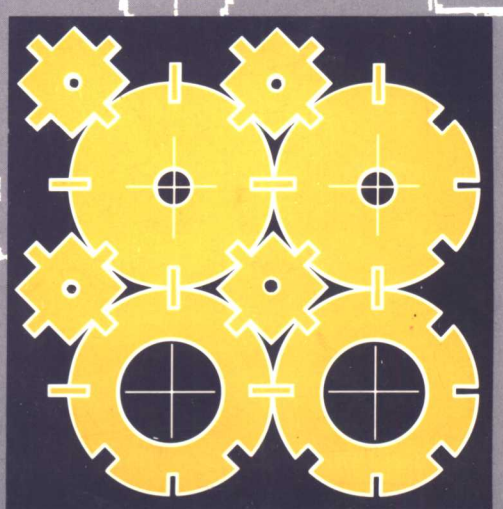
THERMAL REACTOR SAFETY ASSESSMENT



Conference organized by the British Nuclear Energy Society and co-sponsored by the American Nuclear Society, the Atomic Energy Society of Japan, the British Nuclear Forum, the European Nuclear Society, the Institution of Nuclear Engineers and the Safety and Reliability Society

A CIP catalogue record for this book is available from the British Library.

ISBN 0-7277-1993-9

First published 1994

Published on behalf of the organizers by Thomas Telford Services Ltd, Thomas Telford House, 1 Heron Quay, London E14 4JD.

Classification
Availability - Unrestricted
Content - Collected papers
Status - Invited authors' opinion and refereed papers
User - Nuclear plant engineers

Printed and bound in Great Britain.

Contents

Control, instrumentation and electrical reliability

Structural integrity

PWR plant transient analysis

Assessment methods

PSA applications

Accident management

Thermal/hydraulic methods analysis

Fuel performance and integrity

PSA methods

Source term methods and analysis

Graphite core analysis

Containment performance

Safety analysis and accident investigations

Extending operation

Papers 15, 24, 30 and 42, as well as the keynote addresses from T. Bennett and M. R. Hayns, were unavailable at time of publication.

Papers 19, 38 and 43 were withdrawn.

1. The reliability assessment of the control and instrumentation systems for Sizewell B

S. ORME, Engineer, PWR Project Group, Nuclear Electric plc

The Control and Instrumentation (C and I) systems for a nuclear power station must be shown to meet the system requirements set down for them at the beginning of the design phase. These system requirements include the targets for the reliability to be achieved by the systems. It is necessary to show that the systems meet the reliability targets in order to support the assumptions made in the station safety analysis. The purpose of this paper is to describe the work that has been performed by the various organisations to assess the hardware reliability of some of the key C and I systems for Sizewell B.

INTRODUCTION

1. This paper describes the hardware reliability assessment carried out on the Reactor Protection System (RPS) and the Data Processing and Control System (DPCS). Other C and I systems have also been the subject of reliability assessments, such as the Control Rod Drive Equipment (CRDE), but this paper concentrates on the DPCS and the RPS because of their particular roles in the safe operation of the plant.

2. Figure 1 shows these systems and their primary interfaces. The DPCS comprises the systems for performing plant control and providing operator information. It consists of three discreet systems; the High Integrity Control System (HICS), the Distributed Control System (DCS) and the Plant Control System (PCS). The DPCS is a Westinghouse design and the reliability assessment of the DPCS was also carried out by Westinghouse.

3. The RPS consists of two systems; the Primary Protection System (PPS) and the Secondary Protection System (SPS). The functions of the reactor trip and ESF actuation systems are represented in figure 2. The PPS is a computer based protection system whereas the SPS is a non-computer based protection system. These two systems provide both the reactor trip and the Engineered Safety Features (ESF) actuations necessary to protect the reactor against design basis plant faults.

