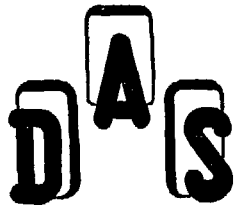
COMMISSARIAT A L'ENERGIE ATOMIQUE

INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE

DEPARTEMENT D'ANALYSE DE SURETE



RAPPORT DAS/743

EVALUATION OF THE RELIABILITY OF THE PROTECTION SYSTEM OF 1300 MWE PWR'S.

BLIN A.*

IAEA SPECIALISTS MEETING ON ANALYSIS AND EXPERIENCE IN CONTROL AND INSTRUMENTATION AS A DECISION TOOL.
Arnhem, the Netherlands, 16-19 octobre, 1990.

RAPPORT DAS/743

EVALUATION OF THE RELIABILITY OF THE PROTECTION SYSTEM OF 1300 MWE PWR'S.

BLIN A.*

IAEA SPECIALISTS MEETING ON ANALYSIS AND EXPERIENCE IN CONTROL AND INSTRUMENTATION AS A DECISION TOOL.
Arnhem, the Netherlands, 16-19 octobre, 1990.

1990

* DAS/SACP

- IAEA -

SPECIALISTS MEETING ON ANALYSIS
AND EXPERIENCE IN CONTROL AND INSTRUMENTATION
AS A DECISION TOOL

16 - 19 October 1990
ARNHEM - The Netherlands

EVALUATION OF THE RELIABILITY OF THE PROTECTION SYSTEM OF 1300 MWe PWR's

A. BLIN

Commissariat à l'Energie Atomique
IPSN/DAS
FONTENAY-AUX-ROSES - FRANCE

* * *

ABSTRACT

An assesment of the reliability of the Digital Integrated Protection System (SPIN) of the 1300 MWe type french reactors has been carried out by treating an example : the emergency shutdown, which can be called upon by several initiating events.

The whole chain, from sensors to breakers and control rods, is taken into account. The reliability parameters used for the quantification are evaluated essentially from the experience feedback of french reactors. The not wellknown parameters being the common cause failure rates of electronic components and the efficiency rate of the self-tests, the results of the study are then presented in a parametric form, according to these two factors.

1 - INTRODUCTION

The numerical techniques have been introduced in equipments of command-control of the 1300 MWe type french reactors. It is the case in particular for the Digital Integrated Protection System (SPIN) of these reactors. The aim of this paper is to give an assessment of the reliability of this system. The example hereafter treated is the calculation of the probability of failure of one of the protection command of the SPIN : the emergency shutdown.

2 - DESCRIPTION OF THE SPIN

The configuration of the SPIN has been already presented in several papers (cf. for example /1/, /2/, /3/). Schematically, the choices selected at the design of the SPIN led to the following characteristics of the whole system :

A) Redundancy of the order of 4 for the sensors.

B) Four redundant Acquisition and Processing Units for Protection (UATP) (Figures 1 and 2). Each UATP carries out all the processing steps required in preparing tripping orders for the protection functions, including :

- . the acquisition and the processing of signals emitted by the sensors,
- . the comparison of calculated results with the protection thresholds,
- . the logic processing (2/4) of tripping data for each parameter,
- . the emission of tripping orders either directly to emergency shutdown breakers (four pairs of breakers, each of them driven by 1 UATP), or to the ULS's for safety actions.

These processing operations are carried out by microprocessors.

Each UATP has a multiprocessor structure comprising autonomous units of two types :

- Functionnal Units (UF's) that carry out all digital and logic processing related to the monitoring of one or several parameters ;

- Exchange units (UE's) which handle the multiplexed links used to exchange partial tripping data between UATP's or to transmit data outside the protection system.

Each functional or exchange unit can operate independantly and is totally asynchronous with the others. The exchange of data between UF's and UE's is carried out via a shared memory network.

C) Two redundant Safety Logic Units (ULS).

Each ULS is associated with an actuation train safety drivers. It receives the tripping orders emitted by the 4 UATP's (Safety Injection, containment spray actuation, etc...) and combines them in a 2/4 logic.

The ULS's make use of fail safe wired techniques.

