CSNI Report No. 23

OECD

NEA

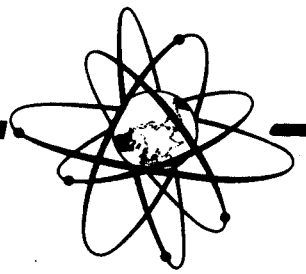
MEETING OF A

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

CEN Saclay, 5-7 September 1977

Organised in collaboration with the
Département de Sûreté Nucléaire of the French
Commissariat à l'Énergie Atomique and the
Safety and Reliability Directorate of the
United Kingdom Atomic Energy Authority

PROCEEDINGS



COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY
38, boulevard Suchet, F-75016 Paris, France

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

PROCEEDINGS+

Meeting of a

TASK FORCE ON PROBLEMS OF RARE EVENTS

IN THE RELIABILITY ANALYSIS OF

NUCLEAR POWER PLANTS

CEN Saclay, 5th-7th September 1977

Meeting organised in collaboration with the Département de Sûreté Nucléaire, Saclay and the Safety and Reliability Directorate of the United Kingdom Atomic Energy Authority under the General Chairmanship of Mr. A. Eric Green, National Centre of Systems Reliability, UKAEA, Culcheth, Warrington, WA3 4NE, United Kingdom

Nuclear Safety Division
OECD Nuclear Energy Agency
38 boulevard Suchet
F-75016 Paris
France

+ A summary report on the work of the Task Force and on the conclusions and recommendations will be issued as document SEN/SIN(77)20.

CONTENTS

INTRODUCTION

In safety problems of nuclear plants interest centres on various types of rare events. These may extend from rare modes of failures in the component parts of the system and plant, the simultaneous occurrence of a very low resistance of a structural member and an extremely high load, to rare catastrophic failures which affect whole plant and system complexes. There is an obvious need to understand the patterns of behaviour of these events and be able to make some adequate estimate of their probability of occurrence.

Following a recommendation of the CSNI Specialist Meeting on the Development and Application of Reliability Techniques to Nuclear Plant held in Liverpool in April 1974, the NEA Committee on the Safety of Nuclear Installations decided in November 1975 to set up a Task Force on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants, the main objective being to explore methods for giving a quantified probabilistic statement on problems of reliability analysis involving rare events. CSNI decided that the Task Force would be composed of a small number of leading experts, selected only for their widely recognized scientific competence and their ability to contribute significantly to the work of the Group. A small meeting of specialists in statistical analysis of rare events, of engineers who specialize in the reliability analysis of automatic protective systems, and of engineers who specialize in the reliability analysis of structures (such as pressure vessels and containments) was considered an appropriate means to

stimulate and intensify the discussion between the experts in the three fields. The particular subjects covered by the invited experts - who would normally be working in specialised fields - included, specifically, statistical modelling of rare events, decision theory applied to rare events, small sampling theory in the case of rare events. Man-made phenomena as well as natural phenomena were to be considered, as they involve different approaches to modelling.

A first Meeting of the Task Force was held at JRC Ispra from 8th to 10th June 1976 (CSNI Report No. 10). The concept of the Task Force and its working provided an excellent vehicle for technical expression and exchange of views in a highly specialized field. The conclusions and recommendations of the Meeting were summarized in document SEN/SIN(76)19, and a programme of action was recommended to CSNI.

To further the state-of-the-art, CSNI decided at its October 1976 Meeting to set up, for a period of two years (1977-1978), a small Research Group on Rare Events. This Group, composed of experts with wide responsibilities for appropriate research programmes, was to investigate and organise the programme of work based on the findings of the Task Force in the following areas:

- rare event data collection and analysis;
- common-mode failure analysis;
- human error analysis and quantification;
- statistics and decision theories applicable to rare events;
- interdisciplinary communication and tutorial programmes on rare events problems and their solution.

CSNI decided that appropriate small meetings of experts would be organised by the CSNI Secretariat in liaison with the Research Group on Rare Events during the next two years (1977-1978) with the aim of preparing an integrated report on the programme of work based on the findings of the Task Force, an interim progress report being presented to CSNI at its next Meeting (to be held in November 1977). After completion of the integrated report, the Task Force would be reconvened to evaluate the findings of the report and to advise the Committee.

CSNI asked the Research Group to put emphasis on the first three areas identified by the Task Force and to concentrate at first, during 1977, on protective systems for nuclear reactors, if possible on specific designs. The Committee also stressed that the Research Group should seek to make significant progress within a year, so as to be able to present some practical results at the next CSNI Meeting.

The Research Group met at the Château de la Muette, Paris on 10th December 1976 and on 18th May 1977; a third (informal) Meeting was held at Gatlinburg, Tennessee, USA on 24th June 1977. The Group shared out the work approved by CSNI among small groups of experts, which were put under the direct control of a member of the Research Group. The basic plan was that each small group of experts would have its generic programme of development until the second Meeting of the Task Force but would also cater for issues being brought up by other groups. In order to ensure orderly and fast progress, information was exchanged continuously and rapidly between the groups, under the control of the Research Group and with the assistance of the CSNI Secretariat.

CSNI had not decided on a definition of protective systems on which the Research Group should concentrate at first (during 1977). Considering the short time available before the next Meeting of CSNI and the necessity to arrive at practical, usable results, the Group decided to select the emergency shutdown system and welcomed a French offer to assess in one of the small groups of experts the actual protective system for automatically shutting down the Fessenheim pressurized-water reactor.

One of the main advantages of the Meeting of the Task Force in June 1976 had been to bring together automatic protective systems engineers, structural engineers, and statisticians. This fruitful multidisciplinary collaboration was somewhat weakened during 1977 because of the requirement to concentrate on protective systems. In order to maintain multidisciplinary communication, and to prepare future work of the Task Force, the Research Group agreed that a paper on "the interaction of systems and structural reliability with respect to rare events" should be prepared for the Task Force Meeting.

The second Meeting of the Task Force was held at CEN Saclay from 5th to 7th September 1977. The proceedings of the Meeting are published in this report; they were approved by the Research Group on Rare Events during its fourth Meeting, held on 8th September.

CSNI Secretariat

PRESENTATION AND DISCUSSION OF THE PAPERS PREPARED BY THE SMALL GROUPS OF EXPERTS

Presentation of the Task Force and Research Group

A.E. Green

Mr A.E. Green, the Task Force general chairman, in his introductory remarks made reference to the request from CSNI to study the problems of rare events in the reliability analysis of nuclear power plants on a quantitative probabilistic basis. The first meeting of the Task Force at Ispra in June 1976 (ref. CSNI report No.10) had identified that techniques for the quantification of rare events were not available, and from that meeting a programme of work had been recommended and accepted by CSNI. In particular, CSNI required that work should concentrate on studies related to automatic protective systems for nuclear reactors, and it was organised under a research group comprised of a limited number of Task Force members which controlled the work of six research sub-groups. These were :

1. Fessenheim Reactor Assessment
   Chairwoman - Mrs A. Carnino
2. Data Collection and Analysis
   Chairman - Mr G. Volta
3. Common Mode Failure Analysis
   Chairman - Mr A.J. Bourne
4. Human Error Analysis and Quantification
   Chairman - Mr J. Rasmussen
5. Statistics and Decision Theory
   Chairman - Mr G. Morlat
6. Interdisciplinary Communication Techniques
   Chairman - Mr E. Hofer

Referring to the outline programme Mr Green stated that the objective on the first day of this meeting was to obtain reports of their work from each of the sub-group chairmen, and to obtain necessary clarification of any points for other members, prior to more detailed discussion on the second day.

Presentation of the Fessenheim I Reactor

B. Gachot

To acquaint Task Force members with the Fessenheim I reactor, they were given copies of EDF brochures (SINDOC(77)127) describing the various systems comprising the plant and its major parameters. Mr. Gachot referred to this in his presentation.

The Fessenheim I reactor is a PWR based on the US plant at Beaver Valley. The decision to build the station was made in September, 1970 by EDF and construction on unit 1 started in November, 1971. Completion was scheduled for 1976, but due to various problems there has been a two years delay.

Discussion

In reply to Mr Vesely's question, Mr Gachot stated that there are separate diesel-generators and electrical buses for emergency power supplies to the two reactors and their associated systems. For each reactor, the diesel generators are common to the ECCS and other auxiliary systems. There is a common building for all electrical auxiliary systems and a common turbine hall for the two turbines. The auxiliary Feedwater System consists of 2 motor and one turbine driven pump.

Mr Stadie and Mr Hums enquired about the possibility of site flooding from the local waterways due to failure of the cooling water dam. In reply Mr Gachot stated that there would only be an initial wave with no continuous hazard, and the plant was safe against this.

Mr Green asked about seismic protection of the plant, and about sensors for detecting these conditions, to which Mr Gachot replied that such considerations were included in the plant design and sensors are available. These are not connected to the automatic protective system, and it would not be expected that the plant would be manually shutdown if it was seen to be still operating normally. Mr Hums had considered that manual shutdown might be an appropriate precautionary action.

The question was raised by several members as to what sizes of primary circuit leaks would require particular actions. To indicate the order of magnitude

Mr Gachot stated that a leak up to approximately 1/2 inch diameter could be tolerated and operation would continue. For a leak larger than 1/2 inch, automatic protection systems would shut down the plant and initiate safety inspection.

Mr Green asked about what would happen in the case of a loss of protection to the electrical grid system. Mr Gachot replied that the reactor power would be reduced so that auxiliary systems would continue to operate (îlotage). As for the complete loss of external electric sources, this event has a duration which is generally less than one minute and rarely greater than half an hour.

SINDOC(77)128

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

WORKING GROUP OF EXPERTS ON THE RELIABILITY ASSESSMENT OF THE PROTECTIVE SYSTEM OF THE FESSENHEIM - REACTOR

Presented by R. Quenée

I - GENERALITIES

The work presented here was done within the framework of a general study on the effect of rare events on the nuclear power plant safety, study initiated by the "Committee for the Safety of Nuclear Installations" (CSIN).

This work has been carried through owing to a very active participation of the competent departments of the "Commissariat à l'Energie Atomique", "Electricité de France" and Framatome. Working in good agreement with other groups made our task very much easier.

The aim of this first study, presented by our group, is to show how important is the impact of some rare events on the results obtained. It brings to light how necessary are the common efforts to achieve a more accurate and meaningful estimation.

Keeping in mind the width of the problem, the time granted and the means at its disposal, our group could only take into account one part of the reactor protection system. We think that the part studied is very representative of the problem and shows the difficulties still to be overcome.

In the future, a better approach will be possible when the answers will be obtained from our questions to the other groups. Extremely interesting information has already reached us (test optimization, suggestions concerning the computing methods). We are not going to develop these subjects further since they will be presented in the reports of the corresponding groups.

.../...

II - PRESENTATION OF THE STUDY

II.1 - Introduction and definitions

From a safety point of view, the main function of a nuclear plant protection system is to reduce to an acceptable value the probability and consequences of dangerous events on the working staff and the environment.

Among the different systems ensuring the protective function, one of the most important systems is the emergency shutdown one whose role is to stop as fast as possible the nuclear reaction in the case of events requiring a reactor scram.

The limitations of the system are often debated (mainly for financial reasons, considering the exceptional quality required from the equipment) and may vary from one country to the other.

In order to eliminate any ambiguity and only for the understanding of the study, we shall give :

- a definition of the scram function
- the limitations of the system ensuring this function.

Function and limitations of the scram system

The function of the scram system is to produce automatically or manually a fast decrease of power in the reactor when the integrity of the radioelements containment barriers is threatened.

The emergency shutdown system consists of :

- sensors monitoring the evolution of the physical parameters representative of the normal or abnormal state of the reactor ;

.../...

- equipments transforming the signals given by the sensors in to measurable electrical currents (amplifiers,... etc) ;

- comparators actuating a signal when the physical parameters measured exceed a set value considered as dangerous (threshold triggers) ;

- logic circuits grouping and processing the signals from the comparators and giving the scram signal ;

- equipments called "high power components" (in opposition to the preceeding ones called "low or medium power") which, from the scram signal, directly actuate the mechanical equipments shutting the reactor ;

- control rods (chesters)

In addition, must also be considered as integral part of the system :

- the test equipments for checking the good functioning of the system ;
- the instructions defining a test and maintenance policy for the system (see example in appendix II) ;

- the signalling.

Nota : When devices or instructions are likely to interface with the scram function, although they are not directly involved with this function, those devices or instructions are considered as a part of the scram system.

Initiating event and accident sequence

An initiating event is any event, which is at the origin of an accident sequence that may degenerate such as to have dangerous consequences. These accident sequences are the subject of thorough studies which aim at evaluate the corresponding risks.

.../...

II.2 - Limits of the study

Numerous studies of accident sequences are carried out by constructors, utilities and safety organisations (see list in appendix). Among these studies, the one which seems to us the most interesting concerns a spurious withdrawal of the control rods, while the reactor is on power and the reactivity insertion rate is high (11).

Initiating events of this sequence beginning may be (non restrictive list) :

- failure of periodic actuators,
- failure of relays
- failure of regulation
- human error.

These events may jeopardize to the first barrier integrity (cladding rupture).

The beginning of the sequence is detected by neutron flux and temperature measurements. The scram system is then actuated.

Two trends of study have been carried out in parallel :

- more thorough study of the accident sequence itself (negative reactivity insertion rate reduced and fuel burn up) ;

- calculations of the scram system reliability.

The calculations presented in this report, do not take into account the last results of the first action, since the two studies were carried out simultaneously.

The control rod drive mechanisms are being studied but numerical values of reliability will not be available before one year. As the computing methods are now well developed, it will be easy in the future to take into account the information from the other working groups.

.../...

We have excluded from the study the effects of external phenomena (earthquakes...) and sabotage, as defined in the program determined by the Research Group of the CSNI.

III - STUDY OF THE ACCIDENT SEQUENCE

III.1 - Description of the sequence

The spurious withdrawal of the control rods on power results in an increase of the thermal flux in the core. Until the opening of the discharge valves or the safety valves of the secondary circuit, the heat removal in the steam generators increases less quickly than the power generated in the primary circuit. The result is an increase of the primary circuit temperature.

If it is not stopped manually or automatically by an emergency shutdown, accident studies show that a boiling crisis could occur. The reactor emergency shutdown system which must intervene is designed to inhibit this boiling by maintaining the DNBR (Departure from Nucleate Boiling Ratio : ratio which gives the rate of thermal exchange between the fuel, the cladding and the coolant) above 1.3. Thus the risk of damaging the fuel rods and initiating a clad ruptureis avoided.

III.2 - Simulations of the sequence

The aim of these simulations is to check the functional redundancy of the protection channels affected by the accident (High nuclear flux, ΔT temperature and ΔT power channels). That is to say that the last scram actuation must allow the protection criterion to be satisfied. We saw that, in this case, the criterion is the DNBR which must be above 1.3.

From these simulations one can determine :

- the times of emergency shutdown for each channel,

.../...

- the maximum duration of emergency shutdown beyond which the DNBR would reach a value smaller than 1.3.

- the dynamic evolution of the main parameters of the reactor (temperatures, flux, pressure...) and of the protective channels (operating rules, measurements...).

III.3 - Choice of the parameters

It is interesting to study in detail the reactor control rods withdrawal on power, since two parameters at least have an effect on the dynamics of the phenomena. These are the reactivity insertion velocity (related to the control rod withdrawal velocity) and the state of the reactivity feedback (Doppler effect and moderator coefficient).

A study of the rod withdrawal on power in several conditions has been performed by Electricité de France. Ref. (1), (5), (6), (7).

The following table sums up the different situations in which these simulations have been made :

Reactivity insertion velocity pcm/s / Reactivity feedback	0,5	2,5	25	80
Minimum : moderator coefficient = zéro beginning of life) Doppler coefficient minimum in absolute value	X	X		X
Maximum : moderator coefficient = - 43 pcm/kg/m^3 (end of life) Doppler coefficient maximum in absolute value		X	X	X

.../...

The reactivity insertion velocities of 0.5 and 80 pcm/s are extreme values which can be anticipated because of the mechanism capabilities.

The velocities of 2,5 pcm/s (mini) and 25 pcm/s (maxi) correspond to an almost simultaneous detection of the accident by the different physical measurements (φ - T).

III.4 - Conditions and assumptions of the simulations

The simulations have been carried out in the general conditions of the accident studies, a characteristic of which is to take into account the measurement errors (it is a conservative assumption). In our case, they were :

Power :..... + 2 %
Mean temperature :..... + 36 ° F
Pressure :..... - 2,1 bars

These errors involve a maximal margin for the DNBR.

Other assumptions :

- the reactor emergency shutdown for high nuclear flux is actuated at the pessimistic value of 118 % of nominal power,

- the emergency shutdown for ΔT temperature and ΔT power takes into account the maximal errors of measurement and calibration,

- the value chosen for the negative reactivity insertion during the emergency shutdown is based on the assumption that the most effective rod is stuck in a high position.

.../...

In our case, all these simulations have been carried through until the intervention of the ultimate emergency shutdown actuation for high flux, ΔT temperature and ΔT power.

III.5 - Results and conclusions

The main results of the study are given in table 1 (figure 1) [5] .

It is to be noted that the accident is detected in all cases which can be anticipated. The functional redundancy evolves with the configuration. It is considerable for high insertion velocity and for a depleted fuel.

IV - DESCRIPTION OF THE SCRAM SYSTEM

IV.1 - Principle

Within the framework of this study, the problem is to avoid exceeding a temperature and pressure in the primary coolant leading to a nucleate boiling in the core hottest parts. The phenomenon is not directly observable, therefore a set of measurement channels giving accessible values has been designed in order to prevent the phenominon.

IV.2 - General structure

The structure adopted is a compromise between requirements of safety and those of functioningcontinuity. This compromise is worked out by a combination of redundancies (safety) and majority of vote systems (continuity of operation).

The protective system structure is schematically described on Figure 2. Upstream is the measurement system S.I.P. which processes the analog signals from the measurement sensors (pressure, flux, temperatures...). In the centre is the relay system R.P.R., consisting of majority of vote elements providing the emergency shutdown order. The interface between S.I.P. and R.P.R. consists of threshold relays which convert the analog signals to logical signals 1 or 0.

.../...

The R.P.R. consists of two identical logical trains in parallel.

Downstream the R.P.R. is the system which actuates the emergency shutdown orders. It is composed of two circuit-breakers in series. If only one of the circuit-breakers receives an opening order, the power to the control rod drive mechanism is switched. The control rods then fall by gravity.

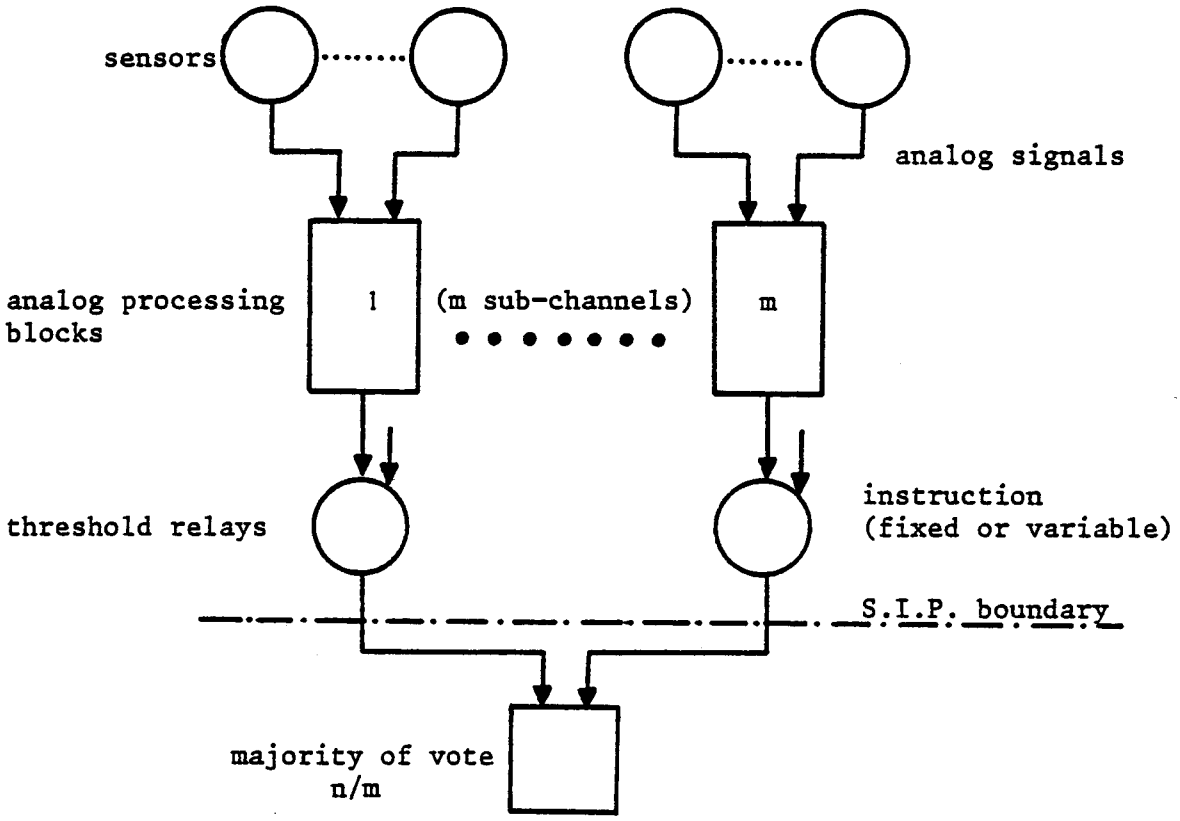
IV.3 - S.I.P. struture

The S.I.P. structure is fairly logically deduced from its functions. The S.I.P. consists of a number of channels, each of which has a particular protective role. There are 27 channels. We do not include the manual emergency shutdown since it intervenes directly on the logical systems. The list of these channels is given in table 2 (figure 3). The channels that will be taken into account in this study are numbered 9, 11, 12.

Nearly all these channels can be further divided into 2,3 or 4 identical sub-channels in parallel. thence, an equipment redundancy has been built up. For an emergency shutdown to be actuated by a channel, it is then necessary that a majority of vote (1/2, 2/3, 2/4) of subch nnels should order it.

The channels structure can be represented by the following diagram :

.../...



The sensors, which deliver the analog signals processed by an analog processing block are in direct contact to the primary circuit. The output value of this processing block is compared to a set-signal in a threshold relay whose output is binary. To illustrate this, Figure 4 shows one of the 3 redundant sub-channels of the emergency shutdown channels by ΔT temperature and ΔT power.

Generally speaking, each sub-channel is part of a protective group and is therefore physically and electrically separated from the other sub-channels. In particular, the sub-channels of a same channel have independent power supplies ; in the same way, the sensors are specific to each of them. On the contrary, there can be, inside the same protective group, sensors or items common to sub-channels of distinct channels. As a significant example of this, are the ΔT temperature and ΔT power channels, where the temperature sensors are common for each sub-channel (Figure 4) of a same protective group. We will see later on that the existence of these common points has a great importance.

.../...

We can also note the presence of measurement output plugs and of test signal input plugs. These devices allow the periodical testing of the channels.

IV.4 - R.P.R. structure

Figure n° 5 gives a more detailed diagram of the relay set (RPR) following the analog part (SIP).

Each logical signal from the SIP (3 signals high ΔT temperature in the figure example) reaches two relays belonging respectively to trains A and B. It is important to point out that the emergency shutdown signal corresponds to a general lack of power of the whole RPR relay set.

The relay contacts cited above are organized into matrices which form the majority of vote elements (2/3 in the case of the example).

Each matrix is followed by "matrix repeater " relays. The repeater relays of the different matri es corresponding to the various emergency shutdown actuations have contacts connected in series to finally supply the circuit-breakers coils. These circuit-breakers trip the scram by switching off the electrical supply to the electromagnets which maintain the control rods in high position.

There is a test device for all these relays. This device is not shown in order to not overload the figure. It is not involved in the study since the possible failures lead to an undesired shutdown order, but never to an inhibition of the system. For the same reasons, the relays supplies are not taken into account.

.../...

IV.5 - Executor system structure

It consists of two circuit-breakers whose coils are fed respectively by trains A and B and the contacts cabled in series to supply the control-rod electromagnets. The by-pass circuit-breakers used to test the main circuit-breakers will only be mentioned since, by instruction, they are constantly maintained in the "disconnected" position and, moreover, when the testing, for example, of breaker A is performed the maintaining of the corresponding by-pass breaker is ensured through the contacts series of train B.

V - RELIABILITY OF THE SYSTEM

V.1. - Problem

Considering what has been said so far, the problem is limited to the following terms :

The reactor being at its nominal power, an event causes the spurious withdrawal of some control rods. The subsequent reactivity insertion velocity and fuel burn up are such that the sequence start is normally detected early enough by the measurement of at least two different physical parameters :

- measurement of the high level neutron flux ;
- measurement and calculation of a high ΔT temperature (temperature variation of the coolant between the core inlet and outlet).

The neutron flux sensors (long ionization chambers) are 4 in number and distributed around the vessel at 90° from one another. The scram decision is taken when at least two of the four measurements have exceeded the safety threshold.

.../...

The ΔT temperature is calculated for each loop and therefore we get 3 redundant pieces of information combined in a 2/3 system.

This being, one attempts to evaluate the probability that the control rods do not fall in response to the event "spurious withdrawal".

Nota : The sequence is described in the Provisory Safety Report of Fessenheim I.

V.2 - Functioning diagram

Figure n° 6 schematizes, from left to right, the sequence resulting from the occurrence of the initiating event followed by an effective scram.

We think that the diagram is clear enough and does not require comments which would be useless and redundant with all that has already been said.

V.3 - Fault tree

The fault tree has been established from the preceeding diagram of operation.

The logical part of the system, particularly complex, has been studied with the CHAMBOR computing code. This code (after transposing the conventional wiring diagrams into equivalent diagrams directly usable by a computer) gives two advantages :

- checking that the diagram contains no error, either in design or in recopy, thanks to the programm ability to simulate a dynamic operation of the system ;

- determining the critical paths.

.../...

Figure n° 7 gives an example of an electric diagram transposed and used by a computer : The two identical A and B logical trains with the 2/4 and 2/3 matrices mentioned above. The signalling has been taken into account but put in stand-by condition. (The work of the group dealing with human factor has not enabled us to go further in this field).

Figure n° 8 gives an example of the program listing enumerating all the single failures which can inhibit the logical part of the system.

Taking all that into account, we comme to the final fault tree shown on figure 9. On this figure (from bottom to top), we recognize successively on each horizontal line the leaves representing :

- the temperature channels(1T, 2T, 3T) and the neutron flux channels(1P, 2P, 3P, 4P) ;

- the matrix relays (331 to 1123), which are the relays ensuring the connection between the analog part (including the tripping device) and the logical part on one hand and the starting points of the A and B trains explicited above on the other hand ;

- the majority of vote logics (2/3, 2/4) ;

- the matrix repeater relays (322, 323....1030) as well as the temperature and neutron flux (power) common mode failures which are logically introduced at this level ;

- the control rod breakers (DJA, DJB) ;

- the relays and circuit-breakers common mode failures ;

- the final event : emergency shutdown.

.../...

This diagram takes into account the dependencies. We notice (for example) that the 1T train (leaves 52 and 55) may affect simultaneously trains A and B.

The numbers below the leaves correspond to a numbering used in the PATREC code which solves fault trees.

V.3 - Data

The problem of the numerical data is always a difficult problem to solve.

The data used here come from :

- the WASH 1400 report (2)

- statistics from "Electricité de France" (13)

- the files established by the DSN on the "Phenix" reactor (14)

Three types of difficulties must be pointed out :

a) the data are presented either in the form of a failure rate, either in the form of a probability of failure on demand ; this led us to present the results in a form which, though quite significant, is nevertheless peculiar. This could be done thanks to the wide capabilities of the PATREC/RCM code (10) ;

b) the data are always global, that is they include safe and unsafe failures. Within the framework of this study, only the safe failures are useful. A ratio of 1/10 between unsafe and global failures is generally admitted. All the experts of the group have agreed to apply this coefficient to the relays and the circuit-breakers. On the contrary, they had divergent opinions concerning the analog part of the system ; the calculations have therefore been made for two values of the ratio : 1/10 and 1/2 ;

.../...

c) we do not have a very clear idea of the value to be assigned to the common mode failures. Some authors [Ref. 12] recommend a ratio $\beta = 1/10$ between common mode and self mode failure rates. As this value is questionable, we have made the calculations for 4 values of the β ratio : 0 (no common mode failure), 10^{-2}, 10^{-1}, 1.

Considering what has been said above, the following values have been adopted in the calculations :

Device designation	Failure rate λ		Probability of failure on demand
	1st estimation UF = 1/10 glob.fail.	2nd estimation UF = 1/2 glob.fail.	
ΔT temperature channel	8.10^{-6}/h	4.10^{-5}/h	
neutron power channel	$9,6.10^{-6}$/h	$4,8.10^{-5}$/h	
relay	$1,4.10^{-7}$/h	$1,4.10^{-7}$/h	
circuit-breaker			3.10^{-5}/d

UF : unsafe failure

$$\beta = [0 - 10^{-2} - 10^{-1}] - 1 = \frac{\lambda \text{ (or proba.) common mode}}{\lambda \text{ (or proba.) self mode}}$$

V.4 - Calculations and results

The calculations have been made from the fault tree (figure 9), with the data defined above and with the help of the PATREC/RCM code, which is a very efficient code taking into account in particular the dependencies (details concerning the PATREC/RCM code are given in the note cited in reference 10).

.../...

The results are given in the following two tables, respectively corresponding to the 2 values of the ratio λ unsafe failures/ λ global failures (1/10 and 1/2) adopted for the analog trains.

Case n° 1

	TCM + PCM	RCM	BCM	Resulting proba.
0	0	0	0	1.10^{-9}
10^{-2}	$1,1.10^{-8}$	1.10^{-6}	3.10^{-7}	$1,3.10^{-6}$
10^{-1}	$4,6.10^{-7}$	1.10^{-5}	3.10^{-6}	$1,3.10^{-5}$
1	4.10^{-5}	1.10^{-4}	3.10^{-5}	$1,7.10^{-4}$

TCM = temperature channels common mode
PCM = neutron flux channels common mode
RCM = relay common mode
BCM = circuit breaker common mode

.../...