4. The PPS is a Westinghouse design and therefore has some hardware similarities to the DPCS. The reliability assessment of the PPS was carried out by Westinghouse. Because the DPCS and the PPS were both assessed by Westinghouse the methodology for addressing the problem of assessing the reliability of computer based systems is the same. The SPS is mainly a GEC Alsthom design and its reliability assessment was carried out by GEC Alsthom, its contractors and Nuclear Electric.

5. There are differences between the target reliabilities for the DPCS and the RPS because of the different functional requirements of the systems. In the case of the DPCS, the important targets relate to the failure to control, spurious control, the failure to provide the operators with the correct information and the transmission of spurious information. The important targets for the RPS, both PPS and SPS, are based on the failure to perform a protection function on demand and spurious protection actuations.

6. The PPS and the DPCS are computer based systems and therefore not as amenable to the application of the FMEA methodology. This is because the particular failure modes of the hardware are dependent on the operating state of the hardware as dictated by the system software. There are therefore a large number of potential failure modes for a given hardware failure. The assessment of such systems requires a different approach.

7. The approach adopted for the software based parts of these systems is based on "Functional Block Analysis", or FBA. This technique is similar to the FMEA, but is centred around the functions of the system being assessed. By using the functional aspects of the system for the analysis, the limitations and drawbacks of the FMEA can be overcome. The FBA methodology enables the reliability of microprocessor based systems to be assessed by grouping the software driven hardware into functional units and by applying specific functional failure analysis in a systematic and thorough way. A detailed insight into the FBA methodology is provided below. The results of the FBA analyses is then used as the infeed to the Fault Tree Analysis for these systems.

8. The SPS has been assessed using both Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). The SPS being a hardware based system is amenable to a complete FMEA of all its constituent parts. The results of the FMEA are used as a basic infeed to the FTA. The paper will describe the methodology used for the assessment of the reliability of the SPS.

9. The reliability assessments of the systems are described below. The programme for the submission of the reliability assessments was determined by the project requirements and in particular the requirements of the licensing process. This point is important for the Westinghouse based systems because the assessment of the PPS, the first system to be assessed, includes some of the hardware components of the DPCS. This resulted in some of the FBAs for the PPS being called up for the DPCS assessment.