3 - ASSESSMENT OF THE PROBABILITY OF FAILURE OF THE SYSTEM

The SPIN is a standby device ready to operate by generating a signal as soon as it is called upon by events requiring :

- *the emergency shutdown of the reactor,*
- *and/or a safeguard action (safety injection, containment spray actuation, etc...).*

Consequently, the reliability of this system cannot be assessed as a whole. We will present, then, as an example, the evaluation of the probability of failure of the first protective function of the reactor : the emergency shutdown, according to the various initiating events which correspond to a given parameter (temperature, pressure, nuclear flux, etc...) overshooting a critical safety threshold. Each parameter is treated independantly of the others.

The study has been carried out by the CEA/IPSN and the ECOPOL Company and recently updated.

In order to obtain a more realistic assessment of the probabilities of failure, and to evaluate the relative importance of the different groups of components :

- *all the components of the complete chain : sensors, instrumentation, trip breakers, control rods assemblies, have been taken into account,*
- *moreover, common cause failures and the influence of auto-tests in the UATP's have been considered.*

3.1. Qualitative modelisation

A study had been carried out previously by FRAMATOME, to determine the reliability of the UATP's of the SPIN - /4/. This had led to a qualitative modelisation of the behaviour of these parts : decomposition into macrocomponents, and use of the ESCAF simulator /5/ to obtain the minimal cut-sets, the failures of the components being supposed independant.

This approach and the qualitative results for the UATP's have been used in the present study.

The failure of the whole system may be modelled, with a sufficient accuracy, when common cause failures are taken into account by the method of fault trees, by regrouping materials of the same type (figure 3) :

- *the failure of the sensors (instrumentation included) of the UF's and of the terminal wired logics of the UATP's, corresponds to the failure of at least 3 components of each group,*

- *the failure of the group of trip breakers corresponds to the failure of at least 4 components (the whole system of the 8 breakers does not work exactly as a 3/8 logic system, according to the diagram of the figure 1),*

- *the trip function will fail if at least 2 control rods assemblies fail to insert into the core.*

3.2. Quantification

3.2.1.

Two Probabilistic safety Assessments have been carried out in FRANCE concerning the EDF (Electricité de France) reactors : one for the 900 MWe reactors, by the CEA/IPSN (Commissariat à l'Energie Atomique / Institut de Protection et de Sûreté Nucléaire) and the other for the 1300 MWe reactors, by EDF. A reliability data base has, in particular, been set up for these studies, based on the french reactors experience. Moreover, all the failures concerning the SPIN are collected in an EDF data base, called the SRDF-A.

The failure rates of the different components of the systems (sensors, electronic and electromechanical parts, trip breakers), as well as the probabilities of human errors for entering the values of the safety thresholds into the SPIN by thumbwheels switches, used in the present study, have been taken from these two data bases /6/ (See Table 1).

3.2.2.

Several self-tests have been incorporated into the software of the SPIN : parity check, watch dog, REPROMS checksum, etc.... This allows the system to reveal certain failures of the electronic components, most but not all. Thus, it is possible to define for each component a factor of "efficiency" of the self-tests (called "f" factor in the study) which corresponds, for a given component, to the percentage of failures not revealed by the self-tests. So, the failure rate to be taken into account for a component is the unrevealed (unsafe) failure rate, which is equal to : λ **total x f.**

For the quantification of the probability of failure upon demand, the unavailability of the components were obtained by using the value of the interval between 2 tests of each UATP, equal to 4 months.

3.2.3.

The failures were not quantified as regards the software. This one is unique for the SPIN, but is submitted to well defined specifications of quality assurance and control /7/.

At the present time, the operating experience being insufficient, the not wellknown parameters are the common cause failure rate β for electronic components of the UATP's and the value of the factor f of the efficiency of the self-tests. The calculation has then been carried out by making them varying in a given range of values :

- *for the β factor of electronic components, between 10^{-1} and 10^{-4},*
- *for the f factor, a global value between 10^{-1} and 10^{-4}.*

4 - *RESULTS*

The values of the probability of failure per demand of the emergency shutdown corresponding to various initiating events considered independantly are given in the Table 2. (They correspond to a value of the β factor for the electronic parts taken equal to 10^{-3} and of the factor f of efficiency of the autotests equal to 10^{-3}).