Case n° 2

1	TCM + PCM 2	RCM 3	BCM 4	Resulting proba. 5
0	0	0	0	$3,6.10^{-7}$
10^{-2}	$4,4.10^{-7}$	1.10^{-6}	3.10^{-7}	$2,1.10^{-6}$
10^{-1}	$1,6.10^{-5}$	1.10^{-5}	3.10^{-6}	3.10^{-5}
1	1.10^{-3}	1.10^{-4}	3.10^{-5}	$1,1.10^{-3}$

The values in the "resulting probability" column must be interpreted as follows :

At the time to, a test of the system is performed and we establish that it is in a good operating condition. After a T period equal to 1 month (720 hours), a second test is performed. The number written in column 5 gives the probability that this second test reveals a failure in the system operation.

Therefore, a simplifying assumption has been made that the system is tested in its whole and instantaneously every month. In reality, things are different and, though it is true to say that the system is tested every month in its whole, one might take into consideration that, in fact, the different parts of the system are sequentially tested. A study will be carried through on this subject (cf human factors group).

These results bring to light that in the two cases the common mode failures are predominant , as could be expected. The relay common mode failure is predominant , except in case n° 2 for $\beta = 1$ (unlikely case).

.../...

We can also notice that in case n° 1, for $\beta = 0$, the circuit-breakers are predominant (9.10^{-10} for the circuit-breakers compared with a total probability of 1.10^{-9}).

V.5 - Credibility of the results

Given the uncertainty on the validity of the numerical values which were used, it was interesting to evaluate the uncertainty factor affecting the global results, by taking into account the uncertainty factors specific to the component failure rates.

Calculations have been made with the following values (taken from WASH 1400) :

- analog trains uncertainty factor : 10
- relays and circuit-breakers uncertainty factor : 3

Data : those from case n° 2 (§ V.4) for $\beta = 10^{-1}$

For these calculations, the PATREC/MC code has been used (version of the PATREC code using a Monte-Carlo method) (Ref. 11) .

A first run was used to simplify the tree of Figure 9 by indentifying the predominant cut sets. So, if we neglect the cut sets lower by a factor 10^4 to the cut sets kept, we come to the simplified tree of Figure 10.

The tree of Figure 10 shows a perfect symmetry in relation to the circuit "ET" numbered 1. This permits (using the properties of the Boolean algebra) a second reduction of the tree which is shown in figure 11.

Figures 12, 13, 14 show the dispersion of the global result value related to the dispersion of the input parameters, respectively after 500, 2500 and 10 000 runs.

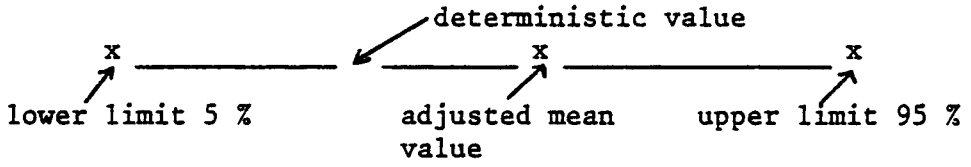
.../...

As can be seen, the curve looks like a lognormal law. With this assumption, for a 90 % confidence level, the code provides the following values :

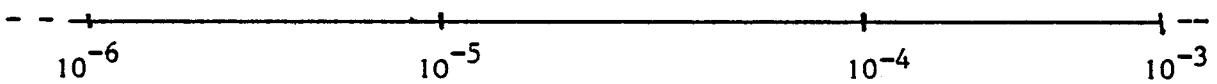
lower limit 5 % : 1,045..... 10^{-5}
upper limit 95 % : 5,663..... 10^{-4}
adjusted mean value : 7,694..... 10^{-5}

That is an uncertainty factor of about 7

If we remember that the deterministic value precedently found was of 3.10^{-5} , we find out that the results are quite consistent :



Probability scale



VI - CONCLUSIONS

This first study is a decision experiment and constitutes a good illustration of the present knowledge in the field of probabilistic estimation of the quality of a complex system. It brings to light the field in which research is further necessary.

Considering the time granted and the means available, the study has been limited to the scram system actuation after a spurious withdrawal of some control rods (reactor being on power). The external events have not been taken into account.

.../...

However, a wider study would not have brought more to the purpose pursued, which was to concretize the possibilities and the draw backs in lacks of the method by studying a real case.

The fault tree analysis has once more shown its value. For example, we have noted that it was possible without expensive modifications to greatly improve the efficiency of the measurements processing by a continuous search for eventual discordance.

Doubts remain on the numerical data. The failure rates are generally given in a global form (safe failures + unsafe failures) while we are only interested in the unsafe failures. The factor β related to the common mode failures is not well known :

$$\left(\beta = \frac{\text{proba. of common mode failure}}{\text{proba. of self mode failure}}\right)$$

We do not yet know exactly how to introduce the human factor in the calculations. Simplifying assumptions had to be adopted for the test procedures.

The parameter calculations (see pages 22 and 23) show the importance of these factors on the global result.

A sensitivity study performed with the help of PATREC/MC code in a case which (in the present state of the art) seemed to us realistic, gives the following results for the non-operating probability of the emergency shutdown system after a one month's period :

adjusted mean value	:	$7{,}7.10^{-5}$
lower limit 5%	:	$1{,}0.10^{-5}$
upper limit 95 %	:	$5{,}6.10^{-4}$

.../...

This means an uncertainty factor of about 7 for a confidence level of 90 %.

We can therefore see the difficulties related to the establishment of a good quality probabilistic criterion and the need to develop research in the adequate fields covered by the different working groups.

INITIATING EVENTS AND ACCIDENT SEQUENCES

1 - Voltage loss on the LGA and LGD bus of the three primary pumps, at full power.

2 - Spurious opening of all primary pumps circuit-breakers, or loss of a phase leading to the protections trip by overintensity of the circuit-breakers - plant being at full power.

3 - Reactor at a power below 40 %, 2 loops out of 3 in service - spurious opening of the circuit-breakers of the two in-service pumps, or loss of a phase leading to the trip by the overintensity protection of the two in-service pumps circuit-breakers.

4 - Loss of flow rate in one loop, reactor at full power.

5 - Loss of flow rate in one loop, the reactor being at a power below 40 %, two loops out of three in service.

6 - Frequency decrease of the network, the reactor being at full power.

7 - Spurious closing of the isolation steam valves, manual regulation of the reactor and control of the pressurizer out of service (discharge valves and spray).

8 - Fault on the turbine regulation, or operator error. leading to an excess load increase, from a low power level.

9 - Spurious withdrawal of the control rods in power at low dp/dt.

10 - Spurious withdrawal of the control rods from zero power (inefficient intermediate level channel).

.../...

11 - Spurious withdrawal of the control rods at power, high reactivity insertion rate.

12 - Uncontrolled spatial distorsion of flux at power.

13 - Turbine trip, with single failure of a stop valve (left open), reactor at full power, fuel cycle at beginning of life, all regulations and control being manual (reactor, pressurizer), turbine by-pass out of service (case of trip by loss of a condenser function, for example).

14 - Spurious closing of the turbine stop valves, turbine by-pass out of service.

15 - Failure of the CVCS, leading to an excessive charge flow compared with the discharge (discharge out of service, for example).

16 - Feedwater turbo-pump trips manual regulation (or turbine power reduction too slow), reactor at full power.

17 - Faults in the regulation of the steam generators level, leading to spurious closure of the regulating valve - reactor at full power leading to a lack of balance between water flow rate and steam flow rate.

18 - Small break on the steam circuit in the containment - reactor at full power.

19 - Loss of primary coolant (small break), excluding the breaks on the pressurizer in steam phase.

20 - Steam drum rupture - reactor at full power.

.../...

21 - Steam drum rupture - reactor at zero power (or beginning of hot shutdown).

22 - Steam piping rupture outside the containment, downstream the isolation valve, without failure of the concerned valve.

23 - Control rod ejection - reactor at intermediate or full power.

24 - Spurious fall of two (or more) control rods into the core - reactor at full power in automatic operation.

25 - Control rod(s) spurious withdrawal - reactor at low power level, below P6 (on the Po 10^{-5} to 10^{-3} % scale) (source level).

26 - Control rod(s) spurious withdrawal - reactor at power equal to or higher than P6 (intermediate level).
Protection channel at source level locked.

27 - Loss of all external electrical supplies - self-energizing unsuccessful - plant at full power.

28 - Break in a feedwater pipe in the containment.
The level sensors in the concerned steam generator are assumed to not work properly.

REACTIVITY INSERTION SPEED

REACTIVITY RETROEFFECTS	0,5 pcm/s	2,5 pcm/s	25 pcm/s	80 pcm/s
MINI	*t = 202 s A.U par ΔT température TU = 275 s instant ultime Ru = 135 pcm	*t = 54 s A.U par ΔT température *t = 65 s A.U par ΔT puissance *t = 67 s A.U par haut flux TU = 75 s instant ultime Ru = 175 pcm		*t = 0,5 s A.U par variation élevée de flux *t = 1,5 s A.U par haut flux nucléaire TU = 2,5 s instant ultime Ru = 200 pcm
MAXI		*t = 326 s A.U par ΔT température TU = 475 s instant ultime Ru = 1200 pcm	*t = 19,5 s A.U par ΔT température *t = 23 s A.U par ΔT puissance *t = 23 s A.U par haut flux TU = 35 s instant ultime Ru = 875 pcm	*t = 0,5 s A.U par variation flux *t = 3,5 s A.U par haut flux *t = 7,5 s A.U par ΔT température *t = 8 s A.U par ΔT puissance TU = 8,5 s instant ultime Ru = 680 pcm

Ru : Réactivité insérée cumulée à l'instant ultime

TABLE 1

FIGURE 1

1 - Tension basse sur les jeux de barres des pompes primaires - Puissance > P_1 (10 %)	15 - Niveau haut au pressuriseur
2 - Disjoncteurs des pompes primaires ouverts - Puissance > P_3 (40 %)	16 - Très bas niveau au G.V.
3 - Disjoncteurs des pompes primaires ouverts - Puissance > P_7 (10 %)	17 - Bas niveau et pression vapeur Débit bas d'eau alimentaire
4 - Débit circuit primaire bas - Puissance > P_8 (40 %)	18 - Signal d'injection de sécurité déclenché sur pression enceinte haute
5 - Débit circuit primaire bas - Puissance > P_7 (10 %)	19 - Signal d'injection de sécurité déclenché par basse pression et bas niveau pressuriseur $P>P_7$
6 - Fréquence basse sur les jeux de barres (LGA et LGB) $P > P_7$	20 - Signal d'injection de sécurité déclenché sur haut débit vapeur et basse pression vapeur
7 - Pression élevée au pressuriseur	21 - Signal d'injection de sécurité déclenché sur haut débit vapeur et basse pression vapeur
8 - Pression basse au pressuriseur - Puissance > P_7	22 - Signal d'injection de sécurité déclenché sur écart de pression vapeur entre file trop élevée
9 - ΔT - Température élevée	23 - Dérivée positive de flux trop forte
10 - Flux haut - Chaîne puissance seuil bas	24 - Dérivée négative de flux trop forte (chaîne puissance)
11 - Flux haut - Chaîne puissance seuil haut	25 - Mesure de flux trop forte - Niveau source
12 - ΔT - Puissance élevée	26 - Mesure de flux trop forte - Niveau intermédiaire
13 - Déclenchement turbine (pression circuit d'huile basse)	27 - Défaut conduisant au manque de tension des mécanismes de grappe
14 - Déclenchement turbine (vannes d'arrêt fermées)	(28) - (Manuel)

FIGURE 3

LIST OF THE PROTECTIVE CHANNELS

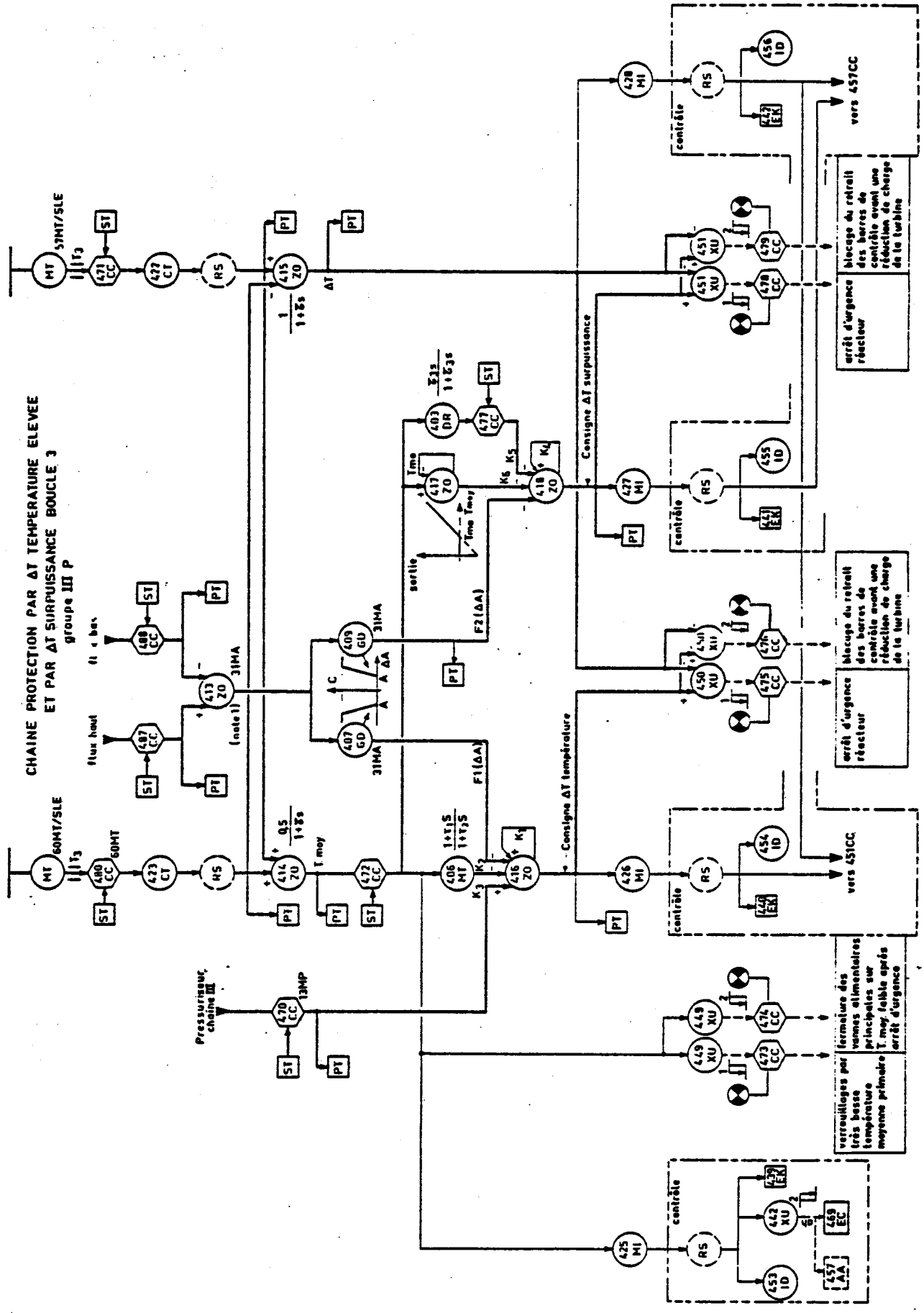
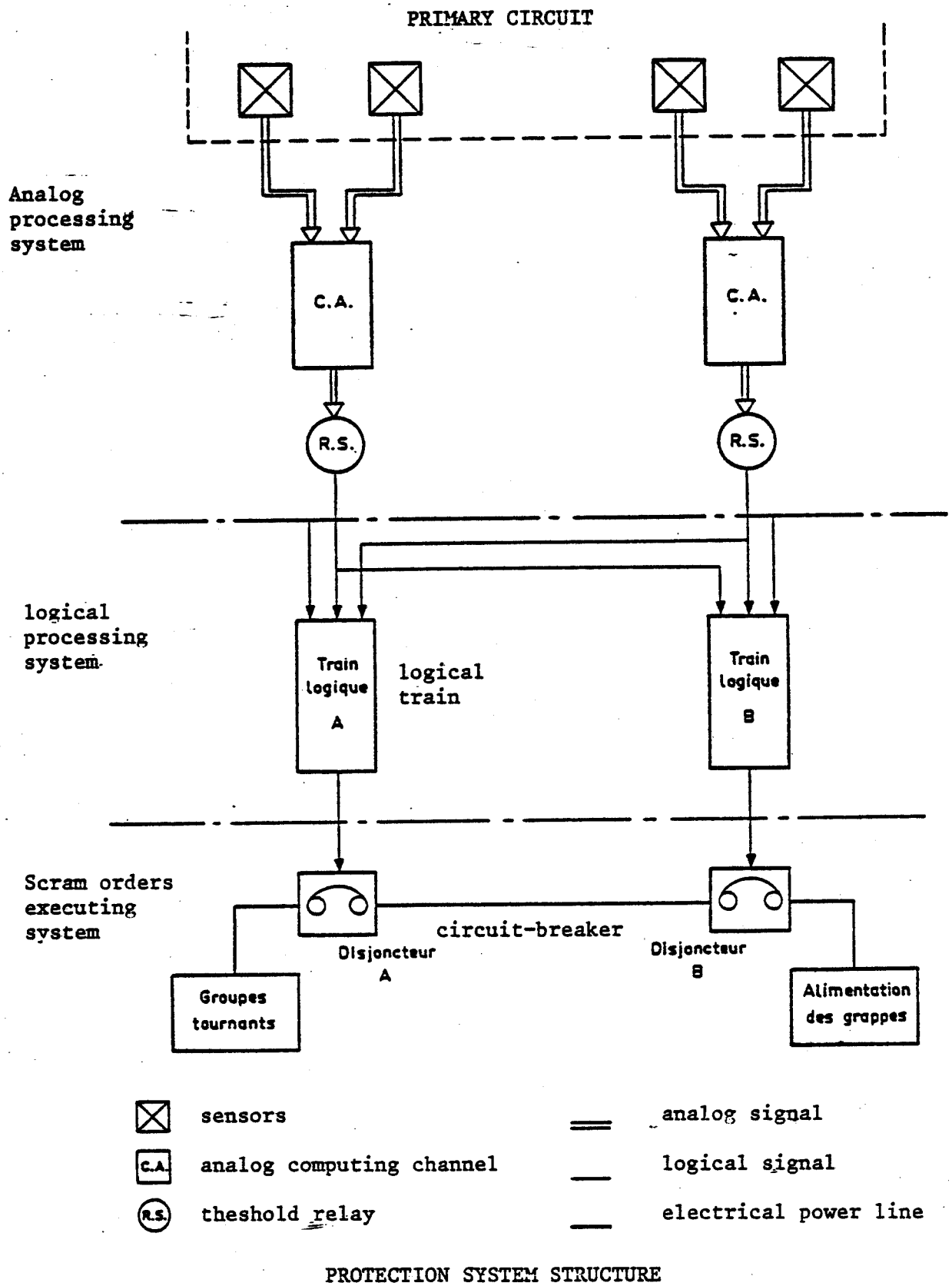

CHAINE PROTECTION PAR ΔT TEMPERATURE ELEVEE
ET PAR ΔT SURPUISSANCE BOUCLE 3
groupe III P
Consigne ΔT surpuissance
Consigne ΔT température
vers 457CC
vers 451CC
arrêt d'urgence réacteur
blocage du retrait des barres de contrôle avant une réduction de charge de la turbine
verrouillages par très basse température moyenne primaire
fermeture des vannes alimentaires principales sur T. moy. faible après arrêt d'urgence
Pressuriseur chaine III
contrôle
Flux haut
sortie
(note 1)

FIGURE 4



PROTECTION SYSTEM STRUCTURE

FIGURE 2

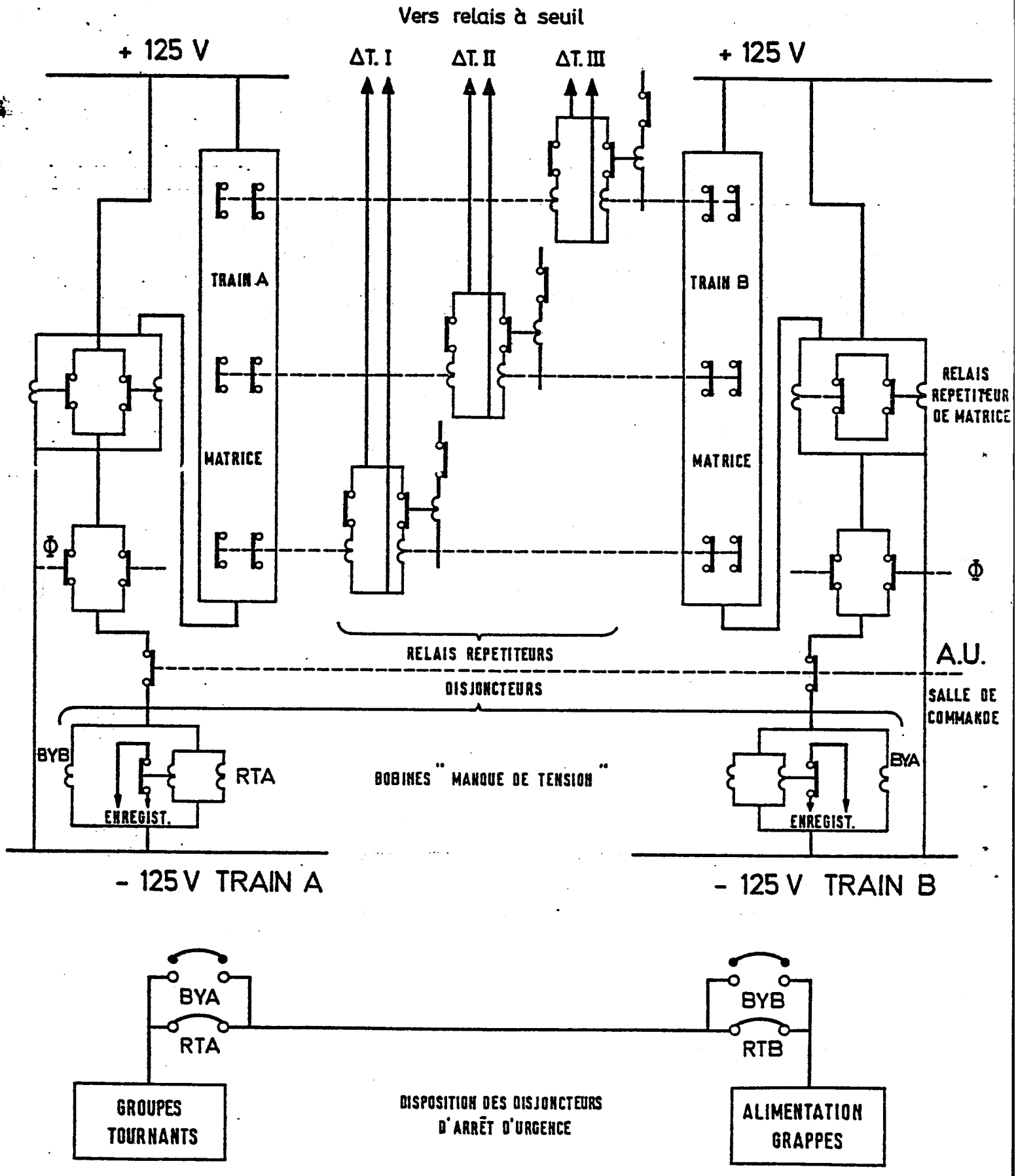

Vers relais à seuil
+ 125 V
ΔT. I
ΔT. II
ΔT. III
+ 125 V
TRAIN A
TRAIN B
MATRICE
MATRICE
RELAIS REPETITEUR DE MATRICE
Φ
Φ
RELAIS REPETITEURS
A.U.
DISJONCTEURS
SALLE DE COMMANDE
BYB
RTA
ENREGIST.
BOBINES " MANQUE DE TENSION "
BYA
ENREGIST.
- 125 V TRAIN A
- 125 V TRAIN B
BYA
RTA
BYB
RTB
GROUPES TOURNANTS
DISPOSITION DES DISJONCTEURS D'ARRÊT D'URGENCE
ALIMENTATION GRAPPES

FIG. 5 - Relay

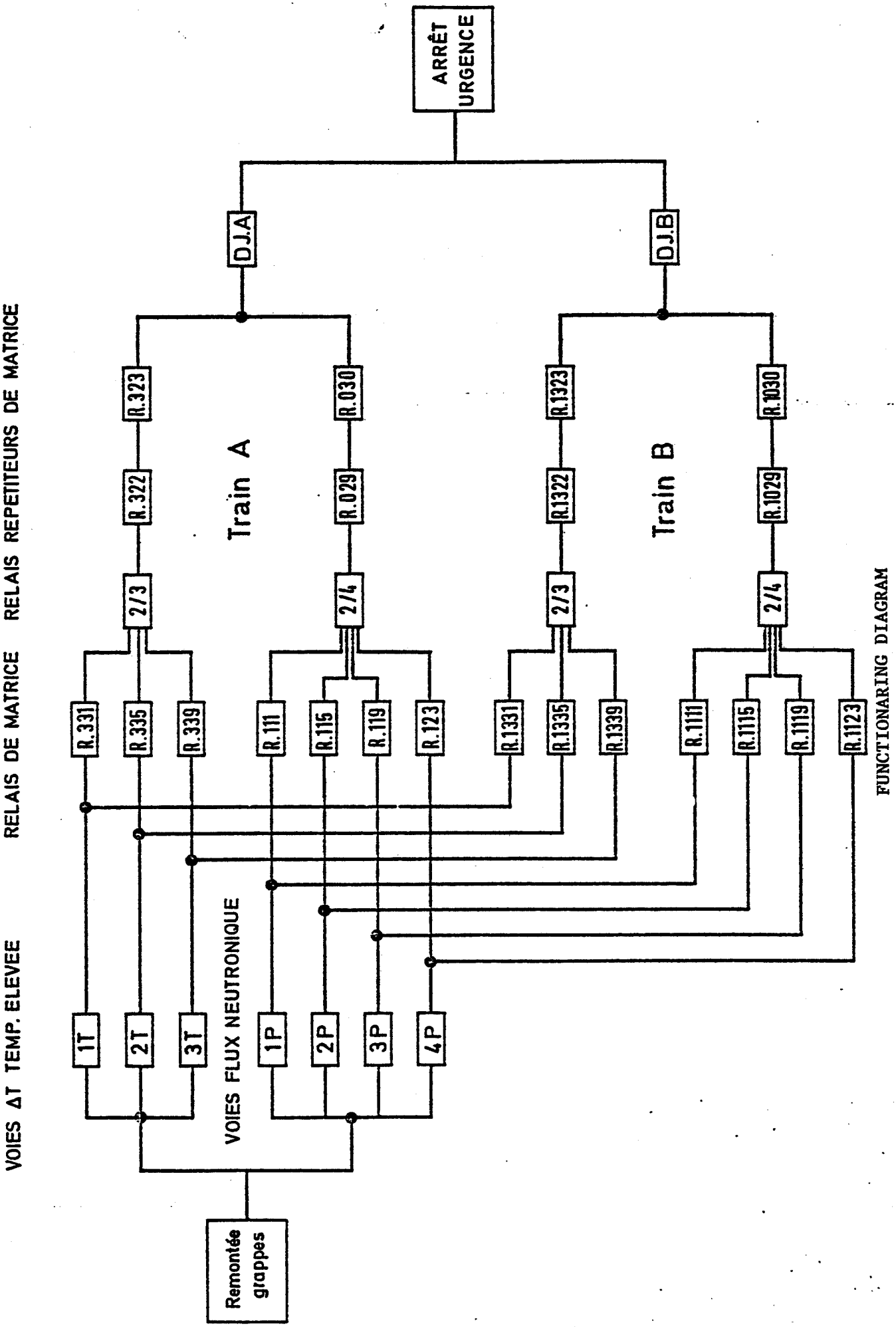

ARRÊT URGENCE
DJ.A
DJ.B
Train A
Train B
R.323
R.322
2/3
R.030
R.029
2/4
R.1323
R.1322
2/3
R.1030
R.1029
2/4
R.331
R.335
R.339
R.111
R.115
R.119
R.123
R.1331
R.1335
R.1339
R.1111
R.1115
R.1119
R.1123
1T
2T
3T
1P
2P
3P
4P
Remontée grappes
VOIES ΔT TEMP. ELEVEE
RELAIS DE MATRICE
VOIES FLUX NEUTRONIQUE
RELAIS REPETITEURS DE MATRICE
FUNCTIONARING DIAGRAM