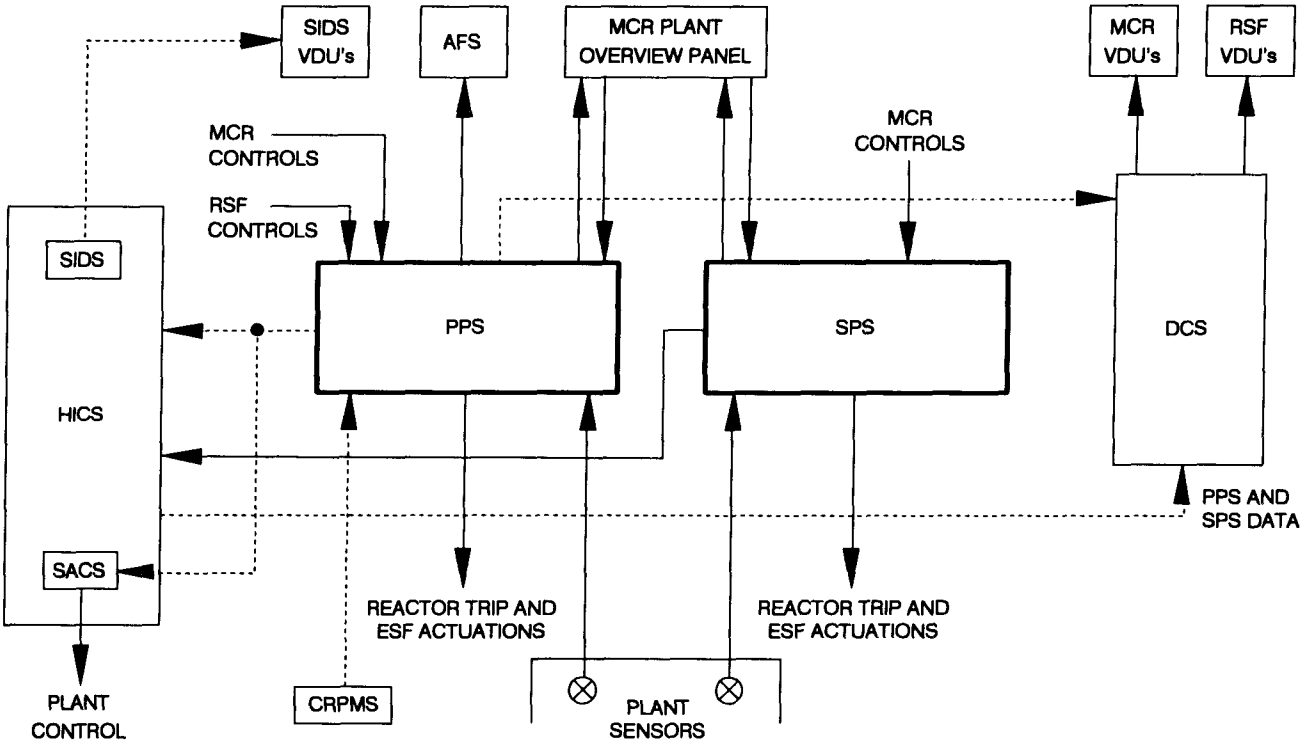


Fig. 1. Reactor Protection System and Data Processing and Control System main interfaces

1.0 The Reliability Assessment of the PPS

10. The reliability assessment of the PPS for Sizewell 'B' involved the following distinct stages:

(i) The performance of Failure Modes Effects Analysis (FMEA) on the non-software based parts of the system;
(ii) The performance of Functional Block Analysis (FBA) on the software based parts of the system;
(iii) The determination of the overall system reliability using Fault Tree Analysis (FTA);
(iv) The production of the Common Mode Failure (CMF) rate using the Multiple Greek Letter method.

11. The PPS reliability requirements include targets for the probability of failure on demand for the initiation of a reactor trip or an ESF actuation for a single input parameter (10^{-3}) and for two input parameters (10^{-4}) based on diverse measurements. In addition targets are also specified for the rate of spurious trips (10^{-1} per year) and spurious ESF actuation (10^{-2} per year). The objective of the reliability assessment is to ensure that the system is acceptable when compared to these targets.

12. In the preliminary reliability analysis it was assumed, in anticipation of the final design of the PPS, that the probability of a fault being revealed was indeterminable, it was here an assumption was made that the probability of detection of any failure would be 90%.

13. With this implicit assumption being one of the main contributing factors to the final reliability figure of the PPS, it has to be substantiated by further analysis, hence the need for a detailed analysis such as the FMEAs and FBAs. The results showed that this initial assumption was in fact pessimistic. The analysis was also used to determine the proportion of faults that result in a safe effect (fail-safe/fail-danger). Results of such further analysis can also be used to support the argument that equivalence to fail-safe design has been achieved.

14. Figure 3 shows a single train of the PPS. The figure includes both the Reactor Trip System, including the Reactor Trip groups, the Trip Enable subsystem, the Global Trip subsystem and the Dynamic Trip Bus and the Engineered Safety Feature Actuation System, including the Engineered Safety Features Actuation Cabinet (ESFAC) and the ESF Interface Cabinets (EICs). The FBA and FTA analysis is applied to all of the sub-systems shown in this figure and also includes the sensors that provide the input signals to the system.

1.1 The application of Failure Modes and Effects Analysis to the PPS

15. The PPS design includes both hardware and software such that the following logical split can be performed:

i) PPS functions conducted using only hardware and no software runs on them.
ii) PPS functions conducted using both hardware and software.

