the safety subsystems only the failure type "b" can initiate a shut down.

The shut down states of block 2 are the following

Shut down State No. 21 = Oil pumps subsystem failed
Shut down State No. 22 = Oil circuit subsystem failed
Shut down State No. 23 = Power supplies subsystem failed
Shut down State No. 24 = Primary coolant pump failed
Shut down State No. 25 = False Trip (failure type "b" of a safety subsystem).

We want to point out that the failure of the primary coolant pump (shut down state 24) can be due either to the failure of the oil pumps subsystem, or to that of the oil circuit. Strictly speaking we should have two different shut down states with primary coolant pump failed. However, since the time needed to repair the pump is much longer than those needed to repair the oil pumps and the oil circuit, we can group the two shut down states together in one alone.

The same considerations have guided us in grouping all the false trips in one state alone (state 25).

In general we can say that all the shut down states, which belong to the same block, and which are characterized by the same (or almost the same) repair rate "$\psi$" and shut down cost "$\beta$", can be grouped in one state alone. This state will have the same repair rate and repair cost, and a failure rate equal to the sum of the failure rates of all the shut down states which have been grouped together.

Fig. 14 shows the trees to go from the initial events to the shut down states for block No. 2. Each tree is shown in details from fig. 15 to fig. 19. These trees give all the minimal paths to go from the initial events to the shut down state to which the tree refers.

From the analysis of these trees, one realizes immediately that, in order to go to the shut down state, some subsystems are required to fail and some other safety subsystems are instead required to function. At the time of the failure of a functional subsystem, the probability that a safety subsystem (related to it) has not failed is much higher than the probability that it has already failed. We shall not make therefore any appreciable error in the evaluation of the failure rate of a minimal path, if we suppose that the safety subsystem, which is required to function, has a probability equal to 1 to function.

The table of fig. 20 shows all the minimal paths of all the trees belonging to block No. 2. Here, for each minimal path, only the subsystems which are required to fail are shown. The minimal paths are shown horizontally: the sign "+" in the column of a subsystem indicates that the subsystem is required to fail. For the safety subsystems we have, as usually, the two types of failure "a" and "b".

We shall indicate with "$\upsilon$" the rates of occurrence (or failure rates) of the minimal paths, with "$\lambda_F$" the failure rates of the functional subsystems and with "$\lambda_S$" the failure rates type "b" of the safety subsystems.

For the shut down state 21 and 22 (fig. 20) we have respectively

$$\upsilon_{21} = \upsilon_{211} = \lambda_{F21} \tag{20}$$

$$\upsilon_{22} = \upsilon_{221} = \lambda_{F22} \tag{21}$$

For the shut down state 23 we have

$$\upsilon_{23} = \upsilon_{231} + \upsilon_{232} + \upsilon_{233} \tag{22}$$

Looking at fig. 20, one realizes immediately that the rates of occurrence of the minimal paths 232 and 233 are much smaller than the rate of occurrence of the minimal path 231

$$\upsilon_{232} = K_{S11}\ \upsilon_{231} \ll \upsilon_{231} \tag{23}$$

and

$$\upsilon_{233} = H_{S11;S12} \cdot K_{S11} K_{S12} \upsilon_{231} \ll \upsilon_{231} \tag{24}$$

where $K_{S11}$ and $K_{S12}$ are the reduction coefficients respectively of the safety subsystems S11 and S12 and $H_{S11;S12}$ is the coupling coefficient between the safety subsystems S11 and S12. Both these coefficients have been defined in para. 2.

Taking into account 23 and 24, eq. 22 becomes

$$\upsilon_{23} \simeq \upsilon_{231} = \lambda_{F23} \tag{25}$$

For the shut down state 24, we notice the following (fig. 20)

$$\upsilon_{244} = K_{S12}\ \upsilon_{243} << \upsilon_{243} \tag{26}$$

and

$$\upsilon_{248} = K_{S12}\ \upsilon_{247} << \upsilon_{247} \tag{27}$$

Taking into account 26 and 27, we can write (fig. 20)

$$\upsilon_{24} \simeq \upsilon_{241} + \upsilon_{242} + \upsilon_{243} + \upsilon_{245} + \upsilon_{246} + \upsilon_{247} \tag{28}$$

Now we have

$$\upsilon_{241} = K_{S22}\ \lambda_{F21} \tag{29}$$

$$\upsilon_{242} = K_{S23}\ \lambda_{F21} \tag{30}$$

$$\upsilon_{243} = K_{S21}\ \lambda_{F21} \tag{31}$$

$$\upsilon_{245} = K_{S22}\ \lambda_{F22} \tag{32}$$

$$\upsilon_{246} = K_{S23}\ \lambda_{F22} \tag{33}$$

$$\upsilon_{247} = K_{S21}\ \lambda_{F22} \tag{34}$$

where with "$K_S$" we have indicated the reduction coefficients of the various safety subsystems.

Taking into account eqs. 29 to 34, eq. 28 becomes

$$\upsilon_{24} = (\lambda_{F21} + \lambda_{F22})(K_{S22} + K_{S23} + K_{S21}) \tag{35}$$

For the shut down state 25 we notice that (fig. 20)

$$\upsilon_{254} = K_{S12}\ \upsilon_{252} << \upsilon_{252} \tag{36}$$

and

$$\upsilon_{255} = K_{S12}\ \upsilon_{253} << \upsilon_{253} \tag{37}$$

Taking into account the expressions 36 and 37, we can write

$$\upsilon_{25} = \upsilon_{251} + \upsilon_{252} + \upsilon_{253} \tag{38}$$

Since we have (fig. 20)

$$\upsilon_{251} = \lambda_{S21} \tag{39}$$

$$\upsilon_{252} = \lambda_{S22} \tag{40}$$

$$\upsilon_{253} = \lambda_{S23} \tag{41}$$

eq. 38 becomes

$$\upsilon_{25} = \lambda_{S21} + \lambda_{S22} + \lambda_{S23} \tag{42}$$

Eqs. 20, 21, 25, 35 and 42 gives the rates of occurrence of the shut down states of block 2 as function of the characteristics of the functional and safety subsystems.

Since the not availability of block No. 2 is given by

$$U_2 = \frac{\sum_{i=1}^{5} \frac{\upsilon_{2i}}{\upsilon_{2i}+\Psi_{2i}}}{1 + \sum_{i=1}^{5} \frac{\upsilon_{2i}}{\upsilon_{2i}+\Psi_{2i}}} \qquad (43)$$

we have to calculate all the repair rates "$\Psi_{2i}$".

The repair rate "$\Psi_{2i}$" is the reciprocal of the mean time needed to bring the power station from shut down state "2i" back into normal operation (state 0). This mean time must include the time needed to repair the subsystems which have failed and that needed to start the plant up again. The repair rates are therefore also very much dependent upon the way in which the repair actions are carried out and organized (for example upon the number of the repair crews). Their values must be obtained by collecting and analysing data coming from experience gained with the operation of previous power plants similar to that which the designer takes under consideration.

In general for a block "j" having "$N_j$" shut down states, we can write

$$U_j = \frac{\sum_{i=1}^{N_j} \frac{\upsilon_{ji}}{\upsilon_{ji}+\Psi_{ji}}}{1 + \sum_{i=1}^{N_j} \frac{\upsilon_{ji}}{\upsilon_{ji}+\Psi_{ji}}} \qquad (44)$$

## 5.3 The overlapping coefficient. Its definition and its influence on the "plant unavailability"

Taking into account that

$$\upsilon_i = \frac{1}{\text{average time interval between two shut down states "i"}} = \frac{1}{t_{oi}} \qquad (1)$$

and

$$\Psi_i = \frac{1}{\text{average time needed to bring the plant into operation from shut down state "i"}} = \frac{1}{t_{ri}} \qquad (2)$$

the partial unavailability $\bar{U}_i$ (eq. 16 of para. 5.2) can also be written as follows

$$\bar{U}_i = \frac{t_{ri}}{t_{oi}+t_{ri}} \tag{3}$$

Putting eq. 3 in eq. 15 of para 5.2, we get for the plant unavailability "U"

$$U = \frac{\sum_{i=1}^{N} \frac{t_{ri}}{t_{oi}}}{1 + \sum_{i=1}^{N} \frac{t_{ri}}{t_{oi}}} \tag{4}$$

If we indicate with "$T_o$" a long time interval, we have

$$t_{oi} = \frac{T_o(1-U)}{a_i} \tag{5}$$

where "$a_i$" is the expected number of times that the shut down state "i" occurs in the time interval "$T_o$". Putting 5 in 4, we get finally

$$U = \frac{\sum_{i=1}^{N} a_i\, t_{ri}}{T_o} = \frac{T_r}{T_o} \tag{6}$$

where "$T_r$" is the total time during which the plant is in shut down. This total repair time is given, as shown by eq. 6, by summing the lengths of time "$a_i t_{ri}$", where "$a_i t_{ri}$" is the total length of time spent by the plant in the shut down state "i". This means that, in the model developed in para 5.2, no overlapping among the individual repair times "$a_i t_{ri}$" has been taken into account. We have practically supposed that a failure of a subsystem creates a situation so dangerous for the plant, that immediate shut down is required.

Many times the failure of a subsystem does not bring the power station in a so dangerous situation that immediate shut down is required. In other words, there are different degrees of danger. Take, for instance, the case of the pressure of the oil which cools the bearings of the primary coolant pump (fig. 13). If a leakage occurs in the oil circuit, the pressure will start to decrease and, when it falls beyond a certain value, there will be an alarm. The operating crew will find out what has caused this alarm, and, on the basis of the evaluation of the amount of oil which is being lost from the oil circuit, can

decide either to shut the plant down and to repair the oil circuit immediately, or to wait for the next routine maintenance. It may happen that, while waiting for the next routine plant maintenance, the oil pressure decreases beyond a value so low that the safety system shuts automatically the plant down. On the other hand, it may also happen that, while waiting for the routine plant maintenance, the failure of another subsystem occurs, which shuts the plant down, and then both the damages will be repaired at the same time.

The above considerations bring to the conclusion that the repair times for the various subsystems may overlap one with another. This effect, as already said, has not been taken into account in the model described in para 5.2. The degree of overlapping depends upon the type of the plant, the repair policy followed by the crew which operates the plant etc.

It seems convenient therefore to define an "overlapping coefficient", $s_p$, to be determined from operating experience. For the definition of this coefficient we should refer to the partial unavailabilities $\bar{U}_i$. Since this would be probably too complicate because of the large number of shut down states, we shall refer to the unavailabilities of the blocks.

With reference to fig. 12, we shall define "$s_p$" as follows (according to a definition suggested by Dr. Vetter and his coworkers of the R.W.E. Essen)

$$s_p = \frac{\sum_{j=1}^{M} \frac{U_j}{1-U_j} - \frac{U}{1-U}}{\sum_{j=1}^{M} \frac{U_j}{1-U_j} - \frac{U_m}{1-U_m}} \qquad (7)$$

where

$U$ = plant unavailability

$U_j$ = "unavailability" of block "j"

$U_m$ = unavailability of the block "m" characterized by having the maximum among the block unavailabilities "$U_j$"

$M$ = number of blocks (equal to 9 in fig. 12)

From 7 we get

$$\frac{U}{1-U} = (1-s_p) \sum_{j=1}^{M} \frac{U_j}{1-U_j} + s_p \frac{U_m}{1-U_m} \qquad (8)$$

The overlapping coefficient "$s_p$" lies always between 0 and 1

$$0 < s_p < 1 \tag{9}$$

When there is no overlapping, we have

$$s_p = 0 \tag{10}$$

and eq. 8 becomes

$$\frac{U}{1-U} = \sum_{j=1}^{M} \frac{U_j}{1-U_j} \tag{11}$$

which is equal to eq. 19 of para 5.2.

The case

$$s_p = 1 \tag{12}$$

corresponds to complete overlapping.

With complete overlapping we mean the case, in which the repairs of the blocks would be all carried out within the repair time of the block which has the maximum unavailability $U_m$.

In this case eq. 8 becomes:

$$\frac{U}{1-U} = \frac{U_m}{1-U_m} \tag{13}$$

## 5.4 The average failure rate of a functional subsystem as function of the characteristics of its units for different strategies

In paragraph 5.2 we have shown how the "plant unavailability "U" can be expressed as function of the failure rates "$\lambda_F$" and "$\lambda_S$" of the functional and safety subsystems and of the reduction coefficients "$K_S$" of the safety subsystems. We want now to express the failure rate "$\lambda_F$" of a functional subsystem as function of the characteristics of its units. The failure rate "$\lambda_F$" depends also upon the type of strategy which is adopted. Here we give the results only for a limited number of strategies. The details of the mathematical developments are given in Appendix 7.

5.4.1 Strategy 1: Functional subsystem consisting of a unit only

The subsystem fails if the unit fails we have simply

$$\lambda_F = \sigma_F = \frac{\int_0^{\Theta_F} h_F(t)dt}{\Theta_F \left[ 1 - \int_0^{\Theta_F} h_F(t)dt \right] + \int_0^{\Theta_F} t\, h_F(t)dt} \qquad (1)$$

where

$t$ = time

$\sigma_F$ = average failure rate of the unit

$h_F(t)$ = failure probability density distribution of the unit

$\Theta_F$ = maintenance period

In the case in which no preventive maintenance is planned ($\Theta_F = \infty$), eq. 1 becomes

$$\lambda_F = \sigma_F = \frac{1}{\int_0^{\infty} t\, h_F(t)dt} \qquad (2)$$

5.4.2 Strategy 2: Functional subsystem consisting of two units one working and the other in stand-by. No preventive maintenance.

If the working unit fails, it is automatically switched off, while the stand-by unit is at the same time automatically switched into operation. The failed unit, after repair, is connected again as stand-by unit. The subsystem fails if the unit, which is working, fails before the repair of the other unit has been completed.

We have

$$\lambda_F = \frac{\sigma_F}{1 + \frac{1}{1 - \lim_{s \to o} (h_F \cdot G_F)^*}} \qquad (3)$$

where

$G_F(t)$ = repair cumulative probability distribution of the unit =

$$= \int_0^t g_F(t)dt \qquad (4)$$

$g_F(t)$ = repair probability density distribution of the unit

$$\sigma_F = \frac{1}{\int_0^\infty t\, h_F(t)dt} \tag{5}$$

s = complex variable of the Laplace domain

"*" indicates Laplace transformation

For the particular case in which the failure probability distribution is exponential

$$h_F(t) = \sigma_F \exp(-\sigma_F t) \tag{6}$$

eq. 3 becomes

$$\lambda_F = \frac{\sigma_F}{1 + \dfrac{1}{1 - \int_0^\infty g_F(t) \exp(-\sigma_F t)dt}} \tag{7}$$

If also $g_F(t)$ is exponential

$$g_F(t) = \mu_F \exp(-\mu_F t) \tag{8}$$

we have

$$\lambda_F = \frac{\sigma_F}{2 + \mu_F/\sigma_F} \tag{9}$$

where

$\mu_F$ = repair rate of the unit

Since $\mu_F/\sigma_F$ is usually very large, eq. 9 can be written as follows

$$\lambda_F \simeq \frac{\sigma_F^2}{\mu_F} \tag{10}$$

It is very interesting to remind that eq. 10 holds approximately also in the case in which $g_F(t)$ is not exponential. In this case

$$\mu_F = \text{average repair rate of the unit} = \frac{1}{\int_0^\infty t\, g_F(t)dt} \tag{11}$$

The demonstration is given in Appendix 7

5.4.3 Strategy 3: Functional subsystem consisting of two units, one working and the other in stand-by. Preventive maintenance.

It is similar to strategy No. 2 with the difference that the working unit is also preventively replaced after having been used a period of time "$\Theta_F$".

We have

$$\lambda_F \simeq \frac{\sigma_F}{1 + \dfrac{1}{1 - \int_0^{\infty} g_F(t)\, \exp(-\sigma_F t)dt}} \qquad (12)$$

where

$$\sigma_F = \frac{\int_0^{\Theta_F} h_F(t)dt}{\Theta_F \left[1 - \int_0^{\Theta_F} h_F(t)dt\right] + \int_0^{\Theta_F} t\, h_F(t)dt} \qquad (13)$$

The following expression holds, only approximately, in the case that $g_F(t)$ is any arbitrary distribution

$$\lambda_F = \frac{\sigma_F^2}{\mu_F} \qquad (14)$$

where

$\sigma_F$ is defined by eq. 14

and $\mu_F$ is defined by eq. 11

5.4.4 Strategy 4: Functional subsystem consisting of "$n_F$" units: "$k_F$" of these units are working and the others "$n_F$-$k_F$" are in stand-by. No preventive maintenance.

If one of the working units fails, it is automatically switched off, while the first of the stand-by units is at the same time automatically switched into operation. If a second unit fails, the second of the stand-by units comes into operation and so on. The failed units, after repair, are mounted again as stand-by units.

The subsystem fails if $n_F$-$k_F$+1 units are failed. We have solved this case only with $h_F(t)$ and $g_F(t)$ being both exponential functions. We obtain

$$\lambda_F = \frac{k_F \sigma_F}{\sum_{i=1}^{n_F-k_F+1} i \left(\frac{\mu_F}{k_F \sigma_F}\right)^{(n_F-k_F+1-i)}} \qquad (15)$$

In the particular case $k_F=1$ (only one unit working), eq. 15 becomes

$$\lambda_F = \frac{\sigma_F}{\sum_{i=1}^{n_F} i \left(\frac{\mu_F}{\sigma_F}\right)^{(n_F-i)}} \qquad (16)$$

Since $\mu_F/\sigma_F$ is usually very large, we have also that eq. 15 can be written approximately

$$\lambda_F \simeq \frac{(k_F \sigma_F)^{(n_F-k_F+1)}}{\mu_F^{(n_F-k_F)}} \qquad (17)$$

In the case $k_F=1$, eq. 17 becomes

$$\lambda_F \simeq \frac{\sigma_F^{n_F}}{\mu_F^{(n_F-1)}} \qquad (18)$$

5.4.5 Strategy 5: Functional subsystem consisting of "$n_F$" units: "$k_F$" of these units are working and the others "$n_F-k_F$" are in stand-by. Preventive maintenance.

It is similar to strategy No. 4 with the difference that the working units are also preventively replaced after having been used a period of time "$\theta_F$".

We have

$$\lambda_F \simeq \frac{(k_F \sigma_F)^{(n_F-k_F+1)}}{\mu_F^{(n_F-k_F)}} \qquad (19)$$

where $\sigma_F$ and $\mu_F$ are given respectively by eqs. 11 and 14.

For $k_F=1$ eq. 19 becomes

$$\lambda_F \simeq \frac{\sigma_F^{n_F}}{\mu_F^{(n_F-1)}} \qquad (20)$$

## 5.5 The reduction and coupling coefficients and the average failure rate of a safety subsystem as function of the characteristics of its units

The parameters of the safety subsystems have already been defined in para. 3, where they are given as function of the characteristics of the units which make the subsystems. Here we repeat only these expressions. The mathematical developments to obtain them are given in the Appendices 3 and 4.

For the reduction coefficient "$K_S$" of a safety subsystem we have

$$K_S = \frac{(n_S)!(\rho_S \tau_S)^{m_S}}{(m_S+1)!(n_S-m_S)!} \qquad (1)$$

where

$n_S$ = number of the units which belong to the safety subsystem

$m_S$ = number of the units which must fail in order to make the unit to fail (failure type "a")

$\tau_S$ = checking period

$\rho_S$ = average failure rate (failure type "a") of a unit and is given by eq. 4 of para. 2

Fig. 3 shows qualitatively "$\rho_S$" as function of "$\Theta_S$" and "$\tau_S$". Figs. 4, 5 and 6 show "$K_S$" as function of the parameter "$\rho_S \tau_S$" for different values of "$m_S$" and "$n_S$". To obtain a smaller value of "$K_S$", one can think to reduce "$\tau_S$" (figs. 4, 5 and 6). But if one reduces "$\tau_S$", $\rho_S$ increases (fig. 3), which means that the units fail more often. The designer will be compelled to make a compromise between these two competing effects.

For the intercoupling coefficient "H" among "N" safety subsystems, we have

$$H_{S1,S2,\ldots,SN} = \frac{\prod_{i=1}^{N} (m_{Si}+1)}{1 + \sum_{i=1}^{N} (m_{Si})} \qquad (2)$$

The failure rate "$\lambda_S$" due to false trip (failure type "b") of a safety subsystem is given by

$$\lambda_S = \frac{\sigma_S}{\sum_{i=o}^{\ell_S-1} \left[ \left(\frac{\mu_S}{\sigma_S}\right)^i \sum_{q=n_S-\ell_S+1+i}^{n_S} \frac{(q-1-i)!}{q!} \right]} \qquad (3)$$

where

$\ell_S$ = number of the units which must fail in order to make the unit to fail

$\sigma_S$ = average failure rate (failure type "b") of a unit and is given by eq. 5 of para. 2

$\mu_S$ = average repair rate of a unit

Fig. 3 shows qualitatively "$\sigma_S$" as function of "$\Theta_S$" and "$\tau_S$".

"$\mu_S$" is given by the following equation

$$\mu_S = \frac{1}{\int_0^\infty t\, g_S(t)dt} \tag{4}$$

where

$g_S(t)$ = repair probability density distribution for a unit.

Since $\mu_S/\sigma_S$ is usually very large, eq. 3 becomes

$$\lambda_S \simeq \frac{n_S!}{(n_S-\ell_S)!} \frac{\sigma_S^{\ell_S}}{\mu_S^{(n_S-\ell_S)}} \tag{5}$$

For the safety subsystems the following relation may hold

$$\ell_S = n_S + 1 - m_S \tag{6}$$

## 5.6 The annual shut down cost "B"

The second term of the annual loss function "Z" is "B", which represents the expected annual cost to repair and to start the plant up after shut down. As we have done for the plant unavailability (para. 5.2), we can also in this case associate to each block the corresponding annual cost for repair and start-up

$$B = \sum_{j=1}^{M} B_j \tag{1}$$

where $B_j$ is the start-up cost related to block "j", and "M" is the number of the blocks.

If we indicate with "$N_j$" the number of shut down states which have been associated to block "j", we have

$$B_j = \sum_{i=1}^{N_j} \bar{B}_{ji} \qquad (2)$$

where $\bar{B}_{ji}$ is the annual shut down cost associated to shut down state "ji".

Finally if we indicate with "$\upsilon_{ji}$" the rate of occurrence of shut down state "ji" and with "$\beta_{ji}$" the shut down cost associated to shut down state "ji", we have

$$\bar{\beta}_{ji} = \beta_{ji}\, \upsilon_{ji} \qquad (3)$$

Taking into account eqs. 2 and 3, eq. 1 becomes

$$B = \sum_{j=1}^{M} \left[ \sum_{i=1}^{N_j} (\beta_{ji}\, \upsilon_{ji}) \right] \qquad (4)$$

## 5.7 The annual subsystems cost "C"

As already done for the plant unavailability and the shut down cost, we can write

$$C = \sum_{j=1}^{M} C_j \qquad (1)$$

where

$C_j$ = annual cost of the subsystems belonging to block "j"

M = number of the blocks

If we indicate with "$C_{Fji}$" the annual cost of the functional subsystem "ji" and with "$C_{Sji}$" that of the safety subsystem "ji" both belonging to block "j", we have

$$C_j = \sum_{i=1}^{L_j} C_{Fji} + \sum_{i=1}^{A_j} C_{Sji} \qquad (2)$$

where "$L_j$" and "$A_j$" are respectively the number of functional and safety subsystems belonging to block "j".

5.7.1 Functional Subsystems

The annual cost of a functional subsystem is given by

$$C_{Fji} = E_{Fji} + V_{Fji} + Y_{Fji} \qquad (3)$$

where

$E_{Fji}$ = annual capital cost of subsystem "$F_{ji}$". This cost includes the design, construction and installation costs divided by the number of years during which the plant is expected to be in operation. The annual interests of the invested capital must be also included.

$V_{Fji}$ = annual operating cost of subsystem "$F_{ji}$"

$Y_{Fji}$ = annual maintenance cost of subsystem "$F_{ji}$"

Now we shall express the costs $E_{Fji}$, $V_{Fji}$ and $Y_{Fji}$ as functions of the costs of the units which belong to the subsystem "$F_{ji}$".

For the sake of simplicity, let us drop the subscript "ji".

We have

$$E_F = n_F \cdot e_F \qquad (4)$$

$$V_F = k_F v'_F + (n_F - k_F) v''_F \qquad (5)$$

and

$$Y_F = \frac{k_F}{\theta_F} \left[ x_F y'_F + y''_F \right] \qquad (6)$$

$n_F$ = total number of units belonging to the functional subsystem

$e_F$ = annual capital cost of a unit

$k_F$ = number of the working units

$v'_F$ = annual operating cost of a working unit

$v''_F$ = annual operating cost of a stand-by unit

$\theta_F$ = maintenance period (years)

$y'_F$ = cost of a non preventive replacement (or repair)

$y''_F$ = cost of a preventive replacement (or repair)

$x_F$ = expected number of non preventive replacements in the time interval "$\theta_F$".

"$x_F$" is given by the following equation which has been obtained in Appendix 8

$$x_F = \int_0^{\Theta_F} L^{-1}\left[\frac{h_F^*(s)}{1-h_F^*(s)}\right] dt \qquad (7)$$

where

$L^{-1}$ indicates antitransformation from the Laplace to the time domain

"*" indicates Laplace transformation

s = complex variable of the Laplace domain

$h_F^*(s)$ = Laplace transform of h(t)

$h_F(t)$ = failure probability density distribution of a unit

5.7.2 Safety Subsystems

The annual cost of a safety subsystem is given by

$$C_{Sji} = E_{Sji} + V_{Sji} + Y_{Sji} \qquad (8)$$

where

$E_{Sji}$ = annual capital cost of subsystem "$S_{ji}$". This cost includes the design, construction and installation costs divided by the number of years during which the plant is expected to be in operation. The annual interests of the invested capital must be also included

$V_{Sji}$ = annual operating cost of subsystem "Sji"

$Y_{Sji}$ = annual maintenance cost of subsystem "Sji"

Now we shall express the costs $E_{Sji}$, $V_{Sji}$ and $Y_{Sji}$ as functions of the costs of the units which belong to the subsystem "Sji".

Also here, for the sake of simplicity, we drop the subscript "ji".

We have

$$E_S = n_S e_S \qquad (9)$$

$$V_S = n_S v_S \qquad (10)$$

$$Y_S = \frac{n_S}{\Theta_S}\left[x_S y'_S + y''_S\right] \tag{11}$$

where

$n_S$ = total number of the units which belong to the safety subsystem

$e_S$ = annual capital cost of a unit

$v_S$ = annual operating cost of a unit

$\Theta_S$ = maintenance period

$y'_S$ = cost of a non preventive replacement (or repair)

$y''_S$ = cost of a preventive replacement

$x_S$ = expected number of non preventive replacements in the time interval "$\Theta_S$".

"$x_S$" is given by the following equation which has been obtained in Appendix 9

$$x_S = \int_o^{\Theta_S} L^{-1}\left[\frac{\bar{h}^*_S(s,\tau_S)}{1 - \bar{h}^*_S(s,\tau_S)}\right] dt \tag{12}$$

where

$\tau_S$ = checking period

$\bar{h}^*_S(s,\tau_S)$ = Laplace transform of $\bar{h}_S(t,\tau_S)$

$\bar{h}_S(t,\tau_S)$ is the total failure probability density distribution and is given by the following equation

$$\bar{h}_S(t,\tau_S) = \left(1 + \frac{\delta'_S}{\tau_S}\right) \cdot h'_S\left[t_S\left(1 + \frac{\delta'_S}{\tau_S}\right)\right] \cdot \left[1 - \int_o^{t(1+\delta'_S/\tau_S)} h''_S(t)dt\right] +$$

$$+ \left(1 + \frac{\delta''_S}{\tau_S}\right) \cdot h''_S\left[t\left(1 + \frac{\delta''_S}{\tau_S}\right)\right]\left[1 - \int_o^{t(1+\delta'_S/\tau_S)} h'_S(t)dt\right] \tag{13}$$

where

$h'_S(t)$ = failure probability density distribution (failure type "a")

$h''_S(t)$ = failure probability density distribution (failure type "b")

$\delta'_S$ = const.