Fig. 6

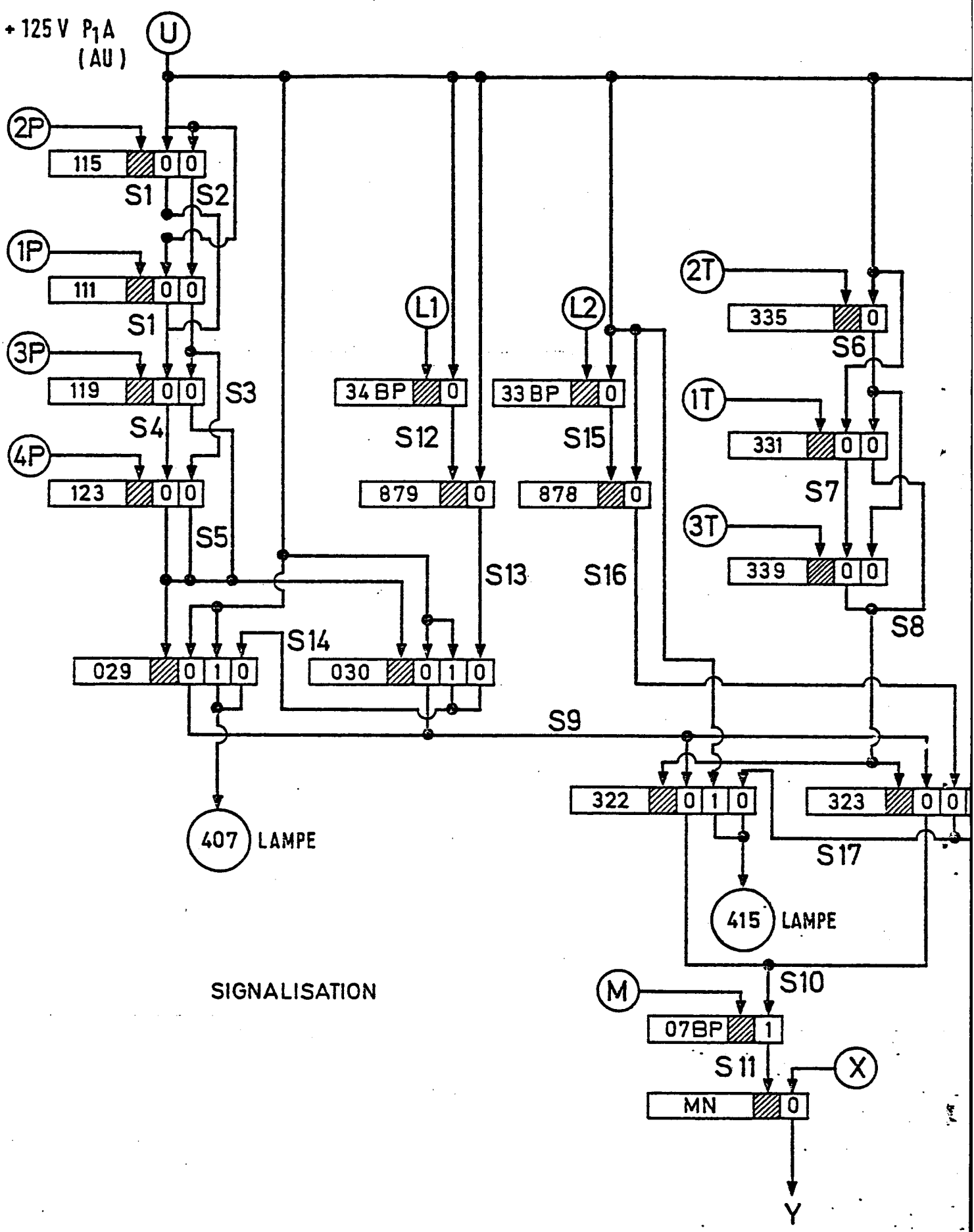


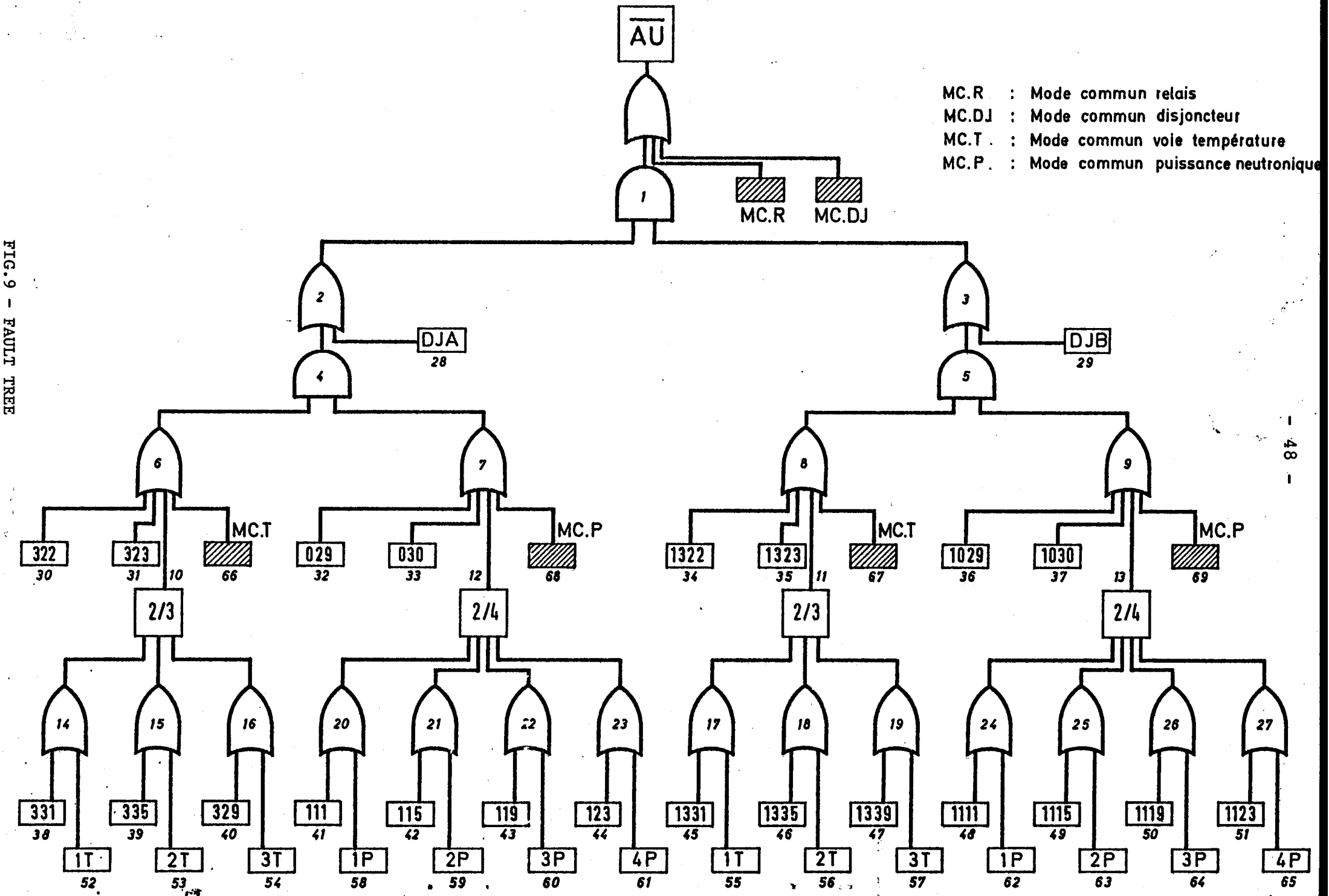
FIG. 7 - RPR Converted diagram

DEFAUTS D'ORDRE 1

RELAIS:029	CONTACT 3	:INVERSION ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: 407		
RELAIS:030	CONTACT 3	:INVERSION ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S14	407	
RELAIS:322	CONTACT 3	:INVERSION ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: 415		
RELAIS:323	CONTACT 2	:INVERSION ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S17	415	
RELAIS:078P	BLOCAGE A 1	DE LA BOBINE	CONTROLE(S) AFFECTE(S)	: S11	Y	
RELAIS:078P	CONTACT 1	:INVERSION ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S11	Y	
RELAIS:MN	BLOCAGE A 0	DE LA BOBINE	CONTROLE(S) AFFECTE(S)	: Y		
RELAIS:MN	CONTACT 1	:INVERSION ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: Y		
RELAIS:338P	BLOCAGE A 0	DE LA BOBINE	CONTROLE(S) AFFECTE(S)	: S17	415	
RELAIS:338P	CONTACT 1	: BLOCAGE ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S17	415	
RELAIS:878	BLOCAGE A 0	DE LA BOBINE	CONTROLE(S) AFFECTE(S)	: S17	415	
RELAIS:878	CONTACT 1	: BLOCAGE ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S17	415	
RELAIS:348P	BLOCAGE A 0	DE LA BOBINE	CONTROLE(S) AFFECTE(S)	: S14	407	
RELAIS:348P	CONTACT 1	: BLOCAGE ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S14	407	
RELAIS:879	BLOCAGE A 0	DE LA BOBINE	CONTROLE(S) AFFECTE(S)	: S14	407	
RELAIS:879	CONTACT 1	: BLOCAGE ETAT INITIAL	CONTROLE(S) AFFECTE(S)	: S14	407	

END OF SINGLE FAILURES RESEARCH

FIGURE 8



MC.R : Mode commun relais
MC.DJ : Mode commun disjoncteur
MC.T . : Mode commun voie température
MC.P . : Mode commun puissance neutronique

FIG.9 - FAULT TREE

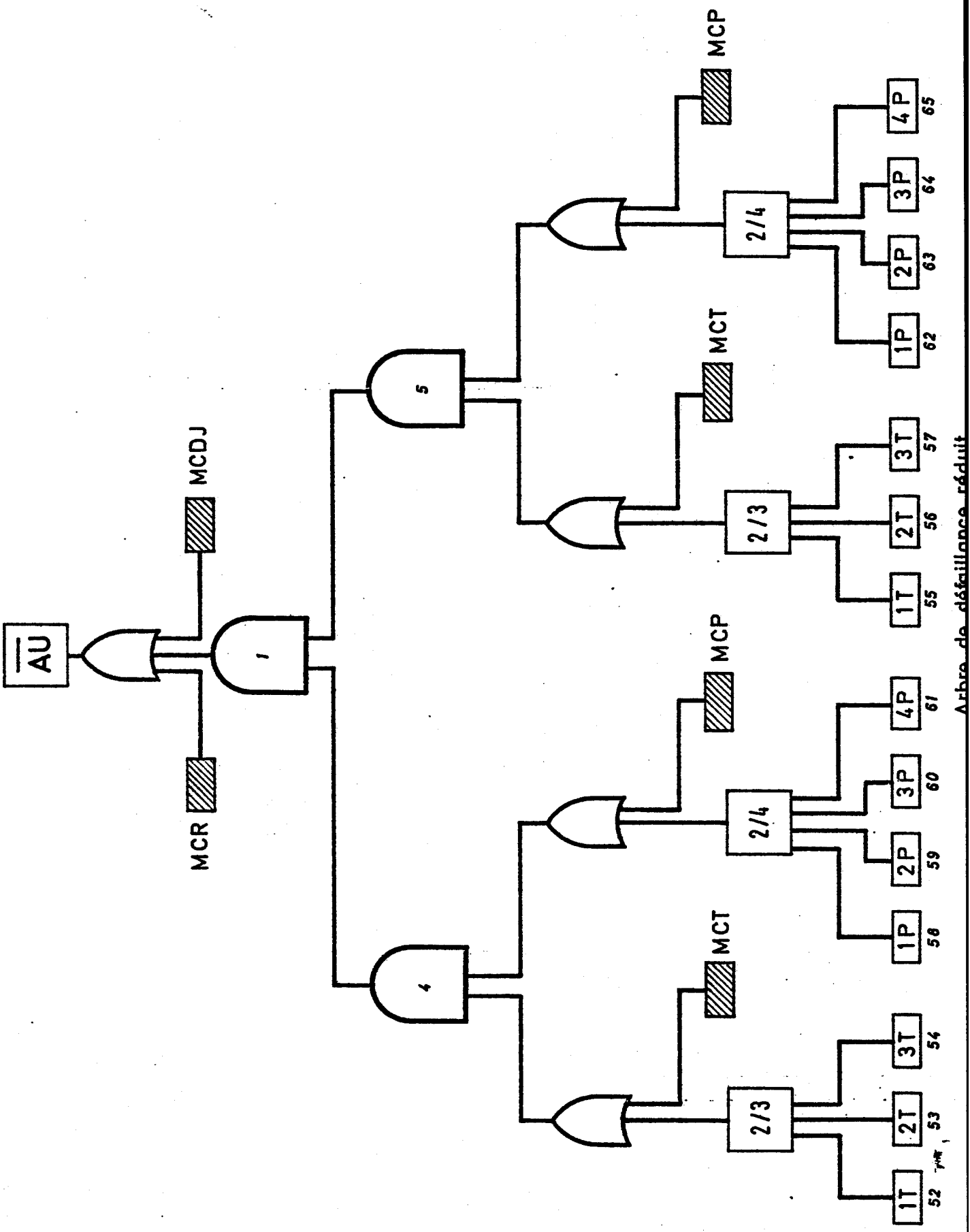


FIG. 10 - REDUCED FAULT TREE

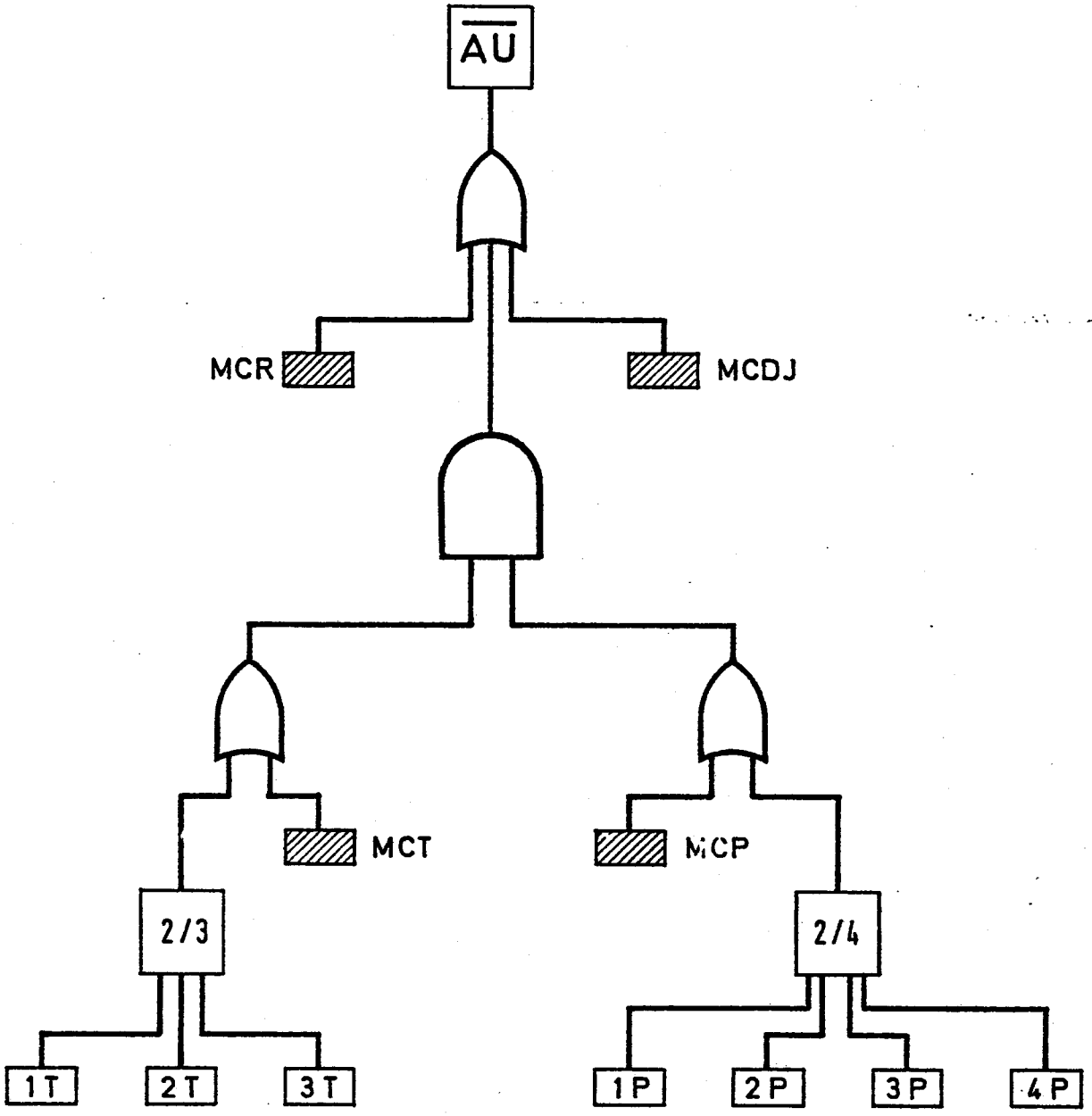


Fig. 11 - REDUCED FAULT TREE

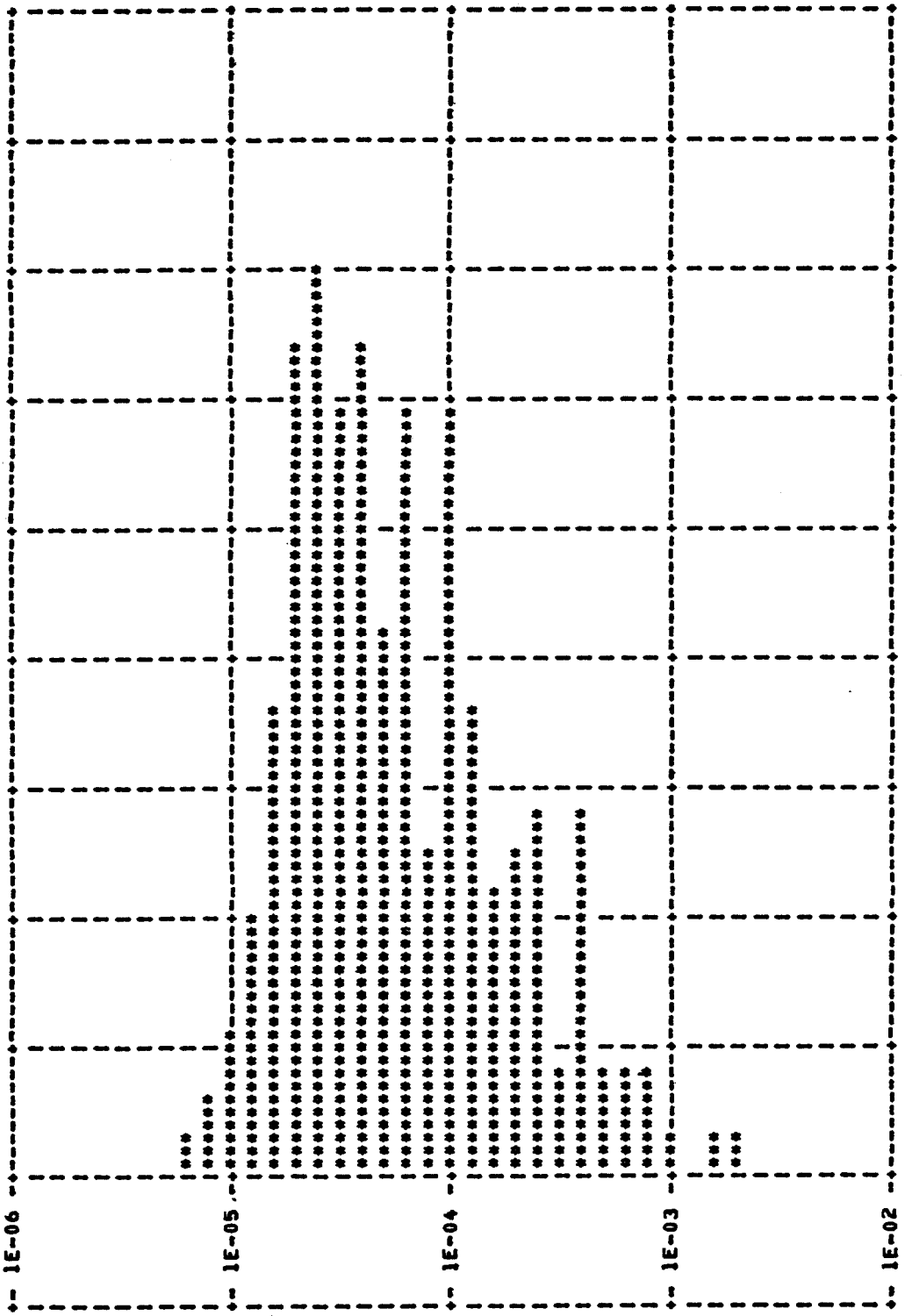

HISTOGRAMME DE LA DISTRIBUTION
1E-06
1E-05
1E-04
1E-03
1E-02
250 runs

FIGURE 12

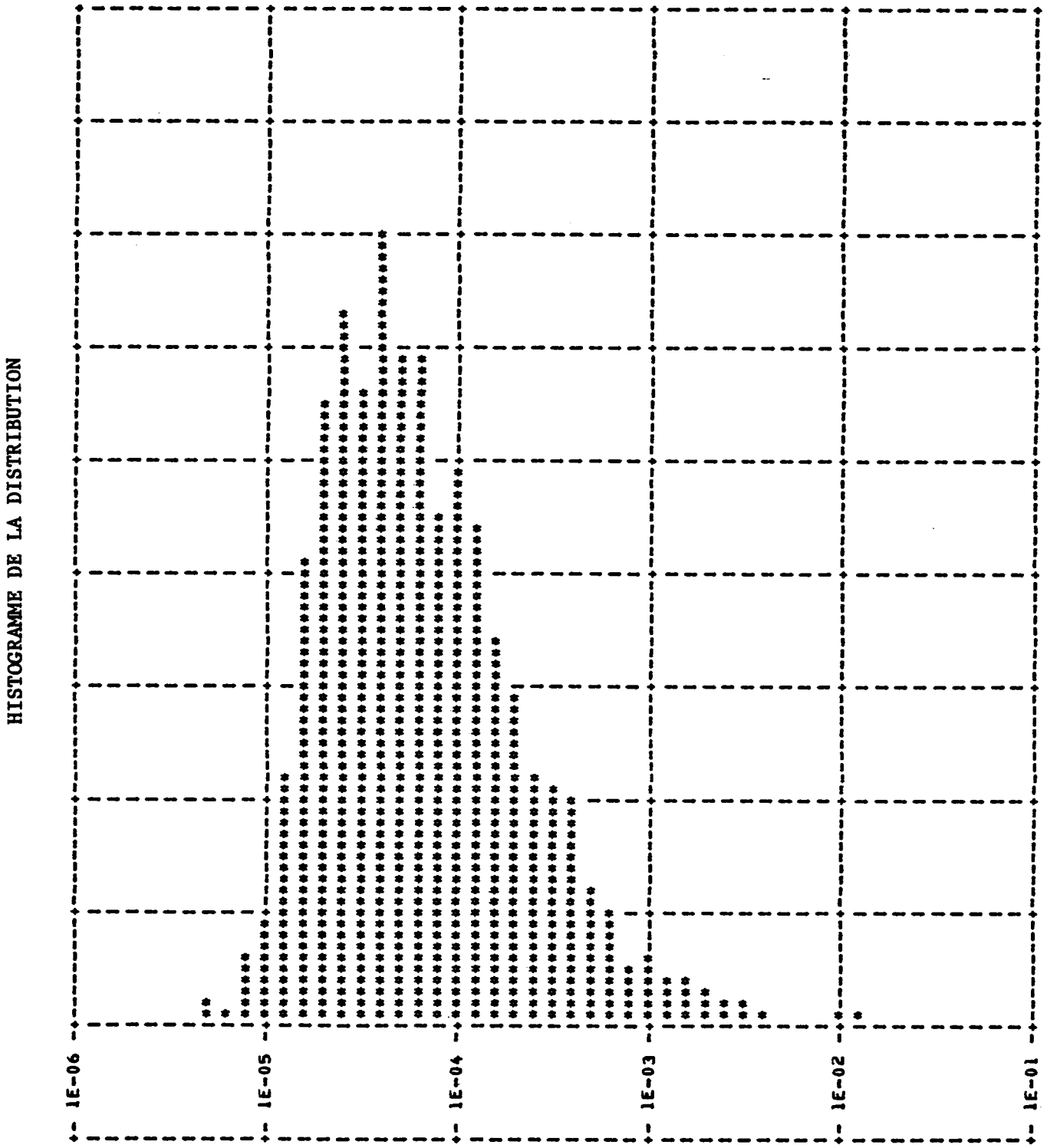

HISTOGRAMME DE LA DISTRIBUTION
1E-06
1E-05
1E-04
1E-03
1E-02
1E-01
2000 runs

FIGURE 13

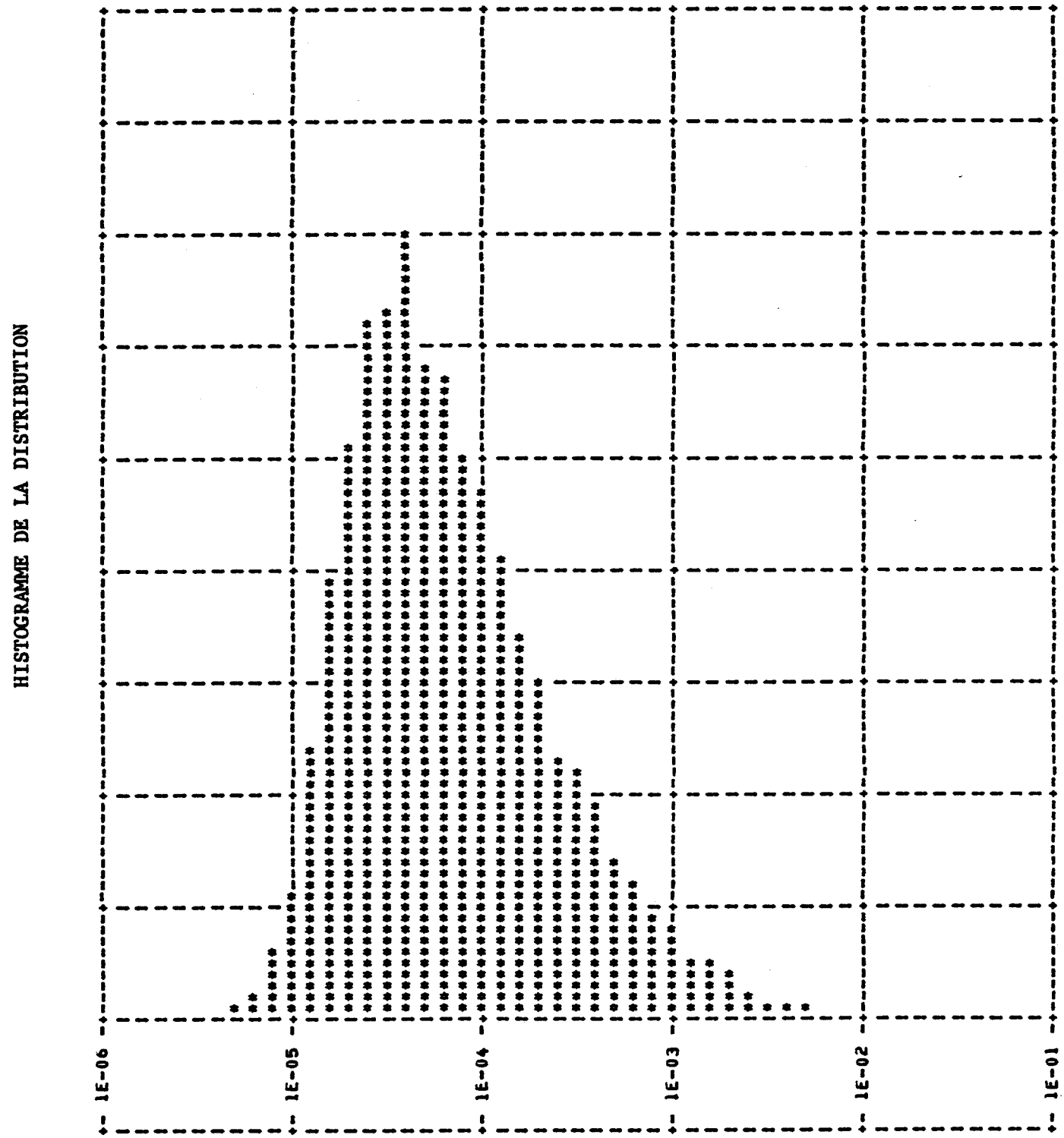

HISTOGRAMME DE LA DISTRIBUTION
1E-06
1E-05
1E-04
1E-03
1E-02
1E-01
10.000 runs

FIGURE 14

Discussion

Mr Vesely referred to the difference between the probability of failure of the circuit breakers to operate quoted in WASH 1400 (10^{-3}), and the value used in the assessment (3.10^{-5}). Mrs Carnino replied that the value used was based on the WASH 1400 data; but that the particular conditions for the Fessenheim system and that the failure-to-open state only was of interest. Mr Green thought that some indication of the possible spread of data values would be of interest, to which Mrs Carnino replied that this was probably an appropriate consideration for the Data Sub-group.

Mr Garribba requested information on the introduction of human factors problems into the fault tree for the system, and in reply it was stated that these would be introduced at a later time when the other sub-groups had completed their studies on this subject. At present they were included with the common mode problems which are shown on the fault tree. Mr Hensley commented that a particular problem for the human factors sub-group considering the Fessenheim system was its complex testing procedures of long duration. These could be interrupted by reactor operations with further error possibilities.

In reply to Mr Hofer, Mrs Carnino stated that the considerations of uncertainty of data did not include the β values.

SINDOC(77)130

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

WORKING GROUP OF EXPERTS ON RARE EVENTS DATA COLLECTION AND ANALYSIS

Presented by G. Volta

1. INTRODUCTION*

The terms of reference for the work of this group have been fixed as follows:

- collect and analyze rare event data;
- specialize the data to reactor shutdown systems and possibly PWR shutdown systems;
- exclude external rare event data like earthquakes, tornadoes, etc.

Given these terms of reference the task of the group was linked to data collection related to shutdown system unavailability, which is also important in consideration of ATWS: anticipated transients without scram. In fact the event "no scram on demand" is an important rare event concerning the shutdown systems where its probability is to be low since its consequence can be relevant from the safety point of view.

Considering the limited population of operating shutdown systems, direct statistical experience of events having a probability less than 10^{-5} cannot be claimed. So the expression "data collection and analysis" has to be interpreted in the sense of "collection, analysis and processing of data relevant to the prediction of the event having that very low probability".

Following this line of thinking the group members have produced various contributions that address various critical aspects of the problem of data collection, analysis, and interpretation.

A first contribution focuses attention upon the data published concerning ATWS and shutdown system unavailability. Three documents issued in the USA and the F.R. of Germany were received from Belgium, Denmark, France, the F.R. of Germany

---

* This is a summary of the complete interim report of the data collection sub-group (SINDOC(77)129).

Italy and the Netherlands. The IEEE Reliability Data Project (Project 500) carried out in the USA has also been reviewed.

2. REVIEW OF THE US AND GERMAN REPORTS: WASH-1270, EPRI NP-261 AND MRR-163

The data collected in WASH-1270 [1] involve power reactor experience accumulated up to 1973 (Table 1). From the data, an upper bound on the shutdown system unavailability is estimated to be 1×10^{-4} at a confidence level of 95%. While WASH-1270 is strictly a data analysis, the EPRI report [2] combines actual experience with subjective judgement (prior distribution) to form updated estimates (posterior distributions) of the system unavailability. In statistical terminology, this is termed a Bayesian analysis as compared to a classical analysis as was done in WASH-1270. The EPRI results are given in table 2. For the fault tree analysis, component data were taken from WASH-1400.

The results in the EPRI report are generally lower than the 10^{-4} value given in WASH-1270 since best estimates were attempted as opposed to the upper bounds given in WASH-1270.

The German report MRR-163 [3] determines the shutdown system unavailability using fault tree analysis with no direct use of the results given in WASH-1270 or the EPRI report. The results are:
5×10^{-6}: shutdown system unavailability for PWR,
5.5×10^{-6}: shutdown system unavailability for BWR.
Within data uncertainties, the results are in general agreement with those of the EPRI report.

The three documents thus give data on:
- system experience,
- component failure rates,
- the effect of subjective judgement.

With regard to techniques, the reports discuss:
- statistical techniques: classical and bayesian,
- modeling techniques, essentially fault-tree techniques.