The weight of the probability of human errors for entering the values of the safety thresholds in the UATP's by thumbwheels switches is the most important factor in the majority of cases, followed by the control rods, the trip breakers and the sensors failures.

The influence of the failures of the UATP's, with the values of β and f defined above, is at a second order of magnitude lower.

On the Figure 4, are given, as an example, the values of the probability of failure of the emergency shutdown in the case of a low level in a steam generator, for values of the parameters β and f varying in the range 10^{-2} to 10^{-4}.

Moreover, the variation of the probability of failure of the UATP's are given, Figure 5, for the same values of the parameters β and f as above, and for the same initiating event.

It may be observed on these curves, by extrapolating towards the lowest values of β, that the probability of failure of the UATP's without common cause failures, will be lower than 10^{-5}. This corresponds to the IEC 231 A guideline which specifies that for the emergency shutdown signal, the probability of failure of the electronic part of the system (not taking into account the common cause failures) should not exceed 10^{-5} per demand value. One may then conclude, that the value of the interval between tests of the UATP's, which plays a direct role in this probability of failure, (4 months between 2 tests of each UATP), is acceptable (at least for the range of values assessed for the factor f).

5 - *CONCLUSION*

This probabilistic study concerning the reliability of the SPIN has been carried out by treating an example : the emergency shutdown called upon by several initiating events, each being treated independantly of the others.

The influence of the probability of human errors for entering the values of the safety thresholds has been shown, as also the weight of the failures of the control rods, of the trip breakers and of the sensors.

The values of the reliability parameters of the different components involved have been evaluated essentially from the experience feedback of the french reactors. Nevertheless, besides the quantification of the software reliability which was not taken into account, two parameters are insufficiently known at the present time : they correspond to the common cause failures of the electronic components and to the efficiency rate of the self-tests.

.../...

6 - REFERENCES

/1/ *H. KROTOFF, C. BENSKI*
"Digital integrated protection system - Quantitative methods for dependability evaluation"
IAEA Meeting of the specialists regarding the application of the programmed digital techniques in systems of critical concern for dependability
SACLAY - November 1984

/2/ *L. REMUS, J.M. COLLING, J. BUISSON*
"Equipment line-up developed for structuring programmed digital systems important to safety"
IAEA Meeting
SACLAY - November 1984

/3/ *R. LARMINAUX, I. MACKOWIAK, H. DALLE*
"La mise en service des automates CONTROBLOC et SPIN dans les tranches nucléaires PALUEL 1 et 2"
Revue Générale Nucléaire
1986 - N° 2 - Mars - Avril

/4/ *A. ELLIA-HERVY, C. MARIE*
"Evaluation de la fiabilité d'un système de protection intégré numérique destiné à la surveillance d'un réacteur électronucléaire Optimisation de la périodicité des tests"
5ème Colloque International de Fiabilité et de Maintenabilité
BIARRITZ (FRANCE) - 1986

/5/ *A. LAVIRON et al.*
"ESCAF - A new and cheap system for complex reliability analysis and computation"
IEEE Trans. on Reliability
Vol. R 31 - N° 4 - October 1982

/6/ *ARENY, GAUTHIER, HEROU*
"Etude de l'indisponibilité de l'automatisme de protection et de sauvegarde sur demande d'action de protection"
EDF/EPS - SPIN 01 - B - 1989

/7/ *BOULCH, GRISOLLET, LE MEUR, COLLART, SEGALARD, UBERSCHLAG*
"Outil d'aide au test des logiciels de sécurité pour les centrales nucléaires"
IAEA Meeting - SACLAY - Novembre 1984

- TABLE 1 -

- RELIABILITY DATA -

- *SENSORS*

  Failure rate, instrumentation included :

. Temperature	8.10^{-7} h^{-1}
. Pressure	$2,8.10^{-6}$ h^{-1}
. Nuclear flux	$1,7.10^{-6}$ h^{-1}
. Level	$1,2.10^{-6}$ h^{-1}