$\delta''_S$ = const.

## 6. The rate of occurrence "$\upsilon_d$" of a "disaster" as function of the characteristics of the units of the plant

The rate of occurrence "$\upsilon_d$" of a disaster (big accident) is obtained by summing the rates of occurrence of all the minimal paths to go from "normal operation" (state 0) to the "disaster state" (fig. 11)

$$\upsilon_d = \sum_{i=1}^{N} \upsilon_{di} \qquad (1)$$

where

$\upsilon_{di}$ = rate of occurrence associated to the minimal path "i"

N = number of the minimal paths

Strictly speaking, eq. 1 is valid only approximately. One should really sum the probabilities of all the mutually exclusive events, which bring to the "disaster state", to get the total probability "$Q_d$".

From this total probability one should calculate $\upsilon_d$

$$\upsilon_d = - \frac{dQ_d/dt}{1-Q_d} \qquad (2)$$

However, since $Q_d$ is extremely small, one does not make any appreciable error if one instead uses the more simple eq. 1.

As done for the plant unavailability, here too we shall illustrate the calculation of the rate of occurrence "$\upsilon_d$" for the particular case of the scheme shown in fig. 13. We shall suppose that only the subsystems F21, F22, F23, S11, S12, S13, S14, S15, S21, S22, S23 can fail.

The "Disaster Tree", with all the minimal paths to go from the initial events to the "Disaster State", is shown in fig. 21. We have also supposed that the feedback from subsystem "S15" to "S22" is 100 % reliable. From the analysis of this tree, one realizes that some subsystems are required to fail and some other safety subsystems are instead required to function.

At the time of the failure of a functional subsystem, the probability that a safety subsystem (related to it) has not failed is much higher than the probability that it has already failed. We shall not make therefore any appreciable error in the evaluation of the failure rate of a minimal path, if we shall suppose that the safety subsystem, which is required to function, has probability equal

to 1 to function. Fig. 22 shows all the minimal paths: only the subsystems which are required to fail have been included.

From fig. 22 we get

$$\upsilon_d = \sum_{i=1}^{15} \upsilon_{di} \tag{2}$$

where "$\upsilon_{di}$" is the rate of occurrence of the minimal path "i".

From fig. 22 we obtain also

$$\upsilon_{d1} = K_{S14}\ \lambda_{F21} \tag{3}$$

$$\upsilon_{d2} = K_{S15}\ \lambda_{F21} \tag{4}$$

$$\upsilon_{d3} = H_{S12,S13,S21} \cdot K_{S12}\ K_{S13}\ K_{S21}\ \lambda_{F21} \tag{5}$$

$$\upsilon_{d4} = K_{S14}\ \lambda_{F22} \tag{6}$$

$$\upsilon_{d5} = K_{S15}\ \lambda_{F22} \tag{7}$$

$$\upsilon_{d6} = H_{S12,S13,S21} \cdot K_{S12}\ K_{S13}\ K_{S21}\ \lambda_{F22} \tag{8}$$

$$\upsilon_{d7} = K_{S14}\ \lambda_{F23} \tag{9}$$

$$\upsilon_{d8} = K_{S15}\ \lambda_{F23} \tag{10}$$

$$\upsilon_{d9} = H_{S11,S12,S13} \cdot K_{S11}\ K_{S12}\ K_{S13}\ \lambda_{F23} \tag{11}$$

$$\upsilon_{d10} = K_{S15} \lambda_{S22} \tag{12}$$

$$\upsilon_{d11} = K_{S14} \lambda_{S22} \tag{13}$$

$$\upsilon_{d12} = H_{S11,S12} \cdot K_{S11}\ K_{S12}\ \lambda_{S22} \tag{14}$$

$$\upsilon_{d13} = K_{S15}\ \lambda_{S23} \tag{15}$$

$$\upsilon_{d14} = K_{S14}\ \lambda_{S23} \tag{16}$$

$$\upsilon_{d15} = H_{S11,S12} \cdot K_{S11}\, K_{S12}\, \lambda_{23} \qquad (17)$$

where the reduction factors and the coupling coefficients of the safety subsystems have been indicated respectively with "$K_S$" and "H", and the failure rates of the various subsystems have been indicated with "$\lambda$". The equations to calculate the "$K_S$" and "H" coefficients are given in the paragraphs 2 and 5.5.

The equations for the failure rates of the functional and safety subsystems are given respectively in paragraphs 5.4 and 5.5.

## 7. Final considerations on the annual loss function "Z"

In the preceeding paragraphs we have shown how to express the annual loss "Z" as function of the characteristics of the units of the plant.

The designer can choose each unit among the different types available on the market. The best constellation of choices will be that which gives the minimum value of "Z" and at the same time satisfies the constraint that the rate of occurrence "$\upsilon_d$" of a disaster is smaller than the value "$\upsilon_{max}$" fixed by the safety committee.

To develop in details a mathematical method to find the minimum of "Z" is a task which needs to be solved, but which exceeds the limits of our report.

We shall make here only some considerations on a particular procedure, which seems to us at the moment to be very convenient.

We shall indicate with $\left[U/(1-U)\right]_{Fji}$ the quantity U/(1-U) calculated by putting in it equal to zero the failure rates and reduction coefficients of all the safety subsystems and the failure rates of all the functional subsystems with the exception of the functional subsystem "Fji".

We shall indicate with $\left[U/(1-U)\right]_{Sji}$ the quantity U/(1-U) calculated by putting in it equal to zero the failure rates and reduction coefficients of all the safety subsystems with the exception of the safety subsystem "Sji". To calculate $U/(1-U)_{Sji}$ one needs therefore to know also the failure rates of the functional subsystems, which are multiplied by $K_{Sji}$.

In the same way for the annual shut down costs "B", we define the two quantities "$B_{Fji}$" and "$B_{Sji}$".

We can now define the functional partial annual loss functions "$Z_{Fji}$"

$$Z_{Fji} = (1-s_p)(1-U)\left[\frac{U}{1-U}\right]_{Fji} PT\gamma + B_{Fji} + C_{Fji} \qquad (1)$$

where "$s_p$" is the overlapping coefficient.

For example, in the case of the functional subsystem F21 (oil pumps subsystem in fig. 13), we have

$$Z_{F21} = (1-s_p)(1-U)\, PT\gamma \frac{\lambda_{F21}}{\gamma_{21}} + \beta_{21}\, \lambda_{F21} + C_{F21} \qquad (2)$$

We can also define the safety partial annual loss function "$Z_{Sji}$"

$$Z_{Sji} = (1-s_p)(1-U)\ PT\gamma \left[\frac{U}{1-U}\right]_{Sji} + B_{Sji} + C_{Sji} \qquad (3)$$

For example, in the case of the safety subsystem S21 (oil pressure measuring channels in fig. 13), we have

$$Z_{S21} = (1-s_p)(1-U)\ PT\gamma \left[\frac{\lambda_{F21}+\lambda_{F22}}{\Psi_{24}} K_{S21} + \frac{\lambda_{S21}}{\Psi_{25}}\right] +$$

$$+ \beta_{24}(\lambda_{F21}+\lambda_{F22})\ K_{S21} + \beta_{25}\ \lambda_{S21} + C_{S21} \qquad (4)$$

We shall say that a safety partial annual loss function "$Z_{Sji}$" is related to a functional partial annual loss function "$Z_{F\chi\eta}$" if "$Z_{Sji}$" contains the failure rate of the functional subsystem "$F\chi\eta$". For instance "$Z_{S21}$" (eq. 4) is related to "$Z_{F21}$" (eq. 2) because it contains $\lambda_{F21}$.

For the functional and safety subsystems, which belong to the block "m" having the maximum unavailability, we shall instead write

$$Z_{Fmi} = (1-U)\ PT\gamma \left[\frac{U}{1-U}\right]_{Fmi} + B_{Fmi} + C_{Fmi} \qquad (5)$$

and

$$Z_{Smi} = (1-U)\ PT\gamma \left[\frac{U}{1-U}\right]_{Smi} + B_{Smi} + C_{Smi} \qquad (6)$$

Taking into account eq. 8 of para. 5.3, we can write

$$U = (1-s_p)(1-U) \left\{ \sum_{\substack{j=1 \\ j\neq m}}^{M} \left[ \sum_{i=1}^{L_j} \left(\frac{U}{1-U}\right)_{Fji} + \sum_{i=1}^{A_j} \left(\frac{U}{1-U}\right)_{Sji} \right] \right\} +$$

$$+ (1-U) \left[ \sum_{i=1}^{L_m} \left(\frac{U}{1-U}\right)_{Fmi} + \sum_{i=1}^{A_m} \left(\frac{U}{1-U}\right)_{Smi} \right] \qquad (7)$$

where

$U$ = plant unavailability

$s_p$ = overlapping factor

$M$ = number of blocks

$L_j$ = number of functional subsystems belonging to block "j"

$A_j$ = number of safety subsystems belonging to block "j"

and "m" indicates the block having the maximum unavailability.

Taking into account eq. 7, one can easily prove that

$$Z = \sum_{j=1}^{M} \left[ \sum_{i=1}^{L_j} Z_{Fji} + \sum_{i=1}^{A_j} Z_{Sji} \right] \qquad (8)$$

where all the $Z_{Fji}$ and $Z_{Sji}$ are given respectively by eqs. 1 and 3 for $j \neq m$ and by eqs. 5 and 6 for $j=m$.

The procedure to find out the minimum of the annual loss function can be now described. It consists of the following steps:

Step No. 1 From previous operating experience we know already what is the block having the maximum unavailability "$U_m$". We know also the value of the overlapping coefficient "$s_p$".

We assume for the plant unavailability an initial value "$U_{in}$" coming from previous operating experience (for instance $U_{in}=0.1$). We use this value "$U_{in}$" in the functional partial annual loss functions "$Z_{Fji}$" defined by eqs. 1 and 5. We find the type of unit, the strategy and the maintenance period of subsystem "Fji", which give the minimum of "$Z_{Fji}$".

For each subsystem "Fji", we get the optimum failure rate $\lambda'_{Fji}$ by which "$Z_{Fji}$" has the minimum.

Step No. 2 We use the values $\lambda'_{Fji}$ in the safety partial loss functions "$Z_{Sji}$" defined by eqs. 3 and 6. We find the type of unit, the maintenance period, the checking period, the total number of units and the type of structure of subsystem $S_{ji}$, which give the minimum of "$Z_{Sji}$". It is important to notice that the constraint

$$\upsilon_d < \upsilon_{max}$$

must be also satisfied.

For each subsystem "$S_{ji}$" we get the optimum values of the reduction coefficient "$K'_{Sji}$" and of the failure rate "$\lambda'_{Sji}$" by which "$Z_{Sji}$" has the minimum.

Step No. 3 We use the values $\lambda'_{Fji}$, $\lambda'_{Sji}$ and $K'_{Sji}$ to calculate the plant unavailability (eq. 7).

We get the value U' which may be different from "$U_{in}$".

Step No. 4 We repeat the steps 1, 2 and 3 until the values of U converge to a final value.

In this way we have found separately the minimals of all the partial annual loss functions "$Z_{Fji}$" and "$Z_{Sji}$". We get the minimum of "Z" by using eq. 8.

This procedure is valid only if the "$Z_{Sji}$" are one or more orders of magnitude smaller than the related "$Z_{Fn\chi}$", when they are near to their minimals. That is

$$Z_{Sji} << Z_{Fn\chi} \qquad (9)$$

This should be normally the case (see numerical example of para. 4), because a safety subsystem has usually a very low value of the reduction coefficient "$K_S$" ($<10^{-5}$) and a subsystem annual cost "$C_S$" much smaller than that of each of the functional subsystems which are related to it.

If the conditions "9" are not satisfied, one has to group together all the $Z_{Sji}$ and $Z_{Fn\chi}$ which are related.

The minimum of each group can then be found, taking also into account that the constraint ($\upsilon_d < \upsilon_{max}$) must be also satisfied. The mathematical procedure would be in this case much more complicated.

## 8. A more general approach to the evaluation of the safety requirements of a power plant.

In the model described in the preceeding paragraphs we have made the following two hypothesis for the evaluation of the disaster failure rate

(i) It is possible to go to the "Disaster" state only from the "Normal Operation" state.

(ii) A disaster is always caused by combined failures of functional and safety subsystems.

These two assumptions may not always be valid. A typical example is that of the "meltdown accident of a dry and subcritical core due to fission product heat" in the case of Sodium cooled fast reactors (Bibl. B16). This would be a case, in which the failure of a functional subsystem (i.e. the vessel subsystem which contains Sodium and core) would lead directly to a disaster.

For this reason a still more general model can be developed (fig. 27). We have now "N" shut down states, and from "n" of these it is possible to go to the disaster state. Each disaster failure rate "$\upsilon_{ti}$" will be given by

$$\upsilon_{ti} = \upsilon_{di} + \lambda_{FSi} \qquad (1)$$

where

$\upsilon_{di}$ = rate of occurrence of a disaster caused by combined failures of functional and safety subsystems, starting from state "i".

$\lambda_{FSi}$ = rate of occurrence of a disaster due to accidents which are either not detectable or not controllable with the safety system, starting from state "i".

For the calculation of "$\upsilon_{di}$" one can use the procedure shown in para. 6.

For the calculation of "$\lambda_{FSi}$", one has to sum the failure rates of all the functional subsystems characterized by failures, which bring the plant in a dangerous situation if the plant is in state "i", and which are either not detectable or not controllable with the safety system.

We shall indicate with "$Q_i$" the probability that the plant is in state "i" at time "t".

Looking at fig. 27, we can write the following equations

$$\frac{dQ_o}{dt} = - Q_o \left[ \sum_{i=1}^{N} \upsilon_i + \sum_{i=o}^{n} \upsilon_{ti} \right] + \sum_{i=1}^{N} \Psi_i \, Q_i \qquad (2)$$

$$\frac{dQ_1}{dt} = + Q_o \, \upsilon_i - Q_1 (\Psi_1 + \upsilon_{t1}) \qquad (3)$$

$$\frac{dQ_n}{dt} = Q_o \, \upsilon_n - (\Psi_n + \upsilon_{tn}) Q_n \qquad (4)$$

$$\frac{dQ_{n+1}}{dt} = Q_o \, \upsilon_{n+1} - \Psi_{n+1} \, Q_{n+1} \qquad (5)$$

. . . . . .

$$\frac{dQ_N}{dt} = Q_o \, \upsilon_N - \Psi_N \, Q_N \qquad (6)$$

$$\frac{dQ_D}{dt} = \sum_{i=1}^{n} \upsilon_{ti} \, Q_i \qquad (7)$$

$$\sum_{i=o}^{N} Q_i + Q_D = 1 \qquad (8)$$

We have "N+3" equations with "N+2" unknowns. Only "N+2" equations will be independent. The last one can be obtained by summing the first "N+2" equations.

According to what we have said in para. 3 and para. 5.2, also here we have that the following property is satisfied

$$\upsilon_t << \upsilon_i << \Psi \qquad (9)$$

Taking into account the expression 9, the approximate solution for "$Q_i$" is given by

$$Q_i \simeq S_i \, R_i \qquad (i=0,1,2,\ldots,N) \qquad (10)$$

where

"$S_i$" is the solution obtained from the first N+1 equations (eqs. 2 to 6) by putting all the "$\upsilon_{ti}$" equal to zero

and

$$R_i = \exp(-\upsilon_{ti} \, t) \qquad (11)$$

The functions "$S_i$" are characterized by asymptotic values $S_{i\infty}$ which are reached

in a very short period of time

$$S_{i\infty} = S_i(\infty) = \frac{\upsilon_i}{\psi_i} S_{o\infty} \qquad (i=1,2,\ldots N) \tag{12}$$

where

$$S_{o\infty} = \frac{1}{1 + \sum_{i=1}^{N} \frac{\upsilon_i}{\psi_i}} \tag{13}$$

Note that $S_{o\infty}$ was indicated in the previous paragraphs with $A_\infty$.

The initial values "$S_{io}$" are

$$S_{oo} = S_o(0) = 1 \tag{14}$$

and

$$S_{io} = S_i(0) = 0 \qquad (i=1,2,\ldots,N) \tag{15}$$

Taking into account eqs. 10 and 11, from eq. 7 we get

$$Q_D = \sum_{i=o}^{n} \upsilon_{ti} \int_o^t S_i R_i dt \tag{16}$$

The occurrence rate "$\upsilon_D$" of a disaster will be

$$\upsilon_D = \frac{dQ_D/dt}{1-Q_D} \simeq \frac{\sum_{i=o}^{n} \upsilon_{ti} S_{i\infty} \exp(-\upsilon_{ti}\, t)}{\sum_{i=o}^{n} S_{i\infty} \exp(-\upsilon_{ti}\, t)} \simeq \frac{\sum_{i=o}^{n} \upsilon_{ti}\, S_{i\infty}}{\sum_{i=o}^{n} S_{i\infty}} \tag{17}$$

If we indicate with "FSji" a functional subsystem whose failure starting from plant state "i" is not controllable (or detectable) with the safety system, we can write

$$\lambda_{FSi} = \sum_{j=1}^{j=Di} \lambda_{FSji} \tag{18}$$

where "Di" is the total number of the functional subsystems characterized by failures which lead directly to a disaster if the plant is in state "i". In eq. 18 "$\lambda_{FSji}$" is the failure rate of the functional subsystem "FSji".

We can associate to each subsystem "FSji" its partial annual cost function "$Z_{FSji}$". Each of the "$Z_{FSji}$" will be a decreasing function with "$\lambda_{FSji}$".

The total annual cost "$Z_{FS}$" of these particular functional subsystems will be

$$Z_{FS} = \sum_{i=1}^{n} \left[ \sum_{j=1}^{Di} Z_{FSji} \right] \tag{19}$$

In order to reduce the dangerous effects due to a nuclear explosion (disaster), the reactor may be provided with a containment system capable of absorbing the explosive energy due to a big accident, once that this has taken place. Task of the containment system is also to avoid the spreading of the radioactive products in the surrounding atmosphere.

It is becoming more and more clear that there is not only one big accident, but a spectrum of possible big accidents. To each accident one can associate the correspondent developable explosive mechanical energy "W", so that a probability density distribution of "W" will describe the spectrum of accidents.

We ask now for the probability, $K_c$, that the containment system will fail to absorb the explosive energy without rupture. For the sake of simplicity we shall limit ourselves to consider only the shock wave effect. We shall imagine that the containment system is just a cylinder as shown in fig. 23 A. Fig. 23 B shows the same cylinder deformed after the explosion has taken place.

The explosive energy will produce the highest stresses at the mid plane of the cylinder (Bibl. B18). These stresses have a probability distribution, $\phi_s$, (curve 1 of fig. 24) about the mean value, $\bar{\eta}_s$, with a standard deviation, $\zeta_s$.

On the other side the strength of the material has also a probability distribution, $\phi_t$, (curve 2 of fig. 24) about the mean value $\bar{\eta}_t$ with a standard deviation $\zeta_t$. The two curves of fig. 24 may overlap and the amount of overlapping gives an indication of how large the probability "$K_c$" is, that during the explosion the stress becomes larger than the strength.

The probability, p, that the strength $\eta_t$ is larger than a fixed value $\eta_s$ is given by (fig. 24)

$$p = \int_{\eta_s}^{\infty} \phi_t(\eta_t) d\,\eta_t \tag{20}$$

The probability, $1-K_c$, that the strength is larger than the stress is the following

$$1-K_c = \int_{\eta_s=-\infty}^{+\infty} \phi_s(\eta_s) \left[ \int_{\eta_s=\eta_t}^{+\infty} \phi(\eta_t) d\eta_t \right] d\eta_s \tag{21}$$

If we assume that both $\phi_s$ and $\phi_t$ are normal distributions, it can be shown that eq. 21 becomes

$$1-K_c = \phi_{Ns}\left(\frac{\bar{\eta}_t - \bar{\eta}_s}{\sqrt{\zeta_t^2 + \zeta_s^2}}\right) \tag{22}$$

where $\phi_{Ns}$ is the cumulative standardized normal distribution.

Eq. 22 can also be written as follows

$$K_c = \phi_{Ns}\left(-\frac{\bar{\eta}_t - \bar{\eta}_s}{\sqrt{\zeta_t^2 + \zeta_s^2}}\right) \tag{23}$$

From eq. 23, at each value of $K_c$, it corresponds a value of

$$\frac{\bar{\eta}_t - \bar{\eta}_s}{\sqrt{\zeta_t^2 + \zeta_s^2}} \tag{24}$$

For given values of $\zeta_t$, $\zeta_s$ and $\bar{\eta}_s$, we get the value of $\bar{\eta}_t/\bar{\eta}_s$, which is directly related to the wall thickness of the cylinder.

This procedure may lead to a rational evaluation of the safety factor $\bar{\eta}_t/\bar{\eta}_s$ and may avoid to overdesign the safety containment system.

The smaller is "$K_c$", the higher $\bar{\eta}_t/\bar{\eta}_s$ will be, and the higher the thickness of the safety container will be. We can conclude that the smaller is "$K_c$", the higher the annual cost "$Z_c$" of the container will be.

The probability of the event that a disaster takes place and that the safety container does not cope with the explosion is given by

$$K_c\left[1-\exp(-\upsilon_D t)\right] \simeq K_c \upsilon_D t \tag{25}$$

with $\upsilon_D$ given by eq. 17.

Now the constraint given by the safety committee can be written as follows

$$K_c \upsilon_D < \upsilon_{max} \tag{26}$$

The total annual loss function "$Z_t$" will be given by

$$Z_t = Z + Z_{FS} + Z_c \tag{27}$$

where

$Z$ = annual loss function as defined in para. 7

$Z_{FS}$ = partial annual loss function given by eq. 19

$Z_c$ = partial annual loss function associated to the reactor containment system

The problem has now became that of finding the minimum of the function "$Z_t$" (eq. 27) with the constraint defined by the expression 26.

## 9. Appendix 1: Calculation of the average failure rate of a unit belonging to a functional subsystem

### A. 1.1 Introduction

The subject of this appendix is to calculate the average failure rate " $\sigma_F$ " of a unit belonging to a functional subsystem.
We introduce the following symbols:

"$h_F(t)$" = failure probability density distribution of the unit

"$t$" = time

" $\Theta_F$ " = maintenance period, that is time between two preventive replacements

The average failure rate "$\sigma_F$" (defined as reciprocal to the meantime to failure) is given by

$$\sigma_F = \frac{1}{\text{meantime between two failures}} =$$

$$= \frac{\int_0^{\Theta_F} h_F(t)dt}{\Theta_F \left[1-\int_0^{\Theta_F} h_F(t)dt\right] + \int_0^{\Theta_F} t\,h_F(t)dt} \qquad (1)$$

Eq. 1 is derived in thefollowing paragraph (A 1.2)

### A 1.2 Calculation of "$\sigma_F$"

A unit is characterized by its reliability "$R_F$", where

$$R_F = P\{\text{unit is not failed at time "t"}\} \qquad (2)$$

Evaluating "$R_F(t)$" for the first maintenance period we get, with "$h_F(t)$",

$$R_F(\Theta_F) = 1 - \int_0^{\Theta_F} h_F(t)dt \qquad (3)$$

For the interval $[0;q \cdot \theta_F]$, i.e. for "q" maintenance periods, we get, taking into account eq. 3,

$$R_F\ (q \cdot \theta_F) = \left[1 - \int_0^{\theta_F} h_F(t)dt\right]^q \tag{4}$$

where $q = 1,2, \ldots.$ (5)

We can write $t = q \cdot \theta_F + \varepsilon$ (6)

Taking into account eqs 4 and 6, we get

$$R_F(t) = \left[1 - \int_0^{\theta_F} h_F(t)dt\right]^q \cdot \left[1 - \int_0^{\varepsilon} h_F(t)dt\right] \tag{7}$$

The average failure rate "$\sigma_F$", can be written as follows

$$\sigma_F = \frac{1}{\int_0^{\infty} R_F(t)dt} \tag{8}$$

where $R_F(t)$ is the reliability of the unit

The integral from "o" to "$\infty$" of the function "$R_F(t)$" can be represented as a sum, i.e.

$$\int_0^{\infty} R_F(t)dt = \sum_{q=0}^{q=\infty} \left[1 - \int_0^{\theta_F} h_F(t)dt\right]^q \int_0^{\theta_F} \left[1 - \int_0^{t} h_F(t)dt\right]dt \tag{9}$$

By partial integration, we get

$$\int_0^{\theta_F} \left[\int_0^{t} h_F dt\right]dt = \left[t \cdot \int_0^{t} h_F dt\right]_0^{\theta_F} - \int_0^{\theta_F} t h_F dt = \theta_F \int_0^{\theta_F} h_F dt - \int_0^{\theta_F} t h_F dt \tag{10}$$

Taking into account 10, we get from 9

$$\int_0^{\infty} R_F(t)dt = \frac{1}{1 - \left[1 - \int_0^{\theta_F} h_F dt\right]} \cdot \left\{\theta_F - \left[\theta_F \int_0^{\theta_F} h_F dt - \int_0^{\theta_F} t h_F dt\right]\right\} \tag{11}$$

Putting 11 into 8, we get finally

$$\sigma_F = \frac{\int_0^{\theta_F} h_F(t)dt}{\theta_F \left[1 - \int_0^{\theta_F} h_F(t)dt\right] + \int_0^{\theta_F} t h_F(t)dt} \tag{12}$$

$$= \frac{\int_0^{\theta_F} h_F(t)\,dt}{\theta_F - \int F(t)\,dt} = \frac{\int_0^{\theta_F} h_F(t)\,dt}{\int_0^{\theta_F} \bar{F}(t)\,dt}$$

## 10. Appendix 2: Calculation of the two average failure rates of a unit belonging to a safety subsystem.

The average failure rates "$\rho_S$" and "$\sigma_S$" of a unit belonging to a safety subsystem will be calculated in this Appendix. They are obtained in a way very similar to that used to evaluate the failure rate of a unit belonging to a functional subsystem. There are however two important distinctions to be made.

(i) It has to be taken into account that there are two types of failures:
   a) Failure type "a" (when a safety unit does not function when it should)
   b) Failure type "b" (when a safety unit functions when it should not).

(ii) The increased failure rate, caused by "on-off-cycling" (due to the periodical testing of the units) has to be taken into account.

Let us indicate with $h'_S(t)$ and $h''_S(t)$ the two failure probability density distributions of a unit respectively for failure type "a" and failure type "b".

The on-off-cycling has practically the effect to change the time scale of the two failure probability cumulative distributions.

The coefficients by which the time scale is changed are

$$1 + \frac{\delta'_S}{\tau_S} \qquad \text{for failure type "a"} \tag{1}$$

and

$$1 + \frac{\delta''_S}{\tau_S} \qquad \text{for failure type "b"} \tag{2}$$

with $\delta'_S$ and $\delta''_S$ being two constants.