3. DATA INFORMATION FROM BELGIUM, DENMARK, FRANCE, ITALY AND THE NETHERLANDS

The availability of relevant data in European countries has been checked by sending a short questionnaire. The answers given by various group members are summarized in Table 3.

4. THE IEEE RELIABILITY DATA MANUAL [4)]

IEEE Std 500-1977 concerns the development and presentation of a reliability data base which includes failure rates, failure rate ranges, failure modes and environmental factor information on generic components actually or potentially in use in nuclear power generating stations. The current edition of this document is limited to electrical, electronic, and sensing components. However future editions are planned which will include mechanical, and nuclear system components.

The sources of information used for the development of the data base were found to exist in the following forms:
- Statistical operating data from nuclear plants
- Statistical operating data from fossil fuel fired generating stations and from other major industries
- Statistical failure data from generating stations, transmission grids, and related industrial plants for which recorded population information was not

available, but for which population estimates could be made to allow calculation of failure rates
- Data extracted from published sources for other industries which had some level of applicability to nuclear power generating station components
- Data generated from both population and failure estimates made by individuals familiar with operating and failure histories of particular generic types of devices.

All these sources were tapped to generate the initial data base contained in the current document, but no claims are made that the data presented would represent exactly data collected from a random sample of nuclear plants. In fact the recommended value (REC) and the interval given may be expected to differ from in-service experience for some of the reported failure data. However, although a particular statistical calculation of a component failure rate based on operating data may not match exactly the recommended point value, it is expected (based on a preliminary analysis given in reference 3) that such a calculation will be well within the range of values listed in the document.

5. CONCLUSIONS

From the preliminary work of the group some important points emerge:

a) The data at a system level are insufficient for directly estimating shutdown system unavailabilities less than 1×10^{-4} per demand.

b) In certain situations, low system probabilities can only be estimated if component data are used through a fault-tree analysis and other modeling techniques. Common mode failures need to be considered of course in these kinds of system analyses.

c) Four sources of component data are available: WASH-1400, CEA-EDF data, SRS data, and IEEE-500.
d) Data at intermediate subsystem level could be derived in principle by abnormal occurrences reported. But a deeper analysis should be carried out.
e) The combination of prior and posterior information has been advocated but the approach needs to be further continued.

6. REFERENCES

1) WASH-1270, Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors (1973).
2) Electric Power Research Institute. ATWS: A Reappraisal. EPRI-NP-261 (1976).
3) W. Ullrich, W. Frisch U.A.; "Untersuchungen von Betriebsstörungen bei Versagen der Reaktor Schnellabschaltung (ATWS) und anderer ausgewählter Sicherheitseinrichtungen", MRR 163, (1976)
4) Project 500 - IEEE Reliability Data Manual Presented by J.R. Fragola, Coordinator Project 500.

Table 1 - Power Reactor Accumulated Operational Time

	No. of units in category	No. of units in operation 3/73	Accumulated Time Reactor years
U.S. Reactors			
Central Station Power Units	36	29	150
Army Power Units	6	3	52
Naval Units	119	115	1005
N.S. Savannah	1	0	10
Total U.S. Units	162	147	1217
Foreign Reactors			
Central Station Power Units	66	66	410
Total U.S. and Foreign	228	213	1627

Table 2 - Upper Bound and Scram System Unavailability

Bayes Prior	Unavailability per Demand			
	95% confidence		50% confidence	
	zero fail.	one fail.	zero fail.	one fail.
Flat (classical results)	1.3×10^{-5}	2.1×10^{-5}	3.1×10^{-6}	3.7×10^{-6}
Step function (10^{-5}/D)	6.0×10^{-6}	6.5×10^{-6}	2.3×10^{-6}	3.1×10^{-6}
BWR fault-tree				
a. beta-fitting (mean value = 3.8×10^{-6}/D, Std. dev. = 3.8×10^{-6}/D)	3.1×10^{-6}	4.0×10^{-6}	3.6×10^{-7}	9.0×10^{-7}
b. numerical representation	3.7×10^{-6}	8.0×10^{-6}	7.0×10^{-7}	1.8×10^{-6}
PWR fault-tree				
a. beta-fitting (mean value= 1.4×10^{-5}/D, std. dev. = 6.1×10^{-5}/D)	2.7×10^{-5}	3.2×10^{-5}	1.3×10^{-5}	1.7×10^{-5}
b. numerical representation	4.1×10^{-5}	4.4×10^{-5}	3.0×10^{-5}	3.0×10^{-5}

Table 3 - Answers to the Questionnaire

Question No. 1:

Have you in your organization any set of information on abnormal occurrencies or failures regarding shut-down systems of commercial power plants in your country?

Answers to Question No. 1:

a) Belgium:

Il n'y a pas eu de panne du système d'arrêt d'urgence entraînant le non-fonctionnement de ce système sur les centrales belges.

Il y a eu des fonctionnemts intempestifs entraînant l'arrêt d'urgence dus à des mauvais contacts sur des diodes enfichables.

Il y a eu aussi blocage de certaines barres de contrôle en position basse car elles avaient été trop enfoncées.

b) France:

Electricité de France (EDF) does not have any specific set of information on abnormal occurences or failures regarding shut-down systems of its commercial power plants.

On the other hand the French Atomic Commission (CEA) has a reporting system of abnormal occurences related to the french reactors under commercial operation. This safety related data collection is filled by general information received from EDF and CEA operations people. Retrievals are available through quaterly reports published by "Service d'Etudes Techniques de Sûreté - Département de Sûreté Nucléaire" of CEA. Access to this information has to be discussed with CEA.

c) F.R. of Germany:

No special compilation but some information.

E.g.

a) Erfassung und Verbesserung der Zuverlaessigkeit der elektronischen Steuerung in den Kraftwerken Pleinting, Block 1. (Published literature: Annexe 1).

b) A report similar to a) but regarding Decontic B system produced by BBC. (Not available, property TUV Rheinland).

c) An expertise on shut-down system for Kruemmel BWR. Informations were obtained from Lingen and Grundemmingen. (Not available, property Arbeitsministerium des Landes Schleswig-Holstein).

d) Collection of abnormal occurrences in german reactors 71-76, partially published in "Zur friedlichen Nutzung der Kernenergie - eine Dokumentation der Bundesregierung". (Full report not available, property Bundesministerium fuer Innen).

d) Italy:

A- Deficiencies and failures regarding Trino Vercellese (PWR) nuclear power plant shutdown system

operating hours to which the list refers	51,000
control rod operation deficiencies or failure	8
control rod position indicator deficiencies or failure	13
spurious shutdown occurencies	8
spurious power reduction occurrencies	5
instrumentation component deficiencies or failures	28
operator errors in operation	1
operator errors in test	2

B- Deficiencies and failures regarding Garigliano (BWR) nuclear power plant shutdown system

operating hours to which the list refers	36,155
control rod operation deficiencies or failures	90
control rod position indicator deficiencies or failures	5
safety system channel deficiencies or failures	5
instrumentation component deficiencies or failures	100

e) The Netherlands:

For Borssele PWR, four failures of single control rods reported. For Dodewaard BWR, one failure on control rods reported.

Question No. 2:

Have you derived from the direct operating experience of shut-down systems of plants in your country any reliability figure for components or subsystems?

If yes, are these data available?

References?

Answers to Question No. 2:

a) Belgium:
No.

b) France:

For its new PWR plants, EDF developed a reliability data collection (SRDF) including systems, sub-systems and components specific to this kind of plant (1762 items/ unit have to be reported).

Certain components for shut-down systems are listed in the system. SRDF operation started a few months ago on two sites: FESSENHEIM and LE BUGEY. So data related to this preoperational units have no statistical meaning yet.

Conditions of access to this information is not yet defined.

c) F.R. of Germany:
The only case is the initial expertise for Kruemmel.

d) Italy:
No.

e) The Netherlands:
No.

Question No. 3:

Could you list the reliability data source regarding components for shut-down systems that you know?

Would you give some comment?

Answers to Question No. 3:

a) Belgium:
No.

b) France:
EDF needs reliability data to feed reliability studies conducted by itself or by other organization as CEA. That is the reason why a provisional document has been prepared by EDF (Ref. D.57-6632-01 rev. 0 "Recueil provisoire de données de fiabilité". This document

collects available data coming from EDF or other sources. Certain components for shut-down systems (sensors, relays) are included in this document.

c) F.R. of Germany:

List of data taken from MRR-1-54 (full report not available). This list has been used for computing the fault-tree reported in MRR-163/IRS-W-22.

d) Italy:

No.

e) The Netherlands:

- WASH-1400
- Ausfall Ratensammlung
  H.P. Balfanz
  IRS-W-8 (December 1973)
- Systems Reliability Service

Discussion

Mr. Vesely commented that the interpretation of the U.S.N.R.C. policy as expressed in section 5 on page 2.9 of the sub-group report (SINDOC(77)129) was not entirely correct. U.S.N.R.C. does not compute a lower boundary to system unavailability because no data are available. Only an upper bound is computed, and the actual unavailability cannot be demonstrated. He said that there could be political problems with such misinterpretations, and requested that the section be modified. Mr. Vesely also referred to his previous comment during discussion of the Fessenheim system where he indicated a difference between WASH 1400 data and that used in the assessment for circuit breakers. Mr. Volta stated taht there was good agreement between the data used and that derived from the German MRR Source.
Mr. Green requested that any problems related to data values be included in the detailed discussions on the second day.

SINDOC(77)131

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

WORKING GROUP OF EXPERTS ON RARE EVENTS IN COMMON MODE FAILURE ANALYSIS

Presented by A.J. Bourne

1. INTRODUCTION AND SCOPE OF STUDY *

In the quantified reliability analysis of any complex engineering system an often significant and sometimes dominant aspect is a phenomenon that is commonly known as 'common-mode failure". This is particularly so with such systems as automatic protective systems in nuclear power stations where high reliability is required. The analysis of common-mode failure can be difficult, because of the various considerations in the analysis such as:-

(a) The recognition of the many possible causes of common-mode failures, and the means of their detection.

(b) The models used in the quantification of system reliability due to common-mode failures.

(c) The use of data from reported common-mode failures or other sources for the reliability assessment of other systems.

(d) The possible rarity of common-mode failure events.

There is therefore a definite requirement to study further this reliability problem to produce more effective solutions for use in reliability analyses, and also in design processes, than have previously been available. An initial part of this current study has been a survey of the available literature on this subject from which further study has proceeded.

The scope of the study is mainly concerned with automatic protective systems for nuclear power plant. This is because these are the type of system in which common-mode failure problems are known to occur, the experience is much greater, and requirements have been identified for further studies in this area. However, aircraft and chemical plant systems have also been considered, and this report contains a preliminary analysis of data and information from all three sources.

Although the term "common-mode failure" is commonly used internationally, it has been found necessary for this study to define the type of system to which they apply, to define the term itself, and to classify the events according to type. However because of the limitations of the scope of the study, these definitions and classifications might not be appropriate for all applications.

2. COMMON-MODE FAILURES IN SYSTEMS

2.1 REDUNDANCY SYSTEMS

Systems are frequently designed which employ redundancy and output voting techniques to achieve some desired reliability. These techniques are usually applied at a sub-system or major component level rather than fundamental component level. The important criterion in a decision on the application of redundancy are the relative reliabilities of the sub-system or component, and that required for the system.

This can either be standby or active redundancy; uniform or diverse redundancy; and the simple general form of redundancy system is illustrated on Figure 1. Complex systems can consist of many combinations of this simple form.

---

* Note

This is a summary of the complete interim report of the common-mode failures sub-group (document SINDOC(77)98).

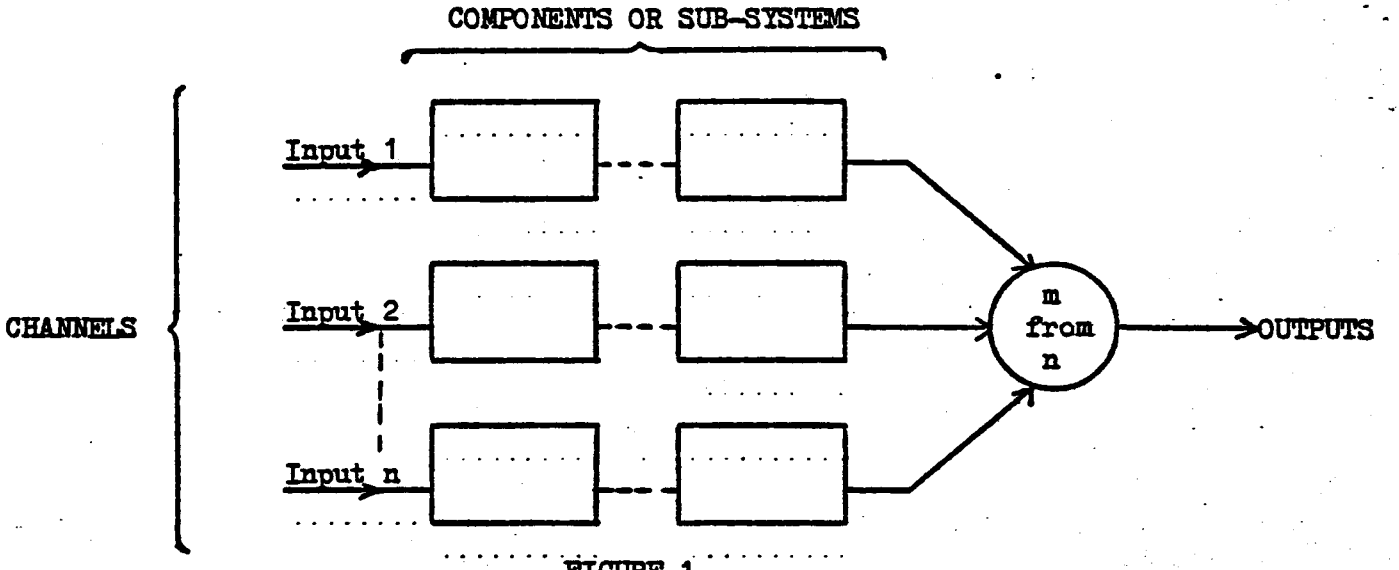


FIGURE 1

2.2 COMMON MODE FAILURES

Systems using redundancy techniques can tolerate a certain number and/or types of failures while continuing to maintain the required relationship between input and output conditions. This is so when the failures are of individual components independently, but these systems are vulnerable to what are generally termed"common-mode failures".

The types of event that can be identified as common-mode failures which lead to the system failing to perform its intended function, for the purposes of this study are:-

(a) The coincidence of failures of two or more identical components in separate channels of a redundancy system, due to a common cause. (The failures will probably have a common failure mode also.)

(b) The coincidence of failures of two or more different components in separate channels of a redundancy system due to a common cause. (The failures will possibly have different failure modes but all will be in the same category.)

(c) The failures of one or more components which result in the coincidence of failures of one or more other components not necessarily of the same type, as the consequence of some single initial cause. (The primary and secondary failures might also be coincident, and any coincident failures might have different failure modes but all will be in the same category.)

(d) In any of the above cases, the failures can be at the same instant or at different times, but at some time the failed states will be coincident.

(e) The failure of some single component or service which is common to all channels in an otherwise redundancy system, (e.g., a common power supply; maintenance). This only includes components or services which are an integral part of the system and on which system operation is dependent.

The category of the failure mode is usually either dangerous or safe, but failures can also have negligible effects and be categorised as neutral.

For some systems any failure mode might be considered as dangerous, for example, as in some aircraft systems. A dangerous failure can be defined as a failure which prevents the required operation of the system or component such that some hazard external to the system is caused or could not be prevented. A safe failure can be defined as a failure which causes the system to operate in a manner which ensures that the external plant or environment is in a safe state. A failure can be complete, such that there is a total loss of the required function, or it may be only a partial failure causing the system to function outside specified limits.

2.3 PROPOSED DEFINITION OF COMMON MODE FAILURES

From the identification of the types of event that are considered as common-mode failures a definition of this phenomenon must include a reference to the cause of failure of separate channels of a redundancy system being common. For the purposes of this study the definitions offered in the available literature do not seem to be adequate in this respect, and so the following definition is proposed by the sub-group as an attempt to summarise explicitly and comprehensively the significant characteristics of these events.

> "A common-mode failure (CMF) is the result of a single event which causes a coincidence of failure states of components in two or more separate channels of a redundancy system, leading to the defined system failing to perform its intended function."

With the scope of this study being mainly concerned with nuclear reactor automatic protective systems, events which cause DANGEROUS common modes of failure of the redundant components, or cause the failure modes to be in a common dangerous category, are of primary interest.

2.4 COMMON-MODE FAILURE CAUSES

Common-mode failures are not usually considered as random independent events occurring within the system, but as influences on the system from some source which is common to the redundant components, resulting in some abnormal output state. This is indicated by figure 2. To study this phenomenon it is necessary to define more explicitly what is included in the system, and what is excluded to be considered as possible causes of common-mode failure, or common influences on the system.

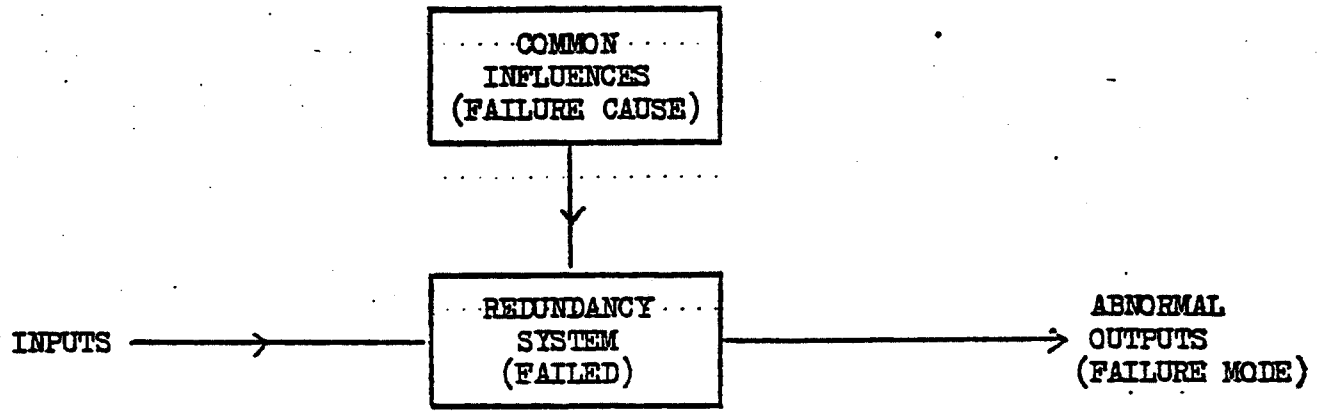


FIGURE 2

3. CLASSIFICATION OF COMMON-MODE FAILURES

3.1 REQUIREMENTS OF A CLASSIFICATION SYSTEM

It is essential for the identification, quantification and minimisation of the effects on a system, of common-mode failures, that these events are classified according to some characteristic that they all possess. There are three main requirements for the general study of common-mode failures and it is therefore necessary to form a classification system which is compatible with all these.

(a) The recognition of the many possible causes of common-mode failures, to assist designers and operators to minimise their rate of occurrence and effects, and to increase the probability of their detection.

(b) To assist with the reliability analysis of a system, and the quantification of system reliability due to common-mode failures.

(c) To enable data from reported common-mode failures to be analysed and recorded for subsequent application in the design, operation and reliability assessment of other systems.

3.2 PROPOSED CLASSIFICATION OF COMMON-MODE FAILURES

From the literature survey, preliminary examination of data for nuclear reactor protection systems, reactor emergency core cooling systems, and other safety applications, and the requirements for a classification system defined in section 3.1, the proposed classification system is as summarised in figure 3.

The significant feature of the system is that common-mode failures are classified by cause of failure, because it is considered that if recommendations are to be made for a policy of prevention of common-mode failures then it is essential that all causes can be prominently identified. This basis of classification is also the basis of the proposed definition in section 2.3.

The binary subdivision of CMF causes was evolved from the initial interpretation of the literature classification systems with further considerations of the different stages in the lifetime of an engineering system and the various influences to which it is subjected. It has not been contrived to form what is probably not a necessary feature of a classification system, but it is considered that such symmetry could be advantageous in its application and use. It is unlikely that any further sub-classification below the third level would provide any advantage, but would probably suffer from serious disadvantages, particularly with regard to the collection and application of data. To enable detailed events to be more readily recognised and classified a list of types of causal event and factors contributing to causal events, are listed under each of the eight classes of CMF. An identification code has been allocated to each class for simplified reference purposes based on the initial letters of the classification terms used.

The classifications can also be grouped according to the characteristics of the event, and the time at which it is introduced into the system, which will be particularly relevant when considering the defences against CMF's. (See Table 2).

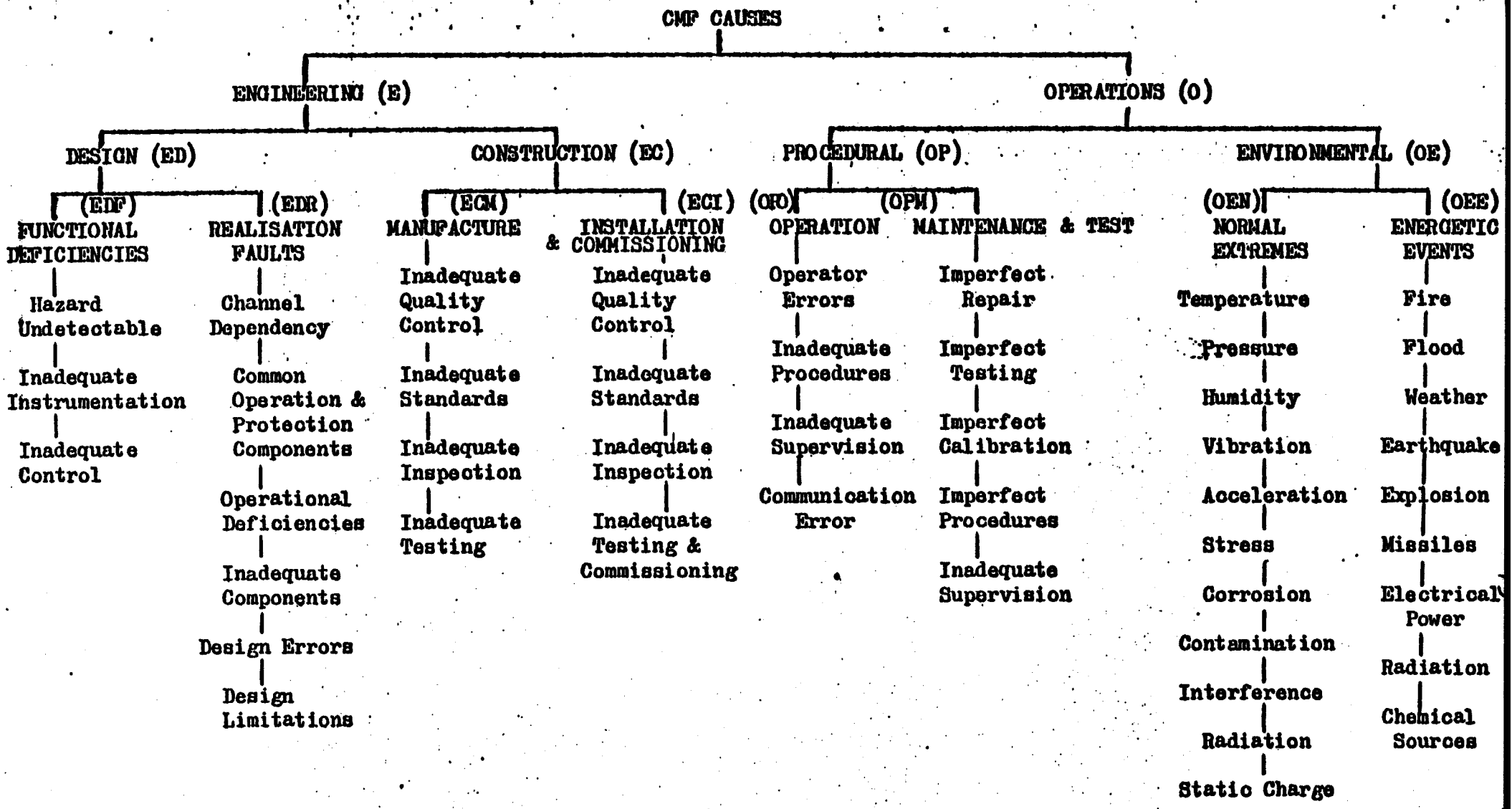


FIGURE 3 PROPOSED CLASSIFICATION SYSTEM FOR COMMON-MODE FAILURES

4. DEFENCES AGAINST COMMON-MODE FAILURES

This section contains references to other authors' work, with interpretations and summaries by the sub-group. Further work is required to enable recommendations to be made to designers and operators.

No author has identified all the possible defences explicitly, and it is surprising that some of the defences have not been more commonly recognised. To some extent this might be because of the method of presentation where the defences have been clearly described and tabulated (3)(4)(5)(14)(19)(36), or they are contained in the text of the reference (7)(17)(18)(23). It will also be due to the different systems of failure classification.

In Table 1 an initial attempt has been made to combine the defences recognised by the different authors into common classifications and where possible to relate these to the failure cause they are defending against. As with the recognition of the defences referred to above, this relationship is explicitly stated or has required a search of the text to establish. In other references the defences are quoted, but no such relationship is given. GANGLOFF (3) and EAMES (23) are probably the extremes of the two methods of presentation. GANGLOFF gives a very brief description in general terms with an explicit tabulation of the relationship between failure cause and defence. EAMES gives a detailed classified list of reliability principles for all design and operational stages of a protective system, but only implicity relates these to the failure causes in some instances.

5. SYSTEM MODELLING FOR COMMON-MODE FAILURES

The work in this section of the report is in abeyance. It is expected that it will initially consist of a literature survey and an identification of the required future work.

6. COMMON-MODE FAILURE DATA

6.1 COMMON-MODE FAILURES IN NUCLEAR REACTOR SYSTEMS

The most extensive source of data relevant to this study is from commercial nuclear power stations in the United States. This is a system operated by the "Office of Operations Evaluation" of the USNRC which requires the stations to submit reports of abnormal safety related occurrences. These were initially known as "Abnormal Occurrence Reports", but are currently known as "Licensee Event Reports". Data is extracted from letters or other written reports of events, and translated and classified by the USNRC for recording on its computer system files. The data for this study has been taken from the computer printouts of these events that are issued monthly, and are for the period 1971 to 1976 inclusive, for all the US commercially operating power stations. For the period considered there are 60 stations with an integrated operating life since achieving criticality of approximately 220 reactor-years. This has yielded approximately 8000 occurrence reports, of which 118 have been identified as common-mode failures of the two systems considered in the study, the automatic protective system (APS) and the emergency core cooling system (ECCS).

FAILURE CAUSE	FAILURE DEFENCES ACCORDING TO REFERENCE											
	PERIODIC PROOF TESTING	ADMINISTRATIVE OPERATIONAL CONTROLS	RELIABILITY ANALYSIS	GOOD OPERATIONAL INTERFACES	DESIGN DERATING & SIMPLICITY	PHYSICAL SEPARATION	FEEDBACK OF EXPERIENCE	EQUIPMENT DIVERSITY	SAFE FAILURE MODES	PROVEN DESIGN & STANDARDISATION	ADMINISTRATIVE DESIGN CONTROLS	FUNCTIONAL DIVERSITY
FUNCTIONAL DEFICIENCIES							5 7	3		5	3 5 19	3 18 5 19
DESIGN REALISATION FAULTS							5 18	5 19	3 5	5 18	3 7 5 19	3 19 5
ENGINEERING ERRORS	7	5				3 5	5 18	5 7		5 18	3 7 19	5
OPERATIONAL INFLUENCES	23	3 7 5 19 23		23	7	5 23	5	3 7 5 19		5		3 19 5
ENVIRONMENTAL EXTREMES	5 7	3				5 7	5 3	3 7 5	3 5	3 5	3 5	3 5
EXTERNAL EVENTS	7	7				5 19 7 3	5	3 7	3 7 5		3 5	3 19 5

REFERENCES

(3) GANGLOFF
(5) MANKAMO
(7) HAYDEN
(18) WASH 1270
(19) FREDERICK
(23) EAMES

TABLE 1 COMMON-MODE FAILURE CAUSES AND DEFENCES DERIVED FROM LITERATURE SURVEY

The data summarised on tables 2 and 3 show the predominance of CMF's in classes EDR and OPM, and the common significant feature of these is that they are concerned with human reliability in design, and the operational support processes of maintenance and testing. The latter is more significant in APS data where 49% of all CMF's are in this class. The problem of human reliability is further identified by the next highest contributor for both systems as class OPO, the plant operators activities. Significant by their absence are failures in class OEE, which are CMF's caused by external energetic events. This could be because greater emphasis is placed in design and construction on the defences against this type of CMF which are probably more tangible than considerations in the future of the effects of operator errors. Also, an analysis of operations procedures might not be as comprehensive and detailed as that for hardware, in a reliability assessment, possibly because the procedures would not be available at that time.

A study of plant hazards and the protection measurements which guard against them has not been included in this report but for the major hazards diversity is usually applied. No CMF's has been identified which has affected channels which have either functional or equipment diversity. They all involve identical equipment or subsystems, and it is therefore appropriate to relate the failures to the integrated operating time for all subsystems to which redundancy is applied.

The integrated operating time for both systems of both reactor types are:-

PWR 116 Reactor-years
BWR 102 Reactor-years.

	PWR	BWR	TOTAL	
APS	1970	1120	3090	Subsystem-years
ECCS	1510	1020	2530	Subsystem-years.

From these values the total CMF rate related to subsystems has been derived on table 2 as 2.10^{-2} and $2.3.10^{-2}$ per subsystem-year respectively. As an aid to comparison with data from other industries the CMF classes are grouped according to the times at which the CMF's are caused, and it is possible that only those that are caused at any time during the plant operating life are relevant to other industries. For example, many of the other CMF's that are caused during the engineering stages could possibly have been prevented by perfect testing and commissioning. It is of interest that of the 30 CMF's in the OPM class for the APS, 20 are defined as PARTIAL subsystem failures only, mainly due to calibration errors. Similar ratios can be obtained for the ECCS, for those CMF's in the EDR class, and also for all CMF's.

It is also desirable to consider the CMF rates for the different types of subsystem as defined for the APS and ECCS of both PWR's and BWR's which have been derived on table 3. For those subsystem types that have yielded a significant number of CMF's the mean rate approximates to the total CMF rates derived in table 2, but where there is relative rarity of events, particularly for the guard lines and APS output subsystems, there are some noticeable deviations. This probably means that there is less confidence in the values, and unfortunately these are the most significant subsystems in the complete system analysis. The PWR APS output subsystem CMF was a safe trip, and one of the two PWR APS guard line CMF's was for ancillary services.