16. The areas of the PPS where only hardware is used to implement the functional requirements can be assessed by conventional FMEA techniques. All FMEAs conducted as part of the PPS analysis are consistent with the guidelines specified in IEC-812 (reference 1) and MIL-1629 (reference 2). The failure rates for the components are derived from MIL-HDBK-217E (reference 3) and

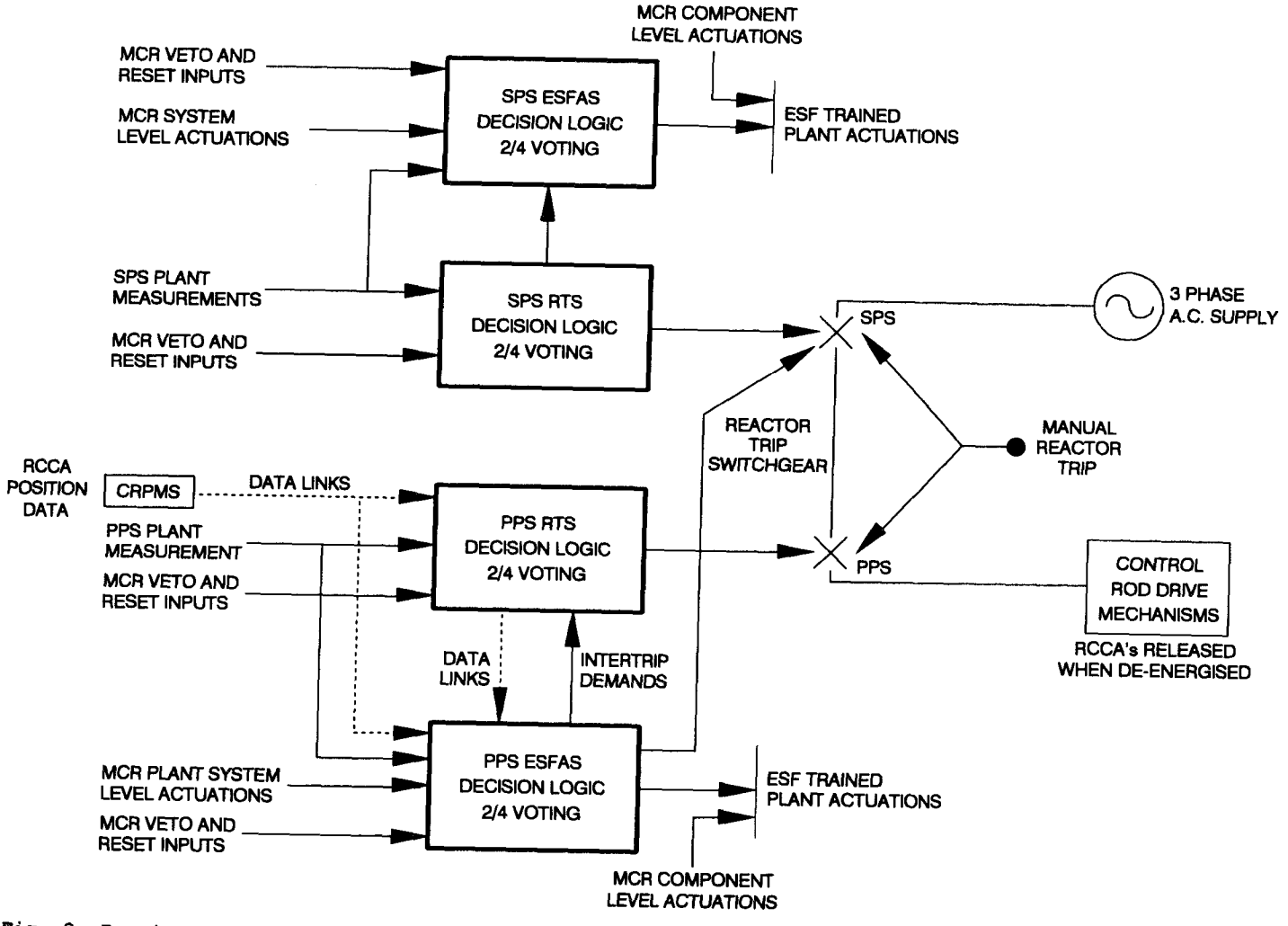


Fig. 2. Reactor Protection System block diagram - PPS and SPS

manufacturer information. The failure rate data, as is the case for the data for all of the C and I assessments, is pessimistic and is based on worst design case conditions.