Introducing these two coefficients, the two new failure probability density distributions, which take into account the cycling effect, will be respectively

$$\left(1 + \frac{\delta'_S}{\tau_S}\right) h'_S\left\{t\left(1+ \frac{\delta'_S}{\tau_S}\right)\right\} \quad \text{(failure type "a")} \tag{3}$$

and

$$\left(1 + \frac{\delta'_S}{\tau_S}\right) h''\left\{t\left(1+ \frac{\delta''_S}{\tau_S}\right)\right\} \text{(failure type "b")} \tag{4}$$

The total failure probability density distribution "$\bar{h}_S(t)$" will be given by

$$\bar{h}_S(t) = \left[(1+\frac{\delta'_S}{\tau_S})\ h'_S\left\{t(1+\frac{\delta'_S}{\tau_S})\right\}\right]\left[1-(1+\frac{\delta''_S}{\tau_S})\int_o^t h''\left\{t(1+\frac{\delta''_S}{\tau_S})\right\}dt\right] +$$

$$+\left[(1+\frac{\delta''_S}{\tau_S})\ h''_S\left\{t(1+\frac{\delta''_S}{\tau_S})\right\}\right]\left[1-(1+\frac{\delta'_S}{\tau_S})\int_o^t h'\left\{t(1+\frac{\delta'_S}{\tau_S})\right\}dt\right] \qquad (5)$$

With a procedure similar to that used in Appendix 1, we can calculate the total unit failure rate "$\rho_S+\sigma_S$" where "$\rho_S$" is the failure rate for failure type "a" and "$\sigma_S$" is that for failure type "b".

$$\rho_S+\sigma_S = \frac{\int_o^{\Theta_S}\bar{h}_S(t)dt}{\Theta_S\left[1-\int_o^{\Theta_S}\bar{h}_S(t)dt\right]+\int_o^{\Theta_S} t\ \bar{h}_S(t)dt} \qquad (6)$$

where

$\Theta_S$ = maintenance period of a unit

We can write also the following equations

$$\frac{\rho_S}{\rho_S+\sigma_S} = \frac{\int_o^{\Theta_S}\left[(1+\frac{\delta'_S}{\tau_S})\ h'_S\left\{t(1+\frac{\delta'_S}{\tau_S})\right\}\right]\left[1-(1+\frac{\delta''_S}{\tau_S})\int_o^t h''_S\left\{t(1+\frac{\delta''_S}{\tau_S})\right\}dt\right]dt}{\int_o^{\Theta_S}\bar{h}_S(t)dt} \qquad (7)$$

and

$$\frac{\sigma_S}{\rho_S+\sigma_S} = \frac{\int_o^{\Theta_S}\left[(1+\frac{\delta''_S}{\tau_S})\ h''_S\left\{t(1+\frac{\delta''_S}{\tau_S})\right\}\right]\left[1-(1+\frac{\delta'_S}{\tau_S})\int_o^t h'_S\left\{t(1+\frac{\delta'_S}{\tau_S})\right\}dt\right]dt}{\int_o^{\Theta_S}\bar{h}_S(t)dt} \qquad (8)$$

Taking into account eq. 6, eqs. 7 and 8 become finally

$$\rho_S = \frac{\int_o^{\theta_S(1+\delta'_S/\tau_S)} h'(t) \left[1 - \int_o^{t(1+\delta''_S/\tau_S)} h''(t)dt\right] dt}{\theta_S \left[1 - \int_o^{\theta_S} \bar{h}(t)dt\right] + \int_o^{\theta_S} t\, \bar{h}(t)dt} \qquad (9)$$

$$\sigma_S = \frac{\int_o^{\theta_S(1+\delta''_S/\tau_S)} h'(t) \left[1 - \int_o^{t(1+\delta'_S/\tau_S)} h''(t)dt\right] dt}{\theta_S \left[1 - \int_o^{\theta_S} \bar{h}(t)dt\right] + \int_o^{\theta_S} \bar{h}(t)dt} \qquad (10)$$

## 11. Appendix 3: Calculation of the reduction and coupling coefficients for safety subsystems

### A 3.1 The reduction coefficient "$K_S$" of a safety subsystem

Let us suppose we have a safety subsystem "S", which is related to the functional subsystem "F". This means that when "F" fails, "S" (if not already failed) will contribute to shut the plant down.

We shall indicate with "$\lambda_F$" the average failure rate of the functional subsystem "F".

The safety subsystem "S" is made of "$n_S$" units connected in such a way that, if at the time at which "F" fails "$k_S$" out of the "$n_S$" units have not already failed (failure type "a"), "S" will operate correctly. We remind here briefly (see para. 2) that the units of a safety subsystem can have two types of failures:

(i) failure type "a". It occurs when the unit does not operate when it is required to operate

(ii) failure type "b". It occurs when the unit does operate when it is not asked to operate.

In this appendix we shall deal with failure type "a" only.
Going back to our subsystem "S", we can easily see that "S" will fail if

$$m_S = n_S + 1 - k_S \qquad (1)$$

units fail.

To find out that a unit is failed with failure type "a", it is necessary to test it from time to time. We shall indicate with "$\tau_S$" the checking period, that is the time interval between two checks (tests).

We ask now for the probability "$P_{SF}(t)$" of the event that, at the time "t" at which "F" fails, "S" has already failed. We indicate with "$\alpha_{SF}$" the probability that this event occurs in the time interval "$\tau_S$" between two checks. The probability "$P_{SF}(q\tau_S)$", that the event occurs during

the first "q" checking intervals, is

$$P_{SF}(q\tau_S) = \alpha_{SF}\left\{1 - P_{SF}\left[\tau_S(q-1)\right]\right\} + P_{SF}\left[\tau_S(q-1)\right] \quad (2)$$

Applying eq. 2 repeatedly, we get

$$P_{SF}(q\tau_S) = 1 - (1-\alpha_{SF})^q \quad (3)$$

Eq. 3 is valid only when "q" is an entire number.
We can write approximately

$$q = \frac{t}{\tau_S} \quad (4)$$

Taking into account eq. 4, eq. 3 becomes

$$P_{SA}(t) = 1 - e^{-\nu t}$$

where

$$\nu = -\frac{\lg(1-\alpha_{SF})}{\tau_S} \quad (5)$$

Since $\alpha_{SF}$ 1, we get finally from eq. 5

$$\nu = \frac{\alpha_{SF}}{\tau_S} \quad (6)$$

"$\alpha_{SF}$" has been calculated in paragraph A 3.2 (eq.17). We have

$$\alpha_{SF} = \tau_S\lambda_F \frac{(n_S)!(\rho_S\tau_S)^{m_S}}{(n_S - m_S)!(m_S+1)!} \quad (7)$$

where

$\rho_S$ = average failure rate of a unit for failure type "a" defined by eq. 4 of para. 3

Taking into account eq. 12, eq. 11 becomes

$$\nu = K_S\lambda_F \quad (8)$$

where

$$K_S = \frac{(n_S)!\,(\rho_S\tau_S)^{m_S}}{(m_S+1)!(n_S-m_S)} \quad (9)$$

"$K_S$" is called reduction coefficient.

Figs. 4; 5 and 6 show "$K_S$" as function of "$\rho_S \tau_S$" for different values of "$n_S$" and "$m_S$".

## A 3.2 Calculation of the probability "$\alpha_{SF}$".

We want here to calculate the probability "$\alpha_{SF}$" of the event that the safety subsystem "S" fails before the functional subsystem "F" in the time interval "$\tau_S$".

The reliability "$R_S$" of "S", that is, the probability that "S" is not yet failed at time "t", is given by

$$R_S = \sum_{i=k_S}^{n_S} \binom{n_S}{i} \bar{R}_S^{\,i} \, (1-\bar{R}_S)^{(n_S-i)} \tag{1}$$

where

$\bar{R}_S$ = reliability of a unit.

The probability "$F_S$" that "S" is already failed at "t" is

$$F_S = 1-R_S = \sum_{i=m_S}^{n_S} \binom{n_S}{i} \, H_S^{\,i} \, (1-H_S)^{(n_S-i)} \tag{2}$$

where

$$H_S = 1-\bar{R}_S \tag{3}$$

If "$F_F$" is the failure cumulative probability distribution of the functional subsystem "F", we get

$$\alpha_{SF} = \int_{t=o}^{t=\tau_S} F_S \, dF_F \tag{4}$$

We have

$$dF_F = \Sigma \, \lambda_F \exp(-\lambda_F t) dt \tag{5}$$

and

$$\bar{R}_S = \exp(-\rho_S t) \tag{6}$$

From eqs. 5 and 6 we obtain

$$dF_F = - \left[ \bar{R}_S \right]^{\lambda_F/\rho_S} \frac{d\bar{R}_S}{\bar{R}_S} \frac{\lambda_F}{\rho_S} \qquad (7)$$

From eq. 1 we get

$$dR_S = \frac{(n_S)!}{(k_S-1)!(n_S-k_S)!} \bar{R}_S^{(k_S-1)} (1-\bar{R}_S)^{(n_S-k_S)} d\bar{R}_S \qquad (8)$$

Taking into account eqs. 3 and 7, eq. 4 becomes

$$\alpha_{SF} = \frac{\lambda_F}{\rho_S} \int_{\bar{R}_S(\tau_S)}^{1} (1-R_S) \left[ \bar{R}_S \right]^{\lambda_F/\rho_S} \frac{d\bar{R}_S}{\bar{R}_S} =$$

$$= 1 - \left[ \bar{R}_S(\tau_S) \right]^{\lambda_F/\rho_S} - \frac{\lambda_F}{\rho_S} \int_{\bar{R}_S(\tau_S)}^{1} R_S \left[ \bar{R}_S \right]^{\left(\frac{\lambda_F}{\rho_S}-1\right)} d\bar{R}_S =$$

$$= - \left[ 1-R_S(\tau_S) \right] \left[ \bar{R}_S(\tau_S) \right]^{\lambda_F/\rho_S} + \int_{R_S(\tau_S)}^{1} \left[ \bar{R}_S \right]^{\lambda_F/\rho_S} dR_S \qquad (9)$$

Taking into account eqs. 2 and 8, we get from eq. 9

$$\alpha_{SF} = \left[ \bar{R}_S(\tau_S) \right]^{\lambda_F/\rho_S} \left\{ - \sum_{i=m_S}^{n_S} \binom{n_S}{i} H_S(\tau_S)^i \left[ 1-H_S(\tau_S) \right]^{(n_S-i)} + \right.$$

$$+ \frac{(n_S)!}{(m_S)!(n_S-m_S)!} \left[ H_S(\tau_S) \right]^{m_S} \cdot \left[ 1-H_S(\tau_S) \right]^{(n_S-m_S)} +$$

$$+ \frac{(n_S)!\left(\frac{\lambda_F}{\rho_S} + n_S - m_S\right)}{(n_S-m_S)!(m_S+1)!} \left[ H_S(\tau_S) \right]^{(m_S+1)} \cdot \left[ 1-H_S(\tau_S) \right]^{(n_S-m_S-1)} +$$

$$\left. + \sum_{i=m_S+2}^{\infty} \left[ \frac{(n_S)!\left(\frac{\lambda_F}{\rho_S} + n_S - m_S\right) \cdots \left(\frac{\lambda_F}{\rho_S} + n_S - i - 1\right)}{(n_S-m_S)!(i)!} \left[ H_S(\tau_S) \right]^i \left[ 1-H_S(\tau_S) \right]^{(n_S-i)} \right] \right\} \qquad (10)$$

Taking into account eq.6, eq.10 finally becomes

$$\alpha_{SF} = \exp(-\lambda_F \tau_S) \frac{(n_S)!}{(n_S-m_S)!(m_S+1)!} \left[H_S(\tau_S)\right]^{(m_S+1)} \left[1-H_S(\tau_S)\right]^{(n_S-m_S-1)} \left\{ \frac{\lambda_F}{\rho_S} + \right.$$

$$+(m_S+1)! \sum_{j=1}^{n_S-m_S-1} \frac{1}{(m_S+1+j)!} \left[\frac{H_S(\tau_S)}{1-H_S(\tau_S)}\right]^j \left[\frac{\Gamma\left(\frac{\lambda_F}{\rho_S} + n_S+1-m_S\right)}{\Gamma\left(\frac{\lambda_F}{\rho_S} + n_S + 1-j\right)} - \frac{(n_S-m_S)!}{(n_S-m_S-1-j)!}\right] +$$

$$\left. + (m_S+1)! \sum_{j=n_S-m_S}^{\infty} \frac{1}{(m_S+1+j)!} \frac{\Gamma\left(\frac{\lambda_F}{\rho_S} + n_S+1-m_S\right)}{\Gamma\left(\frac{\lambda_F}{\rho_S} + n_S-m_S-j\right)} \left[\frac{H_S(\tau_S)}{1-H_S(\tau_S)}\right]^j \right\} \quad (11)$$

Where "$\Gamma$" stands for the "$\Gamma$"-function"

If

$$\frac{H_S(\tau_S)}{1-H_S(\tau_S)} \quad \frac{\lambda_F}{\rho_S} \ll 5 \cdot 10^{-2} \quad (12)$$

eq. 11 can be simplified to

$$\alpha_{SF} \simeq \frac{\lambda_F}{\rho_S} \frac{(n_S)!}{(n_S-m_S)!(m_S+1)!} \left[H_S(\tau_S)\right]^{(m_S+1)} \left[1-H_S(\tau_S)\right]^{(n_S-m_S+1)} \quad (13)$$

If we have

$$\rho_S \tau_S < 10^{-2} \quad (14)$$

we can write

$$H_S(\tau_S) \simeq \rho_S \tau_S \quad (15)$$

and

$$1-H_S(\tau_S) \simeq 1 \quad (16)$$

Taking into account eqs. 15 and 16, eq. 13 can be still simplified

$$\alpha_{SF} \simeq \lambda_F \tau_S \frac{(n_S)!}{(n_S-m_S)!(m_S+1)!} (\rho_S \tau_S)^{m_S} \quad (17)$$

## A 3.3 Calculation of the coupling coefficient

Let us suppose that we have two safety subsystems "S1" and "S2". We want to calculate the probability "$\alpha$" that both fail before the functional subsystem "F" in the time interval "$\tau_S$".

The cumulative probability distribution "$F_{S1;S2}$", that both S1 and S2 fail in a small time interval "t" is given by

$$F_{S1;S2} = \frac{(n_{S1})!(\rho_{S1}t)^{m_{S1}}}{(m_{S1})!(n_{S1}-m_{S1})!} \quad \frac{(n_{S2})!(\rho_{S2}t)^{m_{S2}}}{(m_{S2})!(n_{S2}-m_{S2})!} \tag{1}$$

The failure cumulative probability distribution "$F_F$" of the functional subsystem "F" is

$$F_F = 1-\exp(-\lambda_F t) \cong \lambda_F t \tag{2}$$

The probability "$\alpha$", that both "S1" and "S2" fail before "F" in the small time interval "$\tau_S$", is

$$\alpha = \int_{t=o}^{t=\tau_S} F_{S1;S2} \; dF_F = \frac{\lambda_F (n_{S1})!(n_{S2})!(\rho_{S1}\tau_S)^{m_{S1}}(\rho_{S2}\tau_S)^{m_{S2}}\tau_S}{(m_{S1}+m_{S2}+1)(m_{S1})!(n_{S1}-m_{S1})!(m_{S2})!(n_{S2}-m_{S2})!} \tag{3}$$

Eq.3 can be written as follows

$$\frac{\alpha}{\tau_S} = \lambda_F K_{S1} K_{S2} H_{S1;S2} \tag{4}$$

where

$$K_{S1} = \frac{(n_{S1})!(\rho_{S1}\tau_S)^{m_{S1}}}{(m_{S1}+1)!(n_{S1}-m_{S1})!} \tag{5}$$

$$K_{S2} = \frac{(n_{S2})!(\rho_{S2}\tau_S)^{m_{S2}}}{(m_{S2}+1)!(n_{S2}-m_{S2})!} \tag{6}$$

and

$$H_{S1,S2} = \frac{(m_{S1}+1)(m_{S2}+1)}{(m_{S1}+m_{S2}+1)} \tag{7}$$

$H_{S1;S2}$ is called coupling coefficient

For "N" safety subsystems we have

$$H_{S1;S2\ ....;SN} = \frac{\prod_{i=1}^{N} (m_{Si}+1)}{1 + \sum_{i=1}^{N} m_{Si}} \qquad (8)$$

## 12. Appendix 4: Calculation of the average failure rate of a safety subsystem

Let us suppose that we have a safety subsystem "S" made of "$n_S$" units so connected that, if "$\ell_S$" out of the "$n_S$" units fail with the failure type "b", the subsystem "S" fails (false trip).

We introduce the following symbols

$\sigma_S$ = average failure rate of a unit defined by eq. 5 of para. 2

$\mu_S$ = average repair rate of a unit, that is reciprocal of the mean time to repair.

If $g_S(t)$ is the repair probability density distribution of a unit, we have

$$\mu_S = \frac{1}{\int_o^\infty t\, g_S(t)dt} \qquad (1)$$

The safety subsystem can be at time "t" in one of the following states (fig. 25).

| State | Number of working units | Number of failed units | Comments |
|---|---|---|---|
| 0 | $n_S$ | 0 | |
| 1 | $n_S-1$ | 1 | |
| 2 | $n_S-2$ | 2 | |
| . . | . . | . . | . . |
| i | $n_S-i$ | i | |
| . . | . . | . . | . . |
| $\ell_S-2$ | $n_S-\ell_S+2$ | $\ell_S-2$ | |
| $\ell_S-1$ | $n_S-\ell_S+1$ | $\ell_S-1$ | |
| $\ell_S$ | $\leqslant n_S-\ell_S$ | $\geqslant \ell_S$ | Subsystem failed |

Let us indicate with $Q_i(t)$ the probability that the subsystem "S" is in state "i". We can write the following "$\ell_S+1$" equations

$$\frac{dQ_o}{dt} = - n_S\sigma_S Q_o + \mu_S Q_1 \qquad (2)$$

$$\frac{dQ_1}{dt} = n_S\sigma_S Q_o - \left[(n_S-1)\sigma_S+\mu_S\right] Q_1 + \mu_S Q_2 \tag{3}$$

$$\frac{dQ_i}{dt} = (n_S-i+1)\sigma_S Q_{i-1} - \left[(n_S-i)\sigma_S+\mu_S\right] Q_i + \mu_S Q_{i+1} \tag{4}$$

. . . . . .

$$\frac{dQ_{\ell_S-1}}{dt} = (n_S-\ell_S+2)\sigma_S Q_{\ell_S-2} - \left[(n_S-\ell_S+1)\sigma_S+\mu_S\right] Q_{\ell_S-1} \tag{5}$$

$$\frac{dQ_{\ell_S}}{dt} = (n_S-\ell_S+1)\sigma_S Q_{\ell_S-1} \tag{6}$$

Since

$$\sum_{i=o}^{\ell_S} Q_i = 1 \tag{7}$$

only "$\ell_S$" of the "$\ell_S+1$" equations are independent.

The associated initial conditions are

$$Q_o(0) = 1 \tag{8}$$

and

$$Q_i(0) = 0 \qquad (i=1,2,\ldots,\ell_S) \tag{9}$$

Taking into account the initial conditions 8 and 9, the Laplace transforms of the eqs. 2 to 6 are

$$-1 = -(n_S\sigma_S+s)Q_o^* + \mu_S Q_1^* \tag{10}$$

$$0 = n_S\sigma_S Q_o^* - \left[(n_S-1)\sigma_S+\mu_S+s\right]Q_1^* + \mu_S Q_2^* \tag{11}$$

. . . . . .

$$0 = (n_S-i+1)\sigma_S Q_{i-1}^* + \left[(n_S-i)\sigma_S+\mu_S+s\right]Q_i^* + \mu_S Q_{i+1}^* \tag{12}$$

. . . . . .

$$0 = (n_S-\ell_S+2)\sigma_S Q_{\ell_S-2}^* - \left[(n_S-\ell_S+1)\sigma_S+\mu_S+s\right]Q_{\ell_S-1}^* \tag{13}$$

$$0 = (n_S-\ell_S+1)\sigma_S Q_{\ell_S-1}^* - sQ_{\ell_S}^* \tag{14}$$

where

s = complex variable of the Laplace domain

"*" indicates Laplace transform

The Laplace transform of the reliability "$R_S$" of the subsystem "S" is given by

$$R_S^* = \frac{1}{s} - Q_{\ell_S}^* \tag{15}$$

Taking into account eq. 14, eq. 15 becomes

$$R_S^* = \frac{1 - (n_S - \ell_S + 1)\sigma_S \, Q_{\ell_S - 1}^*}{s} \tag{16}$$

Now we have

$$Q_{\ell_S - 1}^* = \frac{A_{1\ell_S}}{\Delta} \tag{17}$$

where

$\Delta$ = determinant of the coefficients of the first "$\ell_S$" equations (eq. 14 excluded)

$A_{1\ell_S}$ = determinant complementary to the element "$a_{1\ell_S}$" (1st line and "$\ell_S$"th column) of the determinant $\Delta$

The determinant "$\Delta$", having "$\ell_S$" lines and "$\ell_S$" columns, is written below (eq. 18)

$$\Delta = \begin{vmatrix} -(n_S\sigma_S+s) & \mu_S & 0 & 0 & \cdots & 0 & 0 & 0 \\ n_S\sigma_S & -[(n_S-1)\sigma_S+\mu_S+s] & \mu_S & 0 & \cdots & 0 & 0 & 0 \\ 0 & (n_S-1)\sigma_S & -[(n_S-2)\sigma_S+\mu_S+s] & \mu_S & \cdots & 0 & 0 & 0 \\ 0 & 0 & (n_S-2)\sigma_S & \cdots & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & & \cdot & \mu_S & 0 \\ 0 & 0 & 0 & 0 & \cdots & (n_S-\ell_S+3)\sigma_S & -[(n_S-\ell_S+2)\sigma_S+\mu_S+s] & \mu_S \\ 0 & 0 & 0 & 0 & \cdots & 0 & (n_S-\ell_S+2)\sigma_S & -[(n_S-\ell_S+1)\sigma_S+\mu_S+s] \end{vmatrix} \quad (18)$$

Taking into account eq. 17, eq. 16 becomes

$$R_S^* = \frac{\Delta - (n_S - \ell_S + 1)\sigma_S A_{1\ell_S}}{s\,\Delta} \tag{19}$$

On the other hand "$R_S^*$" is also given by

$$R_S^* = \sum_{i=o}^{\ell_S - 1} Q_i^* \tag{20}$$

By solving the system of eqs. 10 to 13, we get

$$Q_i^* = (-1)^i \frac{A_{1i}}{\Delta} \tag{21}$$

where "$\Delta$" is the determinant defined by eq. 18 and "$A_{1i}$" is the determinant complementary to the element "$a_{1i}$" (1st line and "i"th column) of $\Delta$.

Putting 21 in 20, we obtain

$$R_S^* = \frac{\sum_{i=1}^{\ell_S - 1} (-1)^i A_{1i}}{\Delta} \tag{22}$$

By comparing eqs. 22 and 19, we get

$$\frac{\Delta - (n_S - \ell_S + 1)\sigma_S A_{1\ell_S}}{s} = \sum_{i=1}^{\ell_S - 1} (-1)^i A_{1i} \tag{23}$$

By extracting the determinant "$A_{1\ell_S}$" from $\Delta$ (eq. 18), one obtains

$$A_{1\ell_S} = (-1)^{\ell_S} \frac{(n_S)!}{(n_S - \ell_S + 1)!}\, \sigma_S^{(\ell_S - 1)} \tag{24}$$

Putting 24 in 23 for s=o, one gets

$$[\Delta]_{s=o} = (-1)^{\ell_S} \frac{(n_S)!}{(n_S - \ell_S)!}\, \sigma_S^{\ell_S} \tag{25}$$

The average failure rate "$\lambda_S$" of subsystem "S" is given by

$$\lambda_S = \frac{1}{\int_o^\infty R_S dt} = \frac{1}{\lim_{s\to o} R_S^*} \tag{26}$$

Taking into account eqs. 22 and 25, we get

$$\lambda_S = \frac{[\Delta]_{s=o}}{\sum_{i=1}^{\ell_S-1} (-1)^i \left[A_{1i}\right]_{s=o}} = (-1)^{\ell_S} \frac{\sigma_S^{\ell_S}}{\sum_{i=1}^{\ell_S-1} (-1)^i \left[A_{1i}\right]_{s=o}} \frac{(n_S)!}{(n_S-\ell_S)!} \tag{27}$$

By extracting the determinants "$A_{1i}$" from $\Delta$ (eq. 18), we obtain for s=o

$$\left[A_{1i}\right]_{s=o} = (-1)^{(\ell_S-i)} \sigma_S^{(i-1)} \frac{n_S(n_S-1)(n_S-2)\ldots(n_S-i+2)}{(n_S-\ell_S)!} \left[ (n_S-i)!\, \sigma_S^{(\ell_S-i)} + \right.$$

$$\left. + (n_S-i-1)!\sigma_S^{(\ell_S-i-1)} \mu_S + \ldots + (n_S-\ell_S+1)!\sigma_S^{(\ell_S-i-1)} \mu_S^{(\ell_S-i)} + (n_S-\ell_S)!\mu_S^{(\ell_S-i)} \right] \tag{28}$$

Taking into account eqs. 28, eq. 27 becomes

$$\lambda_S = \frac{\sigma_S}{\sum_{i=o}^{\ell_S-1} \left[ \left(\frac{\mu_S}{\sigma_S}\right)^i \sum_{f=o}^{\ell_S-i-1} \frac{(n_S-1-i-f)!}{(n_S-f)!} \right]} \tag{29}$$

Introducing the index

$$q = n_S - f \tag{30}$$

we get finally

$$\lambda_S = \frac{\sigma_S}{\sum_{i=o}^{\ell_S-1} \left[ \left(\frac{\mu_S}{\sigma_S}\right)^i \sum_{q=n_S-\ell_S+1+i}^{n_S} \frac{(q-1-i)!}{q!} \right]} \tag{31}$$

Since in the practical case $\mu_S/\sigma_S$ is very large, eq. 31 can be approximately written as follows

$$\lambda_S \simeq \frac{(n_S)!}{(n_S-\ell_S)!} \frac{\sigma_S}{\left[\mu_S/\sigma_S\right]^{(\ell_S-1)}} \tag{32}$$

The calculation of "$\lambda_S$" developed in this Appendix is strictly rigorous only in the case in which the failure and the repair probability distributions are both exponential. However, due to the conclusions reached in Appendix 6, the result is still valid for any type of distribution if "$\sigma_S$" and "$\mu_S$" are average values defined respectively by eq. 5 of para. 2 and eq. 1 of this appendix.

## 13. Appendix 5: Calculation of the point-availability for a simple plant model

The solution of eqs. (6), (7), (8) of para. 3 will be obtained in this appendix (see also fig. 7). We have three linear differential equations with constant coefficients:

$$\frac{dQ_o}{dt} = -(\lambda_F+\lambda_S+K_S\lambda_F)Q_o + \Psi Q_1 \qquad (1)$$

$$\frac{dQ_1}{dt} = (\lambda_F+\lambda_S)\,Q_o - \Psi Q_1 \qquad (2)$$

$$\frac{dQ_2}{dt} = K_S\lambda_F Q_o \qquad (3)$$

Where $Q_o$ = probability that the plant is in state "o"

$Q_1$ = probability that the plant is in state "1"

$Q_2$ = probability that the plant is in state "2"

$\lambda_F$ = rate of occurrence of the event that the functional system fails

$K_S$ = reduction factor of the safety system

$K_S\lambda_F$ = rate of occurrence of a "disaster" i.e. of the event that the functional system fails and the safety system has already failed before

$\lambda_S$ = rate of occurrence of a false trip

$\Psi$ = repair rate, i.e. reciprocal to the meantime to repair the plant

For $Q_o$, $Q_1$, $Q_2$ the following relation holds

$$Q_o + Q_1 + Q_2 = 1 \qquad (4)$$

Therefore only 2 of the 3 eqs. 1, 2, 3 are independent. The initial

conditions are

$$Q_o(0) = 1; \quad Q_1(0) = 0; \quad Q_2(0) = 0 \tag{5}$$

They mean that at time t = 0 the probability that the plant is in state "0" is equal to 1.

Applying the Laplace transform to eqs. (1), (2) we get

$$-1 = -(s+\lambda_F+\lambda_S+K_S\lambda_F)\, Q_o^* + \Psi Q_1^* \tag{6}$$

$$0 = (\lambda_F+\lambda_S)\, Q_o^* - (s+\Psi)\, Q_1^* \tag{7}$$

Where "s" is the complex variable in the Laplace domain and the asterisk "*" denotes the Laplace transform.