CMF GROUP	CMF CLASS	APS			ECCS		
		CMF's	OPERATING TIME (SS-YRS)	CMF RATE PER SS	CMF's	OPERATING TIME (SS-YRS)	CMF RATE PER SS
CMF's CAUSED PRIOR TO OPERATION AND REMAIN UNLESS ELIMINATED BY MODIFICATION OR REPAIR	EDF EDR ECM ECI	1 12 1 3	3090	0.0055	0 19 3 2	2530	0.0095
CMF's CAUSED MAINLY AT PROOF TEST TIMES, BUT COULD BE AT ANY TIME DUE TO REPAIR. THEY WILL REMAIN UNTIL REVEALED AND REPAIRED	OPM	30	3090	0.0097	19	2530	0.0075
CMF's CAUSED AT ANY TIME DURING OPERATION AND REMAIN UNTIL REVEALED AND REPAIRED	OPO OEN OEE	5 4 0	3090	0.0029	7 3 0	2530	0.004
UNCLASSIFIED		5			4		
TOTALS		61	3090	0.02	57	2530	0.023

TABLE 2 DERIVATION OF SUBSYSTEM COMMON-MODE FAILURE RATES FOR CMF GROUPS

SUBSYSTEM TYPE	CMF CLASS	APS			ECCS		
		CMFs	OPERATING TIME SS-YEARS	CMF RATE PER SS	CMFs	OPERATING TIME SS-YEARS	CMF RATE PER SS
INPUT SUBSYSTEMS PLANT MEASURING EQUIPMENT COMPARATORS VOTING LOGIC INPUT SWITCHING	EDF EDR ECM ECI OPO OPM OEN U/C	1 11 1 3 5 31 2 4 (58)	2760	0.021	0 8 0 1 3 10 0 3 (25)	946	0.026
GUARD LINE SUBSYSTEMS VOTING LOGIC OUTPUT SWITCHING OUTPUT CIRCUIT BREAKERS	EDR OEN	1 1	116	0.017	0	218	-
OUTPUT SUBSYSTEMS CONTROL RODS VALVES & OPERATORS PUMPS & MOTORS	EDR ECM ECI OPO OPM OEN U/C	1	218	0.0046	7 3 1 4 8 3 1 (27)	1360	0.02
NOT KNOWN		-		-	5		-
TOTALS	-	61	3094	0.02	57	2524	0.023

TABLE 3 DERIVATION OF SUBSYSTEM COMMON-MODE FAILURE RATES FOR SUBSYSTEM TYPES

6.2 AIRCRAFT SYSTEMS COMMON-MODE FAILURE DATA

6.2.1 Sources and Definitions

The CAA accident records (29) have been analysed over the period 1959-75, and those due to CMF have been identified and classified. The damage states given in the recorded accidents are almost entirely classified as "substantial" or aircraft "destroyed". Consequently this CMF analysis has been concerned with failures which lead to major incidents or hazards. It is thought that these will be of primary interest and the frequency or rate of occurrence associated with them will give a point on the yardstick of rare event occurrences.

About two thirds of all aircraft accidents are due to pilot error. Most of these are due to overall mishandling or mistaken navigation of the aircraft, e.g., flying too low or in the wrong place. For the purposes of this analysis, only pilot errors which caused CMF in an individual system have been counted. Accidents involving pilot error which did not involve CMF in the aircraft systems have not been counted as CMF for the purposes of this analysis.

Sufficient data was available to identify the occurrence of a CMF causing an accident. In a low percentage of cases insufficient data was available to classify CMF. This would require much more detailed searching, since it is doubtful whether in many of these cases that the published records contain further useful information.

In a significant number of cases it was not possible to be unambiguous in the classification of CMF, so a dual classification was made. This has been generally because an environmental (energetic) occurrence has arguably been due to a design realisation limitation or functional deficiency. Usually it has been possible to decide which is the dominant cause, but the ambiguity remains.

6.2.2 Analysis of CMF Accidents

During the years through 1959 to 1975 the average proportion of all airline accidents considered, which were as identified as arising from CMF, was 4%. The variation in the yearly percentage lies between 0 and 10.3%. Apart from these extremes, the annual figures are evenly spread about the average figure.

The different types of CMF contributing to this average, according to the CMF classifications utilised, are in the following proportions:-

	CMF CLASSIFICATION	% OF TOTAL CMF	
ENGINEERING	E.DF	5.7	25%
	E.DR	19.5	
OPERATIONS	O.PO	18.7	59%
	O.PM	13.8	
	O.EN	2.1	
	O.EE	22.8	
	UNCLASSIFIED		16%

It appears that some aircraft systems are involved in CMF accidents more than others. This is indicated below.

SYSTEM	% OF TOTAL CMF	
• Engines	41	
• Flight control	21	
• Fuel systems	14	(mainly due to mismanagement)
• Landing gear	12	
• Hydraulics	6	

6.2.3 CMF Rates

The aircraft CMF accident rate $CMFR_A$ per year is given by

$$CMFR_A = \frac{\text{No. of CMF accidents}}{\text{Aircraft years}}$$

$$= \frac{\text{No. of CMF accidents}}{\text{No. of aircraft accidents}} \times \text{aircraft accident rate}$$

The aircraft accident rate per year depends on the utilisation. This is about 50% averaged over all airlines, i.e., flight hours are about 50% of total hours (probably less in the case of small airlines, but about 50% for the large airlines which generate the bulk of the traffic). Using the values produced above

$$CMFR_A = \frac{4}{100} \times 3 \times 10^{-6} \times 10^4 \times 0.5$$

$$= 6 \times 10^{-4} \text{ per aircraft-year.}$$

The good airlines will have achieved about 0.6×10^{-4} per year, but the poor organisations will be about 100 times worse than this. Thus an in-plant fatal accident rate due to CMF better than 10^{-4} per aircraft-year appears to be achievable by the best airlines.

Aircraft system CMFR ($CMFR_S$) is given by

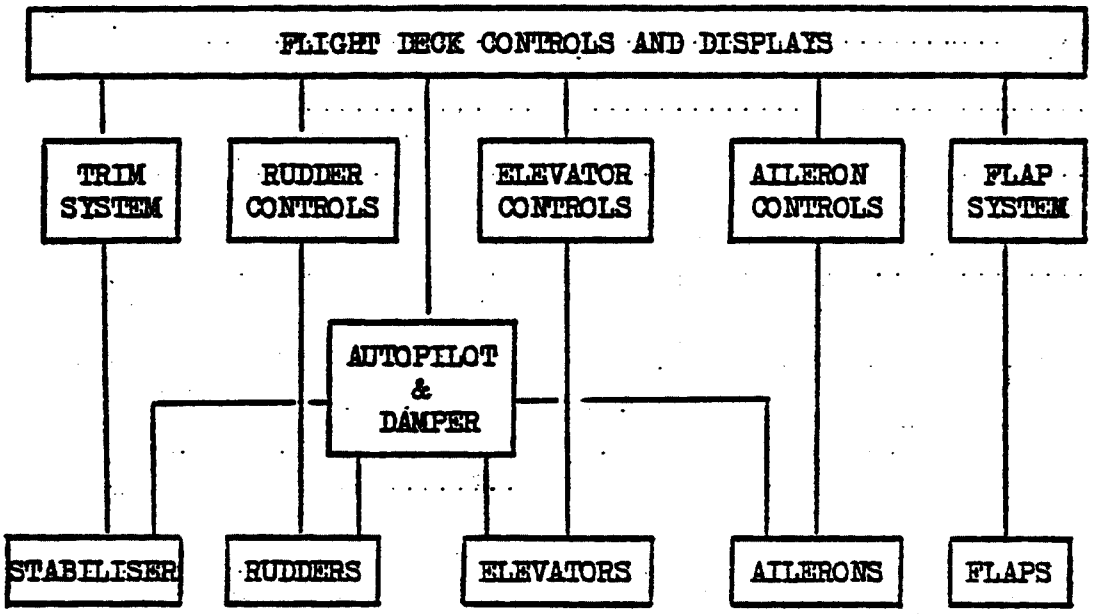
$$CMFR_S = \frac{\text{No. of system CMF}}{\text{No. of aircraft CMF}} \times CMFR_A \times \frac{1}{\text{No. of systems}}$$

Considering the flight control system as a whole

$$CMFR_{FC} = \frac{21}{100} \times 6 \times 10^{-4} \text{ overall}$$

$$= 1.26 \times 10^{-4} \text{ per system-year.}$$

Figure 4 shows a block diagram of a typical transport aircraft total flight control system (FCS).



NB. Each of the systems in an FCS is wholly or partly redundant.

FIGURE 4 FLIGHT CONTROL SYSTEM (FCS)

(The range of sophistication across the aircraft considered is in fact considerable.) It will be seen that there are basically six different systems. The average CMF rate per system is thus:-

$$CMFR_S = \frac{21}{100} \times 6 \times 10^{-4} \times \frac{1}{6} \text{ overall}$$

$$= 2.1 \times 10^{-5} \text{ per-system-year}$$

It would appear that for the best airlines a $CMFR_S$ better than 10^{-5} per subsystem-year is obtainable for high integrity control systems.

Crew flight hours average about 10^3 per year. Hence proceeding as above the CMF rate $CMFR_C$ due to crew is given by:-

$$CMFR_C = \frac{18}{100} \times \frac{4}{100} \times 3 \times 10^{-6} \times 10^3 \text{ per year}$$

$$= 2 \times 10^{-5} \text{ per crew-year}$$

Hence the best airlines probably achieve a $CMFR_C$ of about 10^{-6} per crew-year and the poorer bodies about 10^{-4} per crew-year.

/If the crew themselves were to be considered as a redundant system (in conjunction with air traffic control, since all critical flight phases involve them) the picture is somewhat different. About two-thirds of all accidents are due to crew error, hence the crew fatal error rate (CER) is:-

$$CER = \frac{2}{3} \times 3 \times 10^{-6} \times 10^3$$

$$= 2 \times 10^{-3} \text{ per crew-year./}$$

6.2.4 Discussion

Aircraft power plant suffers the most in comparison with other airborne systems from CMF. At least half of these are due to energetic events either

internally generated or extraneous. Many of these are comparable with high power rotating machines generally, e.g., overspeed failures, highly stressed part failures. Spacing and configuration are often important factors for this type of plant. There may be apparently unavoidable engineering design realisation limitations.

In the case of flight control systems the CMFR achieved is comparable and possibly better than that typically theoretically achievable with statistically independent reactor protective systems for fail dangerous condition. Most of these systems in aircraft are predominantly mechanical. Only the very latest aircraft rely predominantly on non-mechanical controls for which high standards of integrity are being demanded (including CMF). A requirement of about 10^{-6} per operating year (approx. 10^{-10} per flight hour) for dangerous failures would probably be regarded as a desirable target.

The high proportion of dual classifications (28%) confirm the relatedness of engineering design and operational environment classifications. Environmental considerations (particularly energetic events) are therefore very important in carrying out preliminary hazard analysis at the design stage.

No engineering construction cases were found, mainly because of the relatively high frequency of maintenance cycles on airline aircraft, e.g., a mean time between overhaul of about two years, also complete checkouts per flight.

7. CONCLUSIONS AND RECOMMENDATIONS

It is clear that the problem of common-mode failures is one that is inherent in the design and analysis of high reliability redundancy systems, and from the literature surveyed, during this study, it is a problem that is given serious consideration. However there has been found some lack of a uniform and comprehensive definition, and it was therefore thought necessary to define the term itself, the systems which they effect, and the type of events which can occur in those systems. The most significant feature of the definition of the term "common-mode failure" is that the initial event that causes the failure is common in addition to the effect or the mode of failure being common. Only one reference defined the term "common-cause failures", which was similar to other definitions, but it is not at this stage recommended that this term be adopted because it does not have the world-wide understanding that the subject term of this study has.

The events included within the general definitions proposed are from so varied a range that, as most references had done, it was necessary to group the events into a much reduced number of separate classes according to some characteristic of the events. With the exception of one reference which had different unique objectives, the classification characteristic of the events was the common cause of failure. It was decided to adopt this as the basis of a classification system because it identifies the primary event, the definition of common-mode failures is also based on their cause, and one of the objectives of this study is to make recommendations for the minimisation of these events. The classification system that has been proposed has been developed from that which was derived from the literature survey and so it is considered that it should generally be acceptable. It was necessary in this study to make this development so that the system was comprehensive, and identified and segregated the different activities and influences to which an engineering system is subjected during its lifetime, from conception to the completion of operation.

The study has been biassed towards automatic protective systems and emergency core cooling systems for nuclear reactors, but it has also included experience from the aircraft industry. Although to some extent this might be a limiting factor in the study, it is considered that the event definitions and classifications will be applicable to other types of engineered system which complies with the stated system definitions and boundaries. The above systems considered in the study have a high electronics engineering content, but they have significant electrical and mechanical engineering contents also.

It has been demonstrated in the data obtained during the study that events can be identified and classified within the proposals made. The exceptions to this were events that were recorded, but insufficient information on the initial cause or the mode of failure was available. In some cases, classification was impossible, and in others, particularly for aircraft accidents, conflicts in the interpretation of the recorded information led to dual classification. It is suggested that the adoption of definitions and classifications for common-mode failures by organisations recording failure events would lead to a better understanding of the phenomena and their quantification. In the interpretation of the recorded information there is an apparent limited awareness of the significance of the problem in high reliability systems. The significance of the common-mode failure problem in nuclear reactor protection systems is indicated by the failure rates of approximately 0.02 per subsystem-year obtained for both the automatic protection system and the emergency core cooling system of US water reactors. These values, derived on tables 2 and 3, are greater than expected, and the significant features of the data are the predominance of the human factors problem in causes of common-mode failures, the predominance of CMFs in input subsystems, and that only one event has possibly been identified which has affected diverse redundant protection.

The most significant subsystems with regard to a complete APS quantified reliability analysis are the guard lines and output equipment. Adequate experience does not exist in the US reports examined so there is an urgent need for more data to ascertain a reaslistic frequency for CMF events in these subsystems. It is also expected that different designers, hardware, systems, operators, etc., could lead to large differences in subsystem vulnerability to CMF's and so for these reasons some further study should perhaps concentrate on these subsystems.

The data from the aircraft accident records has shown a total failure rate of 6.10^{-5} CMF/aircraft-year and the significant features of these data are the predominance of human factors problems in both design and operation, and unlike the nuclear data show a large proportion of CMF's due to external energetic events (OEE). This is because of design limitations particularly on the segregation of systems and the particular operational environment. The proportion of aircraft Accidents caused by CMF's was 4%, whereas the proportion caused by crew errors generally is approximately two thirds.

To relate the data from the nuclear industry to the aircraft accidents it is necessary to consider the number of sub-systems in each of the main systems considered, and to derive CMF rates per subsystem-year. These subsystems are then roughly comparable in complexity and size, and the CMF rates are:-

nuclear APS	-	2.10^{-2} CMF/subsystem-year
ECCS	-	$2.3.10^{-2}$ " "
aircraft FCS	-	5.10^{-6} " "

These values show an apparently large factor of approximately 4.10^{-3} between the data derived from the two different sources, but when relating these values,

the operating conditions in each case must also be compared. Typically reactor protection systems are proof tested at intervals of 1 - 3 months by instruments personnel, with probably very limited supervision. Repair activities occur at any time, also with limited supervision and it has been shown that these two activities cause the greater proportion of CMF's. An aircraft is tested before every flight which will have a mean flight time of a few hours, and most significantly these tests will be independent of any repair activities and routine servicing, and are also done by the crew, with one performing the tests and another crew member witnessing against a written airworthiness certificated procedure. This will much more dependably test the system. Also because potential CMF's that are detected in these tests do not appear in the accident records the real CMF rate of aircraft systems could be greater. Additionally but not included in the accident records are those CMF's which have produced a potentially hazardous condition in an aircraft system, but which has been overcome by the use of some other diverse or standby system or by the intervention of the crew. Such comparable events in reactor protection systems appear in the records.

For a hazard to exist in a nuclear reactor a plant failure must initiate a demand on the protection system, which must then fail to operate. The hazard probability is therefore the combinational probability of these two low probability events. For an aircraft, the moment it leaves the ground it is in a potentially dangerous state, and so there will be a significant probability that if a CMF occurs it will cause an accident. Therefore, for a particular hazard probability an aircraft sub-system must have greater immunity to causes of CMF, and it is suggested that the higher standard of testing helps to achieve this. From table 4 it can be seen that approximately 84% of CMF's could be eliminated from reactor systems by perfect testing, whilst it is estimated that only 13% of aircraft systems CMF's could be eliminated in this way.

It has not been possible in the timescale of the study up to the writing of this report to include any work on systems analysis and modelling with respect to CMF's. This is the next essential requirement for the quantification of the problem in systems reliability analysis. This will initially consist of a survey of the currently available literature on the subject, and the identification of requirements for further study.

Identified from this study as definite requirements for further consideration are the organisational and human factors problems in both design and operating activities. It is recommended that the defences against common-mode failures be studied and more closely related to the causes of the events. Continuing from this it is recommended that guideline documents are produced for both designers and operators, so that they are made aware of the problems, and the techniques that are available for their elimination or the minimisation of their effects. These two activities should not be considered independently, but should enable each organisation to appreciate the problems of the other.

There is an urgent need for more data on CMF's although a useful start has been made in the data collected during this study. Other possible sources of data which are being examined are the British French and German nuclear power reactors and the British chemical industry, but other sources need to be identified and exploited to supplement these limited quantities. Reference 2 has applied CMF data in a study of US power reactor safety and an analysis of these could be of significant benefit to this study.

REFERENCES

1. G. E. APOSTOLAKIS "Effect of a certain class of potential common-mode failures on the reliability of redundant systems". NUCLEAR ENGINEERING & DESIGN. VOL. 36, NO. 1, JAN 1976, pp 123-133.

2. USNRC "Reactor Safety Study". WASH 1400, Oct 1975.

3. W. C. GANGLOFF "Common-Mode Failure Analysis". IEEE Transactions on Power Apparatus and Systems, VOL. PAS-94, NO. 1, pp. 27-30, Jan/Feb 1975.

4. W. C. GANGLOFF & T. H. FRANKE "An Engineering Approach to Common-Mode Failure Analysis". Proceedings of Developments and Application of Reliability Techniques to Nuclear Power Plants Symposium, Paper SNI 3/9, Liverpool 1974 (SRD R41).

5. T. MANKAMO "Common-Mode Failures". Technical Research Centre of Finland, Electrical Engineering Laboratory Report 18, May 1976.

6. K. N. FLEMMING & G. W. HANNAMAN "Common Cause Failure Considerations in the Prediction of HTGR Cooling System Reliability". General Atomic Report GA-A13658, Feb 1976.

7. K. C. HAYDEN "Common-Mode Failure Mechanisms in Nuclear Plant Protection Systems". ORNL-TM-4984, Dec 1975.

8. E. P. EPLER "Common-Mode Failure Considerations in the Design of Systems for Protection and Control". Nuclear Safety, Vol. 10, No. 1, Jan/Feb 1969, pp 38-45.

9. G. VOLTA "The Common-Mode Failure Analysis". CEC ISPRA, SR76 No. 8, May 1976.

10. K. N. FLEMMING "A Reliability Model for Common-Mode Failures in Redundant Safety Systems". General Atomic Report GA-13284, Dec 1974.

11. Mme. A. CARNINO & M. GACHOT "Defaillances D'un Systeme de Protection d'un Reacteur Considerees en tant Quevenements Rares". Proceedings of Conference on Rare Events, CSNI, ISPRA, June 1976.

12. J. R. TAYLOR "Common-Mode and Coupled Failure". Danish Atomic Energy Commission, Riso-M-1826. Oct. 1975.

13. EOQC "Glossary of Terms Used in Quality Control". 3rd Edition, Rotterdam 1972.

14. I. M. JACOBS "The Common-Mode Failure Study Discipline". IEEE Transactions on Nuclear Science, Vol. NS17, No. 1, Feb 1970.

15. W. C. GANGLOFF "An Evaluation of Anticipated Operational Transients in Westinghouse Pressurised Water Reactors". WCAP 7486, May 1971.

16. J. R. TAYLOR "Design Errors in Nuclear Power Plant". Danish Atomic Energy Commission, RISO-M-1742, Sept 1974.

17. S. H. HANAUER & C. S. WALKER "Design Principles of Reactor Protection Instrument Systems". ORNL-NSIC-51, Sept 1968.

18. USAEC "Anticipated Transients Without Scram for Water Cooled Power Reactors". WASH 1270, Sept 1973.

19. L. G. FREDERICK "An Analysis of Functional Common Mode Failures in GE BWR Protection and Control Instrumentation". General Electric Co. NEDO-10189, July 1970.

20. W. BASTL "What is the Meaning of Rare Events in System Analysis?". CSNI Report No. 10, ISPRA June 1976.

21. D. E. EMBREY "Human Reliability in Complex Systems: An Overview". NCSR-R10, July 1976.

22. IEEE "General Principles for Reliability Analysis of Nuclear Power Generating Station Protection Systems". IEEE-STD-352-1975.

23. A. R. EAMES "Principles of Reliability for Nuclear Reactor Control and Instrumentation Systems". UKAEA, SRD(R)1, 1972.

24. A. E. GREEN "Safety Assessment of Reactor Systems". Nuclear Safety, Vol. 15, No. 2, March/April 1972.

25. A. E. GREEN & A. J. BOURNE "Reliability Technology". Wiley 1972.

26. A. E. GREEN & A. J. BOURNE "Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors". UKAEA Report AHSB(S)R117.

27. D. W. WILLIAMS "Common-Mode Failures in US Commercial Power Reactors". Thesis for MS degree, University of Tennessee, June 1972.

28. NUCLEAR ENGINEERING INTERNATIONAL Supplement, April 1976.

29. WORLD AIRLINE ACCIDENT SUMMARY Published by Civil Aviation Authority.

30. ICAO Accident Digest No. 17.

31. FLIGHT INTERNATIONAL 22 Jan 1975, p. 181.

32. ICAO Digest of Statistics. (Traffice Flow 1975).

33. "Destination Disaster", by Paul Eddy, Elaine Potter and Bruce Page, Sunday Times Insight Team. Hart Davis, MacGibbon, London.

34. ICAO Accident Digests.

35. DIN 25-424 Fault Tree Analysis Methods and Symbols.

36. W. ULRICH et al "Untersuchungen Der Betriebsstoerungen Bei Versagen Der Reaktorschnellabschaltung (ATWS) und Anderer Ausgewaehlter Sicherkeitseinrichtungen". MRR 163, Sept 1976.

37. H. HOERTNER et al "Kernkraftwerk Biblis Block A. Ergebnisse Der Zuverlassigkeitsuntersuchungen Fur Den Auslegungsstorfall 'Bruch Einer Kalten Hauptkuhlmitteleitung". MRR 168, Dec 1976.

38. W. VESELY "Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses". International Conference on Nuclear Systems Reliability Engineering and Risk Assessment, Gatlinburg, Tennessee, June 20-24, 1977.

Discussion

Mr Garribba asked why the proposed definition of common-mode failure was restricted to "two or more channels of a redundancy system", to which Mr Bourne replied that the study was mainly confined to automatic protective systems as required by CSNI which was also a requirement due to the restricted timescale of the work. Mr Garribba considered that the classification system could restrict the possible sources of data that could be exploited, but Mr Bourne argued that consideration of any system could result in a system similar to that presented, based as it was on the causes of failure and the design or operation stage of the system when it was introduced.

Mr Gachot referred to the classification system on figure 3 of the summary report and commented that it was most desirable that designers have a guide to the causes of CMF, but he did not understand the distinction between classes under the headings of "functional deficiencies" and "realisation faults". Mr Bourne explained that these are really differences of software and hardware, the former being the conceptual design involving the dynamic behaviour of the plant, while the latter is the translation of that into an engineered and detailed design.

Mr Vesely made comments on the CMF rates that had been derived from the U.S. NRC reports, with respect to the proportion of the recorded events being calibration errors of say 5% in the dangerous direction rather than complete sub-system failures. He suggested that the rate derived for APS could be reduced to one tenth, and for ECCS to one quarter, of the values quoted because of this. This could reduce the results if these data were applied to the Fessenheim assessment. It was subsequently indicated to Mr Vesely that the report stated that 20 of the 30 failures in the relevant classification OPM were of this type, but they had been recorded because they were in the dangerous direction and no criteria were available to decide if such errors would or would not inhibit the protective action.

Mr Volta asked whether the degree of redundancy had been considered in the U.S. data analysis. Mr Bourne confirmed that it had not, but Mr Vesely stated that it was considered in some U.S. analysis and that there was approximately a factor of three improvement for a 3 channel system compared to a 2 channel system. Mr Hensley referred to work by Taylor in a study of U.S. data that there was little difference in reliability achieved by different levels of redundancy with regard to CMF.

SINDOC(77)99

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

WORKING GROUP OF EXPERTS ON RARE EVENTS IN HUMAN ERROR ANALYSIS AND QUANTIFICATION

Presented by L.P. Goodstein

Introduction

In dealing with the reference problem of rare events in nuclear power plants, the group has concerned itself with the man-machine system and, in particular, with human error analysis and quantification. A statement of work was prepared by the chairman (1)[1] and accepted by the group at the first meeting in March. In addition, a supplementary list of questions aimed at giving some structure to the group's deliberations was generated (2). Briefly, the group was requested to review methods of human reliability prediction, to evaluate the extent to which such analyses can be formalized and to establish criteria to be met by task conditions and system design which would permit a systematic, formal analysis. It was of course clear that time and other resource constraints would restrict the group to a review and critique based on the background and experience of the members with no possibilities for conducting new studies. Therefore, it was particularly gratifying to be able to gather a working team together with a diversity of professional backgrounds and working experience. Instead of detailed exposures of a few areas, this resulted in a relatively broad coverage of the problems involved which nevertheless could be discussed within the following framework:

- Each member's position in general, based on own experience, responsibilities.

- Each member's position with regard to present methods (WASH 1400, etc.).

- Each member's conclusion and recommendations regarding the reference system at Fessenheim.

The discussions of the working group indicated a common attitude and methodological approach to the basic problems in human error analysis and quantification within the given context.

The references given in the text are listed page 105. All of these documents have been reproduced in SINDOC(77)60 (working document).

However, the group has not reached operational conclusions, but rather an agreement on the following formulations regarding key issues which should be studied in more detail with reference to a specific system in order to reach a final statement on the state of the art.

Definition of Human Error

The general definition of human error can be expressed as:

A human error occurs when human behaviour or its effect upon the system exceeds some limit of acceptability.

These limits can be stated explicitly a priori in system specifications and instructions; they can exist implicitly within standard design practices and become explicit only after the fact. In addition, acceptable limits can be subject to reinterpretation, i.e. by operators.

The human behaviour may not be the cause of the effect in question or actively involved in the accidental chain of events, but may be related to factors or conditions which enable or influence the course of events.

In practise, human behaviour outside of "acceptable" limits often can be due to unrealistic task conditions set by the designer which are incompatible with normal physiological or psychological capabilities.

From this it follows that human error is not synonomous with human guilt or fault. This point must be stressed in order to create a positive attitude among operating staff and management which will facilitate the availability of information on human factor in plant disturbances. [1]

[1] see (7) pg. 3, (5) pg. 4

Classification of Human Errors

Human error analysis and quantification and the collection of empirical data imply a scheme for classification of human errors.

The definition of the categories of such a scheme depends upon the intended use of the analysis[1]. Examples are a reliability analysis (prediction) of a specific system, a design optimalization or a post-accident analysis. Even when one specific application is considered, a simple hierarchical, exclusive classification system is unrealistic due to the flexibility of humans and the complexity of error situations. Instead, a multidimensional frame of reference in which to characterize and describe different aspects of human error situations should be created[2].

The difficulty in creating a consistent description is clearly indicated by the following possible distinctions which are essential depending on the particular point of view but which also are very interrelated.

In a given man-machine relation human errors can be due to a functional misfit between normal human functions and system demands[3]. This misfit can be due to technical or human limitations or to adaptation and learning mechanisms and can lead to systematic errors ("design errors"). Human errors can also be due to normal random inter-person or intra-person variations in human characteristics such as variations in manual precision, timing, etc. (random errors), or finally, they can be due to a sporadic change or breakdown of human behaviour (stroke, mischief, inexplicable faux pas) which has unpredictable effects. The group finds these distinctions important due to the methodological implications. However, in reality, it can be extremely difficult to utilize them in a concrete situation. As an example, the identification

[1] see (6)
[2] see (7) pg. 3
[3] see (8) for further details

of the potential for systematic errors in a particular system suffers from the lack of a frame of reference which would make it possible to relate a specific system demand or task situation to specific internal human mechanisms and their properties. Therefore, in data collection, classification of errors is made according to tasks. This means that, at the present state of the art, data on failure modes and frequencies can only be transferred between work situations and tasks which are very similar - and it cannot be explicitly defined what "similar" means[1].

In order to classify according to the origin or cause of human error[2], it is necessary to study human error and variability in relation to human psychological and physiological mechanisms (mental representation and processes, memory structures, training etc.). It is found important to have work psychological expertise involved in post incident analyses and to make detailed information from error situations available to research.

Classification according to the effect on system performance[3]: Different distinctions are drawn to evaluate the consequences of human error and to attach priorities. The effect can be related to a specified function which is not performed (errors of omission, timing errors, sequence errors) or to the performance of a not specified task (extraneous acts, errors of commission).

A coarse indication of the importance and priorities can be obtained making distinctions between fail-to-safe, fail-to-neutral and fail-to-danger characteristics of the effect of human error. The importance of the different distinctions depends upon the goal and method of the analysis.

[1] see (4) pp. 3-5, (5) pg. 4
[2] see (6) pg. 1, (7) pg. 4
[3] see (5) pg. 1

Purpose and Method of Human Error Analysis

Different methods of human error analysis are used in different stages of system design and operation.

Qualitative post-accident analysis of the causal chain of events plays an important role in identifying human error mechanisms and relating them to system properties. Such methods depend to a large extent on expert judgement and, within several areas, especially aviation, have led to an evolution of system design towards high levels of safety based on the use of norms and regulations. However, there is a tendency toward more systematic formulations using fault tree analysis etc. and an increasing use of quantification.

Regulations and norms lag behind the present rapid technological development and methods for systematic reliability and safety analysis are becoming important and effective tools for system development. Quantitative methods are used to compare alternative designs and, being relative, can accept the use of imprecise data and expert judgement to a large extent[1].