- *MICROPROCESSORS MODULES* 10^{-6} h^{-1}

- *REACTOR TRIP BREAKERS (Failure to open on demand)* $3,2.10^{-4}$ d^{-1}

- *CONTROL RODS ASSEMBLIES ($\geq$ 2 not inserting on demand)* $2,8.10^{-5}$ d^{-1}

- *HUMAN ERROR RATE (unsafe) FOR ENTERING SAFETY THRESHOLDS* 6.10^{-4} d^{-1}

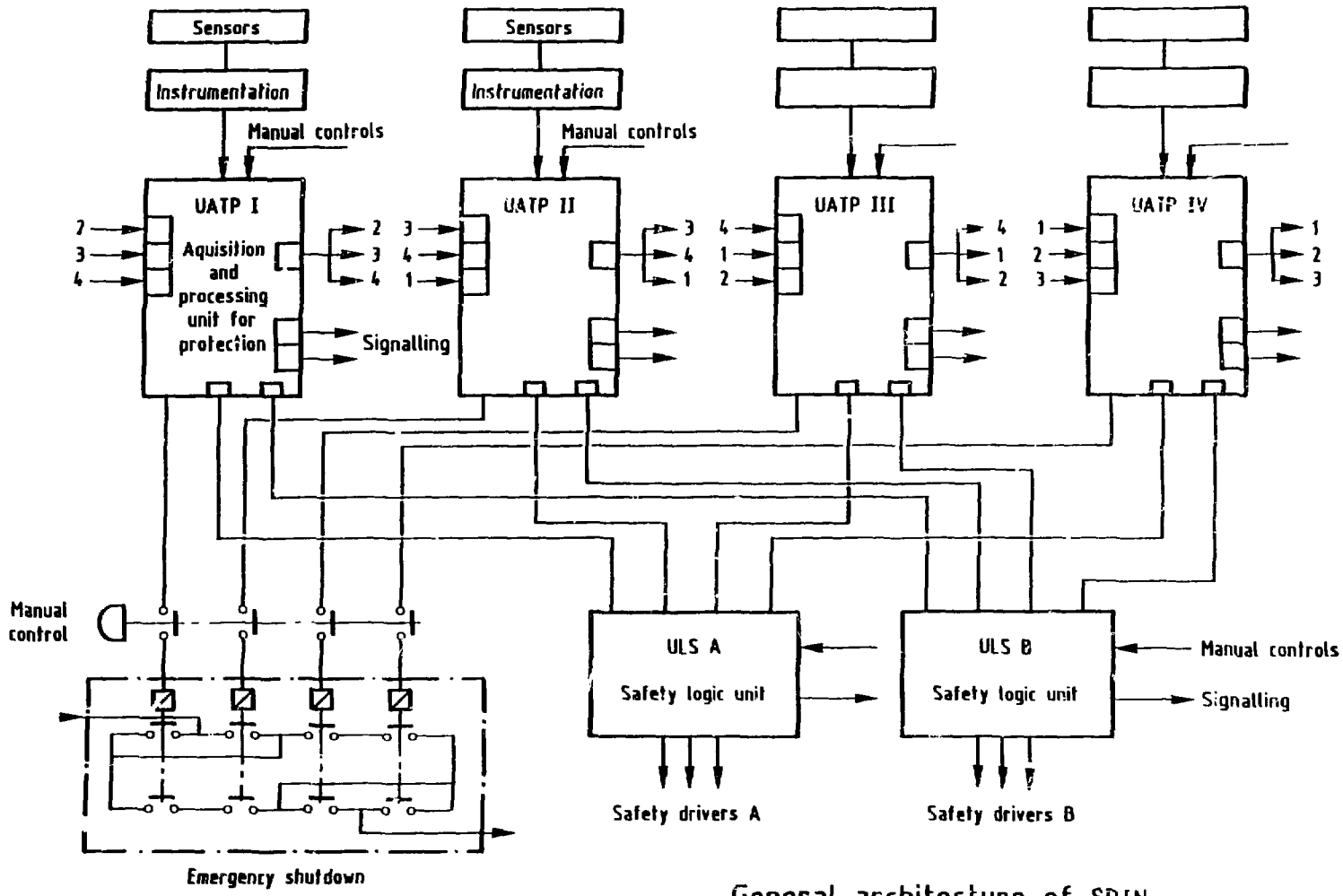
- *COMMON CAUSE FAILURES β factors 2/2*

. Sensors (instrumentation included)	5.10^{-2}
. Reactor Trip breakers	7.10^{-2}

- TABLE 2 -

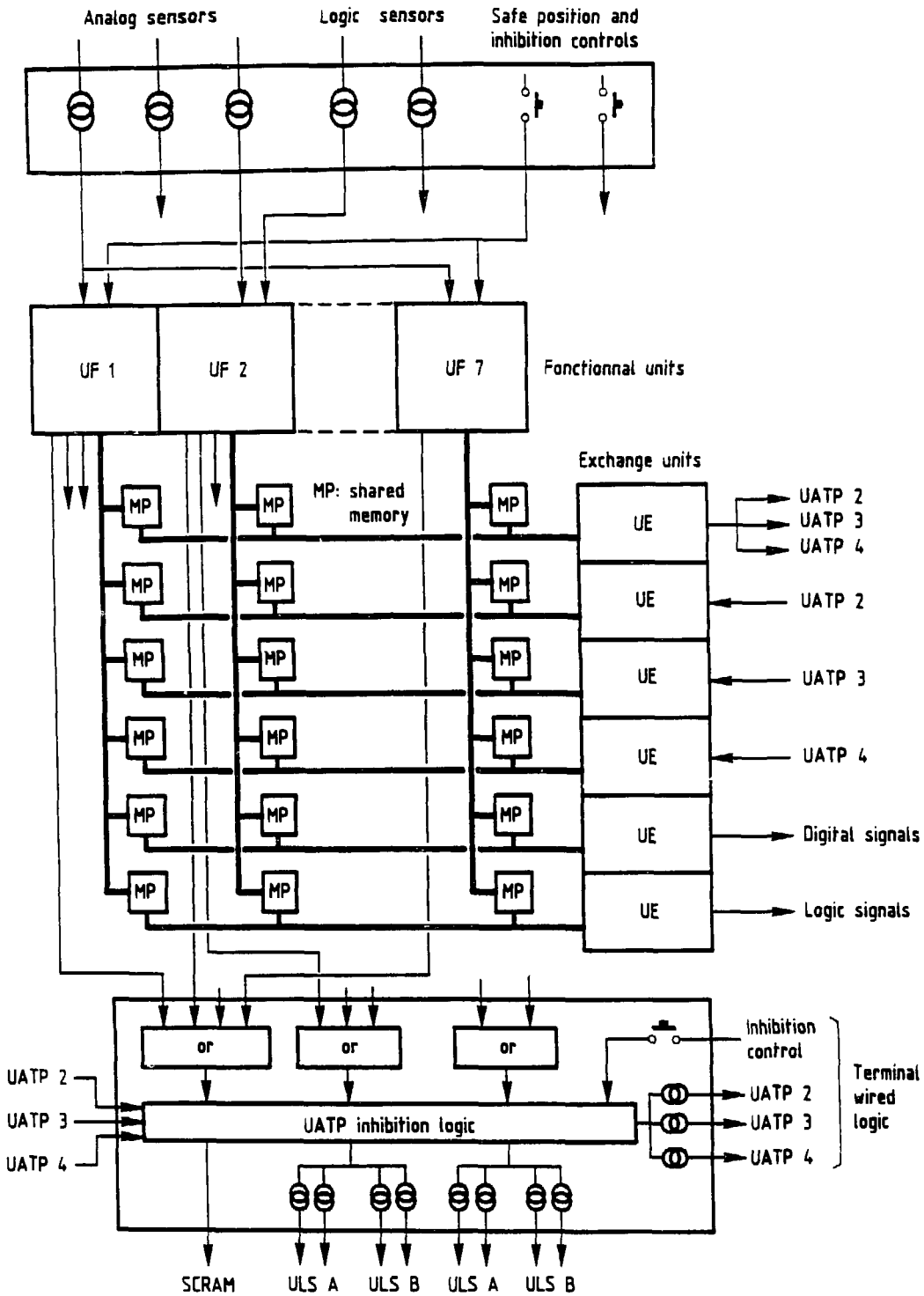
PROBABILITY OF FAILURE OF THE EMERGENCY SHUTDOWN
(with $\beta = 10^{-3}$ and $f = 10^{-3}$)