We get with Cramer's rule from the system (6), (7) for $Q_o^*$

$$Q_o^* = \frac{\begin{vmatrix} -1 & \Psi \\ 0 & -(s+\Psi) \end{vmatrix}}{\begin{vmatrix} -(s+\lambda_F+\lambda_S+K_S\lambda_F) & \Psi \\ (\lambda_F+\lambda_S) & -(s+\Psi) \end{vmatrix}} =$$

$$= \frac{s+\Psi}{(s+\lambda_F+\lambda_S+K_S\lambda_F)(s+\Psi) - (\lambda_F+\lambda_S)\Psi} =$$

$$= \frac{s+\Psi}{s^2+s(\Psi+\lambda_F+\lambda_S+K\lambda_F) - \Psi K_S\lambda_F} \tag{8}$$

To antitrasform eq.8 to the time domain, the roots of the characteristic equation must be found.

$$s^2+s(\Psi+\lambda_F+\lambda_S+K_S\lambda_F) - \Psi K_S\lambda_F = 0 \tag{9}$$

The two roots are

$$s_{1;2} = -\frac{\Psi+\lambda_F+\lambda_S+K_S\lambda_F}{2} \mp \sqrt{\frac{(\Psi+\lambda_F+\lambda_S+K_S\lambda_F)^2}{4} + \Psi K_S\lambda_F} \tag{10}$$

For practical cases, the rate of occurrence of a big accident "$K_S\lambda_F$" is very small compared to the sum of the two failure-rates "$\lambda_F$" and "$\lambda_S$". They are again small compared to the repair rate "$\psi$". The following relation therefore holds:

$$\psi \gg \lambda_F+\lambda_S \gg K_S \cdot \lambda_F \tag{11}$$

This is discussed in more details in para. 3.

With 11 we get also the relation

$$K_S \cdot \lambda_F \psi \ll \frac{(\lambda_F+\lambda_S-K_S \cdot \lambda_F+\psi)^2}{4} \tag{12}$$

Taking into account the expressions 11 and 12, we get from eq. 10

$$s_1 \cong - (\lambda_F+\lambda_S+K_S\lambda_F+\psi) \tag{13}$$

and

$$s_2 \cong - K_S\lambda_F \tag{14}$$

The antitrasform to the time domain of eq. 8 is

$$Q_o(t) = \frac{\psi + s_1}{s_1-s_2} \exp(s_1 t) + \frac{\psi + s_2}{s_2 \cdot s_1} \exp(s_2 t) \tag{15}$$

Taking into account eqs. 13 and 14, eq. 15 becomes

$$Q_o(t) \cong \left\{ \frac{\psi}{\lambda_F+\lambda_S+\psi} + \frac{\lambda_F+\lambda_S}{\lambda_F+\lambda_S+\psi} \exp\left[-t(\lambda_F+\lambda_S+\psi)\right] \right\} \exp(-K_S\lambda_F t) \tag{16}$$

## 14. Appendix 6: Calculation of the point-availability with any type of failure- and repair-probability-density-distributions

### A.6.1 Introduction

The point-availability "A" of the plant (and likewise for a subsystem or a unit) is defined as the probability that the plant (and likewise, the subsystem and the unit) is up at time "t":

$$A(t) = P\left\{\text{plant is up at "t"}\right\} \qquad (1)$$

In the following treatment we shall suppose that all the failures are repairable which, is equivalent to say that no "absorbing state" exists.

### A 6.2 Calculation of the Availability "A"

The availability "A(t)" is given by the following expression

$$A(t) = L^{-1}\left\{\frac{1}{s}\quad\frac{1 - f^{*}(s)}{1 - f^{*}(s)w^{*}(s)}\right\} \qquad (1)$$

where

| | | |
|---|---|---|
| "$f^{*}(s)$" | = | Laplace transform of f(t) |
| "f(t)" | = | failure-probability-density-distribution |
| "$w^{*}(s)$" | = | Laplace transform of w(t) |
| "w (t)" | = | repair-probability-density-distribution |
| "s" | = | complex variable in the Laplace-domain |
| "$L^{-1}$" | = | antitransformation to the time domain |

"$*$" indicates Laplace transformation

We introduce also the failure probability cumulative distribution "F"(t) given by

$$F(t) = \int_{o}^{t} f(t)dt \qquad (2)$$

Now we shall show how to obtain eq. 1. The availability A can be calculated by summing the probabilities "$P\left\{E_n\right\}$" of all the mutually

exclusive events "En" so defined

$$P_n\{E_n\} = P\{\text{the plant has failed "n" times and been repaired "n" times}\} \quad (3)$$

We get

$$A = \sum_{n=o}^{\infty} P\{E_n\} \quad (4)$$

We can write the following expressions for the various $P\{E_n\}$.

$$P\{E_o\} = P\{\text{the plant has never failed until t}\} = 1 - \int_o^t f(t)dt \quad (5)$$

$$P\{E_1\} = P\{\text{the plant has failed at "}t_1\text{", has been repaired at "}t_2\text{" and has not failed between "}t_2\text{" and "t"}\} =$$

$$= \int_o^t \int [1-F(t-t_2)]\, w\,(t_2-t_1) f(t_1)dt_1 dt_2 \quad (6)$$

$$o<t_1<t_2<t$$

The Laplace transforms of eqs. 5 and 6 are

$$P^*\{E_o\} = \frac{1}{s} - f^*(s) \quad (7)$$

and

$$P^*\{E_1\} = \left[\frac{1}{s} - \frac{f^*(s)}{s}\right] f^*(s)\, w^*(s) \quad (8)$$

By an iterated application of the convolution theorem for Laplace transforms, we get for the Laplace-transform of $P\{E_n\}$ defined in (3)

$$P^*\{E_n\} = \left[\frac{1}{s} - \frac{f^*(s)}{s}\right] \cdot \left[f^*(s)w^*(s)\right]^n \quad (9)$$

Substituting $P^*\{E_n\}$ into eq. (4) we get

$$A^* = \sum_{n=o}^{n=\infty} P^*\{E_n\} = \frac{1}{s}\left[1-f^*(s)\right] \sum_{n=o}^{\infty} \left[f^*(s)w^*(s)\right]^n \quad (10)$$

Eq. 10 can be written as follows:

$$A^*(s) = \frac{1}{s} \cdot \frac{1-f^*(s)}{1-f^*(s)w^*(s)} \quad (11)$$

and finally antitransforming

$$A(t) = L^{-1}\left\{\frac{1}{s}\ \frac{1-f^{*}(s)}{1-f^{*}(s)w^{*}(s)}\right\} \qquad (12)$$

A 6.3 Calculation of the asymptotic availability $A_\infty$

For $t\to\infty$ "A(t)" approaches a limit "$A_\infty$" which is largely used for many practical cases. It is given by

$$\lim_{t\to\infty} A(t) = A_\infty = \frac{\Psi}{\nu+\Psi} \qquad (1)$$

where

"$A_\infty$" = asymptotic availability

"$\nu$" = average failure rate

"$\Psi$" = average repair rate

From eq. 1 para A 6.2 we get for $t \to \infty$

$$\lim_{t\to\infty} A = \lim_{t\to\infty} L^{-1}\left\{\frac{1-f^{*}}{s(1-f^{*}w^{*})}\right\} = \frac{\lim_{s\to 0}\left[1-f^{*}\right]}{\lim_{s\to 0}\left[1-f^{*}w^{*}\right]} \qquad (2)$$

We have

$$\lim_{s\to 0} f^{*} = \lim_{t\to\infty}\int_0^t f(t)dt = 1 \qquad (3)$$

and

$$\lim_{s\to 0} w^{*} = \lim_{t\to\infty}\int_0^t w(t)dt = 1 \qquad (4)$$

Eqs. 3 and 4 indicate that de l'Hôpital's rule has to be used to evaluate the limit of eq. 2. We have

$$\lim_{t\to\infty} A = \lim_{s\to 0} \frac{df^{*}/ds}{w^{*}df^{*}/ds + f^{*}dw^{*}/ds} \qquad (5)$$

We have

$$\lim_{s\to o} df^*/ds = -\lim_{t\to\infty} \int_o^t tf(t)dt = -\frac{1}{\Psi} \qquad (6)$$

and

$$\lim dw^*/ds = -\lim_{t\to\infty} \int_o^t tw(t)dt = -\frac{1}{\Psi} \qquad (7)$$

Putting 6 and 7 into 5, we get

$$A\infty = \lim_{t\to\infty} A = \frac{\Psi}{\Psi+\nu} \qquad (8)$$

## A 6.4 Calculation of the instantaneous failure rate "$\chi_f$"

We call instantaneous failure rate, "$\chi_f$", the quantity defined

$$Z(t)dt = \chi_f \cdot dt = \frac{P\{\text{the plant is up at "t" and fails before "t+dt"}\}}{P\{\text{the plant is up at "t"}\}} \qquad (1)$$

We shall calculate "$\chi_f$" as function of the failure-probability-density-distribution, "f(t)", and of the repair-probability-density-distribution "w(t)". The denominator of eq. 1 is the point availability"A" given by eq.1 of para. A 6.1.

We have to calculate the numerator of eq. 1, that is the probability of event "E" so defined

$$P\{E\} = P\{\text{the plant is up at "t" and fails before "t+dt"}\} \qquad (2)$$

To do this, we sum all the probabilities "$P\{E_n\}$ of the following mutually exclusive events

$$P\{E_n\} = P\{\text{the plant has failed n-times and has been repaired n-times before "t" and fails again before "t+dt"}\} \qquad (3)$$

where n = o, 1, 2, .....

With a procedure similar to that developed in para A 6.2, we can calculate the probability of the event "$E_n$" defined by eq. 3

$$P\{E_n\} = dt \cdot L^{-1}\left\{[1-f^*(s)w^*(s)]^n\left[\frac{1}{s} - \frac{f^*(s)}{s}\right]\right\} \qquad (4)$$

where the asterisk "*" denotes the Laplace transform, and $L^{-1}$ indicates antitrasformation to the time domain.

We add all terms given by eq. 4 to get $P\{E\}$

$$P(E) = dtL^{-1}\left\{\left[\frac{1}{s} - \frac{f^*(s)}{s}\right]\sum_{n=1}^{n=\infty}\left[1-f^*(s)w^*(s)\right]^n\right\} \qquad (5)$$

Finally we get

$$P\{E\} = dt\, L^{-1}\left\{\frac{1}{s}\,\frac{1-f^*(s)}{1-f^*(s)w^*(s)}\right\} \qquad (6)$$

Putting eq. 2 of para A 1.1 (the availability "A") and eq. 6 into equation 1, we get

$$\chi_f = \frac{L^{-1}\left(\frac{f^*(s)}{1-f^*(s)\,w^*(s)}\right)}{L^{-1}\left(\frac{1}{s}\,\frac{1-f^*(s)}{1-f^*(s)w^*(s)}\right)} \qquad (7)$$

## A 6.5 Calculation of the instantaneous repair rate "$\chi_w$"

We call instantaneous repair rate the quantity "$\chi_w$", so defined

$$\chi_w \cdot dt = \frac{P\{\text{the plant is down at "t" and is repaired before "t+dt"}\}}{P\{\text{the plant is down at "t"}\}} \qquad (1)$$

We shall calculate "$\chi_w$" as function of the failure-probability-density-distribution, "f(t)" and of the repair-probability-density-distribution "w(t)". The denominator of eq. 1 is equal to "1-A" (where "A" is the availability, given by eq. 1 of para. A 6.1).

The numerator of eq. 1 is the probability of the event "E"

$$P\{E\} = P\{\text{the plant is down at "t" and is repaired before "t+dt"}\} \qquad (2)$$

$P\{E\}$ will be obtained by summation of all the probabilities of the mutually exclusive events "$E_n$" defined as follows:

$$P\{E_n\} = P\{\text{the plant has failed n-times and has been repaired (n-1) times before "t" and is repaired again before "t+dt"}\} \qquad (3)$$

where n = 1, 2, 3 .....

With procedure similar to that developed in para. A 6.2 and A 6.4, we get

$$P\left\{\begin{matrix}E\\n\end{matrix}\right\} = dt\, L^{-1}\left\{f^{*}(s)w(s)\left[f^{*}(s)w^{*}(s)\right]^{n}\right\} \qquad (4)$$

We add all terms given by eq. 4 and we get

$$P\{E\} = dtL^{-1}\left\{\left[f^{*}(s)w^{*}(s)\right]\sum_{n=1}^{\infty}\left[f^{*}(s)w^{*}(s)\right]^{n}\right\} =$$

$$dtL^{-1}\left[\frac{f^{*}(s)w^{*}(s)}{1-f^{*}(s)w^{*}(s)}\right] \qquad (5)$$

Taking into account eq. 5 and eq. 1 of para. A 6.2, eq.1 becomes

$$\chi_{w} = \frac{L^{-1}\left\{\frac{f^{*}(s)w^{*}(s)}{1-f^{*}(s)w^{*}(s)}\right\}}{1-L^{-1}\left\{\frac{1}{s}\,\frac{1-f^{*}(s)}{1-f^{*}(s)w^{*}(s)}\right\}} \qquad (6)$$

## A 6.6 Calculation of the asymtotic values of "$\chi_f$" and "$\chi_w$"

From eq. 8 of para A 6.4 we get

$$\lim_{t\to\infty}\chi_{f} = \frac{\lim_{s\to o}\left[s\,\frac{f^{*}(s)}{1-f^{*}(s)w^{*}(s)}\right]}{\lim_{s\to o}\left[\frac{1}{s}\,\frac{1-f^{*}(s)}{1-f^{*}(s)w^{*}(s)}\right]} \qquad (1)$$

The limit at the denominator of eq. 1 has already been calculated in para A 6.3. We have

$$\lim_{s\to o}\ \frac{1}{s}\ \frac{1-f^{*}(s)}{1-f^{*}(s)w^{*}(s)} = \frac{\psi}{\psi+\nu} \qquad (2)$$

where

$$\psi = \frac{1}{\int_{o}^{\infty} t\,w(t)dt} \qquad (3)$$

and

$$\nu = \frac{1}{\int_{o}^{\infty} t\,f(t)dt} \qquad (4)$$

For the numerator we have to apply the rule of de l'Hôpital. We have

$$\lim_{s\to 0}\left[f^{*}(s)\ \frac{s}{1-f^{*}(s)w^{*}(s)}\right] = -\lim_{s\to 0}\left[\frac{1}{f^{*}\frac{dw^{*}}{ds}+w^{*}\frac{df^{*}}{ds}}\right] =$$

$$= \frac{\psi\nu}{\psi+\nu} \qquad (5)$$

Putting eqs. 5 and 2 into eq. 1, we get finally

$$\lim_{t\to\infty}\chi_{f} = \nu \qquad (6)$$

With analogous procedure it is possible to verify that

$$\lim_{t\to}\chi_{w} = \psi \qquad (7)$$

## A 6.7 Conclusions

The conclusions, which we can draw at the end of this appendix, are very general and very important. If we have a plant (or a subsystem or a unit) with failure and repair probability density distributions respectively f(t) and w(t), the asymptotic values of the point availability "A", of the failure rate "$\chi_f$" and of the repair rate "$\chi_w$" are the following

$$\lim_{t\to\infty} A = A\infty = \frac{\psi}{\psi+\nu} \qquad (1)$$

$$\lim_{t\to\infty}\chi_{f} = \nu \qquad (2)$$

$$\lim_{t\to\infty}\chi_{w} = \psi \qquad (3)$$

Where

$$\psi = \frac{1}{\int_{0}^{\infty} tw(t)dt} \qquad (4)$$

and

$$\nu = \frac{1}{\int_0^\infty t f(t)\,dt} \qquad (5)$$

For the unavailability U we get from eq. 1

$$U = 1 - A_\infty = \frac{\nu}{\psi + \nu} \qquad (6)$$

This means that, for long periods of time ($t \to \infty$), any system (plant- or subsystem or unit) behaves as if it has a failure and repair probability density distributions both exponential with failure and repair rates given respectively by eqs. 4 and 5.

This property of the asymptotic behaviour of the systems allows us to extend many results obtained with exponential distributions to cases where the distributions are not exponential.

## 15. Appendix 7: Calculation of the average failure rate of a functional subsystem for different strategies

### A 7.1 Functional subsystem consisting of two units one working and the other in stand-by - No preventive maintenance

This case has been called "strategy 2" in para. 5.4. If we call with "A" and "B" the two units, the functional subsystem "F" can be in one of the below listed states

State "0" "A" in operation and "B" in stand-by or
"A" in stand-by and "B" in operation

State "1" "A" in operation and "B" in repair or
"B" in operation and "A" in repair

State "2" Both unit failed and subsystem therefore also failed.

The subsystem start with a unit "A" in operation and the other "B" in stand-by (State "0"). If "A" fails, it is automatically switched off, while "B" is automatically switched into operation (State 1). The failed unit "A" is repaired and, when the repair is completed, will be connected as stand-by unit (State 0). The subsystem will fail if the working unit fails before the repair of the other is completed (State 2).

The reliability "$R_F$" of the subsystem "F" will be obtained by summing the following probabilities "$P_i$" of the below listed mutually exclusive events

$$P_o = P\{\text{A is not failed at "t"}\} \qquad (1)$$

$$P_1 = P\{\text{A is failed at "}t_1\text{" and B is not failed at "t"}\}_{0 < t_1 < t} \qquad (2)$$

$$P_2 = P\left\{\begin{array}{l}\text{A is failed at "}t_1\text{"; A is repaired before B fails;}\\ \text{B fails at "}t_2\text{"; A is not failed at "t"}\end{array}\right\}_{0 < t_1 < t_2 < t} \qquad (3)$$

. . . . . .

$$P_i = P\left\{\begin{array}{l}\text{A is failed at "}t_1\text{"; A is repaired before B fails}\\ \text{..... B fails at "}t_i\text{"; A is not failed at "t"}\end{array}\right\}_{0 < t_1 < t_2 \ldots\ldots < t_i < t} \qquad (4)$$

We indicate with $h_F(t)$ and $g_F(t)$ respectively the failure and repair probability density distributions of each of the two units. The two cumulative distributions will be

$$H_F(t) = \int_o^t h_F(t)dt \tag{5}$$

and

$$G_F(t) = \int_o^t g_F(t)dt \tag{6}$$

We can write

$$P_o = 1 - \int_o^t h_F dt = 1 - H_F(t) \tag{7}$$

$$P_1 = \int_o^t h_F(t_1) \left[1-H_F(t-t_1)\right]dt_1 \tag{8}$$

$$P_2 = \int_o^t\int h_F(t_1) \left[h_F(t_2-t_1)G(t_2-t_1)\right]\left[1-H_F(t-t_2)\right] dt_1 dt_2 \tag{9}$$

The Laplace transforms of eqs. 7, 8 and 9 are the following

$$P_o^* = \frac{1}{s} - \frac{h_F^*(s)}{s} \tag{10}$$

$$P_1^* = \left(\frac{1}{s} - \frac{h_F^*(s)}{s}\right) h_F^*(s) \tag{11}$$

$$P_2^* = \left(\frac{1}{s} - \frac{h_F^*}{s}\right) h_F^*(h_F G_F)^* \tag{12}$$

where

s = complex variable of the Laplace domain

"*" indicates Laplace transform

Looking at eqs. 10, 11 and 12, one can easily derive for $P_i^*$ the following expression

$$P_i^* = \left(\frac{1}{s} - \frac{h_F^*}{s}\right) h_F^* \left[(h_F G_F)^*\right]^{i-1} \tag{13}$$

The Laplace transform of the reliability $R_F$ can then be easily calculated

$$R_F^* = \sum_{i=1}^{\infty} P_i^* = \frac{1}{s}\left[1-h_F^* + \frac{h_F^*(1-h_F^*)}{1-(h_F G_F)^*}\right] \tag{14}$$

The average failure rate "$\lambda_F$" of subsystem "F" is given by

$$\lambda_F = \frac{1}{\int_0^{\infty} R_F dt} = \frac{1}{\lim_{s\to 0} R_F^*} \tag{15}$$

From eq. 14 we have

$$\lim_{s\to 0} R_F^* = \lim_{s\to 0} \frac{1-h_F^*}{s}\left[1+ \frac{h_F^*}{1-(h_F G_F)^*}\right] \tag{16}$$

Now we have

$$\lim_{s\to 0} h_F^* = \lim_{t\to\infty} \int_0^t h_F dt = 1 \tag{17}$$

Taking into account eq. 17, eq. 16 becomes

$$\lim_{s\to 0} R_F^* = \left[1 + \frac{1}{1-\lim_{s\to 0}(h_F G_F)^*}\right] \lim_{s\to 0} \frac{1-h_F^*}{s} \tag{18}$$

Applying the theorem of de L'Hôpital, we get

$$\lim_{s\to 0} \frac{1-h_F^*}{s} = -\lim_{s\to 0} \frac{dh_F^*}{ds} = \lim_{t\to\infty} \int_0^t t\, h_F dt = \frac{1}{\sigma_F} \tag{19}$$

where "$\sigma_F$" is the average failure rate of a unit.

Taking into account eqs. 18 and 19, eq. 15 becomes finally

$$\lambda_F = \frac{\sigma_F}{1 + \frac{1}{1-\lim_{s\to 0}(h_F G_F)^*}} \tag{20}$$

Let us consider the particular case in which $h_F(t)$ is exponential

$$h_F(t) = \sigma_F \exp(-\sigma_F t) \tag{21}$$

Taking into account eq. 21, we can write

$$(h_F G_F)^* = \int_0^\infty \sigma_F \exp\left[-t(\sigma_F+s)\right] G_F(t)dt \tag{22}$$

and

$$\lim_{s\to 0} (h_F G_F)^* = \int_0^\infty \sigma_F \exp(-\sigma_F t) G_F(t)dt =$$

$$= \left[\exp(-\sigma_F t) G_F(t)\right]_\infty^0 + \int_0^\infty \exp(-\sigma_F t) g_F(t)dt =$$

$$= \int_0^\infty \exp(-\sigma_F t) g_F(t)dt \tag{23}$$

Taking into account eq. 23, eq. 20 becomes in this particular case

$$\lambda_F = \frac{\sigma_F}{1 + \dfrac{1}{1 - \displaystyle\int_0^\infty \exp(-\sigma_F t) g_F(t)dt}} \tag{24}$$

If $g_F(t)$ too is exponential

$$g_F(t) = \mu_F \exp(-\mu_F t) \tag{25}$$

we have

$$\int_0^\infty \exp(-\sigma_F t) g_F(t)dt = \mu_F \int_0^\infty \exp\left[-t(\sigma_F+\mu_F)\right]dt = \frac{\mu_F}{\sigma_F+\mu_F} \tag{26}$$

Taking into account eq. 26, eq. 24 becomes

$$\lambda_F = \frac{\sigma_F}{2 + \mu_F/\sigma_F} \tag{27}$$

Since $\mu_F/\sigma_F$ is usually very large, we get from eq. 27

$$\lambda_F \simeq \frac{\sigma_F^2}{\mu_F} \tag{28}$$

It is very interesting to notice that eq. 28 holds approximately also in the case in which $g_F(t)$ is not exponential. In this case "$\mu_F$" is defined as average repair rate

$$\mu_F = \frac{1}{\displaystyle\int_0^\infty t\, g_F(t)dt} \tag{29}$$

We have, developing $\exp(-\sigma_F t)$ in a Taylor series

$$\int_0^\infty \exp(-\sigma_F t) g_F(t)dt = 1-\sigma_F \int_0^\infty t\, g_F(t)dt + \sigma_F^2 \int_0^\infty t^2 g_F(t)dt + \ldots \quad (30)$$

If we stop the series at the first term, we get from eq. 30

$$\int_0^\infty \exp(-\sigma_F t) g_F(t)dt \simeq 1 - \frac{\sigma_F}{\mu_F} \quad (31)$$

Putting 31 in eq. 24, we get

$$\lambda_F \simeq \frac{\sigma_F}{1 + \mu_F/\sigma_F} \quad (32)$$

and, for $\mu_F/\sigma_F$ very large,

$$\lambda_F \simeq \frac{\sigma_F^2}{\mu_F} \quad (33)$$

A 7.2 Functional subsystem consisting of two units, one working and the other in stand-by. Preventive maintenance.

This case has been called strategy 3 in para. 5.4.

Eq. 24 of para. A 7.1 is approximately valid where "$\sigma_F$" is the average failure rate defined by eq. 1 of para. 2.

Eq. 33 of para. A 7.1 can also be used, where "$\mu_F$" is the average repair rate defined by eq. 29 of para. A 7.1.

A 7.3 Functional subsystem consisting of "$n_F$" units; "$k_F$" of these units are working and the other $n_F$-$k_F$ are in stand-by (Strategies 4 and 5 of para. 5.4)

If one of the working units fails, it is automatically switched off, while the first of the "$n_F$-$k_F$" stand-by units is at the same time automatically switched into operation. The failed unit is repaired, and then connected as last of the stand-by units. If a second unit fails, the second of the stand-by units is switched into operation, and so on.

The subsystem fails if $n_F$-$k_F$+1 units are failed. The subsystem can be at time "t" in one of the below listed states (fig. 26).

| State | Number of working units | Number of stand-by units | Number of failed units | Comments |
|---|---|---|---|---|
| 0 | $k_F$ | $n_F-k_F$ | 0 | |
| 1 | $k_F$ | $n_F-k_F-1$ | 1 | |
| 2 | $k_F$ | $n_F-k_F-2$ | 2 | |
| . . | . . | . . | . . | . . |
| i | $k_F$ | $n_F-k_F-i$ | i | |
| . . | . . | . . | . . | . . |
| $n_F-k_F-1$ | $k_F$ | 1 | $n_F-k_F-1$ | |
| $n_F-k_F$ | $k_F$ | 0 | $n_F-k_F$ | |
| $n_F-k_F+1$ | $\leq k_F-1$ | 0 | $\geq n_F-k_F+1$ | Subsystem failed |

We shall suppose that the failure and repair probability density distributions are both exponential

$$h_F = \sigma_F \exp(-\sigma_F t) \tag{1}$$

and

$$g_F = \mu_F \exp(-\mu_F t) \tag{2}$$

with $\sigma_F$ and $\mu_F$ both constant.

We indicate with $Q_i(t)$ the probability that the subsystem "F" is in state "i". We can write the following "$n_F-k_F+2$" equations

$$\frac{dQ_o}{dt} = - k_F\sigma_F Q_o + \mu_F Q_1 \tag{3}$$

$$\frac{dQ_1}{dt} = k_F\sigma_F Q_o - (k_F\sigma_F+\mu_F)Q_1 + \mu_F Q_2 \tag{4}$$

. . . . . .

$$\frac{dQ_i}{dt} = k_F\sigma_F Q_{i-1} - (k_F\sigma_F+\mu_F)Q_i + \mu_F Q_{i+1} \tag{5}$$

. . . . . .

$$\frac{dQ_{n_F-k_F}}{dt} = k_F\sigma_F Q_{n_F-k_F-1} + (k_F\sigma_F+\mu_F)Q_{n_F-k_F} \tag{6}$$

$$\frac{dQ_{n_F-k_F+1}}{dt} = k_F\sigma_F Q_{n_F-k_F} \tag{7}$$

Since

$$\sum_{i=o}^{n_F-k_F+1} Q_i = 1 \tag{8}$$

only "$n_F-k_F+1$" of the "$n_F-k_F+2$" equations are independent.

The associated initial conditions are

$$Q_o(0) = 1 \tag{9}$$

and

$$Q_i(0) = 0 \qquad (i=1,2,\ldots,n_F-k_F+1) \tag{10}$$

Taking into account the initial conditions 9 and 10, the Laplace transforms of eqs. 3 to 7 are

$$-1 = -(k_F\sigma_F+s)Q_o^* + \mu_F Q_1^* \tag{11}$$

$$0 = k_F\sigma_F Q_o^* -(k_F\sigma_F+\mu_F+s)Q_1^* + \mu_F Q_2^* \tag{12}$$

. . . . . .

$$0 = k_F\sigma_F Q_{i-1}^* -(k_F\sigma_F+\mu_F+s)Q_i^* + \mu_F Q_{i+1}^* \tag{13}$$

. . . . . .

$$0 = k_F\sigma_F Q_{n_F-k_F-1}^* + (k_F\sigma_F+\mu_F+s)Q_{n_F-k_F}^* \tag{14}$$

$$0 = k_F\sigma_F Q_{n_F-k_F}^* - s\, Q_{n_F-k_F+1}^* \tag{15}$$

where

s = complex variable of the Laplace domain

"*" indicates Laplace transform

The Laplace transform of the reliability "$R_F$" of subsystem "F" is given by

$$R_F^* = \frac{1}{s} - Q^*_{n_F-k_F+1} \tag{16}$$

Taking into account eq. 15, eq. 16 becomes

$$R_F^* = \frac{1 - k_F\sigma_F\, Q^*_{n_F-k_F}}{s} \tag{17}$$

Now we have

$$Q^*_{n_F-k_F} = \frac{A_{1;(n_F-k_F+1)}}{\Delta} \tag{18}$$

where

$\Delta$ = determinant of the coefficients of the first "$n_F-k_F+1$" equations (eq. 15 excluded)

$A_{1;(n_F-k_F+1)}$ = determinant complementary to the element "$a_{1;(n_F-k_F+1)}$", (1st line and "$n_F-k_F+1$"th column) of the determinant "$\Delta$".