On the other hand, there is an increasing demand for a systematic verification to third persons that design targets are met - also concerning high consequence, low probability events. In these cases, expert judgement verified by references to the professional quality of the persons or groups involved would not usually be acceptable.

This raises the following fundamental question:

Which conditions must be satisfied by a technical system and the functions of its operating staff to be accessible to systematic, quantitative risk analysis by accepted methods?

Methods for systematic analysis of reliability and safety of technical systems are generally based on a breakdown of a

[1] see also (6) pg. 3

complex system into parts or components, to a level at which component properties are recognized from widespread use, so that empirical fault data can be collected. At this level then, probabilistic models of system function can be formed and the resulting reliability and safety figures for the total system can be derived.

The characteristic features of the human element of a complex system - and the very reason for his presence - such as adaptability, flexibility, inventiveness etc. do not fit into this scheme unless the work condition constrains his freedom in critical tasks.

Tentative conditions to be satisfied by systems design to allow for systematic safety analyses - which are not necessarily at the same time optimizing safety - have been suggested[1].

Necessary conditions for the use of probabilistic methods based on system decomposition (such as THERP, use of cause-consequence or fault tree analysis) to predict the probability that a specified task is performed satisfactorily are:

- there is no significant contribution from systematic errors due to redefinition of task, interference from other tasks or activities, etc. (such contributions must be identified and treated separately);

and

- the task can be broken down to a sequence of independent subtasks at a level where failure data can be obtained from similar work situations;

and

- the subtasks are cued individually by the system or by other external means, so that modification of procedure does not take place;

[1] see (8)

or

- if task cannot be broken down to independent subtasks, but is performed as one integrated whole or it is based on higher cognitive functions, then the effect of the task must be reversible and surveyed by a predictable monitoring, testing or inspection function. This can be performed by an operator task satisfying the above constraints.

In general, the probability of specific, extraneous human acts cannot be quantified. Such acts, however, can be important contributors to rare chains of events leading to accidents.

The probability of specific, abnormal events cannot be quantified unless

- it can be demonstrated that sporadic human acts are not significant contributors to the probability; if necessary by introduction of interlocks or barriers which prevent human interaction;

or

- the effects of human acts are reversible and detectable by a monitoring or safety function which can be performed by operators or automatically.

If the reliability of such barriers and safety functions can be quantified then an upper limit on the probability of the event in question can be derived.

This approach will not necessarily degrade the responsibility and opportunity for qualified decision making of the operator. It opens the possibility for a strict formalization of some critical tasks of testing, inspection and verification, while other types of tasks are left unconstrained if their

consequences for the system are reversible. In this way, high safety requirements do not necessarily imply strictly proceduralized and possibly dull work conditions. This is considered to be an important possibility which should be considered carefully.

An explicit identification of tasks which are susceptible to systematic analysis can also lead to a selective scheme for the collection of "hard failure data" which is badly needed.

Conclusions

The group wishes to emphasize the important contribution of qualitative and semi-quantitative analyses of human error situations to the evaluation of safe design of complex systems and to stress the importance of promoting a change in attitude to human error and encouraging a multidisciplinary approach to post incident analysis to assure a balanced treatment of the technical, psychological and other relevant factors.

The group also recognizes the need for an identification of the limitations of the present methods of task breakdown, human error quantification and the derivation of design criteria for work situations which are or can be made accessible to systematic verification of risk design targets. The group has tentatively formulated such a set of criteria but wishes to point out that there remain several serious methodological problems in connection with the analysis of specific work situations.

In addition, the group's brief review[1] of the testing and calibration of the Fessenheim protective system has corroborated the opinion of CEA-EDF that an optimization of the current procedures is desirable. Such a project would serve as an excellent test case for exploring and evaluating the criteria and methods discussed here.

[1] see (9), for example

Recommendations

As stated above, the group finds the task of testing the Fessenheim safety system suitable for further study but is aware of the considerable amount of work to be done. However, meaningful progress can only be expected within the current framework if the participating organizations can accept the task of undertaking sub-problems within their special fields of interest as part of a coordinated effort over a period of 1-3 years.

Such Fessenheim-related projects include:

(1) An optimization and simplification of the test and calibration of the protective system (as regards both content and frequency) by means of a technical reliability analysis performed by the instrumentation engineers.

(2) A redesign of the test situation based on a human factors evaluation. This evaluation should include a quantitative human reliability prediction based on decomposition techniques. Therefore the design will have to be based on suitable design criteria. (See pg. 7; also (5) below).

(3) A specification of the assumptions behind the reliability analysis and an evaluation of the sensitivity to changes in these (e.g., management policies, organizational factors, etc.).

(4) Design and implementation of a selective data collection system compatible with (2) for verification of the design.

These studies will involve contacts and interviews in the Fessenheim plant. In order to minimize the resistence to such studies which is commonly encountered, it will be necessary to establish a positive relationship with operational and maintenance staff as well as management.

Other more general studies which are necessary to support the specific tasks named above include:

(5) The generation of criteria for the design of work situations which will make them amenable to quantitative prediction by decompositional analysis methods (such as THERP and other similar methods based on fault tree and event analysis).

(6) An investigation of the following methodological problems:

- the completeness of methods for identification of risk potential which can be released by extraneous human acts[1].
- the effectiveness of methods for screening the design of a work situation for the potential for systematic human errors.
- the empirical verification of reliability predictions.

(7) A study of the relation between external task conditions and internal human functions and failure mechanisms.

(8) Design of selective data collection systems compatible with the established criteria together with a formulation of the conditions for the exchange of data.

[1] see (5) pg. 2

Reference Material

(1) Manus CSNI Meeting on Rare Events, Dec. 10, 1976 - Jens Rasmussen Dec. 9, 1976

(2) List of Questions - Jens Rasmussen, L.P. Goodstein, March 30, 1977

(3) Minutes of Meeting No. 1 in CSNI Group on "Human Error Analysis and Quantification", March 2, 1977

Minutes of Meeting No. 2 in CSNI Group on "Human Error Analysis and Quantification", April 20-21, 1977

Minutes of Meeting No. 3 in CSNI Group on "Human Error Analysis and Quantification", June 2-3, 1977

(4) Note for the Meeting of the CSNI Working Group on Human Error Analysis and Quantification in June 1977 at Risø - W. Preuss, dated May 30, 1977

(5) Working paper by G. Hensley, dated March 23, 1977

(6) Working paper by Dr. J. Wirstad, dated April 1977

(7) Working paper by Prof. J. Leplat, dated April 1977 (in English and French)

(8) Working paper by Jens Rasmussen on "Human Error Analysis and Quantification"

(9) Working paper for CSNI Task Force on Rare Events - Subgroup on Human Error Analysis and Quantification - Laboratoire de Physiologie du Travail et d'Ergonomie (in English and French)

(10) Working paper from Dr. A.D. Swain, Comments on "Interim Progress Report from Group on Human Error Analysis and Quantification", dated June 1977.
Note: This was received after Meeting No. 3 and has not been discussed by the group.

Discussion

The report had been presented by Mr Goodstein in the absence of Mr J. Rasmussen. Mr Vesely commented that he had discussed the report with Mr A. Swain and considered that it was very generalised. He disagreed with a statement such as "human error cannot be quantified," and considered that the report avoids the issue. He suggested that the difficulty of quantification should be recognised, but it is still possible. Mr Hensley stated that the sub-group consisted of people from varied experiences who had individually considered the problem and the report was a consensus of their opinions. He did not think there was significant fundamental differences of opinion between Mr Vesely and the sub-group and he anticipated that further progress could be made in the detailed discussions on the second day.

Mr Garribba suggested that relationships between human factors and other disciplines should be investigated, for example, cybernetics, ergonomics, where data are available.

Mr Hensley stated that the sub-group would consider how the operators could cause the complete system to fail, and generally there would be more than one line of protection against failures. During the short timescale of the study it was inevitable that the report would be pessimistic, and he referred to the particular difficulties of the decomposition task of the Fessenheim system because of the long and complex test procedures.

Mr Hunns asked if the problem of recognition of combinations of failures had been considered, and Mr Goodstein replied that this was referred to in the report, but the techniques for quantifying other than simple sequential operations are not available.

Mr Green asked if the sub-group consider that moving towards more automation of procedures is the solution to human error problems.

Mr Hensley considered that the problem would never be eliminated, but removed to a different level. There would still be a requirement for

testing and maintenance, and some form of monitoring system requiring testing.

Mr Vesely informed the meeting that data are being planned to be collected on complex situations involving sequential operations from U.S.A. sources; and could be available within a year. He considered that absolute accuracy is not essential and factors of 2 error for example can be of no great significance.

SINDOC(77)132

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

WORKING GROUP OF EXPERTS ON STATISTICS AND DECISION THEORIES APPLICABLE TO RARE EVENTS

Presented by G. Morlat

PROBABILISTIC APPROACH TO RARE EVENTS : SOME THEORETICAL THOUGHTS*

1. A DEFINITION PROBLEM

Let us first ask a few questions - naive or insidious ones : what is a rare event ? This expression has become of common use to designate incidents to nuclear reactors. Why ask a statistician for the methods applicable to the study of rare events rather than ask him what are the methods applicable to the study of incidents to nuclear reactors ? One shall first state a few hypotheses with respect to this second question. This could simply be an euphemism, used so as to avoid mentioning mishaps the consequences of which are taken, a priori, as being unacceptable. But this is the case of engineers' discourse and this interpretation must be rejected : they were accused enough of being immune to the human consequences of their technical realizations so as not to suspect them with this hypocrisy. One must rather look for the causes of this vocabulary in two directions : a historical reason and a methodological back thought. The historical reason is as follows : one thought in the past being able to deal with the problem of major mishaps to nuclear reactors by attempting making them impossible to occur. This is the so-called "barriers" theory, which will be summarized by the following over-simplification : rupture of the first barrier (the fuel can) is little frequent - simultaneous rupture of the second barrier (the reactor's vessel) is highly improbable - and the compounded rupture of the third barrier is a practically impossible occurance. This theory realized a more-or-less acceptable first modelization inasmuch one could accept both the strength of the barriers and the independence of their respective rupturings. These hypotheses not being rigorously ascertained, one must accept the possibility of an accident (entailing radioactive release) and study it as an event the probability of which must be rendered small enough for the nuclear reactors' technology to become acceptable. This historic train of thoughts makes it rather normal for the attention to be focused on any type of rare events and not specifically on reactor mishaps. Now here is the methodological back

* The complete report is given in SINDOC(77)133.

thought : if one refers to methods applicable to rare events, one may well imagine that these methods have been proven, or could be proven, in a wide scope of situations, and if these methods are satisfactory for miscellaneous problems (related to rare events), one will naturally trust them more to solve a specific problem (nuclear reactor mishaps). It is legitimate to be cautious about ready-made methods, especially when one can fear (or hope) that no actual check will be practically possible.

It is thus for perfectly legitimate reasons that we are asked the question on methods applicable to rare events. But let us return to the first question : what is a rare event ?

We must acknowledge that defining a rare element by "an event the probability of which is very small" is highly unsatisfactory - mainly for two reasons : the first one is that this definition cannot be issued before having agreed upon a specific probabilistic model, and the statistician is indeed asked to suggest probabilistic methods, thus models, for the study of "rare events". The second reason is that once a probabilistic model is selected, the events which occur are usually of a very small probability : for a probability law with continuous density along the actual line, the probability for any special result from an observation is nil ! Thus, small-probability events are not being in cause when one speaks of rare events.

The discussions which occured within the group of experts on statistical methods and on the theory of decision as applied to rare events led to a certain agreement to consider that when one talks of rare events, he in fact refers to events the consequences of which are serious. This might seem paradoxical since the decision theory shows that an action must be appreciated by means of a kind of convolution between the events' probabilities and the impacts of the consequences (mathematical expectation utility in the classical form). Theory thus leads to distinguish, with some strictness, between the set of events (exterior to the decision maker) and the set of consequences of his actions. If one accepts that "rare event" means "event with serious consequences", he recognizes that the word "rare" which apparently is a characteristic of the events in fact designates events liable to lead to specific consequences. If one was to remain there, the expression "rare event" should be considered as being a figure of speech meaning "event able to lead to serious consequences and to which the decisions taken must allow alloting a very small probability". In fact, if one wants to fully apply the decision theory to the options

taken in the field of nuclear safety, one should be more radical and consider that the expression "rare event" actually simply means "serious consequence". Indeed, a reactor mishap must not be considered as an event (as meant in the decision theory) but as a consequence (resulting from the compounding of exterior events and of the decisions taken when designing and operating the reactor). This is the point of view which will have to be used if one wants to use, one day, the decision theory to back-up the basic options pursuant to the development of nuclear reactors. Until one is able to do this, it seems advisable not to speak of "rare events" when designating nuclear reactor mishaps : this must certainly be the expression best suited to steer thoughts along wrong paths.

On the other hand, if one considers as basic data all decisions taken with respect to the design, realization and operation of a reactor, then an accident is indeed an event (as meant in the decision theory). It remains that one is interested in "rare events" only when they may entail serious consequences. This is then a concept fairly close to the "risk" one, as defined, for instance, by Rowe in a late publication formalizing in a novel manner rather familiar ideas in the field of insurance.

"A risk is the functional combination of the occurance probability of a consequence and its value for the person taking the risk" (Rowe, An Anatomy of Risk).

2. ESTIMATING THE RISKS

The conditions under which a risk is estimated and the quality of this estimation and its accuracy depend on the value of the probability linked with the risk in question. One must note that the word "probability" only has a meaning with respect to a reference set : in nuclear safety problems, one usually speaks in terms of probability per reactor per year. A probability risk of 10^{-1} is usually well known; a probability risk of 10^{-2} is usually known and described with acceptable accuracy; things get more vague for risks of 10^{-3} : this is a highly improbable event, the accuracy with which its probability, as well as its consequences, are estimated becomes poor. One usually tries to palliate this by reasoning about the accidents which may occur not to a single reactor but to a set of 100 reactors, even 1000 reactors or more if one reasons on a world-wide scale. One thinks then reasoning about an event liable to be observed at least once. This might not be so ... one may well imagine that when an accident occurs in one of these numerous reactors, it will be noticed afterwards that this same accident could not have occured in another

reactor and that it was caused by highly specific local conditions. It is thus absolutely wrong to recognize this as occurance of this event with a probability of 10^{-3} about which one had reasoned in the first place for the computations. This will most probably be another event no one had thought of ... see the Brown Ferry accident among others.

What has just been stated is plausible for an accident with a probability of 10^{-3}. It must be all the more applicable to events with an even smaller probability such as 10^{-4}, 10^{-5}, etc. We must stress the fact that as one moves along the ladder of small probabilities, both the probabilities and the consequences are being estimated with less and less accuracy.

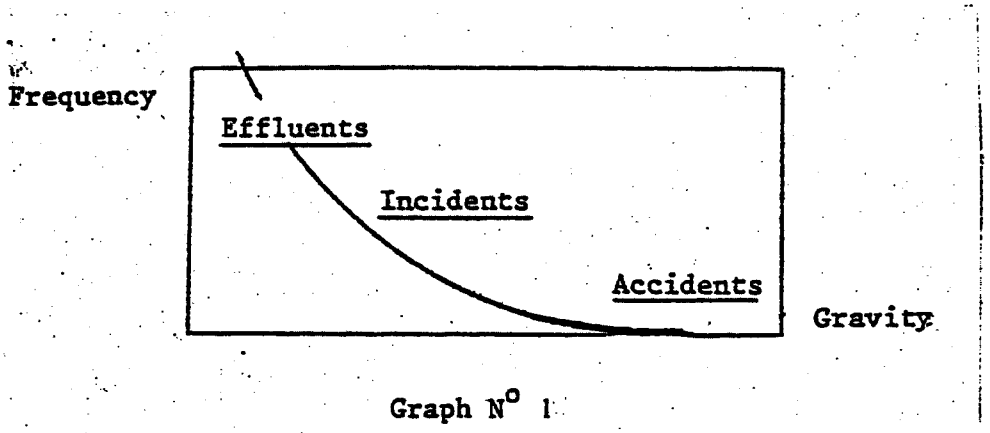
In the case of older technologies (such as large dams), it had been wisely accepted to avert only such risks the probability of which kept an acceptable meaning. This is why the flood for which the spillway gates were sized often was the once-in-a-millenium flood (although the estimation of this flood led to many sleepless nights among hydrologists). Naturally, a certain amount of sometimes high "safety coefficients" increased the safety - a dam does not necessarily rupture when subjected to a flood exceeding the capacity of the spillway gates. However, dams do rupture from time to time. This is rather often not caused by stresses larger than the ones upon which the safety computations were based, but by the occurance of an event no one had taken into consideration. (In Fréjus the rocks onto which the dam rests give way, in Vaiont a landslide ends in the lake and empties it, etc.). Such events, with serious consequences (hundreds of casualties, destroyed villages, etc.) do not lead to scrapping the technology of large dams and reconsidering the very existence of hydraulically-generated electricity.

It is easy to stress the contrast with the situation prevailing for nuclear electricity : on the one hand one often performs safety computation accounting for mishaps with a probability of 10^{-5}, 10^{-6} or even 10^{-8} and, on the other hand, one often hears that a single accident could lead to reconsidering the very existence of nuclear electricity technology. This indeed indicates that the most important aspect is evaluating the risk (perception and meaning, reaction of public opinion, etc.) probably than estimating it.

3. RISKS AND NUISANCES

One may notice that the field of nuclear safety (accidents) does not basically relate to phenomenons different from the ones relative to

standard protection against radiations : there is a continuity of events, which can be put forward if one admits the possibility of representing these events in a frequency vs. gravity graph.



Graph N° 1

One imagines characterizing by its gravity and frequency any event caused by a nuclear installation and liable to have consequences detrimental to the health or life of certain persons (one could just as well also account for material losses of all kinds). Serious and frequent events do not exist; if they would, nuclear plants would never come into being.

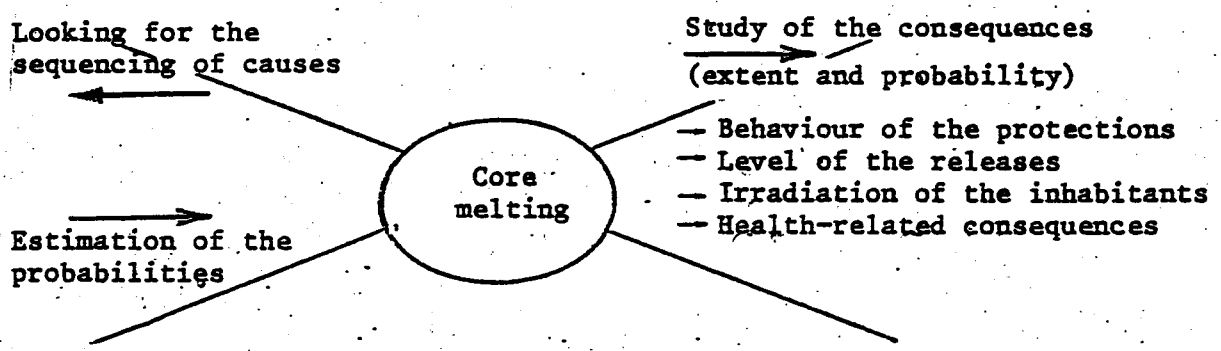
Events simultaneously little serious and little frequent are deemed as being without importance. What remains is a continuous series of events ranging from the daily release of small amounts of radioactive matter to the most serious accidents which are necessarily rare. Within these limits are found incidents with varying frequencies and moderate consequences. (Note the analogy of this representation with Farmer's curve).

It is usual to heavily look into both ends of this range to stress the specific problems entailed by estimation of the risks. As regards effluents (in small amounts), the health-related effects of radiation are hypothetical for a large part, they might even be nil as long as one remains below the levels recommended by the I.C.P.R., and this heavy uncertainty about the biological effects makes it very difficult to apply optimalization techniques to the decisions related to protection and release : this must however be subjected to much efforts so as not to have the recent recommendations of the I.C.P.R. go ineffectual.

As regards accidents, the usual train of thinking consists in specifying a given type of accident and in looking how to compute its probability.

Having defined such an accident at an intermediate level (for instance : melting of a reactor core), one first attempts defining all sequences of

events which might lead to it (moving upstreams toward the causes), then one applies this thinking in the reverse direction from an initiating event so as to evaluate the probabilities. One must note that an important phase of the work must cover everything happening downstream of the event being considered (core melting) to be able estimating the level of the possible health-related consequences and their probability.



Graph n°2

Another approach consists, starting with common operational incidents (median area of graph n°1), in asking oneself under which circumstances some of these incidents could have degenerated and led to more serious accidents : this is how one can put to best use the safety data basis - at least as much as using these data basis to directly estimate the frequency of the failures of the type in question. As has been stressed in the preceding paragraph, it is indeed important to imagine as thoroughly as possible all possible accident sequences.

4. AVAILABLE STATISTICAL THEORIES AND TECHNIQUES

It is well known that the history of statistics abounds with controversies between different schools of thought (classical and bayesian, probabilistic statistics and data analysis, etc.). Without going into these quarrels, one can consider that larger or smaller abundancy of available observations largerly controls the selection of the theory best suited to a specific problem. The correspondence could be established as follows :

Observations available	Convenient Theory
Inexistant	Decision in uncertainty
Rare	Bayesian methods
In average amount	Inductive statistics
Very numerous	Data analysis

This should not be taken as a final recommendation since the nature and quality of the physical knowledge pursuant to the phenomenon being studied must also play a part in the selection of the theory. However, it

is out of the question to perform analysis of data based on inexistant or rare observations. One can also state that a priori knowledge (prior to the observation of the phenomenon being studied) - does not play any part in the decision in uncertainty - intervene in the bayesian methods together with the data supplied by the observation - have a practically negligible influence on classical inductive statistics as proven by various authors (Halphen, Savage, de Finetti) - and are deliberately put aside in data analysis, as has been often stressed by J.P. Benzecri. One indeed sees that the range of attitudes the use of these theories implies comes together with more and more numerous observations, supplying an increasing amount of data, until becoming exclusive in the case of data analysis.

One could expect that the techniques best suited to the study of nuclear reactor accidents (rare events) be connected to the theory of decision in uncertainty or the bayesian methods (rare observations).

In fact this is not so and the main part of the statistical work in this field (extreme values, use of random processes, reliability models) are explicitly connected to classical statistics. Among the reasons able to explain this situation (and even justify it), the two following ones seem predominant to us :

1-Most of present statisticians have been schooled in classical statistics and the bayesian methods are still little widespread and developed in many universities and even less so in the technical fields.

2-When it is possible to study rare events such as conjunction (failure trees) or extrapolation (extreme values) of more frequent events, one reaches situation where rather numerous observations can be available and where one can thus apply the methods of classical inductive statistics. One certainly realized a profitable operation if the assumptions required to revert to such a situation are valid enough.

One may however be led to put aside phenomenons which lend themselves little or not at all to this type of breakdown or extrapolation. It seems to us this would suffice in justifying spending more and more effort to study the conditions for using bayesian methods in the field of nuclear reactor safety.

Discussion

Following Mr Morlat's introductory presentation and the outline of the complete report (see SINDOC(77)133) which has been read by Mr Tenaglia, Mr Garribba questioned the definition of damage as given in Chapter 2 of the report. He felt that a single factor does not suffice, for the real world problem is much more complicated and it is also very hard to include consequences. Mr Morlat replied that in decision theory one has to have a value for damage and in agreeing, Mr Tenaglia said that the following costs and the lives of people should be included as well. This could increase the damage factor by 5 or 10. Mr Schueller then queried that in optimisation it is a very common procedure to express the damage as a percentage of structural; i.e., initial costs. Mr Vesley asked if the benefits were considered : this was answered positively by Mr Tenaglia. In following up his questions, Mr Vesely wanted to know if definite criteria were addressed for design decisions and what they were. Mr Tenaglia replied that the group did not go that far into detail as insufficient time was available. But basically, these criteria are needed.
Mr Bourne expressed his opinion on that point in saying that a whole spectrum of criteria would be needed. Following these remarks, Mr Garribba queried that he saw some differences in the definition of the CMF between this group and the one which is chaired by Mr Bourne. The Chairman, Mr Green felt that the two groups should communicate on this issue.
In concluding this issue Mr Bourne said that he sees only very little difference in the definition of CMF of the two groups.
Mr Hensley drew the attention of the meeting to the fact that political decisions can affect the policy with particular reference to the energy resources of a nation. Mr Green thought that, although this might be an extremely interesting topic, this would put us outside the problems that the Task Force has been asked to study. He thanked Messrs Morlat and Tenaglia for their fine presentations.

SINDOC(77)134

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

RESEARCH SUB-GROUP ON COMMUNICATION TECHNIQUES

Presented by Mr E. Hofer

What are communication techniques?*

Communication is exchange of information, is to make information common. "Only news that is understood is information" /1/, or in other words: "Communication is possible only through a degree of novelty in a context that is familiar" /2/. Information is always structure with meaning. Therefore communication theory deals with two problem areas, namely the transmission of structures and the understanding of meanings.

Communication techniques are concerned with problems of the realization and questions of practicability and efficiency of the communication.

Technology and natural science consider especially the transmission of symbols or structures as the central problem of communication theory. Therefore communication techniques are only considered in context with the realization of the coding, the communication canal, the decoding etc. and its practicability and efficiency.

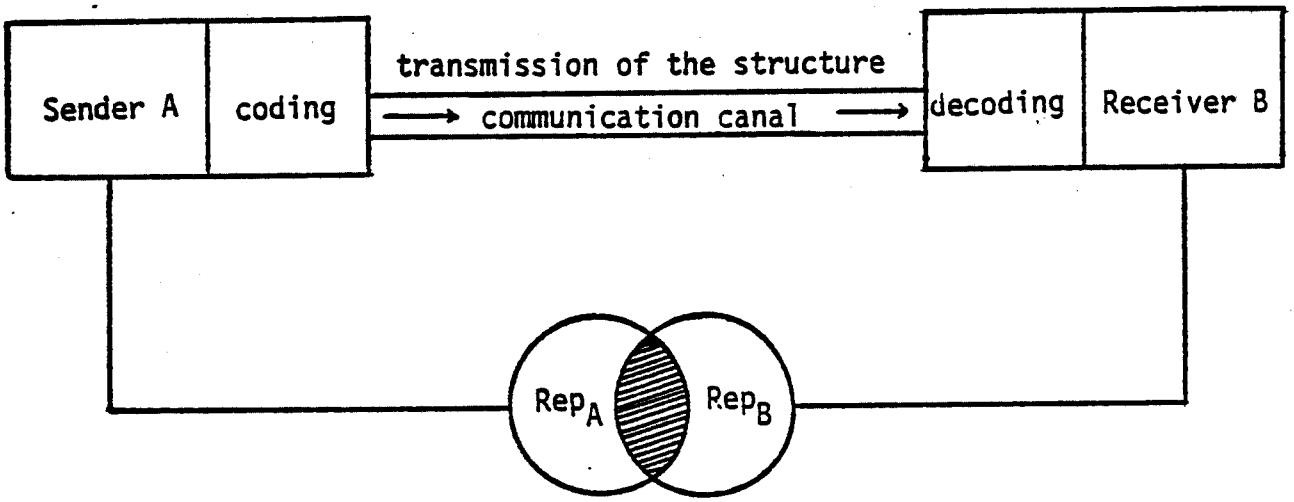


Fig. 1 Simplification of the general communication scheme by Shannon and Weaver

/1/
E.v. Weizsäcker ed., Offene Systeme I, Ernst Klett Verlag, Stuttgart, 1974;

/2/
J.R. Pierce (1972), quoted in /1/;

* The complete report is given in SINDOC(77)135

However, there is a strong tendency towards the opinion that intelligibility is the central problem since perfectly transmitted structures may be differently or even not at all understood by the receiver. This is the case if the transmitted news is not in the intersection of the repertoires (see fig. 1) which comprises the vocabulary, knowledge and experience sender and receiver have in common. Communication techniques in this aspect of communication theory are to process the news, so that it may be effectively transmitted and understood on the basis of the intersection of the repertoires.

Suppose A wants to communicate concept X to B. Depending on the degree to which X is unknown to B, A has to

i) make the background or the formulation of the problem or the idea of X comprehensible;
ii) introduce the basic variables and terms of X;
iii) introduce the basic relations between the variables and
iv) point out eventual discrepancies between X and the actual formulation of the problem.

For this purpose A will consider which parts of Rep_A (see fig. 1) may also be in Rep_B and will try to communicate the concept X on the basis of $R=Rep_A \cap Rep_B$ (intersection of the repertoires). Depending on how many and which parts of the news to be transmitted are present in R, more or less extensive techniques will be needed to communicate efficiently concept X to B. These communication techniques and their application in context with rare events in the reliability analysis of nuclear power plants are subject-matter of the work of our group. They comprise single steps like:

i) reduction of the concept (scope);
ii) simplification of the concept (complexity);
iii) decomposition of the concept (subconcepts);
iv) limitation to a special characterizing situation (model case);
v) connection to parts of R (analogies);
vi) examples (which may either explain the concept or subconcept, fully or in part, directly or indirectly by showing what is

not meant or by pointing out the situation if there were no such concept etc.);

vii) various forms of visual and acustical illustration;

viii) experiments and games (series of familiar steps with novel functional relationships and outcomes);

etc.

The single steps are elementary and in use almost since Adam and Eve. It would hardly be possible for us and definitely was not our task to add new ones. We have rather attempted to compose from single steps like the above, and to apply, communication techniques suitable for problems of rare events in the reliability analysis of nuclear power plants. For this purpose we had to make some distinction. The choice of the communication technique is influenced by

i) the news to be transmitted,

ii) the initial intersection of the repertoires and thus by the communication participants,

iii) the available communication media and finally

iv) the intended effect.

By far the largest portion of literature on communication (mainly in politics, sociology, psychology and economics) deals with communication, the intention of which is to exert influence. Our intention is not to exert influence but to achieve the highest possible degree of understanding. With respect to the communication participants we distinguish two areas of communication, referred to as C1 and C2 where C1 comprises the communication between reliability engineers and statisticians and C2 comprises the communication between reliability specialists and -nonspecialists.