EMERGENCY SHUTDOWN (Initiating event)	TOTAL FAILURE PROBABILITY (per demand)	SENSORS and INSTRUMENTATION	UATP's	CONTROL RODS and TRIP BREAKERS	HUMAN ERRORS (safety thresholds)
Steam generator low level	$6,4.10^{-5}$	$9,0.10^{-6}$	$3,3.10^{-6}$	5.10^{-5}	-
High source flux	$7,4.10^{-4}$	$2,6.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	6.10^{-4}
Pressurizer low pressure	$7,7.10^{-4}$	$5,5.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	6.10^{-4}
Pressurizer very high pressure	$7,6.10^{-5}$	$2,1.10^{-5}$	$3,3.10^{-6}$	5.10^{-5}	-
High flux change	$6,8.10^{-5}$	$1,3.10^{-5}$	$3,3.10^{-6}$	5.10^{-5}	-
High power flux	$1,3.10^{-3}$	$1,3.10^{-5}$	$3,3.10^{-6}$	5.10^{-5}	$1,2.10^{-3}$
Low steam pressure	$8,0.10^{-5}$	$2,1.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	-
Low flowrate loop (1,2,3,4)	$6,9.10^{-4}$	$3,3.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	6.10^{-4}
Cold loop very low temperature	$1,3.10^{-3}$	$4,0.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	6.10^{-4}
Steam generator very high level	$7,5.10^{-4}$	$2,2.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	6.10^{-4}
Reactor coolant pump low speed	$7,6.10^{-4}$	$2,6.10^{-5}$	$6,6.10^{-6}$	5.10^{-5}	6.10^{-4}