The determinant $\Delta$, having "$n_F-k_F+1$" lines and $n_F-k_F+1$ columns, is written below (eq. 19).

$$\Delta = \begin{vmatrix} -(k_F\sigma_F+s) & \mu_F & 0 & \cdots & 0 & 0 & 0 \\ k_F\sigma_F & -(k_F\sigma_F+\mu_F+s) & \mu_F & \cdots & 0 & 0 & 0 \\ 0 & k_F\sigma_F & -(k_F\sigma_F+\mu_F+s) & \cdots & 0 & 0 & 0 \\ 0 & 0 & k_F\sigma_F & \cdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & k_F\sigma_F & -(k_F\sigma_F+\mu_F+s) & \mu_F \\ 0 & 0 & 0 & \cdots & 0 & k_F\sigma_F & -(k_F\sigma_F+\mu_F+s) \end{vmatrix} \tag{19}$$

Taking into account eq. 18, eq. 17 becomes

$$R_F^* = \frac{\Delta - k_F\sigma_F\, A_{1;(n_F-k_F+1)}}{s\Delta} \tag{20}$$

On the other hand "$R_S^*$" is also given by

$$R_S^* = \sum_{i=o}^{n_F-k_F+1} Q_i^* \tag{21}$$

By solving the system of eqs. 11 to 14, we get

$$Q_i^* = (-1)^i \frac{A_{1i}}{\Delta} \tag{22}$$

where "$\Delta$" is the determinant defined by eq. 19 and "$A_{1i}$" is the determinant complementary to the element "$a_{1i}$" (1st line and "i"th column) of $\Delta$.

Putting 22 in 21, we obtain

$$R_S^* = \frac{\sum_{i=1}^{n_F-k_F+1} (-1)^i A_{1i}}{\Delta} \tag{23}$$

By comparing eqs. 21 and 20, we get

$$\frac{\Delta - k_F\sigma_F A_{1;(n_F-k_F+1)}}{s} = \sum_{i=1}^{n_F-k_F+1} (-1)^i A_{1i} \tag{24}$$

By extracting the determinant $A_{1;(n_F-k_F+1)}$ from $\Delta$ (eq. 19), one obtains

$$A_{1;(n_F-k_F+1)} = (-1)^{(n_F-k_F+1)} (k_F\sigma_F)^{(n_F-k_F)} \tag{25}$$

Putting 25 in 24 for s=0, one gets

$$[\Delta]_{s=o} = (-1)^{n_F-k_F+1} (k_F\sigma_F)^{(n_F-k_F+1)} \tag{26}$$

The average failure rate "$\lambda_F$" of subsystem "F" is given by

$$\lambda_F = \frac{1}{\int_o^\infty R_F dt} = \frac{1}{\lim_{s\to o} R_F^*} \tag{27}$$

Taking into account eqs. 23 and 26, we get

$$\lambda_F = \frac{[\Delta]_{s=o}}{\sum_{i=1}^{n_F-k_F+1} (-1)^i \left[A_{1i}\right]_{s=o}} = (-1)^{n_F-k_F+1} \frac{(k_F\sigma_F)^{(n_F-k_F)}}{\sum_{i=1}^{n_F-k_F+1} (-1)^i \left[A_{1i}\right]_{s=o}} \qquad (28)$$

By extracting the determinants "$A_{1i}$" from $\Delta$ (eq. 19) we obtain for s=o

$$\left[A_{1i}\right]_{s=o} = (-1)^{n_F-k_F+1-i} (k_F\sigma_F)^{(i-1)} \left[ (k_F\sigma_F)^{n_F-k_F+1-i} + \right.$$

$$\left. + (k_F\sigma_F)^{n_F-k_F-i} \mu_F + \ldots + (k_F\sigma_F)\mu_F^{(n_F-k_F-i)} + \mu_F^{(n_F-k_F+1-i)} \right] \qquad (29)$$

Taking into account eq. 29, eq. 28 becomes

$$\lambda_F = \frac{k_F\sigma_F}{\sum_{i=1}^{n_F-k_F+1} i \left(\frac{\mu_F}{k_F\sigma_F}\right)^{n_F-k_F+1-i}} \qquad (30)$$

In the particular case $k_F$=1 (only one unit working), eq. 30 becomes

$$\lambda_F = \frac{\sigma_F}{\sum_{i=1}^{n_F} i \left(\frac{\mu_F}{\sigma_F}\right)^{(n_F-i)}} \qquad (31)$$

Since $\mu_F/\sigma_F$ is usually very large, we can have the two following approximate expressions derived from eqs. 30 and 31

$$\lambda_F \simeq \frac{(k_F\sigma_F)^{n_F-k_F+1}}{\mu_F^{(n_F-k_F)}} \qquad (32)$$

and for $k_F$=1

$$\lambda_F = \frac{\sigma_F^{n_F}}{\mu_F^{n_F-1}} \qquad (33)$$

For analogy with what we have found for the case of two units in para. A 7.1, eqs. 32 and 33 should be valid also in the case in which "$\sigma_F$" is an average failure distribution given by eq. 1 of para. 2 (with any type of failure distri-

bution), and $\mu_F$ is given by

$$\mu_F = \frac{1}{\int_0^\infty t\, g_F(t)dt} \tag{34}$$

with $g_F(t)$ being also not essentially exponential.

16. Appendix 8: Calculation of the expected number of non preventive replacements (or repairs) carried out in one maintenance period of a unit belonging to a functional subsystem.

In this appendix we want to calculate the expected number "$x_F$" of non preventive replacements (or repairs) carried out in one maintenance period "$\theta_F$" of a unit belonging to a functional subsystem (eq. 7 of para. 5.7).

We indicate with $h_F(t)$ the failure probability density distribution of a unit.

We indicate with $P_i(t)$ the probability that "i" units have failed (and therefore replaced) before time "t" and that the "i+1" unit is working.

We have

$$P_o = 1 - \int_o^t h_F(t)dt \tag{1}$$

$$P_1 = \int_o^t h_F(t_1)\left[1-H_F(t-t_1)\right]dt_1 \tag{2}$$

$$0 < t_1 < t$$

$$P_2 = \int_o^t \int_o^{t_2} h_F(t_1)\, h_F(t_2-t_1)\, \left[1-H_F(t-t_2)\right] dt_1 dt_2 \tag{3}$$

$$0 < t_1 < t_2 < t$$

where

$$H_F(t) = \int_o^t h_F(t)dt \tag{4}$$

The Laplace transforms of eqs. 1, 2 and 3 are

$$P_o^* = \frac{1}{s} - \frac{h_F^*(s)}{s} \tag{5}$$

$$P_1^* = \left[\frac{1}{s} - \frac{h_F^*(s)}{s}\right] h_F^*(s) \tag{6}$$

$$P_2^* = \left[\frac{1}{s} - \frac{h_F^*(s)}{s}\right] \left[h_F^*(s)\right]^2 \tag{7}$$

where "*" indicates Laplace transform, and "s" is the complex variable of the Laplace domain.

Looking at the eqs. 5, 6 and 7, we can easily derive the following equation

$$P_i^* = \left[\frac{1}{s} - \frac{h_F^*(s)}{s}\right] \left[h_F^*(s)\right]^i \qquad (8)$$

Antitransforming eq. 8 to the time domain, we get

$$P_i = L^{-1} \left\{ \frac{\left[h_F^*(s)\right]^i}{s} - \frac{\left[h_F^*(s)\right]^{i+1}}{s} \right\} \qquad (9)$$

where $L^{-1}$ indicates antitransformation to the time domain.

The expected number "$x_F(t)$" of failed units at time "t" is given by

$$x_F(t) = \sum_{i=o}^{\infty} i\, P_i = \sum_{i=o}^{\infty} L^{-1} \left\{ \frac{i}{s} \left[h_F^*(s)\right]^i - \frac{i}{s} \left[h_F^*(s)\right]^{i+1} \right\} = L^{-1} \left\{ \frac{1}{s} \frac{h_F^*(s)}{1-h_F^*(s)} \right\} \qquad (10)$$

Eq. 10 can be written as follows

$$x_F(t) = \int_o^t L^{-1} \left[ \frac{h_F^*(s)}{1-h_F^*(s)} \right] dt \qquad (11)$$

For $t=\Theta_F$, we get finally

$$x_F = \int_o^{\Theta_F} L^{-1} \left[ \frac{h_F^*(s)}{1-h_F^*(s)} \right] dt \qquad (12)$$

17. Appendix 9: Calculation of the expected number of non preventive replacements (or repairs) carried out in one maintenance period of a unit belonging to a safety subsystem.

We indicate with $h'_S(t)$ and $h''_S(t)$ the two failure probability density distributions respectively for failure type "a" and type "b".

The two modified failure probability distributions, which take into account the on-off-cycling due to the checks with checking periods "$\tau_S$", are respectively (eqs. 3 and 4 of Appendix 2)

$$\left(1 + \frac{\delta'_S}{\tau_S}\right) h'_S \left[t\left(1+ \frac{\delta'_S}{\tau_S}\right)\right] \qquad (1)$$

and

$$\left(1 + \frac{\delta'_S}{\tau_S}\right) h''_S \left[t\left(1+ \frac{\delta''_S}{\tau_S}\right)\right] \qquad (2)$$

where "t" is still the real time and $\delta'_S$ and $\delta''_S$ are two constants.

Taking into account eqs. 1 and 2, the total failure probability density distribution $\bar{h}(t,\tau_S)$ will be

$$\bar{h}(t,\tau_S) = \left(1+ \frac{\delta'_S}{\tau_S}\right) h'_S \left[t\left(1+ \frac{\delta'_S}{\tau_S}\right)\right]\left[1- \int_o^{t(1+\delta''_S/\tau_S)} h''_S(t)dt\right] +$$

$$+ \left(1+ \frac{\delta''_S}{\tau_S}\right) h''_S \left[t\left(1+ \frac{\delta''_S}{\tau_S}\right)\right]\left[1- \int_o^{t(1+\delta'_S/\tau_S)} h'_S(t)dt\right] \qquad (3)$$

Taking into account eq. 3, with procedure similar to that developed in Appendix 8, we get the expected number "$x_S$" of units failed in one maintenance period "$\Theta_S$" (eq. 12 of para. 5.7)

$$x_S = \int_o^{\Theta_S} L^{-1}\left[\frac{\bar{h}^*_S(s,\tau_S)}{1 - \bar{h}^*(s,\tau_S)}\right] dt \qquad (4)$$

where

$L^{-1}$ indicates antitransformation to the time domain

"*" indicates Laplace transformation

"s" is the complex variable of the Laplace domain.

## 18. Bibliography

### A. Books

1. System Engineering Handbook, ed. R.E.Machol
Mc Graw-Hill Book Company Inc. 1965
(Ch. 33: H.D.Ross, Reliability)

2. P.L.Meyer, Introductory Probability and Statistical Applications
Addison-Wesley, 1965

3. Statistical Theory of Reliability (Advanced Seminar, Math. Res. Center,
University of Wisconsin) ed. M.Zelen

4. E. Barlow, F. Proschan, L. C. Hunter
Mathematical Theory of Reliability
J. Wiley and Sons, Inc. New York, 1965

5. I. Bazovsky
Reliability Theory and Practice
Prentice Hall Space Technology Series, 1965

6. S. R. Calabro
Reliability principles and practices,
Mc Graw-Hill, 1962

7. D. K. Lloyd, M. Lipow
Reliability: Management, Methods and Mathematics
Prentice Hall Space Technology Series, 1964

8. E. Pieruschka
Principles of Reliability
Prentice Hall, Inc., 1963

9. G. Sandler
System Reliability Engineering
Prentice Hall Space Technology Series, 1963

10. Stanford University, Calif., Dept. of Industrial Engineering Reliability
Handbook, ed. W. Grant Ireson,
Mc Graw Hill Book Co. Inc., New York, 1966

11. L. A. Zadek and Ch. A. Desoer,
Linear System Theory (The State Space Approach)

12. A. G. J. Macfarlane
Engineering Systems Analysis
G. G. Harrap & Co. Ltd., London, 1964
(Deutsche Übersetzung: Analyse Technischer Systeme, Bibl. Institut,
Mannheim, 1967, Hochschultaschenbücher 31/81a)

13. Y. v. Neumann
Probabilistic Logics and the Synthesis of reliable Organisms from unreliable
components, Automata Studies, Annals of Math. Studies no. 34, Princeton
University Press 1956

14. W. H. Pierce
Failure-tolerant Computer-design,
Academic Press, New York, 1965

15. V. Weyh,
Elemente der Schaltungsalgebra
R. Oldenbourg, München 1964

16. K. E. Iverson
A Programming Language
John Wiley and Sons, Inc., New York 1962
(Ch. 7, Logical Calculus)

17. P. L. Ivanescu
Pseudo-Boolean Programming and Applications (Lecture Notes in Mathematics)
Springer-Verlag, Berlin, 1965

18. G. Doetsch
Anleitung zum praktischen Gebrauch der Laplace-Transformation
R. Oldenbourg, München, 1961

19. W. Feller
Introduction to Probability Theory and its Applications
New York, Wiley 1950, 2. ed. 1958

20. B. W. Gnedenko
Lehrbuch der Wahrscheinlichkeitsrechnung (übersetzt aus dem Russischen)
Akademie-Verlag, Berlin 1958

21. M. Loève
Probability Theory
D. van Norstrand Compan, Inc., 1963

22. D. Morgenstern
Einführung in die Wahrscheinlichkeitsrechnung und Mathematische Statistik
Springer-Verlag, Berlin, 1964

23. W. Uhlmann
Statistische Qualitätskontrolle
B. G. Teubner, Stuttgart, 1965

24. J. W. Pratt, H. Raiffa, R. Schlaifer,
Introduction to statistical Decision-Theory
Mc Graw Hill Book Company, New York, 1965

25. S. Vajda
An Introduction to Linear Programming and the Theory of Games
Methuen & Co. Ltd., London 1960
(Deutsche Übersetzung: Einführung in die Linearplanung und die Theorie der Spiele, R. Oldenbourg, München, 1961)

26. E. J. Gumbel
Statistical Theory of Extreme Values and some Practical Applications
(A Series of Lectures)
National Bureau of Standards (NBS)
Applied Mathematics Series, 33, 1954

27. D. R. Cox
Renewal Theory
Methuen & Co. Ltd., London, 1962
(Deutsche Übersetzung: Erneuerungstheorie, R. Oldenbourg Verlag, München 1966)

28. N. U. Prabhu
Stochastic Processes
The Macmillan Co., New York, 1965

29. L. Takács
Stochastic Processes
Methuen & Co. Ltd., London, 1960
(Deutsche Übersetzung: Stochastische Prozesse, R. Oldenbourg Verlag, München, 1965)

B. Reports and Publications

1. E. F. Moore, C. E. Shannon
Reliable Circuits using less reliable relays
J. Franklin Inst., Vol. 262, part I and II, 1956

2. C. E. Shannon
A symbolic Analysis of Relay and Switching Circuits
Trans. AIEE, Vol. 57, 1938, pp. 713-723

3. C. E. Shannon
The synthesis of two terminal switching cirucits
Bell System Technical Journal, Vol. 28, No. 1, Jan. 1949, pp. 85-98

4. C. W. Griffin
Introducing the Fault-Tree as a Tool for Nuclear Safety Analysis
ANS-Transactions 9, 157 (1966)

5. W. Schikarski
Überlegungen zu schweren Reaktorunfällen (Ansätze zu einer neuen quantitativen Unfallphilosophie)
KFK-530, GfK, Karlsruhe, 1967

6. J. C. Moore,
Research Reactor Fault Analysis, Part I, II
Nucl. Eng. March, April 1966

7. R. J. Mulvihill, F. C. Reed
A probabilistic Methodology for the Safety Analysis of Power Reactors
AEC-Report No. SAN.-570-2

8. P. Dosch, M. Oehmann, E. Benz
Sicherheitsschaltungen für schnelle Reaktoren
(PSB-Bericht Nr. 13/64) GfK m.b.H., Karlsruhe, 1964

9. A. E. Green and A. J. Bourne
Reliability Considerations for Automatic Protective Systems
Nucl. Eng., August 1965

10. L. Cave, R. E. Holmes
Suitability of the AGR for Urban siting
Atomic Power constructions Ltd.

11. O. Knecht, Interatom Bensberg
Correlation between Reactor siting and Containment
(IAEA-Symposium on the Containment and siting of nuclear power plants, Vienna, 3-7 April, 1967)

12. W. R. Wise, J. F. Proctor,
Explosion Containment laws for Nuclear Reactor Vessels,
NOLTR-63, US-NOL, (Final Report), White Oak, Maryland, 1965

13. C. A. Willis, W. J. Carlson (AI),
Fault tree Analysis for SNAP-Reactor Disposal Systems,
ANS-Transactions, vol. 9, no. 1 (1966) 159

14. Aerospace Safety-Program-Safe Disposal of SNAP Reactors
(AEC Research and Development Report),
AI, by R. L. Detterman, A. Weitzberg, C. A. Willis

15. J. W. Croach
Quantitative Analysis of Hazards
(Subcommittee on Nuclear Space Safety Ad Hoc Committee on Nuclear Space Program, Atomic Industrial Forum, Inc.) Dec. 8, 1964

16. E. G. Schlechtendahl et al.
"Safety Features of a 300 MWe Sodium Cooled Fast Breeder Reactor"
Conference in Aix-en-Provence, September 1967

17. Military Specification, "System Safety Engineering of Systems and Associated Subsystems and Equipment; General Requirements For", MIL-S-38130A

18. A. B. Mearns
Bell Telephone Laboratories, Inc., "Fault Tree Analysis: The Study of Unlikely Events in Complex Systems"

19. David F. Haasl, System Safety Engineer, Missile Branch, Aero-Space Division, The Boeing Company, Seattle, Washington,
"Advanced Concepts in Fault Tree Analysis"

20. Concepts of System Safety Mathematics, Kazuo Konda, System Safety Engineer, The Boeing Company, dated June 1965

21. Computer Evaluation of Fault Tree Model, John M. Michels, Analog Applications Engineer, The Boeing Company, dated June 1965

22. Phyllis M. Nagel, Applied Mathematics Research Engineer, Engineering Analysis Missile Branch, Aero-Space Division, The Boeing Company,
"A Monte Carlo Method to Compute Fault Tree Probabilities"

23. R. J. Feutz and T. A. Waldeck,
"The Application of Fault Tree Analysis to Dynamic Systems"
The Boeing Company, dated June 1965

24. Fault Tree Analysis as a Tool for System Safety Engineering,
J. B. Beller, Autonetics, dated June 14, 1965

25. Observations Relative to Fault Tree Analysis, C. O. Miller, Aerospace Safety Division, USC, dated October 1, 1965

26. Proceedings, System Safety Symposium, by Neil E. Classon and W. R. Owens, The Boeing Company, Seattle, Washington, dated June 1965

27. Preston T. Farish, "Launch Vehicle Safety Engineering for Standard Payload Module", NASA TM X-53282 (Revised October 20, 1965)

28. Dr. Norman H. Roberts and Mr. David Haasl, Department of Mechanical Engineering, University of Washington, Lecture Notes - Systems Safety Analysis, Supplementary Notes - "Monte Carlo Techniques", "Elementary Logic", "Probability Theory","Distribution and Estimation", "Boolean Algebra and Switching Circuits", "Elementary Concepts in Game Theory and Decision Theory".

29. G. E. Ingram
The Probabilistic Nature of Engineering and Experimental Mechanics (SP-338), July 1965, GE, Santa Barbara, Calif.

30. E. L. Welker
The System Effectiveness concept (66 TMP-17), February 1966
GE, Santa Barbara, Calif.

31. E. L. Welker
The Basic Concepts of Reliability Measurement and Prediction
(65 TMP-63), September 1965, GE, Santa Barbara, Calif.

32. E. L. Welker
Predicting Reliability and Maintenance of Complex Systems by non-parametric methods (Ninth Symposium on Reliability and Quality Control, San Francisco, Calif., January 1963)

33. E. L. Welker
Preventive Maintenance from the System viewpoint
(not published)

34. John A. Connor, Calculations of the risk of component application in electronic systems, Trans. of IRE on Reliability and Quality Control (RQC), Januar 1957

35. Feyerherm, Prediction of tube failure rate variations, Trans. of IRE on RQC, Januar 1957

36. Bille, Reliability indices for missile electronics component parts, Trans. of IRE on RQC, Juni 1957

37. Munson, On the measurement of component reliability, Trans. of IRE on RQC, August 1957

38. Youtcheff, Statistical aspects of reliability in system development, Trans. of IRE on RQC, November 1957

39. IRE Convention Record 1956, Part 6, Manufacturing Electronics, The effects of environmental and operating conditions on the reliability studies of electronic equipments

40. Oetson, Wagener, Holmes, Child, Oxide cathodes in modern receiving valves, Trans. of IRE, 1952, part III, page 69

41. Schoer, Reliability in complex electronic equipment, Electrical Engineering, December 1955

42. Harris, Tall, Prediction of electronics equipment reliability, Electrical Engineering, November 1955

43. Kao, A new life quality measure for electron tubes, Trans. of IRE on RQC, April 1956

44. Marous A. Acheson, Electron tube life and reliability - Built in tube reliability, Trans. of IRE on RQC, April 1956

45. Sanford A. Moltzer, Desighing for Reliability, Trans. of IRE on RQC, September 1956

46. D. Hill, D. Voegtlen and J. Yueh, Parts vs. systems: the reliability dilemma, Trans. of IRE on RQC, Februar 1956

47. R. G. Miles, Statistical design - a means to better products, Trans. of IRE on RQC, April 1955

48. E. G. Rowe, P. Welch, Developments in trustworthy valve techniques, Trans. of IRE on RQC, December 1954

49. H. E. Blanton, R. M. Jacobs, A survey of techniques for analysis and prediction of equipment reliability, IRE Trans. RQC-11, no. 2, July 1962, pp. 18-35

50. R. S. Robins, On Models for Reliability Prediction, IRE Trans. RQC-11, no. 1, May 1962, pp. 33-43

51. F. M. Gryna et al. (editors), Reliability Training Text, Institute of Radio Engineers, 1960

52. L. Hellermann, A Computer Application to Reliable Design, IRE Trans. RQC-11, no. 1, May 1962

53. F. K. Buelow, Improvements in Current Switching, IRE Trans. El. Computers, vol. EC-9, no. 4, December 1960

54. R. H. Doyle et al., Automatic Failure Recovery in a Digital Data Processing System, IBM Journal Res. Development, January 1959

55. siehe unten

C. Journals and Periodicals

1. Proceedings of the National Symposium on Reliability and Quality Control, IRE

2. Annals of Reliability and Maintainability
(papers from the Annual Reliability and Maintainability Conference, sponsored by the American Institute of Aeronautics, and Astronautics, the Society of Automotive Engineers, and the Society of Mechanical Engineers, New York, American Institute of Aeronautics and Astronautics).

---

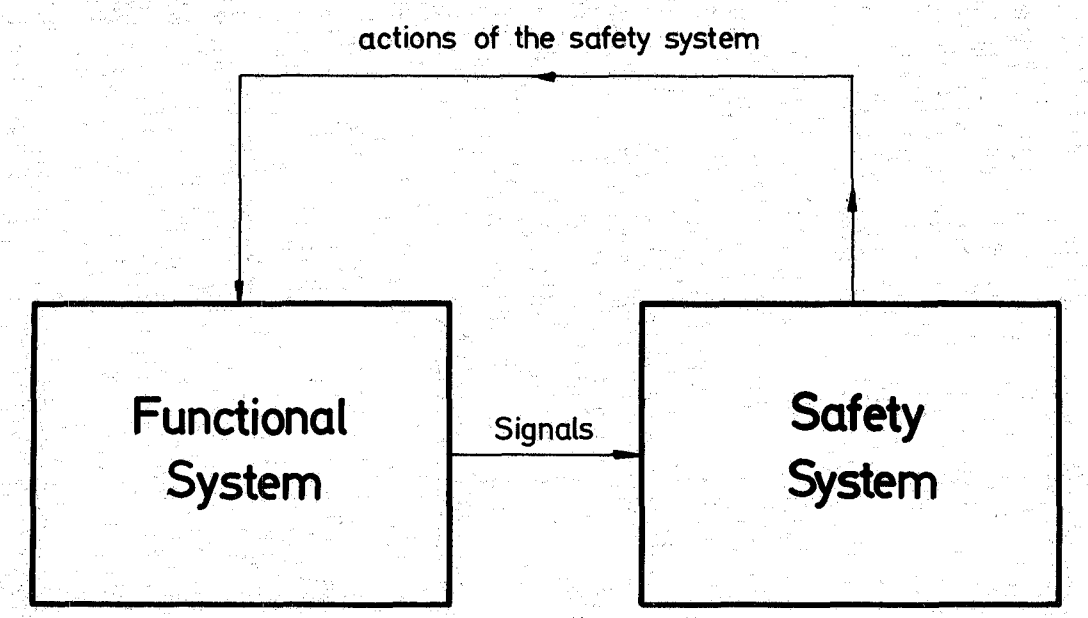
55. Dr. Vetter, Verfügbarkeitsuntersuchungen für Grundlastkraftwerke, Mitt.d.Ver.der Großkesselbesitzer e.V., Heft 96, Juni 1965, S.135
Dr. Vetter, Dr. Neuroth, Dipl.-Math. Lautz, unpublished work and private communications, RWE Essen, Abt. W. (for para 5 and 7)

3. IEEE-Transactions on Reliability
(IEEE Reliability Group),
Published aperiodically

4. Reliability Abstracts and Technical Reviews (RATR)
Published monthly by US-Government, NASA, Reliability and Quality Assurance Office, prepared by the Research Triangle Institute, Durham, N.C.