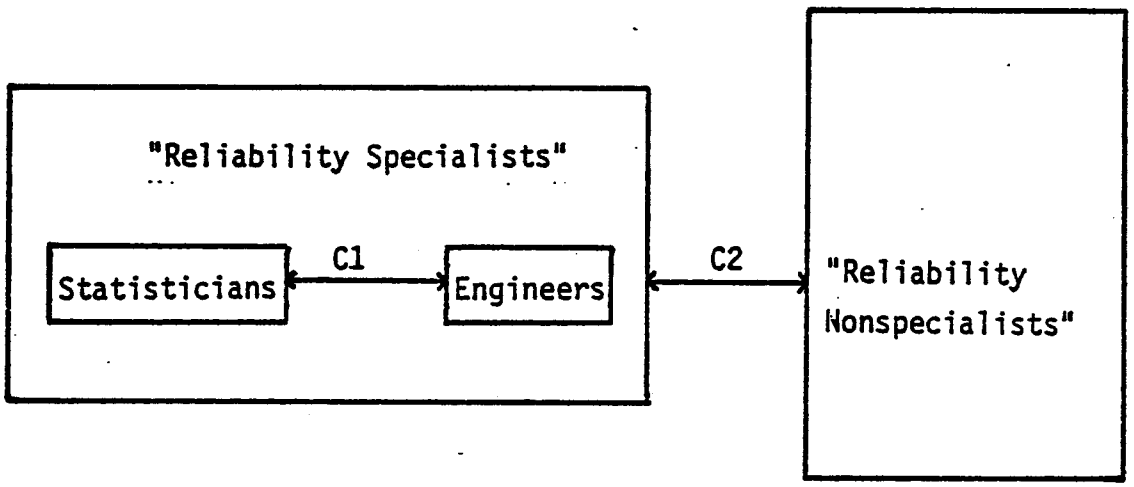


Fig. 2 Communication areas C1 and C2

Sample communications and their techniques

To demonstrate communication techniques and their application, two examples from communication area C2 have been chosen. The first deals with the term risk and the second with the meaning of small probabilities.
At the end of each of these sample communications, the communication technique used is described.

Communication efforts in communication area C1

It was considered necessary to prepare a paper on extreme value theory, using a suitable communication technique to make the basic concept, the potentials, the proper application and practical limitations transparent for non-statisticians. Unfortunately, the aim has not quite been reached in the time available. Further work will have to be done as far as the communication technique is concerned. The paper, as it stands now, has therefore been included in the work of the group dealing with statistics and decision theories.
Furthermore, a need has been seen for a short illustrative paper on the theory of fuzzy sets and logic and its application in the reliability context. The paper is included in the interim report. It presents a brief introduction of the concept of fuzzy set and logic with application to the modelling of structure functions. An example of the fuzzy set concept applicable to reactor shut-down

system design is outlined.

Quite clearly a suitable technique is required to successfully communicate the meaning of the rare event, the Task Force is engaged in. A corresponding paper has been prepared and included in the interim report. It gives an example of a true multiple-event situation which caused many fatalities and injuries. The question is posed, "On what basis is the accident mechanism categorized as a rare event?". A study of the qualitative features of the rare event idea in the hazard context is pursued. This is followed by a definition of the rare event. In conclusion, reference is made to the problem of finding an objective basis for resolving what to do about a rare event once it has been identified and quantified.

Discussion

Mr Volta asked for clarification of the terms "structure" and "repertoire" used in the report. Mr Hofer stated that they referred to the structure of the information that was being transmitted, and the repertoires of the transmitter and receiver of the information included their state of training, knowledge, experience, etc. These overlap, and this overlap must include the communicated information.

Mr Green asked how it was known if the information had been communicated correctly, by means of the diagrams in the report showing quantities of dots to represent the meaning of probability values. It was noted that no comments were made on these diagrams and no clarification requested.

Mr Bourne considered that in making a 1 in 10^4 selection the interpretation of this value might be different and dependent on the consequences. If the alternatives are desirable and undesirable extremes (e.g. wealth or death), then this could be so.

There was no available time for discussion of Mr Hunns' presentation, and this was considered by the discussion groups on the second day, (SINDOC(77)136).

GENERAL DISCUSSION ON THE PAPERS PREPARED BY THE SMALL GROUPS OF EXPERTS

Mr Hensley suggested investigating consequences which are more familiar to the general public and which are desirable rather than the opposite; for example, a large win on football pools. He also considered that there should be a search for words and phrases which can be understood by the general public, which are a large group of non-specialists receiving the category C2 of communicated information. Mr Volta commented that the term "probability" would not be in the vocabulary of many receivers, and Mr Hensley thought that terms "likelihood" and "chance" would be more universally understood. Mr Morlat referred to the general public understanding of the effects of a nuclear accident. Mr Hofer commented that communication of fuzzy logic or extreme value theory is not required for non-specialists.

Mr Tenaglia compared the problems of the continuous risk involved with fossil fuelled power stations with the rare risk of a nuclear station accident. People making political decisions must appreciate the values of these risks which makes some reference point necessary.

Mr Green referred to the problem of evaluating the β factor required for the Fessenheim assessment. Mr Vesely considered that insufficient information was available, including that from the CMF sub-group, and this aspect should receive more study by the Fessenheim sub-group. Mrs Carnino stated that their assessment indicated the significance of CMF and further work was required to identify the human factors problems that were involved.

Mr Bourne considered that the solutions of reliability problems are basically the manipulation of the problem so that it involves the consideration of events which are familiar and relatively frequent. Mr Green posed the question of whether this was possible or not in this case.

The proceedings for the first day were concluded by arranging the chairmen and membership of the three discussion groups for the second day.

PRESENTATION, CLARIFICATION AND DISCUSSION OF REPORTS FROM THREE INTERDISCIPLINARY DISCUSSION GROUPS

Guidelines (SINDOC(77)123)

The group then separated into three sub-groups, each consisting of about seven "inter-disciplinary" members. The names of the members are listed at the end of the report. The "guidelines" according to which the discussions were held are listed below :

1. What are the general methods which have emerged for investigating rare events in connection with protective systems for shutting down nuclear reactors?
2. How do you see the basic role which is developing for each of the following :
   - 2.1 Common-mode failures
   - 2.2 Human factors
   - 2.3 Statistics and decision making
   - 2.4 Communication techniques
   - 2.5 Data
3. What work requires to be undertaken and how should it be organised for the following :
   - 3.1 Common-mode failures
   - 3.2 Human factors
   - 3.3 Statistics and decision making
   - 3.4 Communication techniques
   - 3.5 Data
4. What additional points, if any, will require to be investigated and developed for electrical, mechanical, and structural systems for nuclear reactors?
5. Has the point now been reached where a specialist meeting should be considered and what form should it take?

In the following, the results of the discussions in terms of summary reports are given :

GROUP 1

The group decided to address itself first to item (1) of the "guidelines" which poses the question of "What are the general methods which have emerged for investigating rare events in connection with protective systems for the shut-down of nuclear reactors?"
It was felt that - as far as one could see it - the main problem lies in the development of capable decomposition techniques. As we have got high redundant system, the question might be posed if the fault tree analysis is the most suitable approach of all? One might consider starting a systematic search for other methods. Moreover, doubts were expressed that decomposition applies in all cases. The group then came to the conclusion that there is a similarity of problems which arise in structural engineering, that is one has to extrapolate beyond the range in which data are available. In one case one has to start from more frequent events to reach events with extremely low probability. For the latter events, there are hardly any observations available. In the other case, one starts with small crack sizes or with yield stresses, respectively. This lead the discussion into the closely related problem area of quality assurance.
The question of the role of the uncertainty factor in systems analysis was then brought up. It was suggested that one should deal with the uncertainties of the estimates, i.e., mean values. From experience, one can expect to verify some of the data and the associated logical structures used in decomposition techniques. But common modes might be involved and cannot be observed in such a way. In this case, the propagation of the uncertainty related to these common mode could give an interesting quantification of the problem. The Monte Carlo simulation method, for example, proves to be a useful tool in carrying out the analysis.
In summarizing the group could not foresee in the near future any other method beside the decomposition method. It has been agreed that one should work towards an improvement of this method in terms of investigating conditional probabilities rather than assuming independence between events. Reference has been made to CSNI Report No. 10. Improvements of the method should certainly be based upon experience.
The group then decided to discuss simultaneously items (2) and (3) of the agenda as no fundamental difference between those points could be seen.

The discussion started out with a definition of a rare event which can be described as an event with extremely low probability of occurrence. The group had realised that the definition they had used last year in the Task Force was different.
The discussion then dealt with the data collection. The group felt that when collecting data, in the case of rare events, it might prove to be useful to alsc look at the consequences which are associated with incidents and/or accidents.
The discussion then moved on as to how these incidents and/or accidents have to be recorded. It has been referred to the barrier method, to show how in regulations those events can be defined which must be reported. It has been realised that CMF had been classified in terms of mechanisms of failure by the CMF group and in terms of probability models by the Statistics group. A third classification might be envisaged, namely by the consequences or effects. Would it not be interesting to compare all these classifications? Modeling of systems is required with respect to the correlation between the random variables, as CMF are not really independent.
With reference to human factors one should include the psychological aspect of how people do behave in special cases like stress due to accidents. A quantification of this will be difficult. Quantitative analysis of this fact will always be based on expert judgement - at least to some degree. Design and maintenance human errors should be analysed differently.
In present times the public becomes more and more conscious of risk. Therefore, the improvement of communication about low probabilities with this group should be given increased attention, particularly because people became very ambiguous about statistics. This is due to the fact that results have been interpreted wrongly by people. Comparisons with other types of risks may be useful. Communication should be sought on different levels. The emotional factor should also be kept in mind as very often the public only pays attention to the consequences and not to the low probability of occurrence.

With reference to item (4), there was a discussion on the fact that initiating events should be discussed in greater depth. A study should be made, investigating the spectra of the representative sets of initiating events. Furthermore the entire chain, such as "Initiating events Protective System - Structures - Release of radioactive materials - Consequences" should be investigated globally with possible reference to cost of action in relation to risk allocation. The theory of decision can be applied for that purpose. Although it has been recognised by the group that this is a great task, it has been felt that one should start somewhere despite the fact that one has to make many assumptions in the beginning. It has also been discussed that

systems and structural reliability analysis should be used in connection with the risk allocation in licencing procedures for the future. Reference has been made to the aircraft industry where design regulations have been set up to meet a certain risk level (4 categories of situations with 3 of them leading to consequences more and more severe - probability numbers to be met being between 10^{-7} and 10^{-9}/hr of flight).
As far as item (5) is concerned, the group agreed that a specialist meeting should not be held before the end of next year, i.e., after the third year of the Task Force. The papers presented at the ANS - Meeting on "Probabilistic Reactor Safety Analysis" to be held in May, 1978 in Los Angeles should be watched, for there will be a session on very low probabilities (SINDOC(77)124).
To the report of Group 1, its chairman Mr Morlat added the following personal comments:
It seems to me more and more apparent that the natural development of the work of this Task Force on rare events, should be the investigation of some kind of cost-benefit analysis (understood in a broad sense) concerning the decisions of reactor safety. The possibility of such a research could be tested on a practical example, for example, adding or modifying some safety feature on a reactor. It would consist of comparing the cost of such a modification, with the improvement of safety which can be obtained, whatever the complexity may be. Only this kind of approach should justify the intervention of decision theory in our work, and probably clarify questions of definition. Only this kind of approach, would make it possible to integrate the results of the different specialized working groups, and finally make their work useful to the decision-maker.

GROUP 2

1. General
The method of working was to follow the "guidelines" where possible, but in many cases common topics were discussed exhaustively before proceeding to the next topic.

2. General methods that have emerged
Strong use is being made of probabilistic methodology following the use of fault trees to first identify the faults. Although qualitative statements may be helpful, they need to be backed up by quantification. However, there is a need for decision makers (e.g., regulatory bodies, politicians) to have some understanding of the terms. For redundant systems independent hardware failures do not make a dominant contribution rather, the limiting areas are

those where system performance is affected by common mode faults which include internal and external hazards. This appears to be the case for the Fessenheim reactor. One important area is that of human error which makes its first impact in the design of a system and goes through to manufacture, installation, commissioning and operation. Many of these errors should be found by test and calibration but at the same time, many errors could be introduced here.

For example, in the Fessenheim reactor, testing could take several hours. It was very complex and required people at different points with imperfect communication. Furthermore, it was found that though the system was designed so that each significant fault should be detected by at least two protective channels, in some cases only one would be effective.

For the future, it was suggested that a continuous variable approach should be considered in which the complete distribution of failures, particularly in mechanical systems should be taken into account. The complexity of cost of such a degree of sophistication was discussed and whilst it was felt that the cost could be high, the method would be more embracing with regard to potential faults.

IT IS RECOMMENDED that means of identifying and classifying common faults (as put forward by the CMF group) should be passed on to designers and other interested parties.
Considering CMFs at present it is considered that the probability of system failure for Fessenheim lies in the range of about 10^{-5} to 10^{-7}. Some value could be gained if two independent design groups were involved. Also, there is a need for validation in the future of prediction made for reactor systems.

3. Common mode faults

WASH 1400 has provided a lot of new work on CMF. Other work has been reported recently (at Gatlinburg) by such people as Fussell, Vesely, General Atomic staff, etc. Automatic programmes are being developed for common susceptibility factors.

4. Human Factors

The view was taken, almost unanimously, that the report put forward by the Human Factors group was somewhat unrealistic in asserting that quantification of human factors could not be carried out. During discussion the relevant

phrase was examined which stated that ... "in general, the probability of specific, extraneous acts cannot be quantified". By way of explanation, it was pointed out by members of the Human Factors group that this phrase was not meant to be considered in isolation but was intended to be read in the context of the adjoining text.

5. Composition of groups

It was felt that the number of groups presently formed should be reduced. Various views were expressed for 2, 3 or 4 groups, and much discussion involved the question of whether these should be advisory or working groups. In the main, it was felt that there should be a human factors group which should act in an advisory role from the point of view of assisting in the reduction of human errors and of formulating methods for the collection of appropriate data; both of single and combined tasks. Collaboration with the Fessenheim team and others actively involved in this work, such as the U.S. NRC could assist in achieving a consistent approach.

Several members felt that a "risk evaluation group" should be formed to include the "statistics and decision making", "communication techniques", "data" and possibly the CMF groups. Others felt that the "common mode" group should remain independent but with the others amalgamated. Some members felt that a structures group might be formed but overall, the group felt it had little to contribute with regard to a structures group and its work.

6. Future work and specialist meeting

The group's view was that considerable benefits would accrue from keeping the groups in existence for the next year or two. During that time, there should be enhanced communication between the groups with a common meeting being held to allow an exchange of views to assist in the interaction of this work.

It was also felt that the need for a specialist meeting could be deferred until the latter end of this period.

GROUP 3

Meaning of the term 'rare event'

It was argued that we were still without an agreed definition for 'rare event' following the presentations of Day 1. Further discussions within the group failed to produce a common total agreement. However, all did agree :

(a) the basis for the definition should not be quantitative.

(b) the "beyond experience" or "beyond consideration" ideas are an important part of the concept.

(c) the rare event of concern is the event mechanism.

There was a strong body of opinion which agreed that the concept of rare event should be independent of severity of consequence.

General methods

Analytical methods at a general level were not seen yet to have emerged. On the other hand, difficulties were very evident in the areas of event synthesis and quantification.

As a reaction against the difficulties experienced on the quantification side a trend has emerged towards extracting the maximum qualitative information from past experience. In doing this it has been notable that the 'rareness' component has often not been clearly separated. The qualitative data has been used to establish classifications and in the formulation of general 'defense' measures.

Roles of Groups and Future Work

1. Common Mode Failures Group

The group was seen to have made a praiseworthy contribution in the field of general common mode failures. Qualitative and quantitative data had emerged and a policy of "defence in the first place" had been advocated and general principles had been detailed. The group had other worthwhile areas of the problem yet to explore, particularly on the data side. Two comments are relevant. (a) So far the rare event component has not been separated from the general information. (b) Interest was expressed in the group giving attention to a more specific development of the causes to increase their use as a reference-check-list in reliability assessment.

2. Human Factors Group

The considerable difficulty of the group's work was well recognised and sympathy was felt with the decision that for the present purposes the decomposition and quantification problem should be regarded as within solution only in the very long term. The proposition to eliminate many of the potential hazard paths by the policy of restricting freedom of design in defined ways was thought to be worthy of development. However, the first level of the human factors problem in the rare event context was seen to be the identification of the error chains which lead to the undesired outcome. It was strongly hoped that the group might be prepared to look again at this problem area. The possibility was suggested of attempting to classify the factors which comprise event chains and to attempt to find some ground rules which describe how they can link together, perhaps with a view to harnessing a computer to carry out a systematic search of all combinational possibilities. On the data side it is suggested that the group might consider proposing methods of generating or collecting human factors data at the event chain factor level.

3. Statistics and Decision Making Group

It was understood that the group had addressed themselves to two basic problem areas, namely, (a) to investigate means of specifying reliability goals in the rare event context, (b) starting with typical rare events data, to develop means of statistically modelling the event mechanisms so that their probabilities may be compared with the defined goals. Further research into the broad factors and shape reliability goals appears to be part of the future work of the group. Also, work is scheduled to continue in the study of the use of subjective judgement for the extrapolation of data.

4. Communications Techniques Group

This group sees its role in two areas, (a) within the reliability specialists, between engineers and statisticians, (b) between specialists and non-specialists (the public). While work in the first area continues to be of great importance, the second area will be playing a more important role in the future. The group recognises that the man producing ideas has two problems; (a) to generate the ideas, (b) to communicate these ideas effectively. The problem areas have much about them which is separate. The role of the group is to assist in the second problem area in whatever way is possible.

5. Data Group

The collection and analysis of data is seen as an on-going, clear-cut but difficult task. The use of the Bayesian prior approach to bolster past evidence was very much welcomed and further developments of the idea would be received with considerable interest.

Future Organisation of Groups

If it was decided to continue the work of the Task Force for a further period it was felt that there would be a need to develop stronger links between the groups. The human factors, Fessenheim and CMF groups were seen to have a great deal of common ground in their respective tasks and this particularly suggests a case for ensuring that there is a good working communication channel between these groups. This might be achieved by an increased overlap of memberships.

It was felt that there was a need for a more specific project definition so that the groups could have a clear communal objective and a full awareness of the necessary co-ordination of each others' contributions. The idea was floated of designating an emissary to travel between the groups.

Additional Points to be Investigated

(i) The study of rare events associated with large structures.

(ii) The setting-up of information systems (qualitative data banks) to contain the accounts and analyses of recorded accidents in all industries. It was seen that each nation might set up its own bank in its own language but based on a commonly agreed information and system format.

(iii) The communication of risk ideas to the public - a co-operative effort between Groups 3 and 4.

(iv) The communication of the need for reliability data to the level of employees normally at the grass-roots (at the data face) of the data collection activities in their companies. Also to the companies themselves, as a general policy - a co-operative effort between Groups 1, 2, 4 and 5.

Specialist Meeting

A specialist meeting has not been considered as desirable immediately; but at a later date.

Summary of Points of Clarification

As to the application of the Monte Carlo method in fault tree analysis it was stated that continuous distributions rather than point estimates should be used in the analysis in order to account for the uncertainties in the estimates of the failure rate. It was also stressed that the simple binary mode assessment (either failure or no failure) - although it might prove adequate for electronic systems - shows deficiencies when applied to a system with mechanical components. For these components, partial failure with regard to cracks should be considered. The continuous variable approach might be a useful tool for this purpose. In particular the extreme value theory seems to be applicable to this problem. Common mode failure classification should not only be passed on to the designer, as suggested by group 2, but also to operators and others. The opinion was voiced that CMF can only be eliminated by evaluating experiences in a systematic manner (i.e. by testing, etc.). It was added that independent failures do not make a dominant contribution to highly redundant systems as opposed to systems with low redundancy.

Arguments were exchanged on the definition of what is a rare event in the context of nuclear safety. These arguments were: relation between rare event and the event mechanism, the concept of a rare event beyond the design specification, whether a fear of the unexpected was part of what constitutes a random rare event and whether a systematic rare event has no serious consequence because it is expected, and whether or not consequences should be considered. In spite of these differences on certain aspects of rare event definition there was consensus that a formal definition was not necessary for the determination of techniques and analysis which are suitable for rare event quantification.

Doubts were raised regarding the possibility of establishing national and international data banks as proposed by discussion groups 1 and 3, this because of the confidential nature of much of the information. The problems of confidentiality had been recognized; however some members thought that bilateral international agreement could possibly be achieved if data were collected and recorded to some previously agreed guidelines. Names could be excluded. In the USA data were being planned to be collected by mandatory procedures, because voluntary methods had failed. The CMF sub-group had collected data from aircraft accident records from worldwide source which were freely available and this could be a beginning of system formulation.

Summary of Detailed Discussion

The Chairman said that the Task Force work required by CSNI during 1977 was to be related to automatic protection systems and be proposed that each of the items in the guidelines that had been used by the discussion groups should be discussed by the complete Task Force.

For item 1, Group 1 found that fault tree analysis was being used successfully for the Fessenheim assessment (the PATREC code employed Monte Carlo simulation), although it was recognized that fault tree verification from experience was still a problem. A significant aspect is CMF in the top event as in the Fessenheim assessment.

The Fessenheim assessment was made in two parts: the measuring instruments and the relay system. The assessment could be improved when human factors and CMF would be considered further and in the latter respect the CMF classification system

would be a useful aid to qualitative, and perhaps quantitative, analysis.

Group 2 had not discussed methods in detail, but did recognize the existence of methods such as fault trees. A particular recommendation was that the CMF classification work was valuable and should be made available for consideration in system design for the intention of minimisation of the CMF possibilities. The Chairman posed the question of whether or not human factors quantification methods were adequate for CMF assessment. General feeling was expressed that improvements should be made in this direction.

Group 3 was somewhat pessimistic about the adequacy of the method in relation to the Fessenheim assessment. However, more optimistic opinions were expressed that in general decomposition methods can be applicable. By protective system design policy the top event in a fault tree involves sequences of multiple events, and any system can logically be analyzed by decomposition techniques. Thus a rare event can be broken down into events which are not rare and for which data are available.

It was then agreed to treat items 2 and 3 of the guidelines together. The discussion was confined to the protective system.

Common-mode failures

The feeling was expressed that the CMF analysis was not only a problem of data but also of modeling. The chairman then injected the remark that CMF events can be qualitatively examined even if there are no data available for these events.

He also pointed out that today the emphasis is on CMF rather than on component failure analysis. It was remarked that today enough knowledge on this subject is already available to start the preparation of guidelines for the designer regarding CMF. It was pointed out that there were several papers presented on CMF analysis at the recent conference at Gatlinburg. A number of techniques - such as the multivariat, β, Markov and multiattribute - are already available. The development in this area has already progressed to such a state where many CM are quantifiable. The chairman suggested that the future work of the Task Force should concentrate on the Fessenheim reactor, where CM sub-group work has already made an initial positive impact.

Human factors

Group 1 again stressed the fact, that human errors should be examined and evaluated differently, for routine operations (testing and calibrating) and acting under stress in non-routine actions (in case of an accident). With regard to quantification the psychological aspect might turn out to be a very important factor which is difficult to quantify. Group 2 pointed out that a quantification of the effect of human error would be highly desirable and data should be collected. It was suggested that one might consider relegating people from non-routine tasks where they are not quantifiable. One should aim towards simplifying test and maintenance tasks by design and put more emphasis on CMF aspects of system design. In other words, one should really be concerned with total system effects. The role of the management of a plant should be also kept in mind.

The chairman then emphasized the positive advisory role of the human factors group to the Fessenheim plant, particularly in the area of improving testing and calibration.

Decision making and statistics

Group 1 stressed the fact that decision making methods could be applied whether, or not, decomposition methods did or did not apply.

Group 2 stressed the fact that risk evaluation techniques should be further developed. It has been also recognized that the level of acceptability should not be part of the overall problem of decision theory, although the work of the groups should be only directed towards nuclear safety. It has been suggested that title of the group should be changed to "Statistics and statistical techniques for decision making". It was felt that this group should take on an advisory role for the other groups and should therefore also focus in more detail on Fessenheim.

The chairman expressed his satisfaction about the progress of this group in particular with respect to their elaborations of extreme value theory and development of techniques for evaluating the spreading of uncertainties in the fault tree analysis.

Communication

The chairman referred to the impact that the contributions from this sub-group had made on him, and considered that the possibility of some film or other demonstration to communicate to non-specialists was of great interest. He suggested that the sub-group could only operate in an advisory role and consider problems presented by the other sub-groups.

Data

The chairman recalled that the problem of data had been reported by all of the other sub-groups. Group 1 expressed their concern about the circuit breakers data in the Fessenheim assessment, but also repeated the main problems

of CMF and human factors, which had been stressed in their report.

A reference was made to the IEEE project 500 data manual which had recently become available and also to an IAEA data committee,

Group 3 outlined the proposal that had been made previously for national data banks to common guidelines to be established, not only to record quantitative data, but qualitative information from accidents. It was considered that qualitative information was important and was also applied for human factors work.

In considering item 4 of the guidelines the chairman asked Mr. Becher to summarize the paper by Becher, Schmitt and Schuëller "On the Interaction of Systems and Structural Reliability with respect to Rare Events" (SINDOC(77)137).

Mr. Becher said that the paper tried to define the differences between systems and structures and using the Fessenheim reactor as a reference had considered the interaction of them. This was to examine the transient conditions which could be initiated and lead to vessel failure. This should be evaluated on a probabilistic basis.

The Fessenheim assessment group had included an analysis of transients which could lead to pressure vessel failure, from their own and U.S. experience of such transients. They had tried to identify those due to rare events, defined as less than 10^{-3} per year, based on considerations of possible initiating events and construction defects. Mr. Becher queried whether all possible abnormal transients including these due to interactions from the protective system, such as thermal shock, had been considered. The chairman asked that any further points arising from the paper should be communicated directly to Mr. Becher and to the CSNI Secretariat.

GENERAL DISCUSSION AND CONCLUSIONS

The chairman summarized the general situation regarding the research group and the six sub-groups. In the discussion various proposals were made for the orientation and the convergence of effort onto the Fessenheim reactor assessment.

There was a general view that it would be useful to propose finishing the work on the Fessenheim protective system during the next year and further that a review of mechanical aspects should be carried out in some parallel manner. The interaction of protective systems and other mechanical systems could well be considered.

It emerged from the discussion that the method of working by which the Research Group acted in a coordinating role could be the method of ensuring the completion of the Task Force programme within the next twelve months.

The question of holding a specialist meeting was discussed and the overall feeling was that this matter should be left until the end of the Task Force programme. On the present information it could not be visualised that a worthwhile specialist meeting could be held before that time.

It was agreed that the chairman would be considering outside the meeting, in liaison with the CSNI Secretariat, the best methods of framing the proposals for submission to the mid-November 1977 Meeting of CSNI. The chairman noted the general agreement on combining and focusing on the Fessenheim reliability assessment (as a test case) the efforts of the groups in achieving the Task Force programme. He

commented on how essential it had been to have the cooperation of CEA, EdF and Framatome in this matter and expressed the thanks of the Task Force.

The Chairman closed the meeting by expressing thanks to all members for their work in the previous year and their enthusiasm shown at this meeting and in the discussion groups. He particularly thanked Mrs. Carnino and her CEA staff for the excellent arrangements for the meeting and looked forward to further work in the future.

LISTS OF EXPERTS

PARTICIPANTS IN THE TASK FORCE MEETING

Task Force Members:

P.E. Becher
A.J. Bourne
A. Carnino
G. Edwards (Scientific Secretary)
B. Gachot
S. Garribba
A.E. Green (Chairman)
E. Hofer
G. Morlat
G.I. Schuëller (Scientific Secretary)
G. Tenaglia
R.W. van Otterloo
W.E. Vesely
G. Volta

In attendance:

J. Boutin (on behalf of Prof. A. Wisner)
J. Dubau
L. Goodstein
G. Hensley
P. Hömke
D. Hunns
P. Namy
J.P. Pagès (part time)
R. Quenée
W. Schmitt

OECD Nuclear Energy Agency:

J. Royen (Secretary)
K.B. Stadie (part time)
M. Stephens (part time)

Apologies for absence were received from A. Aitken, A.M. Freudenthal and J. Rasmussen.

INTERDISCIPLINARY DISCUSSION GROUPS

Group 1: A.J. Bourne
J. Boutin
A. Carnino
G. Morlat (Chairman)
W. Schmitt
G.I. Schuëller (Technical Secretary)
G. Volta

Group 2: B. Gachot
S. Garribba
L. Goodstein (Technical Secretary)
G. Hensley (Chairman)
P. Hömke
R. Quenée
J. Royen
R.W. van Otterloo
W.E. Vesely

Group 3: P.E. Becher (Chairman)
J. Dubau
G. Edwards
E. Hofer
D. Hunns (Technical Secretary)
P. Namy
M. Stephens
G. Tenaglia

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

SINDOC(77)67 (Rev. 1)

RESTRICTED

Paris, 5th September 1977

STEERING COMMITTEE FOR NUCLEAR ENERGY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The addresses which follow are those of the experts who participate in the work sponsored by CSNI on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants. Changes of addresses and corrections deemed necessary should be notified to Mr. Jacques Royen, Nuclear Safety Division, OECD Nuclear Energy Agency, 38 boulevard Suchet, F-75016 Paris, France as soon as possible.

ORGANISATION DE COOPERATION
ET DE DEVELOPPEMENT ECONOMIQUES

AGENCE POUR
L'ENERGIE NUCLEAIRE

SINDOC(77)67 (1ère Révision)

DIFFUSION RESTREINTE

Paris, le 5 septembre 1977

COMITE DE DIRECTION DE L'ENERGIE NUCLEAIRE

COMITE SUR LA SURETE DES INSTALLATIONS NUCLEAIRES

Les adresses qui suivent sont celles des experts qui participent aux activités patronnées par le CSIN sur les problèmes d'événements rares dans l'analyse de fiabilité des centrales nucléaires. Les changements d'adresses et les corrections jugés nécessaires devraient être signalés à M. Jacques Royen, Division de la Sûreté Nucléaire, Agence de l'OCDE pour l'Energie Nucléaire, 38 boulevard Suchet, F-75016 Paris, France dès que possible.