17. The FMEA methodology has been used to assess the following functional areas of the PPS:

1) Nuclear Instrument Modules of the PPS .
2) Control portions of the Dynamic Logic Units.
3) Power Converter Card.

Because the PPS is predominantly a computer based system, the number of functional areas implemented in hardware alone is much less than those implemented in hardware and software.

1.2 The Application of Functional Block Analysis to the PPS

18. As stated above the majority of the PPS functional requirements are implemented with both hardware and software and hence there can be a multitude of possible failure-modes. There exist obvious drawbacks and limitations to applying traditional FMEA to complex systems with such multiple functions. This is because of the quantity of detailed system information being processed by the system and the number of possible operating modes of the hardware and software at particular points in time. Because of this, the method of Functional Block Analysis (FBA) has been adopted to overcome these restrictions by specifically addressing the limitations of the FMEA approach.

19. The FBA method involves an organising of the analysis on a purely functional basis rather than hardware which is the approach used with the FMEA method. The functional blocks are derived in such a way as to produce easily manageable assessment blocks. It is important to note that the FBA method covers the same hardware that is covered by the FMEA approach and hence is an equally systematic and comprehensive approach.

20. The PPS is broken down into the following 9 different distinct functional areas for analysis by the FBA method:

1) "Nuclear Instrument System Input"
2) "PROCESS Input"
3) "CONTACT Input"
4) "Rod Position Indication Datalink"
   "Serial DataLink"
   "Data Highway Datalink"
5) "EIC CONTACT Input"
6) "EIC RELAY DRIVER"
7) "PROCESSING"
8) "PARALLEL DATALINK"
9) "Dynamic Trip Bus INTERFACE"

21. Each FBA first determines the function of the part of the PPS to which it relates. It is thus possible to identify how any failure can inhibit this operation i.e. all functional failure modes are listed. The application of the FBA method can been seen by looking at the analogue inputs to the PPS during the analogue to digital conversion function. The possible functional failures would be:

- the output of the A/D is output is out of range,
- the output is within range and linear,
- the output is within range and non-linear.