5. Technische Zuverlässigkeit in Einzeldarstellungen
Herausgegeben von A. Etzrodt, Oldenbourg Verlag, München

List of the figures




Block diagram of the links between the functional and safety system in a plant

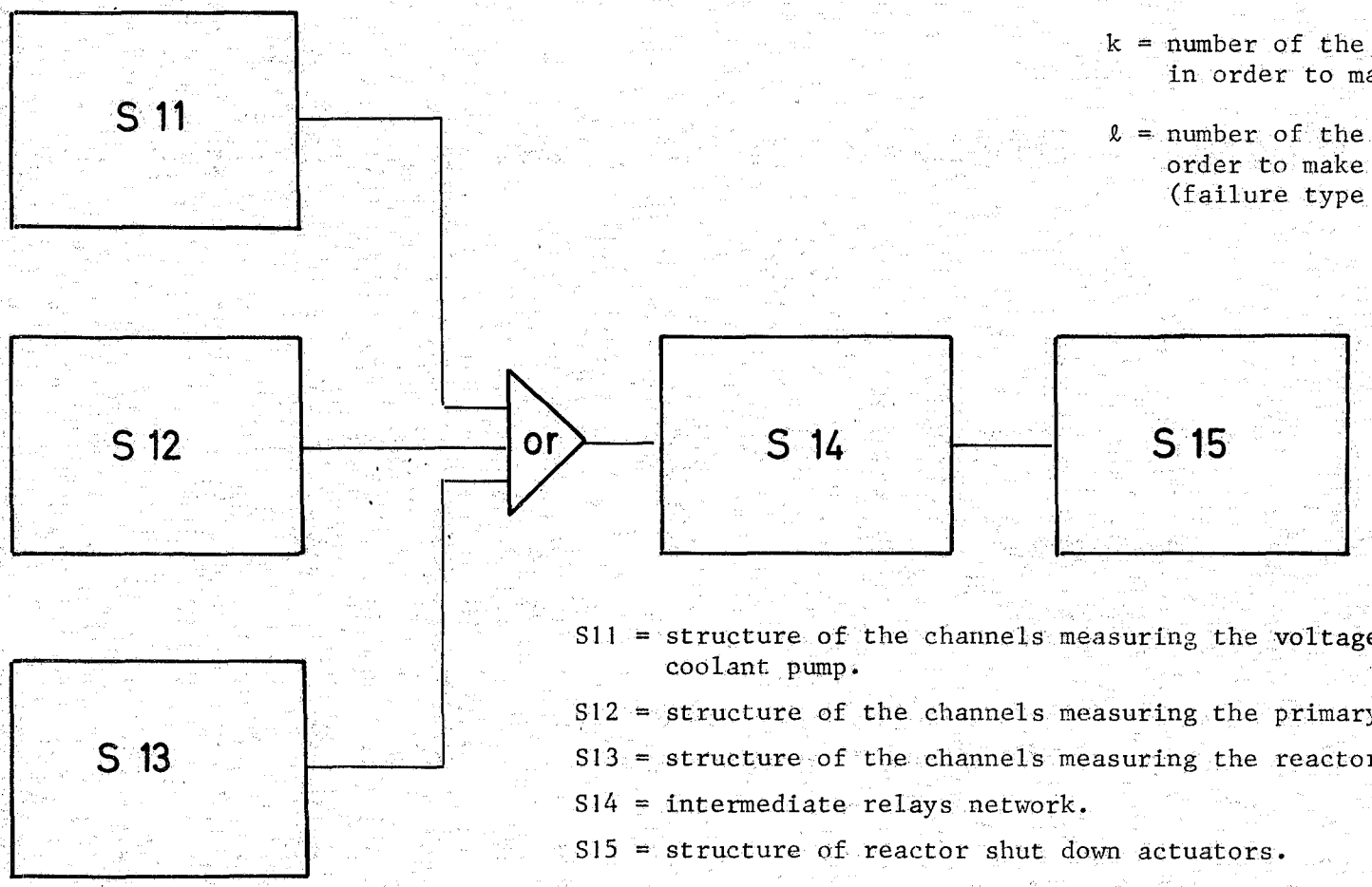
Fig. 1

n = number of the units

m = number of the units which must fail in order to make the subsystem to fail (failure type "a")

k = number of the units which must function in order to make the subsystem to function

ℓ = number of the units which must fail in order to make the subsystem to fail (failure type "b")




S11 = structure of the channels measuring the voltage to the motor of the primary coolant pump.

S12 = structure of the channels measuring the primary coolant flow.

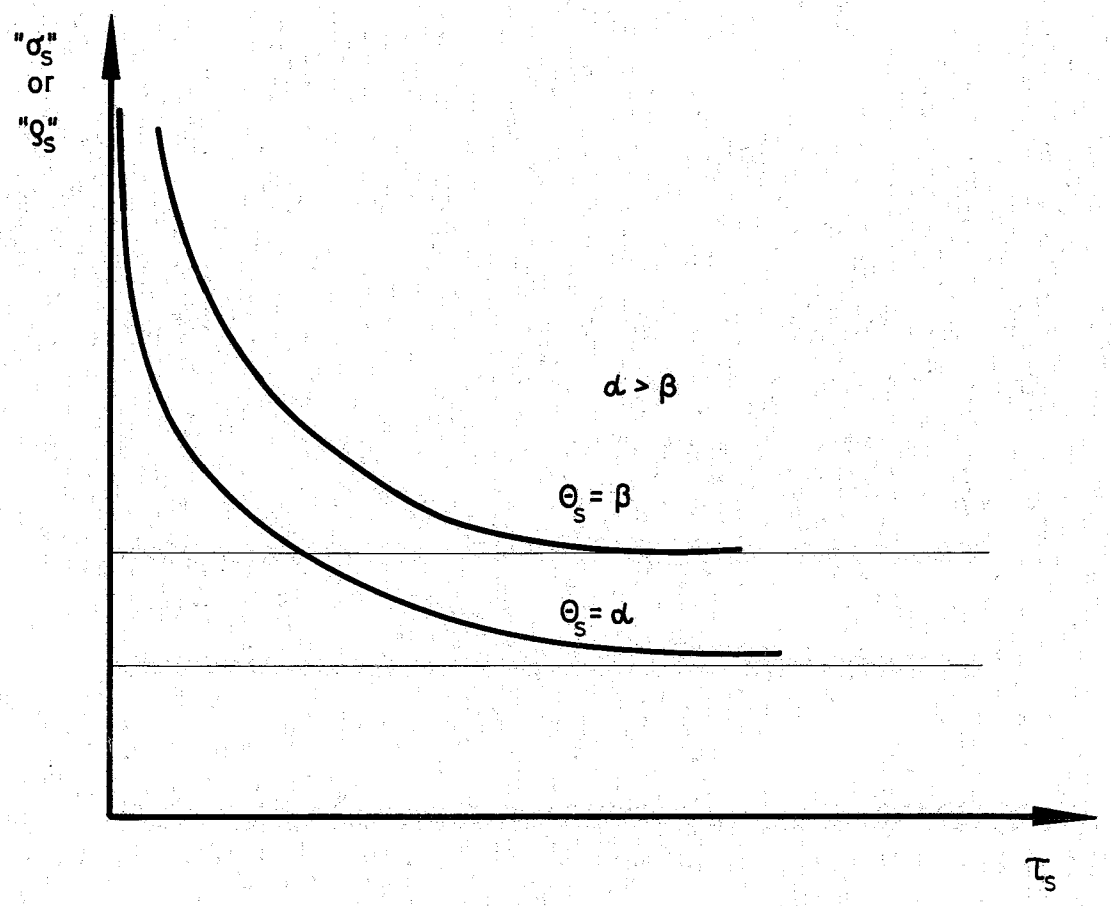
S13 = structure of the channels measuring the reactor outlet coolant temperature.

S14 = intermediate relays network.

S15 = structure of reactor shut down actuators.

SCHEMATIC BLOCK DIAGRAM OF THE CONNECTIONS AMONG SOME SAFETY SUBSYSTEMS

Fig. 2




$\varrho_s$ = unit failure rate ( failure type "a" )

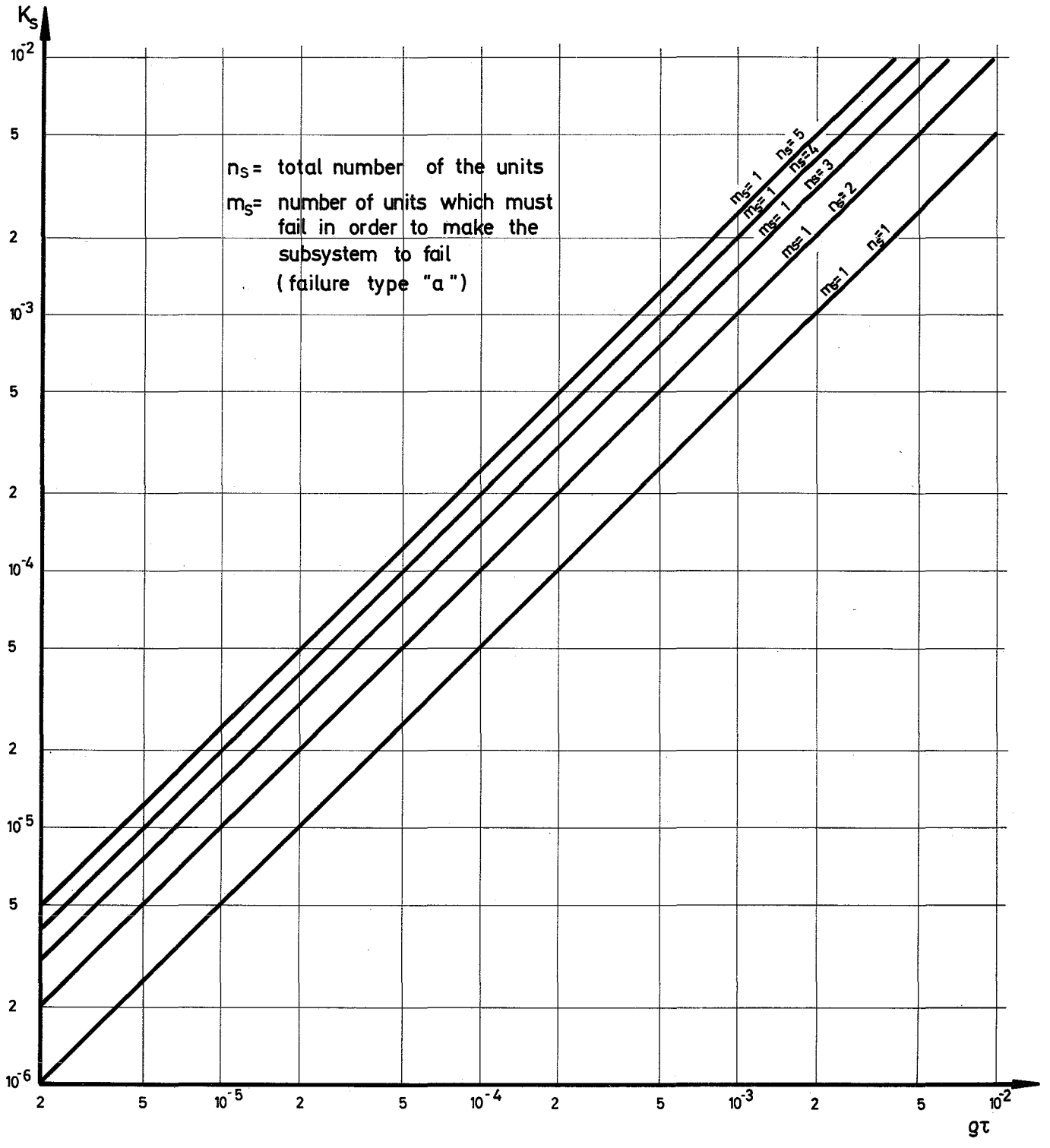
$\sigma_s$ = unit failure rate ( failure type "b" )

$\tau_s$ = time interval between two checks

$\Theta_s$ = time interval between two preventive replacements (or repairs )

**Failure rates of a unit belonging to a safety subsystem**

**Fig. 3**




# Fig. 4

The reduction coefficient "$K_s$" of a safety subsystem as function of the product between the unit average failure rate "$\varrho_s$" (failure type "a") and the checking time interval "$\tau_s$". (Case $m_s = 1$)

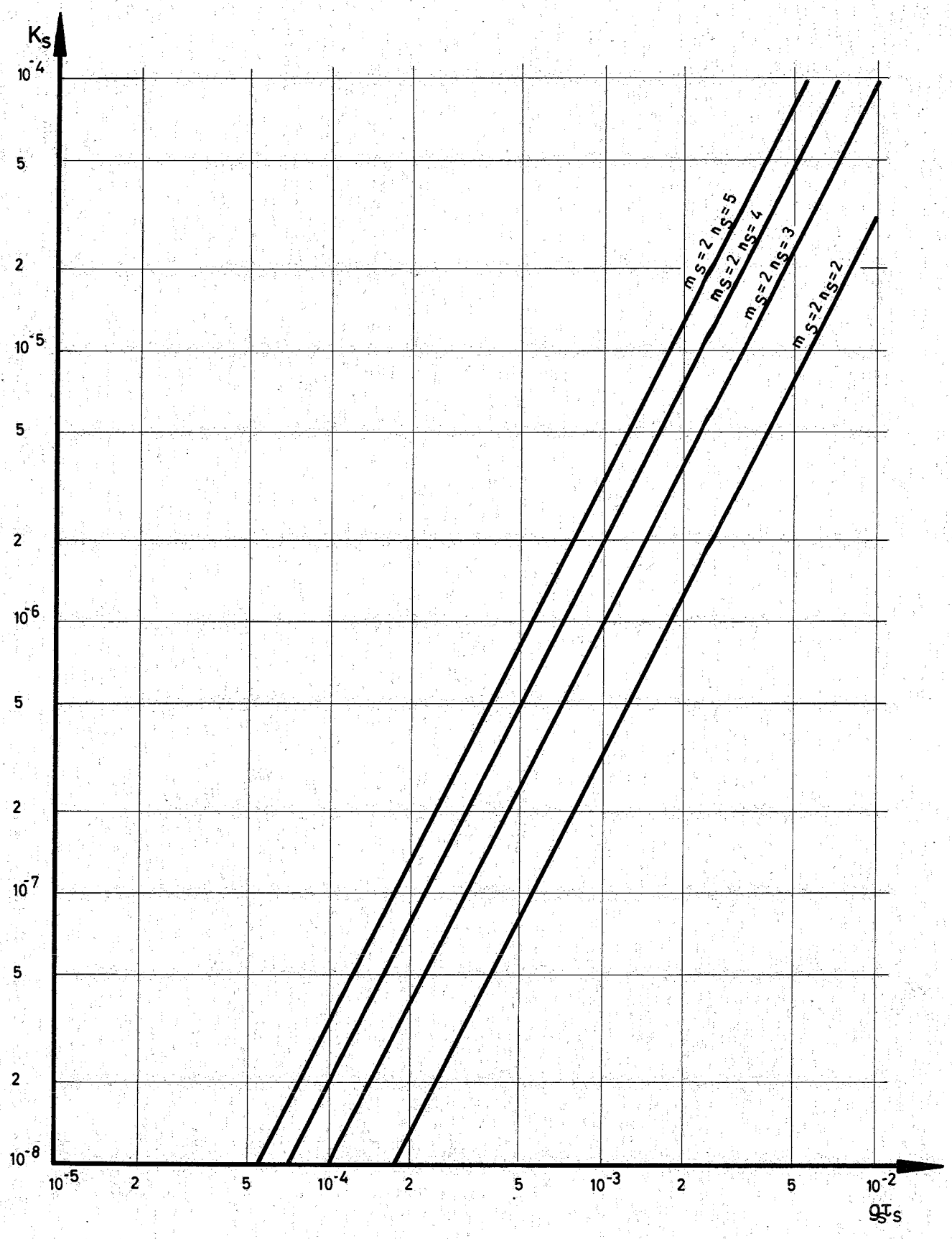



**Fig. 5**

The reduction coefficient "$K_s$" of a safety subsystem as function of the product between the unit average failure rate "$g_s$" (failure type "a") and the checking time interval "$\tau_s$". ( Case $m_s = 2$ )

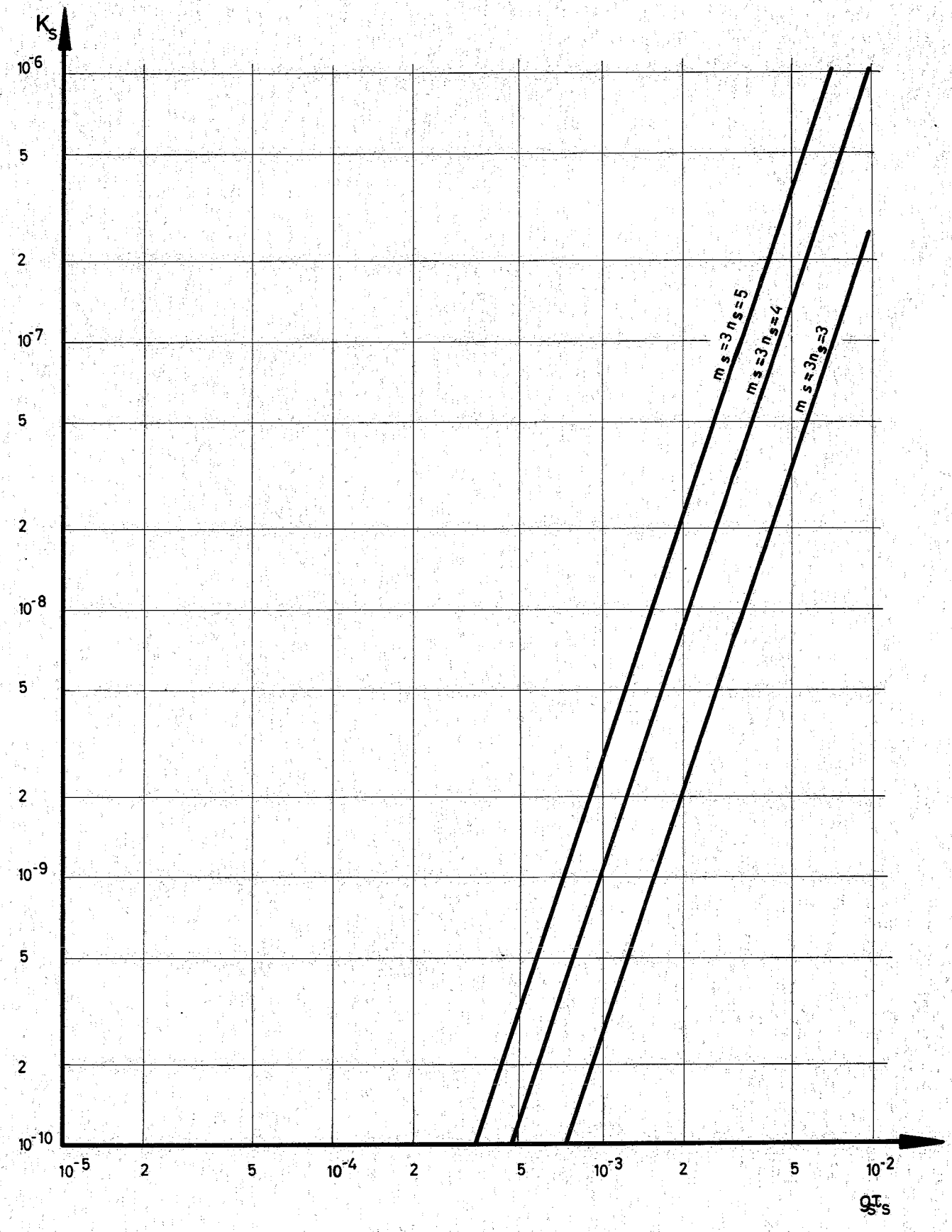
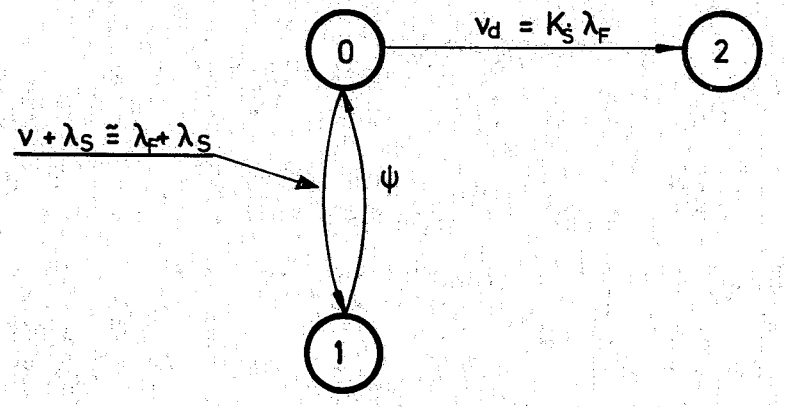



**Fig. 6**

The reduction coefficient "$K_s$" of a safety subsystem as function of the product between the unit average failure rate "$g_s$" (failure type "a") and the checking time interval "$\tau_s$". (Case $m_s = 3$)



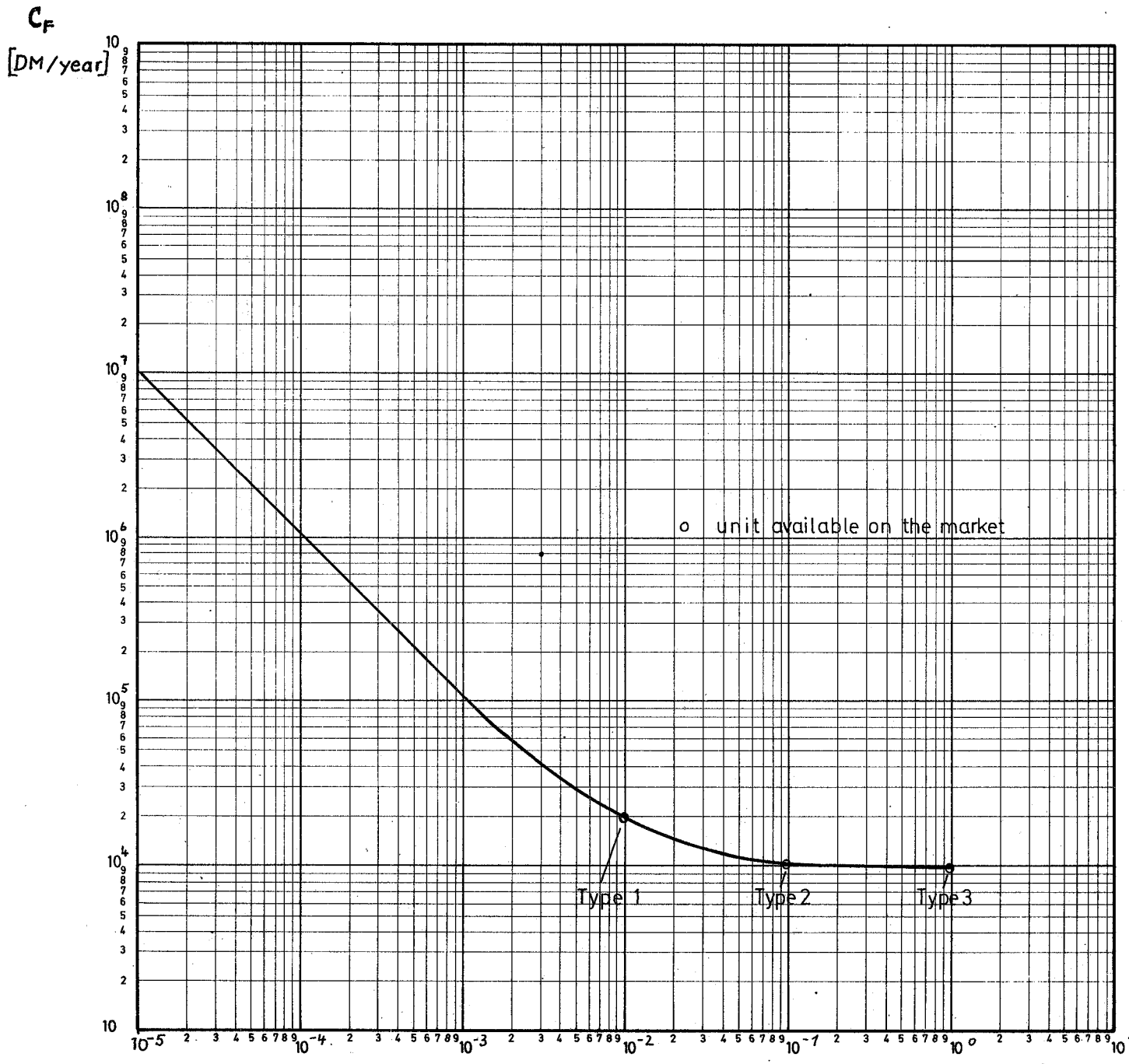

State "0" = Normal Operation

State "1" = Shut Down

State "2" = Disaster

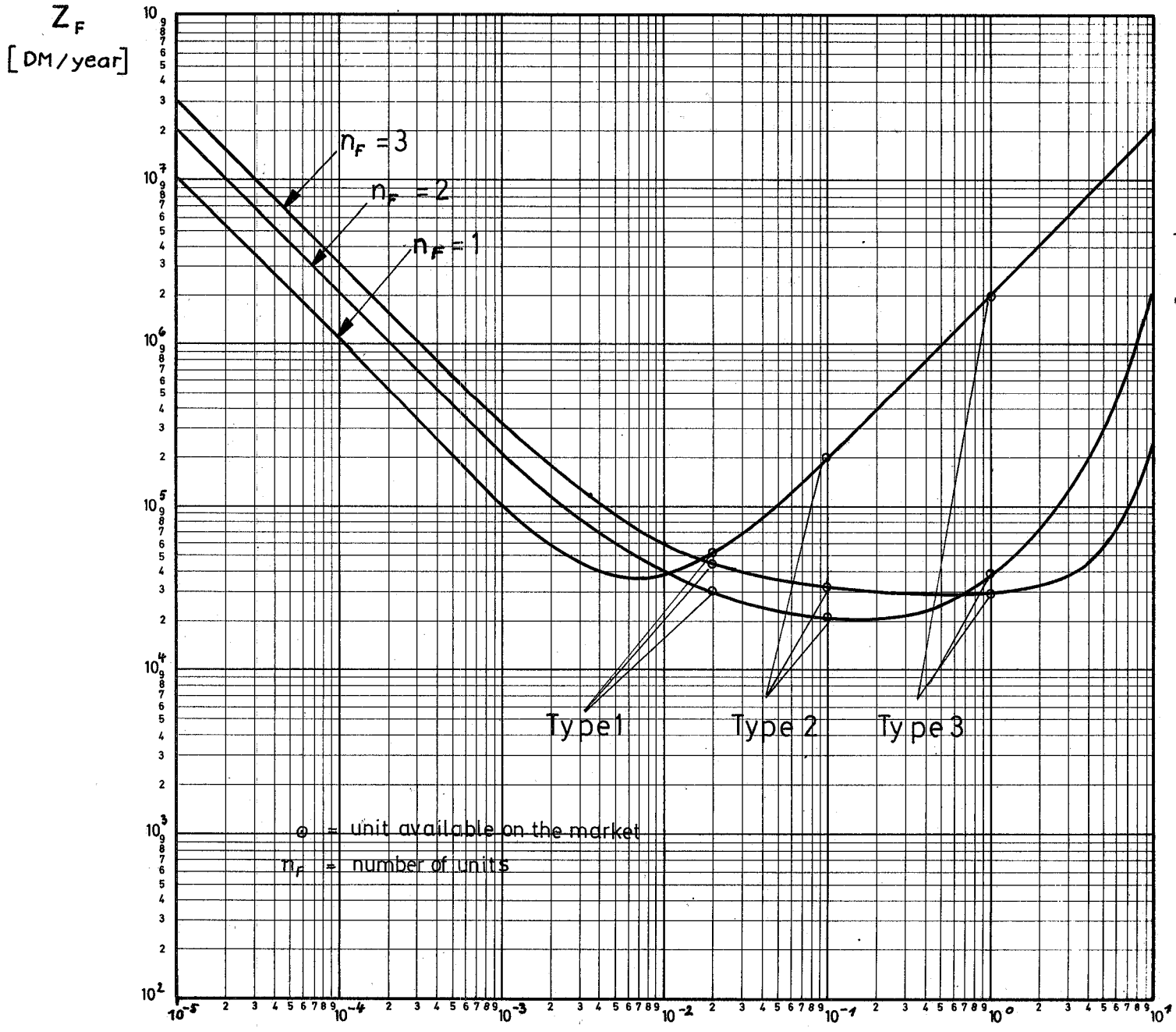
Flow diagram of plant states (Simple Model)