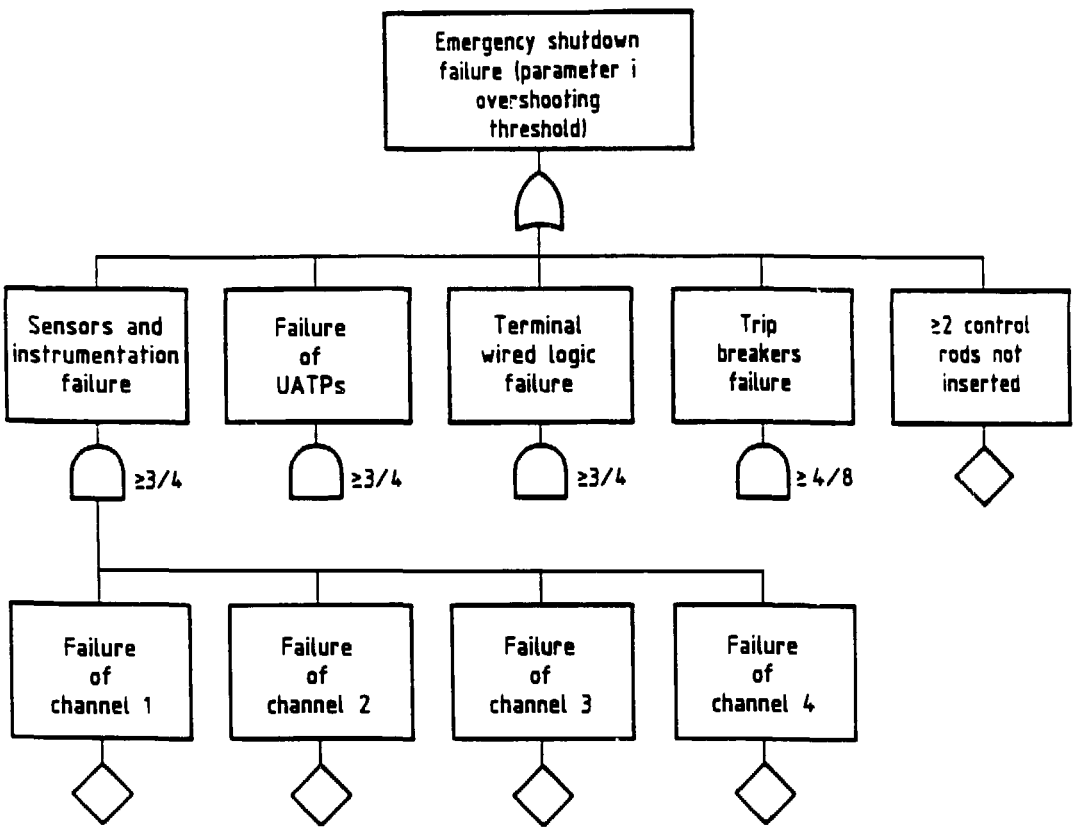
General architecture of SPIN

Figure 1



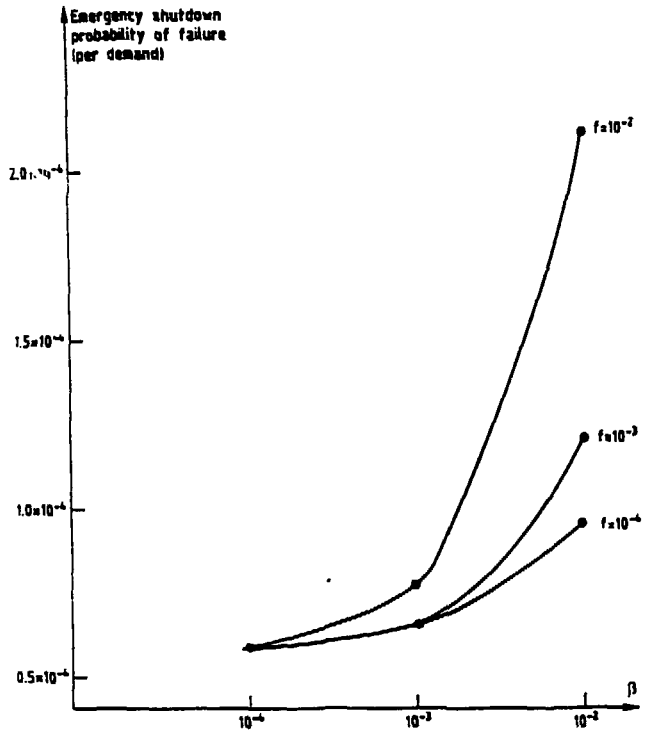
Structure of 1 UATP

Figure 2



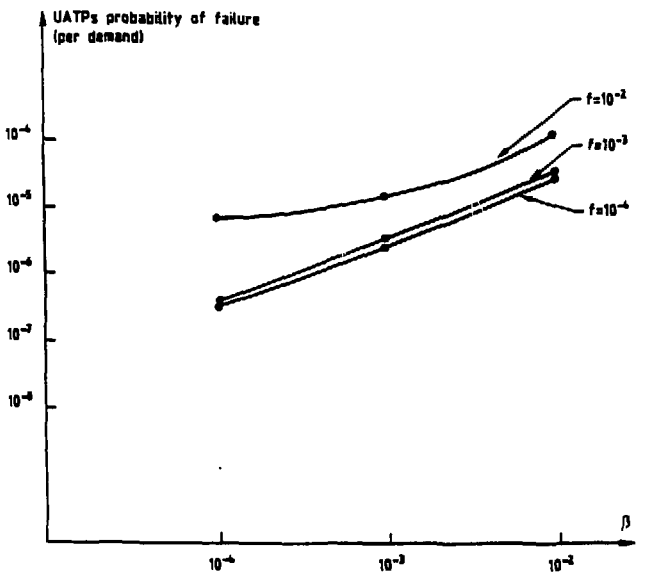
Failure of emergency shutdown
(general fault tree)

Figure 3



Emergency shutdown probability of failure
(initiating event = steam generator low level)

Figure 4



Probability of failure of the UATPs
(initiating event = steam generator low level)

Figure 5