CSNI TASK FORCE ON PROBLEMS OF RARE EVENTS IN THE RELIABILITY ANALYSIS OF NUCLEAR POWER PLANTS

GROUPE SPECIAL DU CSIN SUR LES PROBLEMES D'EVENEMENTS RARES DANS L'ANALYSE DE FIABILITE DES CENTRALES NUCLEAIRES

Mr. Andrew AITKEN (Scientific Secretary, Secrétaire Scientifique)
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON
Substitute: Mr. Gordon T. Edwards, (same address);
remplaçant: Mr. Gordon T. Edwards, (même adresse)

Dr. Werner BASTL
Gesellschaft für Reaktorsicherheit m.b.H.
Forschungsgelände
D-8046 Garching
F.R. Germany
Tel. (089)32092260
Telex 5215110 GRS MD

Mr. Per E. BECHER
Head, Section of Reactor Engineering
Department of Reactor Technology
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Mr. A. John BOURNE
Manager, Reliability Technology
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244 ext. 214
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Mme Annick CARNINO
Service d'Etudes Techniques de Sûreté
et de Sûreté Radiologique
Département de Sûreté Nucléaire
Institut de Protection et de
Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2
F-91190 Gif-sur-Yvette
France
Tel. 9418000 ext. 2669
Telex 690641 F
ENERGAT SACLAY

Professor Alfred M. FREUDENTHAL
Department of Civil, Mechanical
and Environmental Engineering
School of Engineering and Applied Science
The George Washington University
Washington, D.C. 20052
U.S.A.
Tel. (202)6766749
Telex 578229278
(via GWU Library)

M. Bernard GACHOT
Division Sûreté Nucléaire
Service Etudes et Projets
Thermiques et Nucléaires
Direction de l'Equipement
Electricité de France
Tour EdF-GdF
Cedex 8
F-92080 Paris-la-Défense
France
Tel. 7754444
Telex EDF EPTE 610634 F

Professor Sergio GARRIBBA
Centro Studi Nucleari Enrico Fermi
Istituto di Ingegneria Nucleare
Viale G. Ponzio 34/3
I-20133 Milano
Italy
Tel. (02)2360396
Telegr. NUCLEARCESNEF
MILANO

Mr. A. Eric GREEN
(Chairman, Président)
Head of
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244
ext. 213
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Dipl.-Math. Eduard HOFER
Gesellschaft für Reaktorsicherheit m.b.H.
Forschungsgelände
D-8046 Garching
F.R. Germany
Tel. (089)32092268
Telex 5215110 GRSM D

Professor M. Ross LEADBETTER
Department of Statistics
University of North Carolina
at Chapel Hill
Chapel Hill, North Carolina 27514
U.S.A.
Tel. (919)9332308

Professeur Georges MORLAT
Conseiller scientifique
Service Informatique et Mathématiques
Appliquées
Direction des Etudes et Recherches
Electricité de France
1 avenue du Général de Gaulle
Boîte Postale 27
F-92141 Clamart
France
Tel. 6452161
Telex 270400 F EDFERIM

Mr. Jens RASMUSSEN
Electronics Department
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Dr. Gerhart I. SCHÜELLER
Lehrstuhl für Massivbau
Institut für Bauingenieurwesen III
Technische Universität München
Arcistrasse 21
Postfach 202420
D-8000 München 2
F.R. Germany
Tel. (089)286017
Telex 522854 TUMUE D

Mr. Giancarlo TENAGLIA
Direzione Centrale della Sicurezza
Nucleare e della Protezione Sanitaria
Comitato Nazionale per l'Energia
Nucleare
Viale Regina Margherita 125
Casella Postale N. 2358
I-00100 Roma A.D.
Italy
Tel. 8528
Telex 61183 NUCLIT ROMA
Telegr. TLX 61183
NUCLIT-ROMA

Professeur Dr. J. TIAGO DE OLIVEIRA
Gabinete do Secretário de Estado
Secretaria de Estado da
Investigação Cientifica
Ministerio da Educação e
Investigação Cientifica
Avenida 5-2 Outubro
Lisboa
Portugal

Mr. R.W. van OTTERLOO
Department RF
N.V. tot Keuring van Elektrotechnische
Materialen
Utrechtseweg 310
Arnhem
The Netherlands
Tel. (085)457057
Telex 45016 KEMA NL

Dr. William E. VESELY. Jr.
Probabilistic Analysis Branch
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
U.S.A.
Tel. (301)4436947
Telex 578240415 BHDA

Dr. Giuseppe VOLTA
Engineering Division
Commission of the European Communities
Euratom-Joint Research Centre
Ispra Establishment
Casella Postale N.1
I-21020 Ispra (Varese)
Italy
Tel. (0332)780131/271
Telex 38042-38058 EURATOM
Telegr. EURATOM ISPRA

OECD Nuclear Energy Agency:

Agence de l'OCDE pour l'Energie Nucléaire:

Dr. Jacques ROYEN (Secretary, Secrétaire)
Nuclear Safety Division/Division de la Sûreté Nucléaire
OECD(NEA) - OCDE(AEN)
38 boulevard Suchet
F-75016 Paris
France
Tel. 5249692
Telex 630668 AEN NEA
Telegr. NUCLAGENCE PARIS

Dr. Michael STEPHENS
Nuclear Safety Division/Division de la Sûreté Nucléaire
OECD(NEA) - OCDE(AEN)
38 boulevard Suchet
F-75016 Paris
France

Tel. 5249693
Telex 630668 AEN NEA
Telegr. NUCLAGENCE PARIS

CSNI RESEARCH GROUP ON RARE EVENTS
GROUPE CSIN DE RECHERCHES SUR LES EVENEMENTS RARES

Mr. Andrew AITKEN
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON
(Substitute: Mr. Gordon T. Edwards, same address;
remplaçant: Mr. Gordon T. Edwards, même adresse)

Mr. A. John BOURNE
Manager, Reliability Technology
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244 ext.214
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Mme Annick CARNINO
Service d'Etudes Techniques de Sûreté et de
Sûreté Radiologique
Département de Sûreté Nucléaire
Institut de Protection et de
Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2
F-91190 Gif-sur-Yvette
France
Tel. 9418000 ext. 2669
Telex 690641 F ENERGAT SACLAY

Mr. A. Eric GREEN
Head of
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
(Chairman, Président)
Tel. Warrington 31244
ext. 213
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Dipl.-Math. Eduard HOFER
Gesellschaft für Reaktorsicherheit m.b.H.
Forschungsgelände
D-8046 Garching
F.R. Germany
Tel. (089)32092268
Telex 5215110 GRSM D

Professeur Georges MORLAT
Conseiller scientifique
Service Informatique et
Mathématiques Appliquées
Direction des Etudes et Recherches
Electricité de France
1 avenue du Général de Gaulle
Boîte Postale 27
F-92141 Clamart
France
Tel. 6452161
Telex 270400 F EDFERIM

Mr. Jens RASMUSSEN
Electronics Department
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Dr. Gerhart I. SCHUËLLER
Lehrstuhl für Massivbau
Institut für Bauingenieurwesen III
Technische Universität München
Arcisstrasse 21
Postfach 202420
D-8000 München 2
F.R. Germany
(Scientific Secretary,
Secrétaire Scientifique)
Tel. (089)286017
Telex 522854 TUMUE D

Dr. William E. VESELY, Jr.
Probabilistic Analysis Branch
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
U.S.A.
Tel. (301)4436947
Telex 578240415 BHDA

Dr. Giuseppe VOLTA
Engineering Division
Commission of the European Communities
Euratom-Joint Research Centre
Ispra Establishment
Casella Postale N. 1
I-21020 Ispra (Varese)
Italy
Tel. (0332)780131/271
Telex 38042-38058 EURATOM
Telegr. EURATOM ISPRA

OECD Nuclear Energy Agency:
Agence de l'OCDE pour l'Energie Nucléaire:

Dr. Jacques ROYEN (Secretary, Secrétaire)
Nuclear Safety Division/Division de la Sûreté Nucléaire
OECD(NEA) - OCDE(AEN)
38 boulevard Suchet Tel. 5249692
F-75016 Paris Telex 630668 AEN NEA
France Telegr. NUCLAGENCE PARIS

Dr. Michael STEPHENS
Nuclear Safety Division/Division de la Sûreté Nucléaire
OECD(NEA) - OCDE(AEN)
38 boulevard Suchet Tel. 5249693
F-75016 Paris Telex 630668 AEN NEA
France Telegr. NUCLAGENCE PARIS

CSNI GROUP OF EXPERTS ON THE RELIABILITY ASSESSMENT OF THE PROTECTIVE SYSTEM OF THE FESSENHEIM REACTOR

GROUPE CSIN D'EXPERTS SUR L'EVALUATION DE LA FIABILITE DU SYSTEME DE PROTECTION DU REACTEUR DE FESSENHEIM

Mme Annick CARNINO (Chairwoman, Présidente)
Service d'Etudes Techniques de Sûreté
et de Sûreté Radiologique
Département de Sûreté Nucléaire
Institut de Protection et de
Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2 Tel. 9418000 ext. 2669
F-91190 Gif-sur-Yvette Telex 690641 F
France ENERGAT SACLAY

M. Jacques DUBAU
Service d'Etudes Techniques de Sûreté
et de Sûreté Radiologique
Département de Sûreté Nucléaire
Institut de Protection et de
Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2 Tel. 9418000 ext. 4217
F-91190 Gif-sur-Yvette Telex 690641 F
France ENERGAT SACLAY

M. Bernard GACHOT
Division Sûreté Nucléaire
Service Etudes et Projets Thermiques
et Nucléaires
Direction de l'Equipement
Electricité de France
Tour EdF-GdF
Cedex 8
F-92080 Paris-la-Défense Tel. 7754444
France Telex EDF EPTE 610634 F

M. P. NAMY
Framatome
Tour Fiat
Cedex 16
F-92084 Paris-la-Défense
France

M. R. QUENEE
Service d'Etudes Techniques de Sûreté
et de Sûreté Radiologique
Département de Sûreté Nucléaire
Institut de Protection et de Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2
F-91190 Gif-sur-Yvette
France

Tel. 9418000 ext. 2029
Telex 690641 F
ENERGAT SACLAY

CSNI GROUP OF EXPERTS ON RARE EVENT DATA COLLECTION AND ANALYSIS

GROUPE CSIN D'EXPERTS SUR LA COLLECTE ET L'ANALYSE DES DONNEES RELATIVES AUX EVENEMENTS RARES

Mr. A.B.J. AL
c/o Schnell-Brüter Kernkraftwerksgesellschaft
Postfach 1120
D-4192 Kalkar (Niederrhein 1)
F.R. Germany
Tel. (02824)3001

Mr. S. CONTINI
Società Impianti Generazione
Energia Nucleare SpA
46 Viale Europa
I-20093 Cologno Monzese (Milano)
Italy

Mr. Joseph R. FRAGOLA
Sr. Standards Engineer,
Nuclear Specialist
Standards Office
The Institute of Electrical and Electronics
Engineers, Inc.
345 East 47th Street
New York, N.Y. 10017
Tel. (212)6447960
U.S.A.

M. Bernard GACHOT
Division Sûreté Nucléaire
Service Etudes et Projets
Thermiques et Nucléaires
Direction de l'Equipement
Electricité de France
Tour EdF - GdF
Cedex 8
F-92080 Paris-la-Défense
Tel. 7754444
France
Telex EDF EPTE 610634 F

M. P. GOVAERTS
Département Environnement et
Sécurité Nucléaire
Association Vinçotte
B-1640 Rhode-Saint-Genèse
Belgique
Tel. (02)3583580
Telex 22550

M. J.F. GREPPO
Service de la Production Thermique
Direction de la Production et du Transport
Electricité de France
3 rue de Messine
F-75008 Paris
France
Tel. 7642222, 2569400
Telegr. ELECFRANCEXPLOI PARIS

Mr. Paul HOMKE
Gesellschaft für Reaktorsicherheit m.b.H.
Glockengasse 2
Postfach 101650
D-5000 Köln 1
F.R. Germany
Tel. (0221)2068-1
Telex 8881807 GRS D

Mr. T.A.W. LOW
(Provisionally, provisoirement)
Plant Engineering Department
Generation Development and
Construction Division
Central Electricity Generating Board
Barnwood
Gloucester GL4 7RS
United Kingdom
Tel. Gloucester 652222
Telex 43501

Mr. Luigi NOVIELLO
Direzione delle Costruzioni
Ente Nazionale per l'Energia Elettrica
Via G.B. Martini 3
C.P. N. 386
I-00100 Roma
Italy

Mr. J.R. TAYLOR
Electronics Department
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Mr. R.W. van OTTERLOO
Department RF
N.V. tot Keuring van Elektrotechnische
Materialen (KEMA)
Utrechtseweg 310
Arnhem
The Netherlands
Tel. (085)457057
Telex 45016 KEMA NL

Dr. Giuseppe VOLTA (Chairman, Président)
Engineering Division
Commission of the European Communities
Euratom-Joint Research Centre
Ispra Establishment
Casella Postale N. 1
I-21020 Ispra (Varese)
Italy
Tel. (0332)780131/271
Telex 38042-38058 EURATOM
Telegr. EURATOM ISPRA

CSNI GROUP OF EXPERTS ON COMMON MODE FAILURE ANALYSIS

GROUPE CSIN D'EXPERTS SUR L'ANALYSE DES DEFAILLANCES DE MODE COMMUN

Mr. Andrew AITKEN
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Mr. M. BLIN
Service d'Etudes Techniques de Sûreté
et de Sûreté Rédiologique
Département de Sûreté Nucléaire
Institut de Protection et
de Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2
F-91190 Gif-sur-Yvette
France
Tel. 9418000
Telex 690641 F ENERGAT SACLAY

Mr. A. John BOURNE (Chairman, Président)
Manager, Reliability Technology
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244 ext. 214
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Mr. Gordon T. EDWARDS
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Mr. George HENSLEY
Principal Inspector
Health and Safety Executive
Nuclear Installations Inspectorate
Branch 3
Silkhouse Court
Tithebarn Street
Liverpool L2 2LZ
United Kingdom
Tel. (051)2273621 ext. 49
Telex 628596 NUINSP G

Mr. H. HÖRTNER
System Analysis Section
Gesellschaft für Reaktorsicherheit
m.b.H.
Forschungsgelände
D-8046 Garching
F.R. Germany
Tel. (089)32091
Telex 5215110 GRSM D

Dr. LINDAUER
Abteilung Betriebstechnik
Gesellschaft für Reaktorsicherheit
m.b.H.
Glockengasse 2
Postfach 101650
D-5000 Köln 1
F.R. Germany
Tel. (0221)20681
Telex 8881807 GRS D

Mr. J.R. TAYLOR
Electronics Department
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Dr. William E. VESELY, Jr.
Probabilistic Analysis Branch
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
U.S.A.
Tel. (301)4436947
Telex 578240415 BHDA

CSNI GROUP OF EXPERTS ON HUMAN ERROR ANALYSIS AND QUANTIFICATION

GROUPE CSIN D'EXPERTS SUR L'ANALYSE ET LA QUANTIFICATION DES ERREURS HUMAINES

Mlle J. BOUTIN
Département des Sciences de l'Homme au Travail
Laboratoire de Physiologie du Travail et d'Ergonomie
Conservatoire National des Arts et Métiers
41 rue Gay-Lussac
F-75005 Paris
France
Tel. 0331827, 0338394

Mr. Len P. GOODSTEIN
Electronics Department
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Mr. George HENSLEY
Principal Inspector
Health and Safety Executive
Nuclear Installations Inspectorate
Branch 3
Silkhouse Court
Tithebarn Street
Liverpool L2 2LZ
United Kingdom
Tel. (051)2273621 ext. 49
Telex 628596 NUINSP G

Professeur J. LEPLAT
Directeur du Laboratoire de Psychologie du Travail
Ecole Pratique des Hautes Etudes
41 rue Gay-Lussac
F-75005 Paris
France
Tel. 0338394

Mr. Jens RASMUSSEN (Chairman, Président)
Electronics Department
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

Dr. Alan D. SWAIN
Systems Reliability Division 1222
Sandia Laboratories
Albuquerque, New Mexico 87115
U.S.A.

Dr. A. TIETZE
Head, Institute for Accident Research
Technischer Ueberwachungs-Verein
Rheinland e.V.
D-5000 Köln 1 Telex 8873659
F.R. Germany
(Substitutes: Mr. G. Reinartz and Mr. W. Preuss, same address;
remplaçants : MM. G. Reinartz et W. Preuss, même addresse)

Mr. Jan WIRSTAD
Head, Division of Biotechnology
Försvarets Forskningsanstalt
S-651 80 Karlstad Telex 66350 KAROLIN S
Sweden

Professeur A. WISNER
Directeur du Département des
Sciences de l'Homme au Travail
Laboratoire de Physiologie du
Travail et d'Ergonomie
Conservatoire National des
Arts et Métiers
41 rue Gay-Lussac
F-75005 Paris Tel. 0331827, 0338394
France

CSNI GROUP OF EXPERTS ON STATISTICS AND DECISION THEORIES APPLICABLE TO RARE EVENTS

GROUPE CSIN D'EXPERTS SUR LES STATISTIQUES ET LES THEORIES DE LA DECISION APPLICABLES AUX EVENEMENTS RARES

Monsieur J. LARISSE
Département A
Commission des Communautés Européennes
Euratom-Centre Commun de Recherches
Etablissement d'Ispra
Casella Postale N. 1
I-21020 Ispra (Varese)
Italie
Tel. (0332)780131/271
Telex 38042-38058 EURATOM
Telegr. EURATOM ISPRA

Professor M. Ross LEADBETTER
Department of Statistics
University of North Carolina
at Chapel Hill
Chapel Hill, North Carolina 27514
U.S.A.
Tel. (919)9332308

Professeur Georges MORLAT
Conseiller scientifique
Service Informatique et
Mathématiques Appliquées
Direction des Etudes et Recherches
Electricité de France
1 avenue du Général de Gaulle
Boîte Postale 27
F-92141 Clamart
France
Tel. 6452161
Telex 270400 F EDFERIM

Mr. David NORMAN
Generation Development and
Construction Division
Central Electricity Generating Board
Barnwood
Gloucester GL4 7RS
United Kingdom
Tel. Gloucester 652222
Telex 43501

Monsieur Jean-Pierre PAGES
Chef du Groupe Calcul et Statistiques
Service de Protection Sanitaire
Département de Protection
Commissariat à l'Energie Atomique
Centre d'Etudes de Fontenay-aux-Roses
Boîte Postale 6
F-92260 Fontenay-aux-Roses — Tel. 6571326
France

Mr. O. PLATZ
Electronics Department
Research Establishment Risø — Tel. (03)355101
DK-4000 Roskilde — Telex 43116 RITOM DK
Denmark — Telegr. RISATOM

Monsieur SAPORTA
57 rue de Vouillé - 5ème étage
F-75015 Paris
France

Mr. Giancarlo TENAGLIA
Direzione Centrale della Sicurezza
Nucleare e della Protezione Sanitaria
Comitato Nazionale per l'Energia
Nucleare
Viale Regina Margherita 125
Casella Postale N. 2358 — Tel. 8528
I-00100 Roma A.D. — Telex 61183 NUCLIT ROMA
Italy — Telegr. TLX 61183 NUCLIT ROMA

Professeur Dr. J. TIAGO DE OLIVEIRA
Gabinete do Secretário de Estado
Secretaria de Estado da Investigação
Cientifica
Ministério da Educação e Investigação
Cientifica
Avenida 5-2 Outubro
Lisboa
Portugal

CSNI GROUP OF EXPERTS ON INTERDISCIPLINARY COMMUNICATION TECHNIQUES AND TUTORIAL PROGRAMMES ON RARE EVENT PROBLEMS AND THEIR SOLUTION

GROUPE CSIN D'EXPERTS SUR LES TECHNIQUES DE COMMUNICATION INTERDISCIPLINAIRE ET LES PROGRAMMES DE FORMATION RELATIFS AUX PROBLEMES D'EVENEMENTS RARES ET A LEURS SOLUTIONS

Professor Jerry B. FUSSELL
Department of Nuclear Engineering
Nuclear Engineering Building
The University of Tennessee
Knoxville, Tennesse 37916
U.S.A.
Tel. (615)9742525
FTS 8552525

Dipl.-Math. Eduard HOFER (Chairman, Président)
Gesellschaft für Reaktorsicherheit
m.b.H.
Forschungsgelände
D-8046 Garching
F.R. Germany
Tel. (089)32092268
Telex 5215110 GRSM D

Mr. David M. HUNNS
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Safety and Reliability Directorate
Wigshaw Lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tel. Warrington 31244 ext. 260
Telex 629301 ATOMRY G
Telegr. ATEN WARRINGTON

Dr. Brian W. ROBINSON
Mond Division
Imperial Chemical Industries Limited
P.O. Box No. 7 Winnington
Northwich
Cheshire CW8 4DJ
United Kingdom
Tel. Northwich 74444
Telex ICIMONDIV NTWCH 669082
Telegr. CRESCENT NORTHWICH TELEX

Monsieur SAPORTA
57 rue de Vouillé - 5ème étage
F-75015 Paris
France

Mr. Yoshikuni SHINOHARA
Reactor Engineering Division
Japan Atomic Energy Research Institute
Tokai-mura
Naka-gun
Ibaraki-ken, 319-11
Japan
Telex 24596 JAERI J

Professor L.A. ZADEH
College of Engineering
Department of Electrical Engineering
and Computer Sciences
Computer Science Division
University of California - Berkeley
Berkeley, California 94720
U.S.A.

PRELIMINARY WORK ON THE RELIABILITY ASSESSMENT OF REACTOR STRUCTURAL COMPONENTS

TRAVAUX PRELIMINAIRES SUR L'EVALUATION DE LA FIABILITE DES ELEMENTS DE STRUCTURE DES REACTEURS

M. AVET-FLANCART
Département de Sûreté Nucléaire
Institut de Protection et de
Sûreté Nucléaire
Commissariat à l'Energie Atomique
Centre d'Etudes Nucléaires de Saclay
Boîte Postale 2
F-91190 Gif-sur-Yvette
France
Tel. 9418000
Telex 690641 F ENERGAT SACLAY

Mr. Per E. BECHER
Head, Section of Reactor Engineering
Department of Reactor Technology
Research Establishment Risø
DK-4000 Roskilde
Denmark
Tel. (03)355101
Telex 43116 RITOM DK
Telegr. RISATOM

M. COSTAZ
Service Etudes et Projets
Thermiques et Nucléaires
Direction de l'Equipement
Electricité de France
Tour EdF - GdF
Cedex 8
F-92080 Paris-la-Défense
France
Tel. 7754444
Telex EDF EPTE 610634 F

Professor Alfred M. FREUDENTHAL
Department of Civil, Mechanical
and Environmental Engineering
School of Engineering and
Applied Science
The George Washington University
Washington, D.C. 20052
U.S.A.
Tel. (202)6766749
Telex 578229278 (via GWU Library)

Dr. Winfried SCHMITT
Reaktortechnik
Kraftwerk Union Aktiengesellschaft
Hammerbacherstrasse 12 + 14
Postfach 3220
D-8520 Erlangen
F.R. Germany

Tel. (09131)181 ext. 2920
Telex 629866
Telegr. KRAFTWERKUNION ERLANGEN

Dr. Gerhart I. SCHUËLLER
Lehrstuhl für Massivbau
Institut für Bauingenieurwesen III
Technische Universität München
Arcisstrasse 21
Postfach 202420
D-8000 München 2
F.R. Germany

Tel. (089)286017
Telex 522854 TUMUE D

Dr. William E. VESELY. Jr.
Probabilistic Analysis Branch
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
U.S.A.

Tel. (301)4436947
Telex 578240415 BHDA

Vues du dîner qui a réuni les participants

quelques vues des

séances de travail

SECRETARIAT

Technical Secretariat	G. Edwards L. Goodstein D. Hunns G.I. Schuëller
Administration	G. Katz, CEA
Secretariat	A. Casseville, NEA L. Truran, NEA (CCDN)

LIST OF DOCUMENTS

SEN/SIN(76)19	Report of a Special Task Force on the Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants; 30 August 1976.
SEN/SIN(76)37	Summary Record of the Decisions and Conclusions of the 4th Meeting of the NEA Committee on the Safety of Nuclear Installations (26-28 October, 1976); 30 November 1976.
SEN/SIN(77)1	Summary Record of the Decisions and Conclusions of the 1st Meeting of the CSNI Research Group on Rare Events (10 December 1976); 10 January 1977.
SEN/SIN(77)10	Summary Record of the Decisions and Conclusions of the 2nd Meeting of the CSNI Research Group on Rare Events, (18 May 1977); 20 May 1977.
CSNI Report No. 10	Proceedings of the Task Force on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants (JRC Ispra, 8-10 June 1976).
SINDOC(77)25	An example of the fuzzy set concept applicable to the design of a reactor shutdown system and to the choice of threshold levels for scram; short note by Y. Shinohara; March 1977.
SINDOC(77)31	Fuzzy sets as a basis for a theory of possibility; L.A. Zadeh; 23 February 1977; (memorandum No. UCB/ERL M77/12).
SINDOC(77)46	CSNI Group of experts on rare event data collection and analysis; reliability data acquisition for IEC Technical Committee 45 "Nuclear Instrumentation" (TC45), Subcommittee (SC45-A) "Reactor Instrumentation", Working Group (WG A-3) of Subcommittee 45-A; J.R. Fragola.

SINDOC(77)47	Agenda proposed by the Chairman for the 2nd Meeting of the Research Group on Rare Events, Château de la Muette, Paris, 18 May 1977.
SINDOC(77)48	Programme of work of the CSNI Group of experts on the reliability assessment of the protective system of the Fessenheim reactor, January 1977.
SINDOC(77)49	CSNI Group of experts on the reliability assessment of the protective system of the Fessenheim reactor (B. Monnier).
SINDOC(77)50	CSNI Group of experts on the reliability assessment of the protective system of the Fessenheim reactor. Compte rendu de la réunion du Groupe du 18 avril 1977.
SINDOC(77)51	Preliminary programme of work of the CSNI Group of experts on rare event data collection and analysis, December 1976.
SINDOC(77)52	Programme of work of the CSNI Group of experts on rare event data collection and analysis, March 1977.
SINDOC(77)53	CSNI Group of experts on rare event data collection and analysis.
SINDOC(77)54	Programme of work of the CSNI Group of experts on common mode failure analysis, December 1976.
SINDOC(77)55	CSNI Group of experts on common mode failure analysis. Notes of the 1st Meeting of the Group, 17th February 1977.
SINDOC(77)56	CSNI Group of experts on common mode failure analysis.
SINDOC(77)57	Programme of work of the CSNI Group of experts on human error analysis and quantification, December 1976.
SINDOC(77)58	CSNI Group of experts on human error analysis and quantification.

SINDOC(77)59	CSNI Group of experts on human error analysis and quantification.
SINDOC(77)60	CSNI Group of experts on human error analysis and quantification (notes of the 3rd Meeting of the Group, 2-3 June 1977) (working document).
SINDOC(77)61	Programme of work of the CSNI Group of experts on statistics and decision theories applicable to rare events.
SINDOC(77)62	CSNI Group of experts on statistics and decision theories applicable to rare events.
SINDOC(77)63	CSNI Group of experts on statistics and decision theories applicable to rare events (notes of the 2nd Meeting of the Group, 21-22 April 1977).
SINDOC(77)64	CSNI Group of experts on interdisciplinary communication techniques and tutorial programmes on rare event problems and their solution.
SINDOC(77)65	CSNI Group of experts on interdisciplinary communication techniques and tutorial programmes on rare event problems and their solution.
SINDOC(77)66	Brief progress report on the work of US corresponding Members of the CSNI Groups of experts on rare events.
SINDOC(77)67 (Rev.1)	Lists of experts participating in the work sponsored by CSNI on problems of rare events in the reliability analysis of nuclear power plants.
SINDOC(77)75	CSNI Group of experts on common mode failure analysis. (Second Meeting of the Group, 13-14 June 1977).
SINDOC(77)76	CSNI Group of experts on rare event data collection and analysis (First Meeting of the Group - 27 April 1977).
SINDOC(77)77	CSNI Group of experts on rare event data collection and analysis (Questionnaire).

SINDOC(77)78	CSNI Group of experts on rare event data collection and analysis. Papers on data bases: - IEEE Std 500-1977 - The IEEE Reliability Data Manual for Nuclear Plant Electrical Equipment; (J.R. Fragola). - Reliability Data Bases - A Review; (L.O. Hecht and J.R. Fragola).
SINDOC(77)86	Deuxième réunion du Groupe Spécial du CSIN sur les problèmes d'événements rares dans l'analyse de fiabilité des centrales nucléaires; Ordre du Jour, 5, 6 et 7 septembre 1977, Saclay, France.
SINDOC(77)87	CSNI Group of experts on interdisciplinary communication techniques and tutorial programmes on rare event problems and their solution. Note of Dr. Y. Shinohara.
SINDOC(77)98	Interim report to the CSNI Task Force on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants of the Group of experts on common-mode failure analysis; July 1977 (working document).
SINDOC(77)99	Summary report to the CSNI Task Force on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants of the Group of experts on human error analysis and quantification; June 1977.
SINDOC(77)123	Task Force on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants. 2nd Meeting, 5-7 September 1977. "Guide Lines" for the Interdisciplinary Discussion Groups - 6th September 1977 (prepared by the Chairman of the Task Force).
SINDOC(77)124	The problems of rare events in the reliability analysis of nuclear power plants by the Special Task Force of the Committee on the Safety of Nuclear Installations (Abstract for the ANS Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety to be held at Los Angeles, California on 8-10 May 1978).
SINDOC(77)127	Centrale Nucléaire de Fessenheim - Tranches 1 et 2 ; Electricité de France ; 1976.

SINDOC(77)128 Rapport du Groupe de travail sur l'estimation de la fiabilité du système de protection du réacteur Fessenheim I; août 1977 (document de travail).

SINDOC(77)129 Report of the Group of Experts on Rare Events Data Collection and Analysis; August 1977 (working document).

SINDOC(77)130 Summary report of the Group of Experts on Rare Events Data Collection and Analysis; August 1977.

SINDOC(77)131 Summary report of the Group of Experts on Common Mode Failure Analysis; August 1977.

SINDOC(77)132 Summary report of the Group of Experts on Decision Theories and Statistics Applicable to Rare Events; August 1977.

SINDOC(77)133 Rapport du Groupe de travail sur les Statistiques et les Théories de la Décision Applicables aux Evénements Rares ; août 1977 (document de travail).

SINDOC(77)134 Summary report of the Group of Experts on Interdisciplinary Communication Techniques and Tutorial Programmes on Rare Event Problems and their solution; August 1977.

SINDOC(77)135 Interim Report of the Group of Experts on Interdisciplinary Communication Techniques and Tutorial Programmes on Rare Event Problems and their solution; August 1977.

SINDOC(77)136 The Rare Event Problem; D. Hunns; August 1977.

SINDOC(77)137 On the Interaction of Systems and Structural Reliability with Respect to Rare Events; P.E. Becher, W. Schmitt and G.I. Schuëller; 30 August 1977.