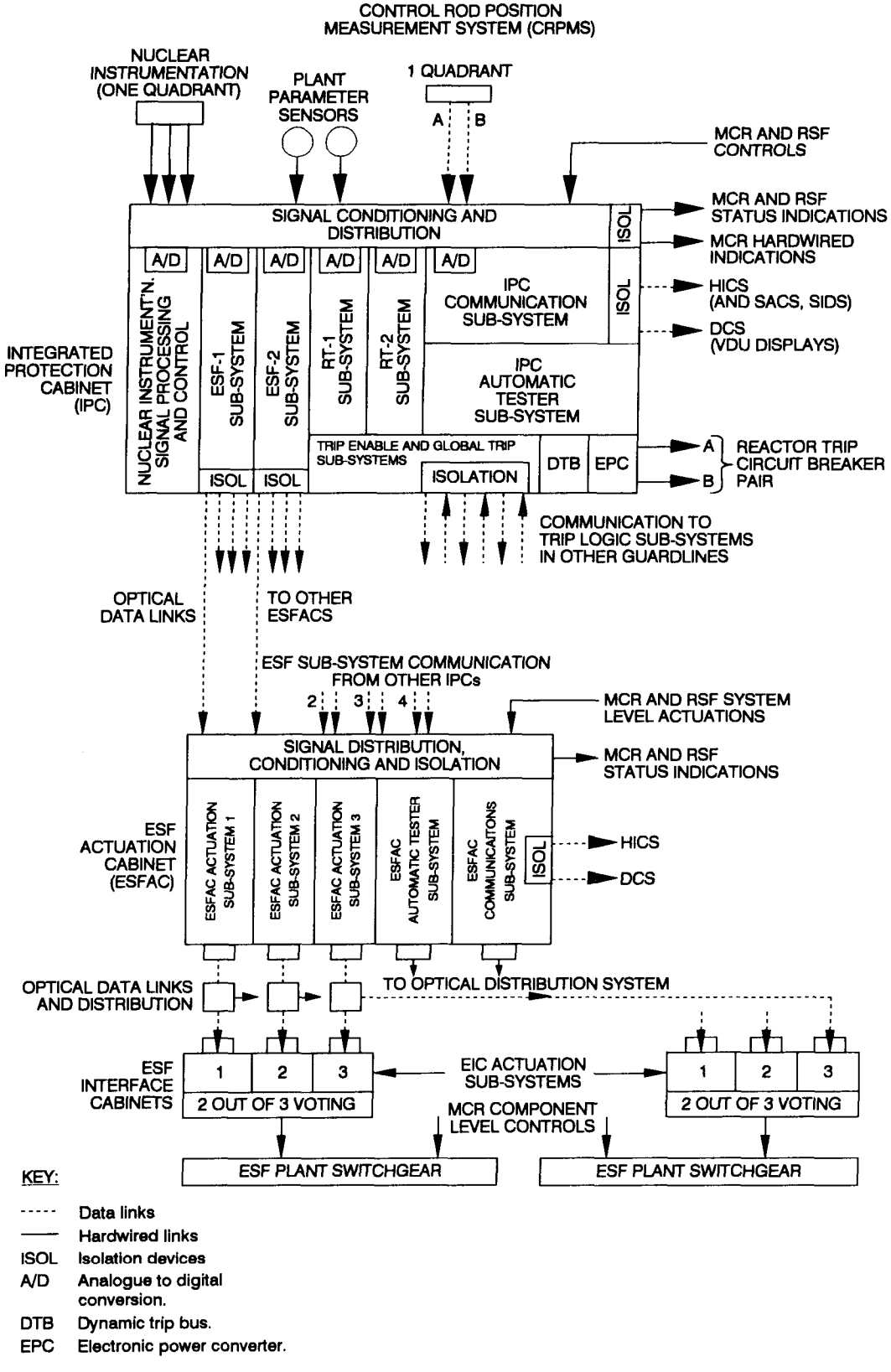


Fig. 3. Sub-systems within one PPS train

22. Each failure mode is then analysed to determine if a detection method exists to detect the fault (the detection method must not be inhibited by the failure itself). If the failure is detectable then a default action will result. If the failure is undetectable then the result may lead to a dangerous failure of the system ie. prevention of the protection action in the case of failure on demand. The resultant effect of that failure mode is then stated and a contribution to the failure of the PPS is determined based on the effects of the failure.

23. In general, failure modes of functions that have no comprehensive detection method, or partial detection coverage, are further assessed at a lower functional or component levels to

determine their failure modes and to identify their appropriate coverage/level of impact. Failure modes of higher level functions which can adequately be addressed by one or more methods of detection, are not broken down any further. This approach ensures that the detailed analysis effort is applied where it is required.

1.3 The Application of Fault Tree Analysis (FTA) to the PPS

24. The FTA methodology is applied to the assessment of the PPS to produce the quantitative reliability estimates for the various specified functions such as failure to trip, failure to actuate an ESF and spurious tripping and ESF actuations. The FTAs also provide the graphical output of the logic and arrangement of the FTA models and tabular outputs of the dominant contributors for each of the specified functions.

25. The code used to generate the FTA for the PPS was the GRAFTER FTA code developed by Westinghouse. The code has been fully verified and is used in other Westinghouse work areas such as Probabilistic Safety Assessment.