Fig. 7



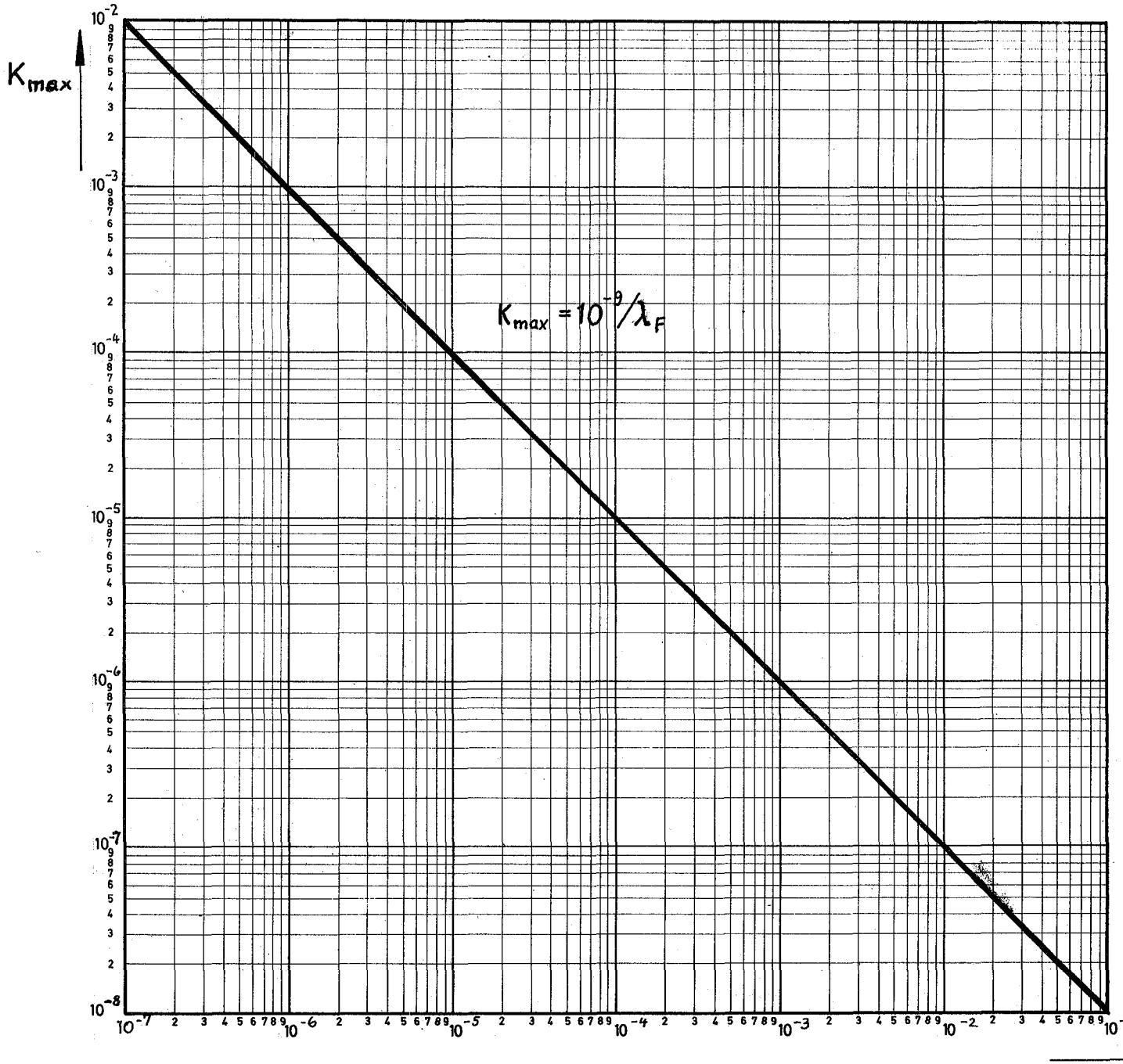

Annual costs "$C_F$" of a power supply unit as function of the unit failure rate "$\sigma_F$"

Fig. 8



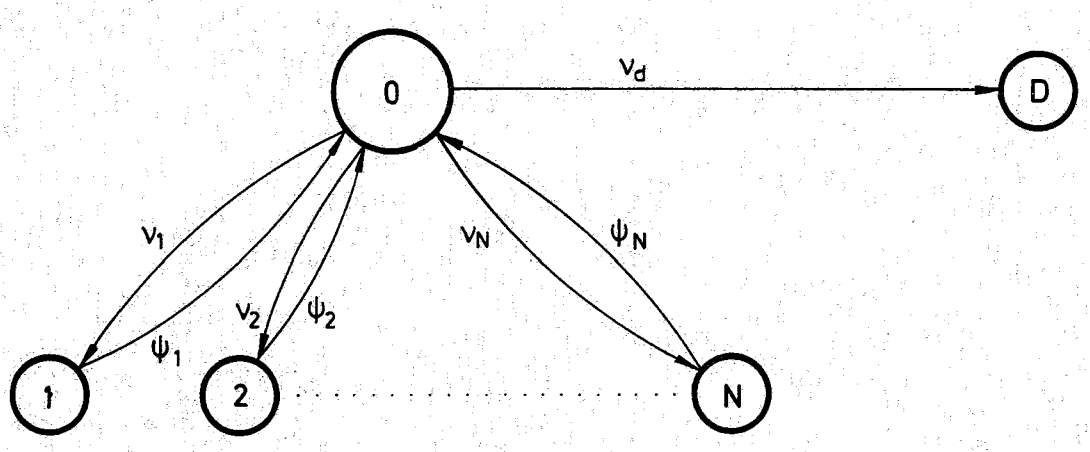

The partial annual loss "$Z_F$" as function of the failure rate "$\sigma_F$" of the power supply unit

Fig. 9




Maximum allowable reduction coefficient "$K_{max}$" as function of the failure rate $\lambda_F$ of the power supplies subsystem

Fig. 10



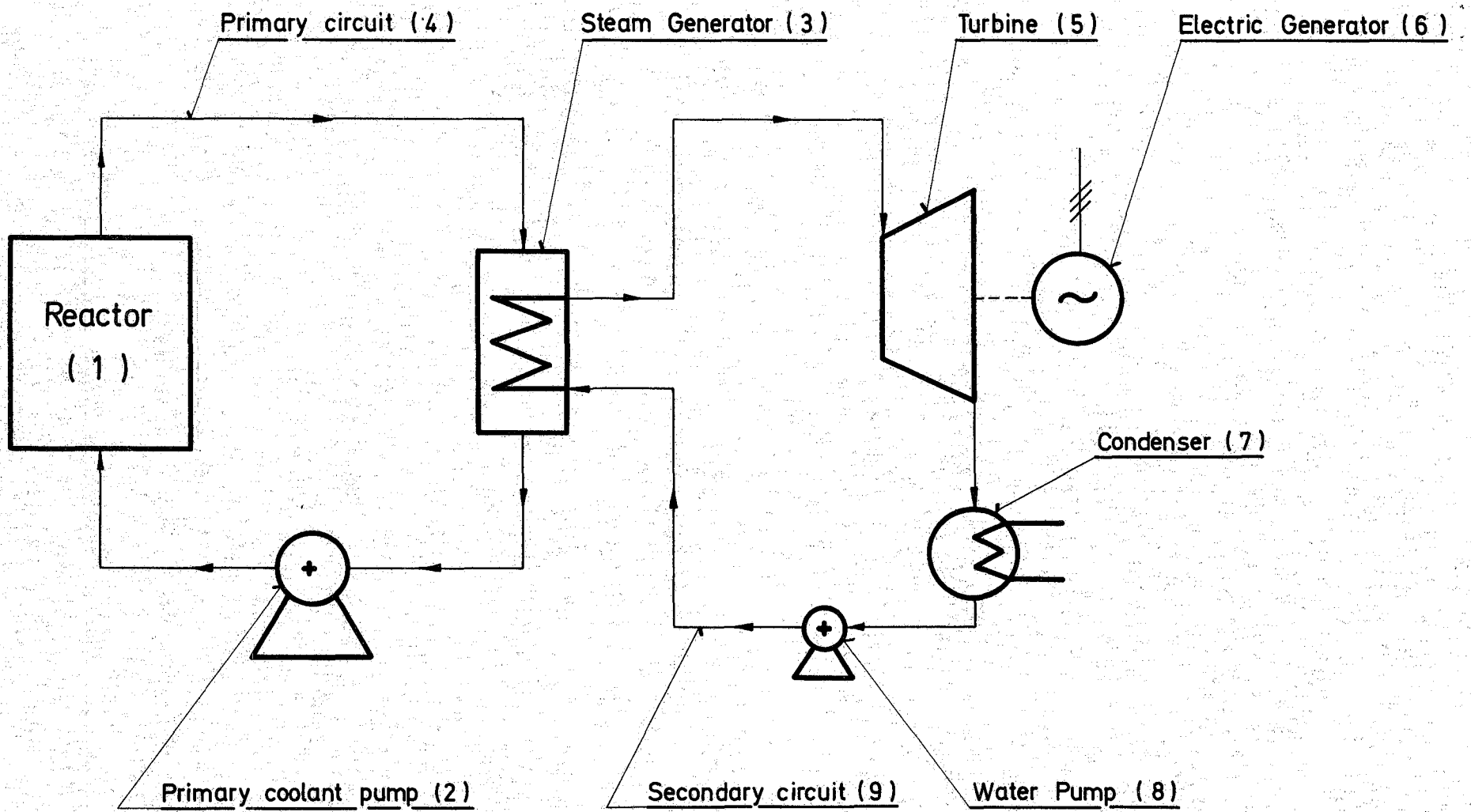

State "0" = Normal Operation

States "1" to "N" = Shut Down

State "D" = Disaster

Flow diagram of plant states

Fig. 11




Schematic diagram of the blocks of a nuclear power plant

Fig. 12

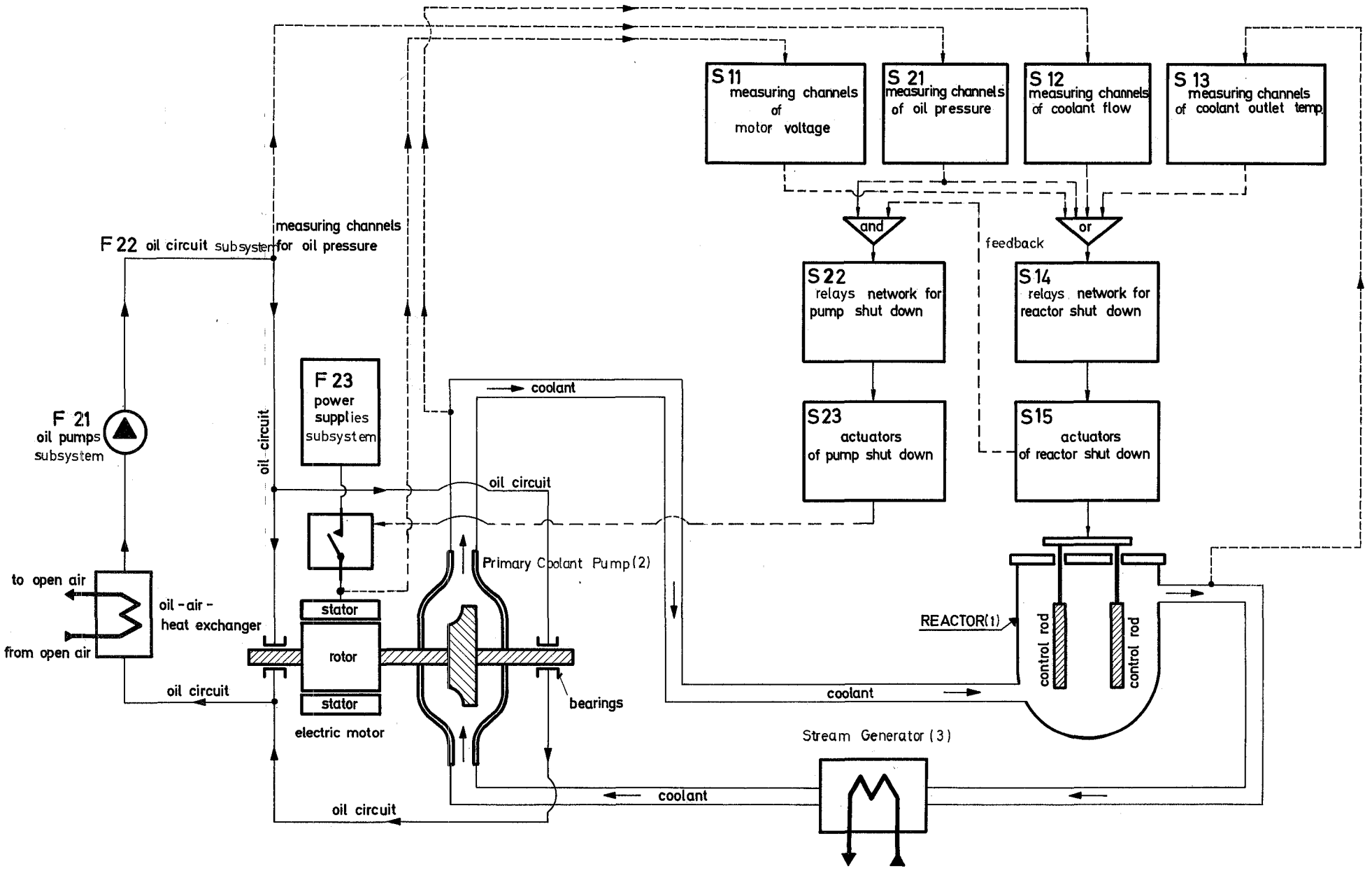
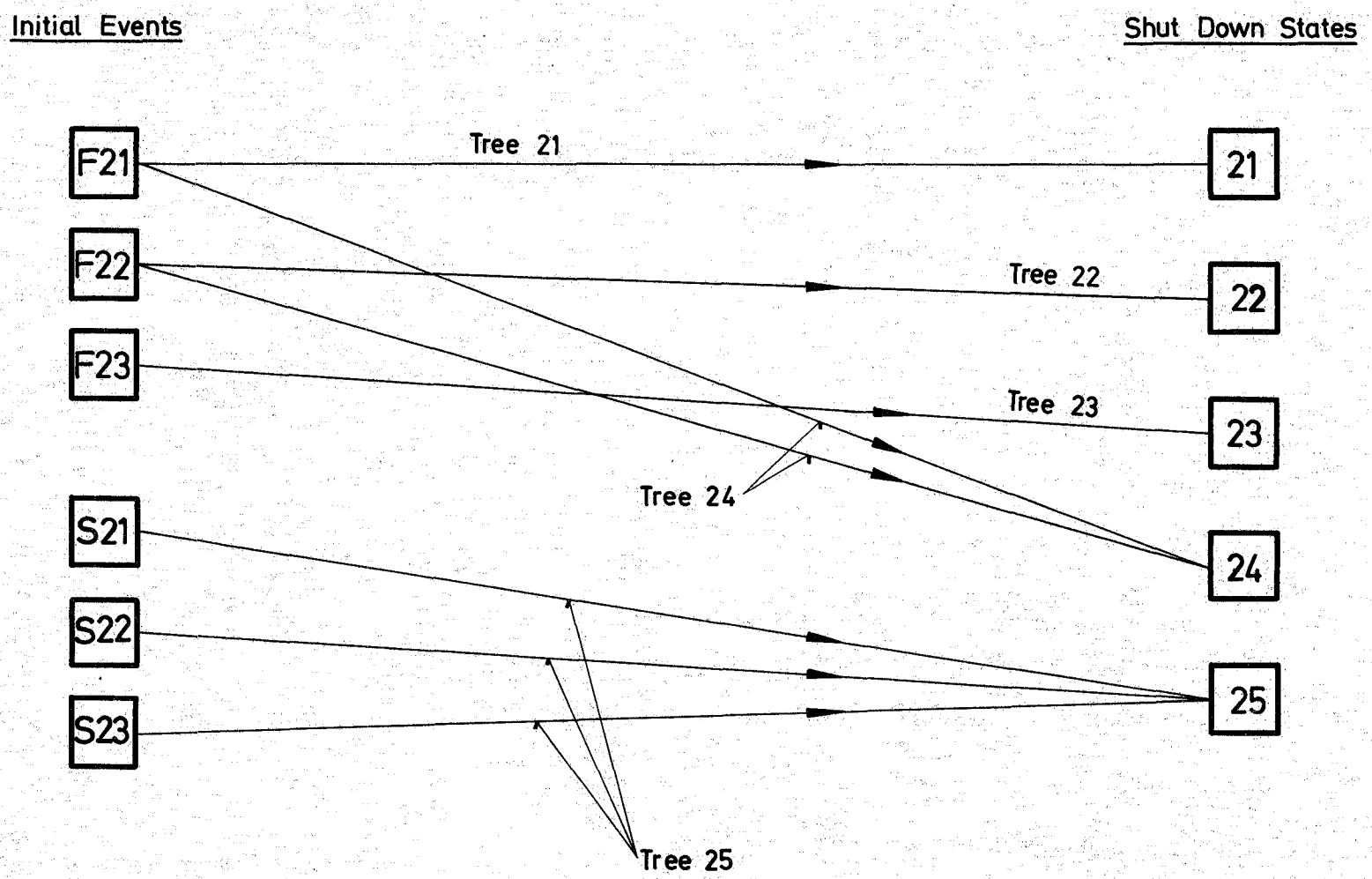



FIG. 13 Schematic diagram of the primary coolant circuit and of the primary coolant pump




Schematic diagram of the trees which link the initial events to the shut down states

Fig. 14

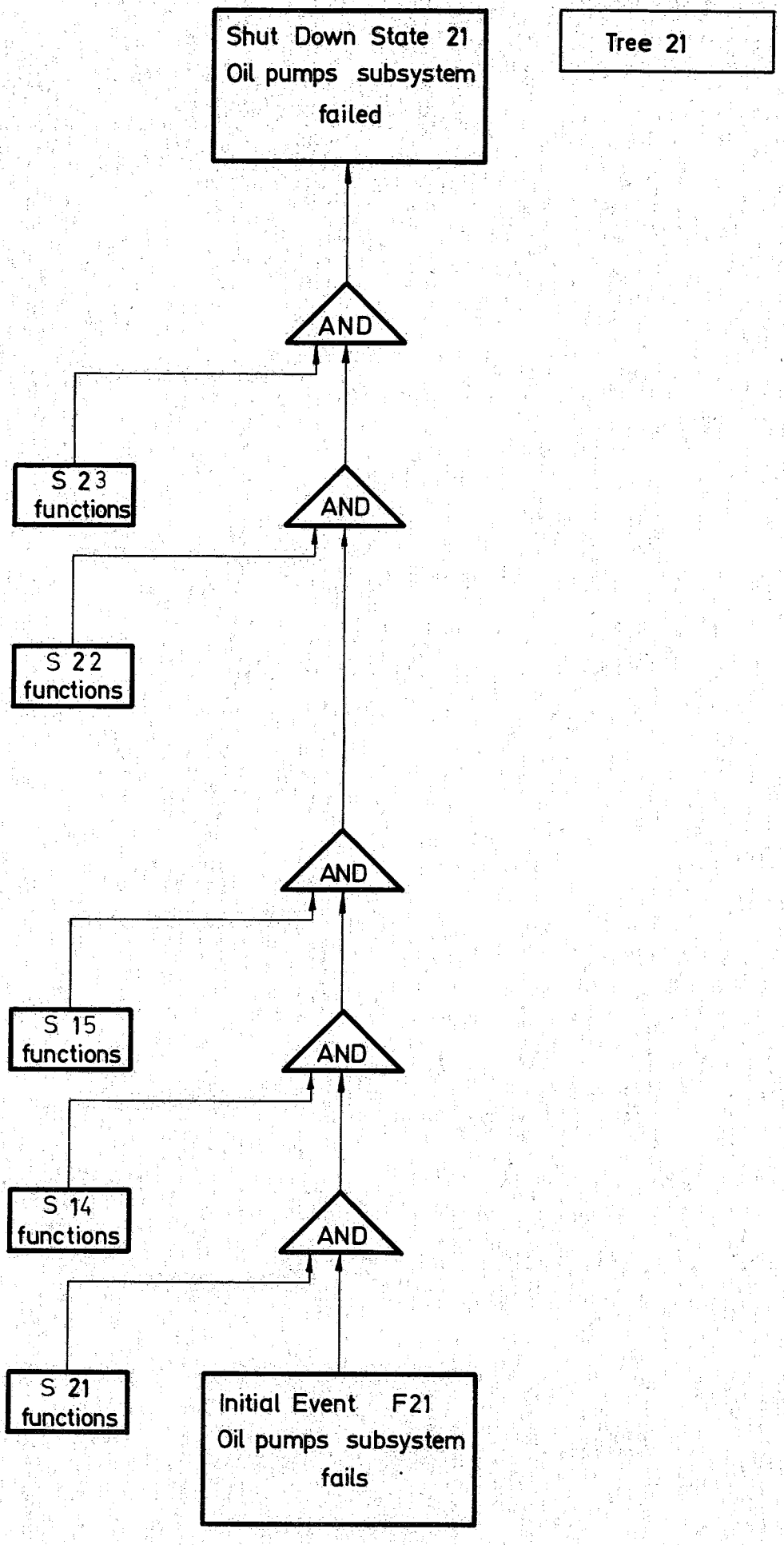

Shut Down State 21
Oil pumps subsystem
failed
Tree 21
AND
S 23
functions
AND
S 22
functions
AND
S 15
functions
AND
S 14
functions
AND
S 21
functions
Initial Event F21
Oil pumps subsystem
fails

Fig. 15

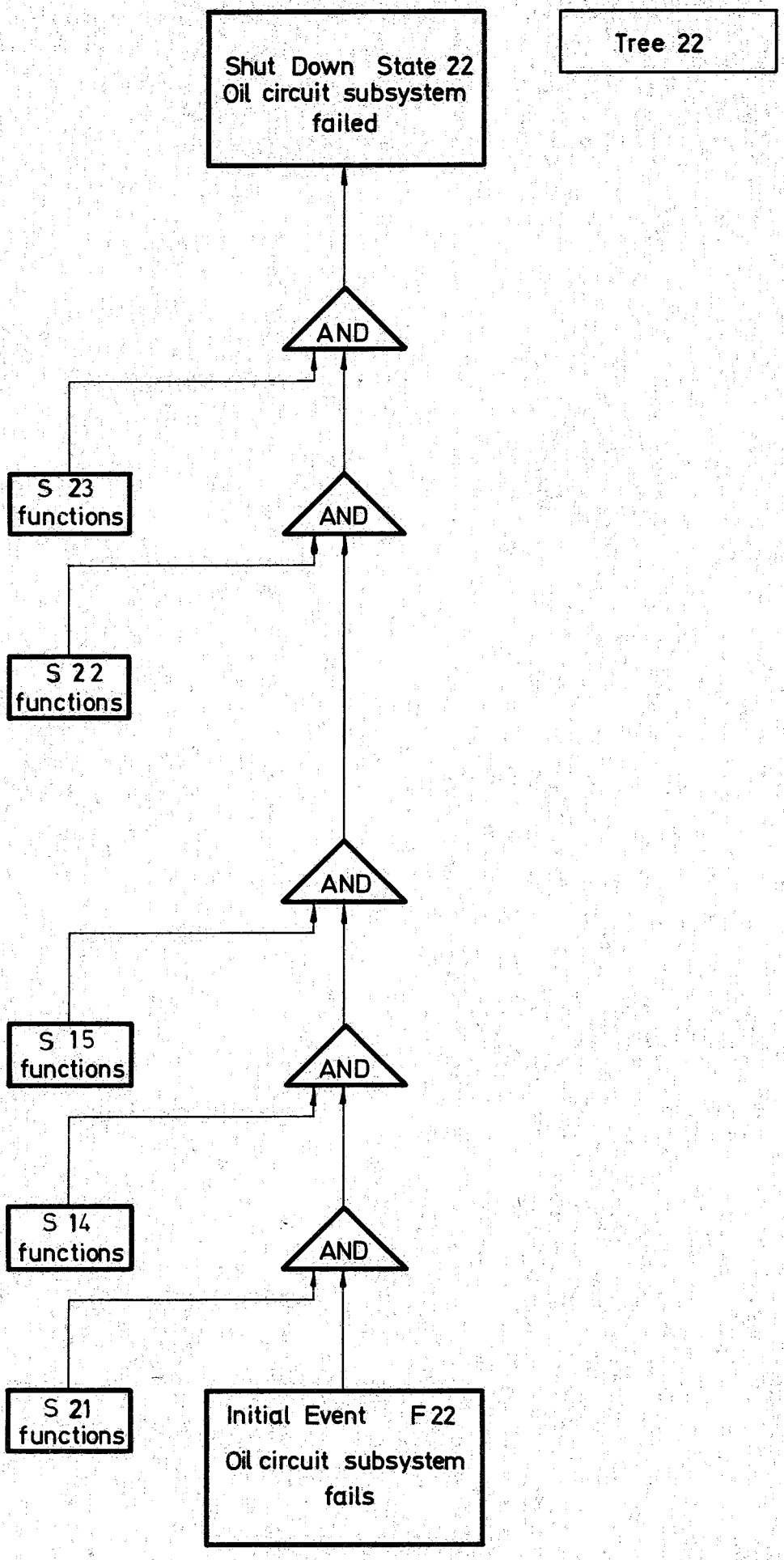

Tree 22
Shut Down State 22
Oil circuit subsystem
failed
AND
S 23
functions
AND
S 22
functions
AND
S 15
functions
AND
S 14
functions
AND
S 21
functions
Initial Event F 22
Oil circuit subsystem
fails

Fig. 16

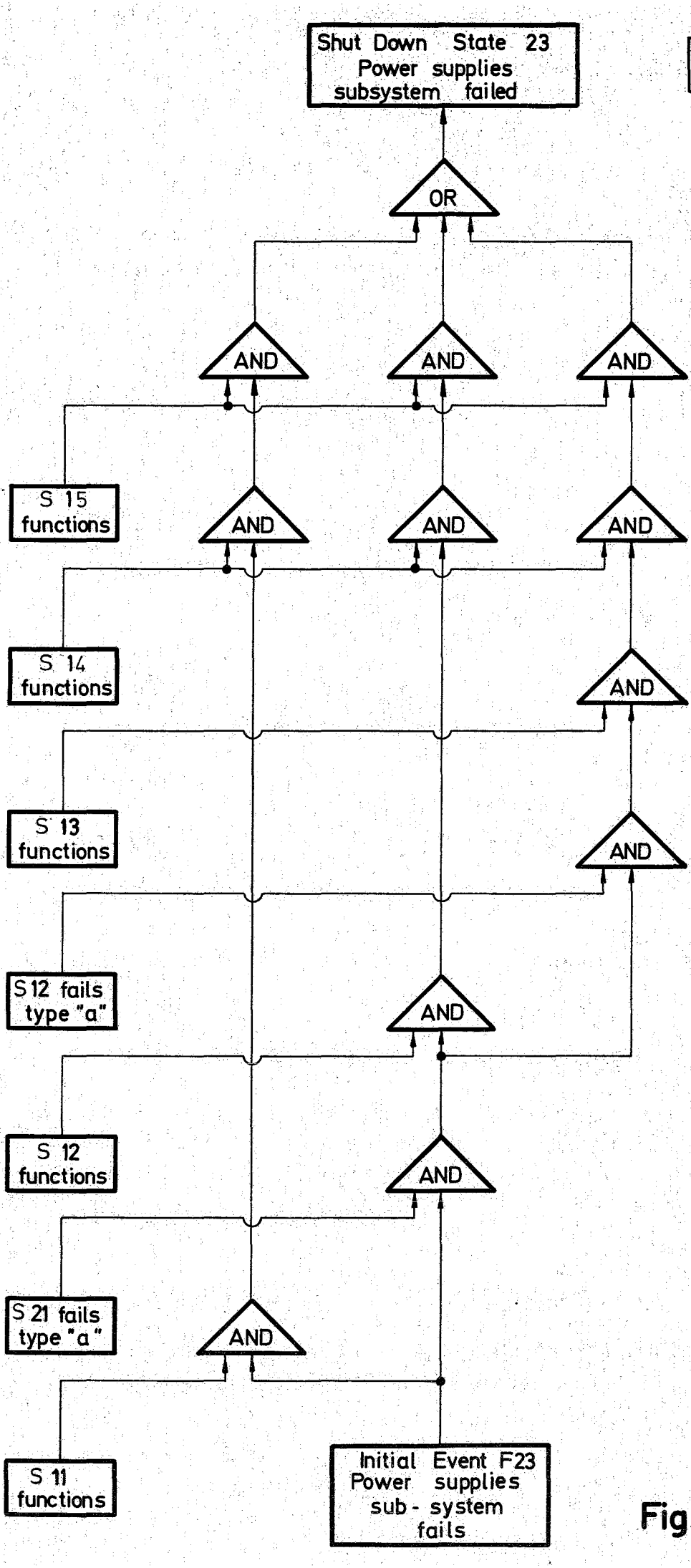

Shut Down State 23
Power supplies
subsystem failed
Tree 23
OR
AND
AND
AND
S 15
functions
AND
AND
AND
S 14
functions
AND
S 13
functions
AND
S12 fails
type "a"
AND
S 12
functions
AND
S 21 fails
type "a"
AND
S 11
functions
Initial Event F23
Power supplies
sub - system
fails

Fig. 17

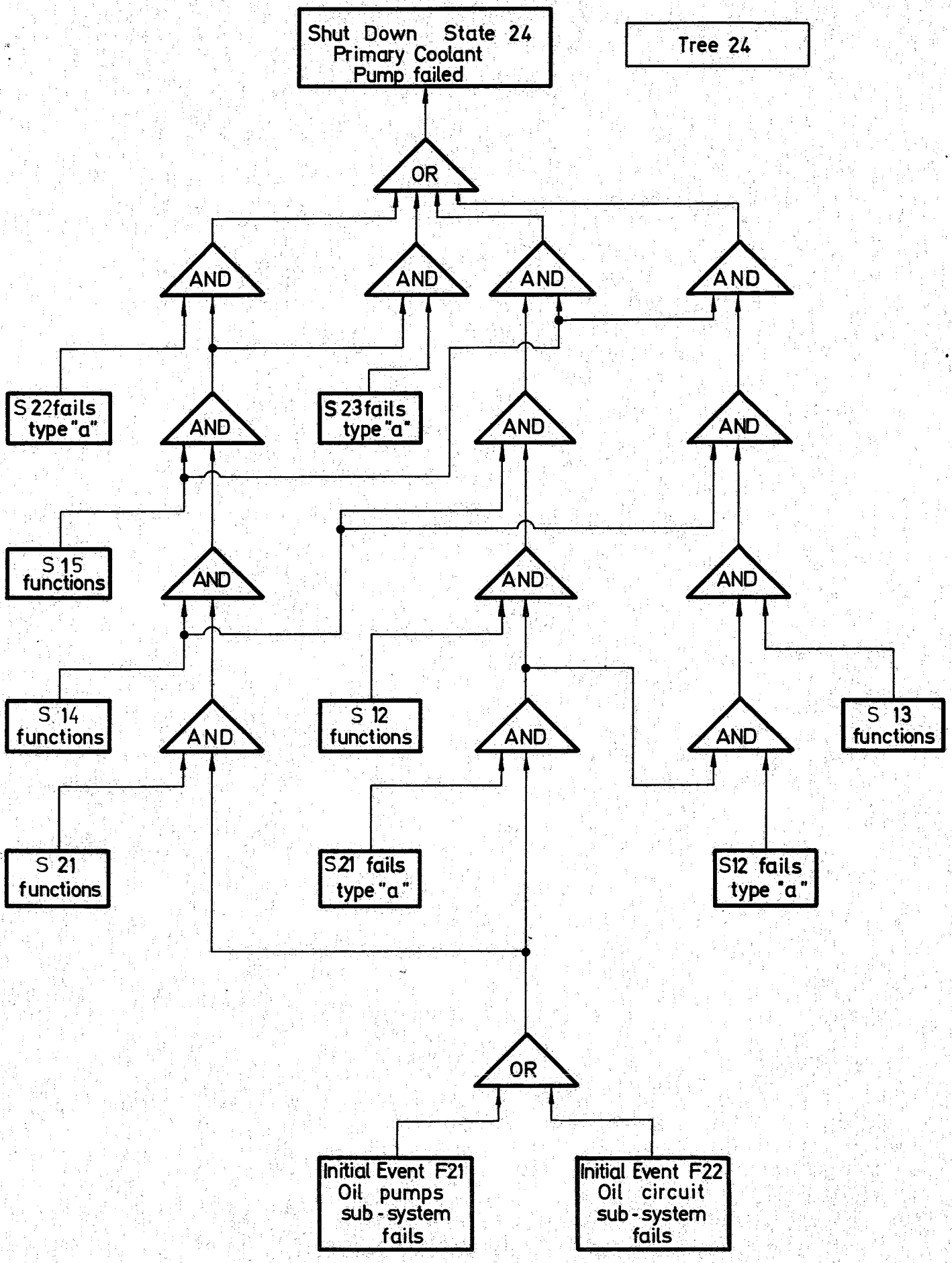
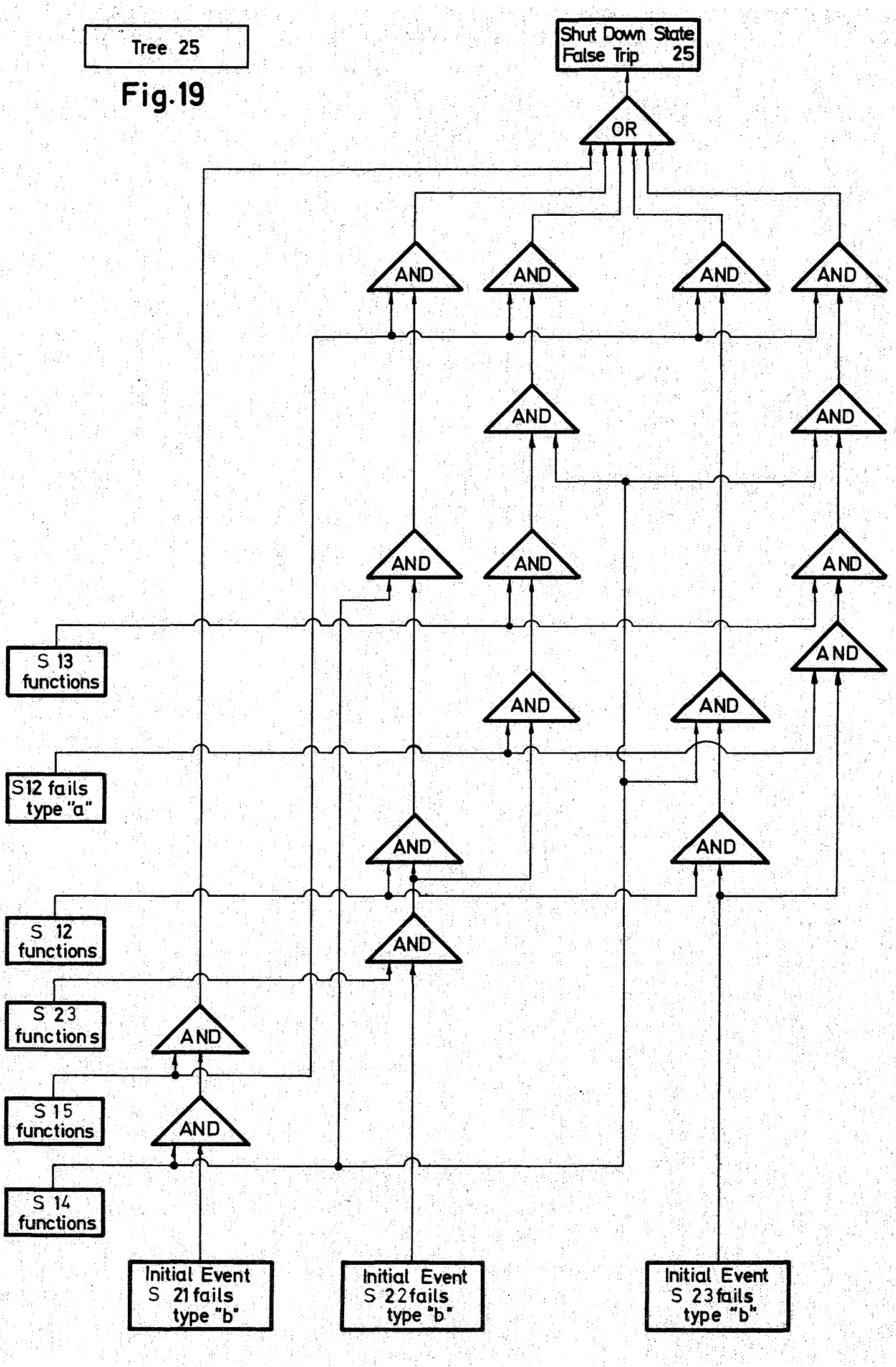

Shut Down State 24
Primary Coolant
Pump failed
Tree 24
OR
AND
AND
AND
AND
S 22 fails
type "a"
AND
S 23 fails
type "a"
AND
AND
S 15
functions
AND
AND
AND
S 14
functions
AND
S 12
functions
AND
AND
S 13
functions
S 21
functions
S 21 fails
type "a"
S 12 fails
type "a"
OR
Initial Event F21
Oil pumps
sub-system
fails
Initial Event F22
Oil circuit
sub-system
fails

Fig. 18

Tree 25

Fig.19



| Shut Down States with Minimal Paths \ Subsystems | | | F21 | F22 | F23 | S 21 | | S 22 | | S 23 | | S 11 | | S 12 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | type "a" | type "b" | type "a" | type "b" | type "a" | type "b" | type "a" | type "b" | type "a" | type "b" |
| 21 | Oil pumps subsystem failed | 211 | + | | | | | | | | | | | | |
| 22 | Oil circuit subsystem failed | 221 | | + | | | | | | | | | | | |
| 23 | Power supplies subsystem failed | 231 | | | + | | | | | | | | | | |
| | | 232 | | | + | | | | | | | + | | | |
| | | 233 | | | + | | | | | | | + | | + | |
| 24 | Primary coolant pump failed | 241 | + | | | | | + | | | | | | | |
| | | 242 | + | | | | | | | + | | | | | |
| | | 243 | + | | | + | | | | | | | | | |
| | | 244 | + | | | + | | | | | | | | + | |
| | | 245 | | + | | | | + | | | | | | | |
| | | 246 | | + | | | | | | + | | | | | |
| | | 247 | | + | | + | | | | | | | | | |
| | | 248 | | + | | + | | | | | | | | + | |
| 25 | False Trips | 251 | | | | | + | | | | | | | | |
| | | 252 | | | | | | | + | | | | | | |
| | | 253 | | | | | | | | | + | | | | |
| | | 254 | | | | | | | + | | | | | + | |
| | | 255 | | | | | | | | | + | | | + | |

Legend

Subsystem F21 = Oil Pumps

F22 = Oil Circuit

F23 = Power Supplies

S 21 = Oil Pressure Measuring Channels

S 22 = Pump Intermediate Relays Network

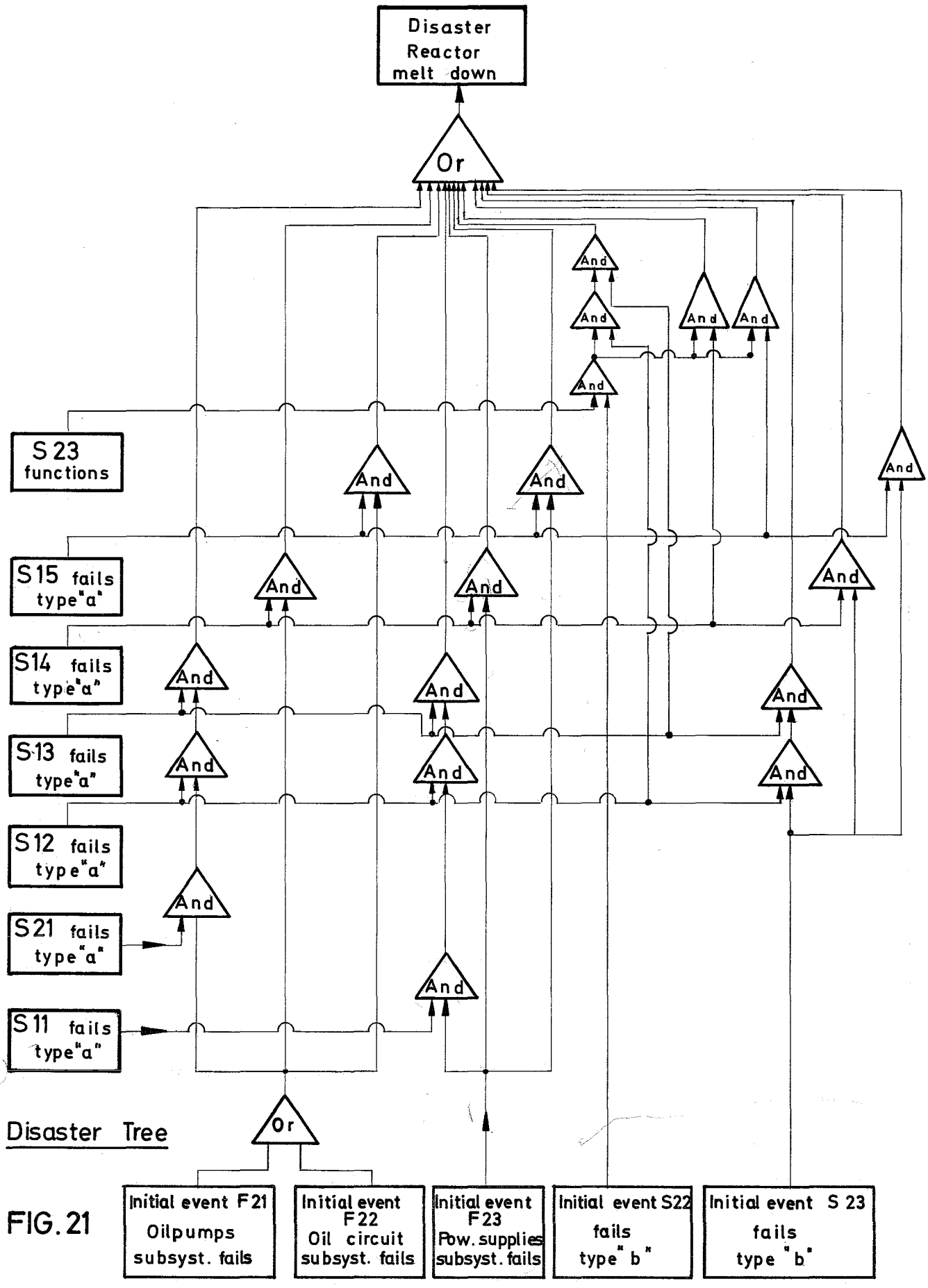
S 23 = Pump Actuators

S 11 = Motor Voltage Measuring Channels

S 12 = Coolant Flow Measuring Channels

**Minimal paths of the shut down states belonging to the block Nº 2**

**Fig. 20**



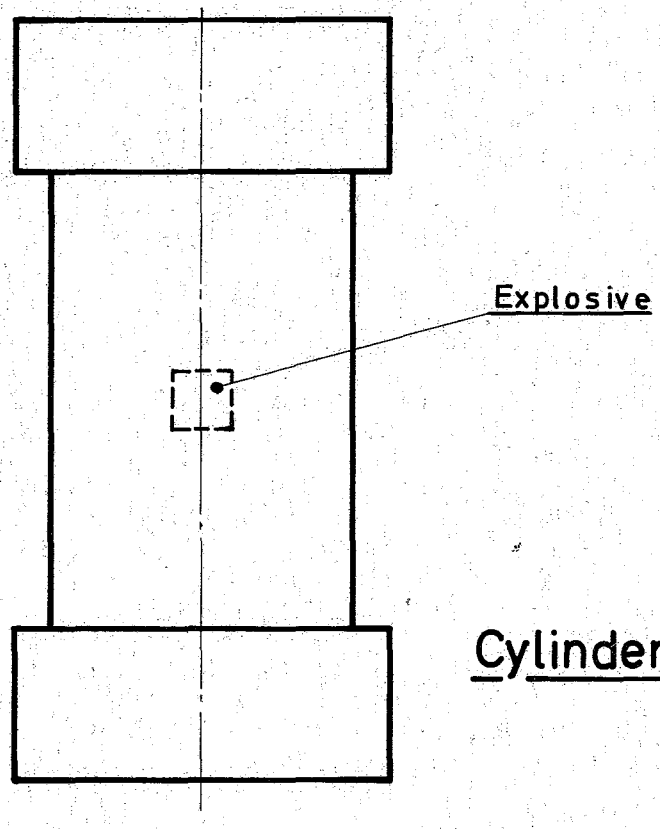

Disaster Tree

FIG. 21

| Subsystems / Minimal paths | F21 | F22 | F23 | S11 | | S12 | | S13 | | S21 | | S14 | | S22 | | S15 | | S23 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | "a" | "b" | "a" | "b" | "a" | "b" | "a" | "b" | "a" | "b" | "a" | "b" | "a" | "b" | "a" | "b" |
| d1 | + | | | | | | | | | | | + | | | | | | | |
| d2 | + | | | | | | | | | | | | | | | + | | | |
| d3 | + | | | | | + | | + | | + | | | | | | | | | |
| d4 | | + | | | | | | | | | | + | | | | | | | |
| d5 | | + | | | | | | | | | | | | | | + | | | |
| d6 | | + | | | | + | | + | | + | | | | | | | | | |
| d7 | | | + | | | | | | | | | + | | | | | | | |
| d8 | | | + | | | | | | | | | | | | | + | | | |
| d9 | | | + | + | | + | | + | | | | | | | | | | | |
| d10 | | | | | | | | | | | | | | + | | + | | | |
| d11 | | | | | | | | | | | | + | | + | | | | | |
| d12 | | | | + | | + | | | | | | | | + | | | | | |
| d13 | | | | | | | | | | | | | | | | + | | | + |
| d14 | | | | | | | | | | | | + | | | | | | | + |
| d15 | | | | + | | + | | | | | | | | | | | | | + |

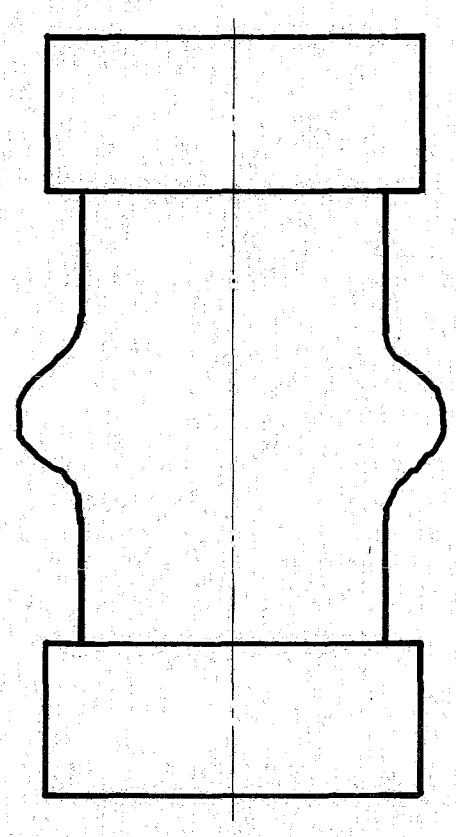
Minimal paths to the "disaster state"

Fig. 22




Cylinder before explosion

Fig. 23 A



Cylinder after explosion

Fig. 23 B

Fig. 23 Schematic reactor container

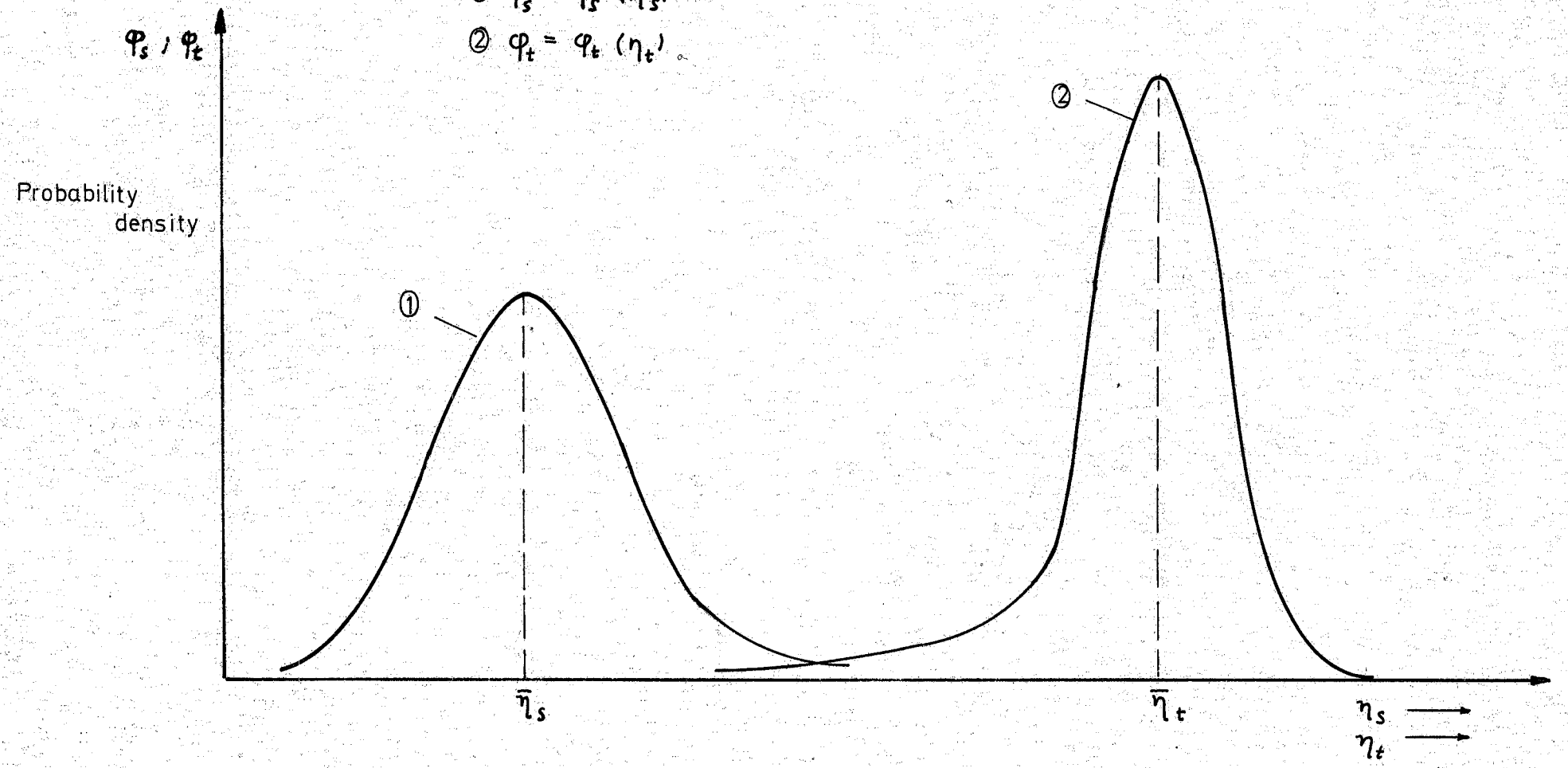



Fig.24 Stress and strength probability distributions

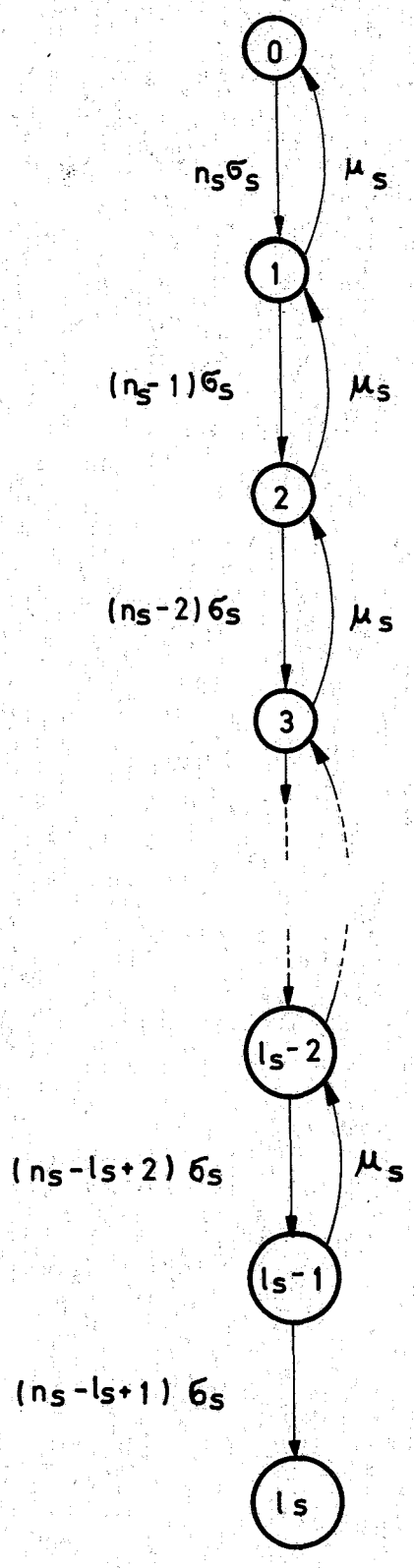



FIG. 25

Flow diagram of the states of a safety subsystem (failure type "b")

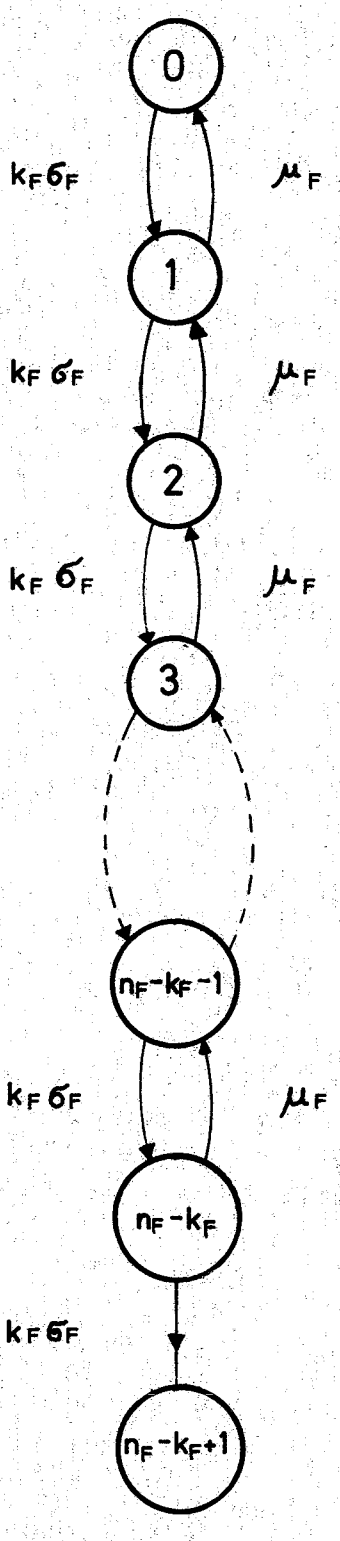
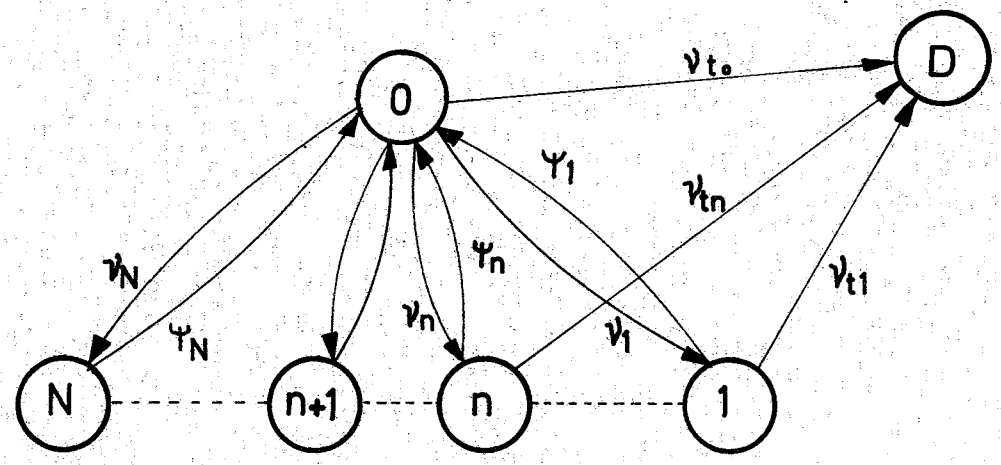



Fig. 26 Flow diagram of the states of a functional subsystem




| | |
|---|---|
| State 0 | = Normal Operation |
| States 1 to n | = Shut Down with possibility to go to the disaster state |
| States "n+1" to "N" | = Shut Down |
| State D | = Disaster |

Fig. 27 Flow diagram of plant states