2.0 The Reliability Assessment of the DPCS

26. As in the case of the PPS, the DPCS is a computer based system and hence is not amenable to the FMEA technique for the determination of its reliability. It is therefore necessary to use the FBA technique to overcome the limitations of the FMEA technique. As stated above although this technique overcomes the limitations of the FMEA technique with respect to computer based systems, it still provides a comprehensive approach for assessing and determining the performance of such systems.

27. The reliability requirements for the DPCS are based on the failure mode (ie failure to control/indicate and spurious control/indication), the number of failures and also the number of separation groups affected by the failure. Hence for failure to control via the HICS for a single separation group the reliability requirement is 10^{-2} per demand, but for multiple failures to control within a separation group the target is 10^{-3} per demand and for failures across separation groups the requirement is 10^{-4} per demand. Similar requirements are set down for spurious control within and across separation groups.

28. As in the case of the PPS the assessment of the DPCS follows a systematic route for the determination of the reliability of the particular functions:

(i) The performance of Functional Block Analysis (FBA) on software based parts of the system;
(ii) The determination of the system reliability using Fault Tree Analysis (FTA);
(iii) The production of the Common Mode Failure (CMF) rate using the Multiple Greek Letter method.

It can be seen from this list that there were no specific FMEAs performed on the DPCS.

2.1 The application of Functional Block Analysis to the DPCS

29. As in the case of the PPS, the DPCS is split into functional groups for the purposes of the FBA. The DPCS consists of three specific functional areas:

- The High Integrity Control System (HICS),
- The Distributed Control System (DCS),
- The Process Control System (PCS).

The DPCS hardware within these areas is organised into discrete functional groups for the purpose of the FBA assessments. Hence in the case of the HICS, there are ten functional groups from the "Main Control Room Handstation Functions" and Interface to the "Network Interface". All of these functional groups are subjected to the FBA technique as described in the section on the PPS.

2.2 The Application of Fault Tree Analysis to the DPCS

30. The FTA methodology is used, as in the case of the PPS, to produce the quantitative reliability results for the different functional areas of the DPCS. The FTAs also provide a graphical output of the logic and arrangement of the FTA models. As in the case of the PPS, the GRAFTER FTA code was used to produce the FTA models.

31. Because of the size of the DPCS the size of individual trees was large and the whole system required several hundred trees to model all of the functional aspects of the system.

3.0 The Reliability Assessment of the SPS

32. As stated above, the SPS is a diverse system to the PPS and hence is not computer based. The assessment of the SPS can therefore be based on conventional FMEA techniques.

33. The reliability assessment of the SPS for Sizewell 'B' involves three distinct stages:

(i) The production of failure rate database for the components used in the systems.
(ii) The production of the Failure Modes and Effects analysis for the units which comprise the system.
(iii) The production of the overall reliability assessment for the system to determine if the reliability targets have been achieved.

34. The results of the FMEA on the individual units which make up the system were used in the overall reliability assessment. The general arrangement of the SPS is shown in figure 4. The reliability database provides the infeed into the FMEAs. The results of the FMEAs are used as the basic event data for the Fault Trees.

35. The assessment of the probability of failure on demand and the spurious trip/actuation rate was carried out using fault tree analysis. The decision to use fault tree analysis was made because it provided a systematic method of producing the reliability model of the SPS and in particular the more complex aspects of the SPS such as the initiation of the ESF's.

3.1 Sizewell 'B' Reliability Data

36. The failure rate data used in the SPS reliability assessment was derived using the MILSTRESS computer programme which uses MIL HDBK 217E as its data source. Apportionment data is taken from the IEE Electronic Reliability Manual but where data is not available the general rule of 90% open circuit, 10% short circuit has been used for the apportionment of data. This applies to both two terminal and three terminal devices.

37. The derivation of the failure rate is based on several assumptions of which the following are examples:

- The average ambient temperature is 35°C.
- The equipment operates in a Ground Benign environment.
- The style and quality factors used in the derivation of the failure rates are obtained from the designers Code Register. Other components are assumed to be of low quality (where low refers to the fact that the components are not "burnt-in").

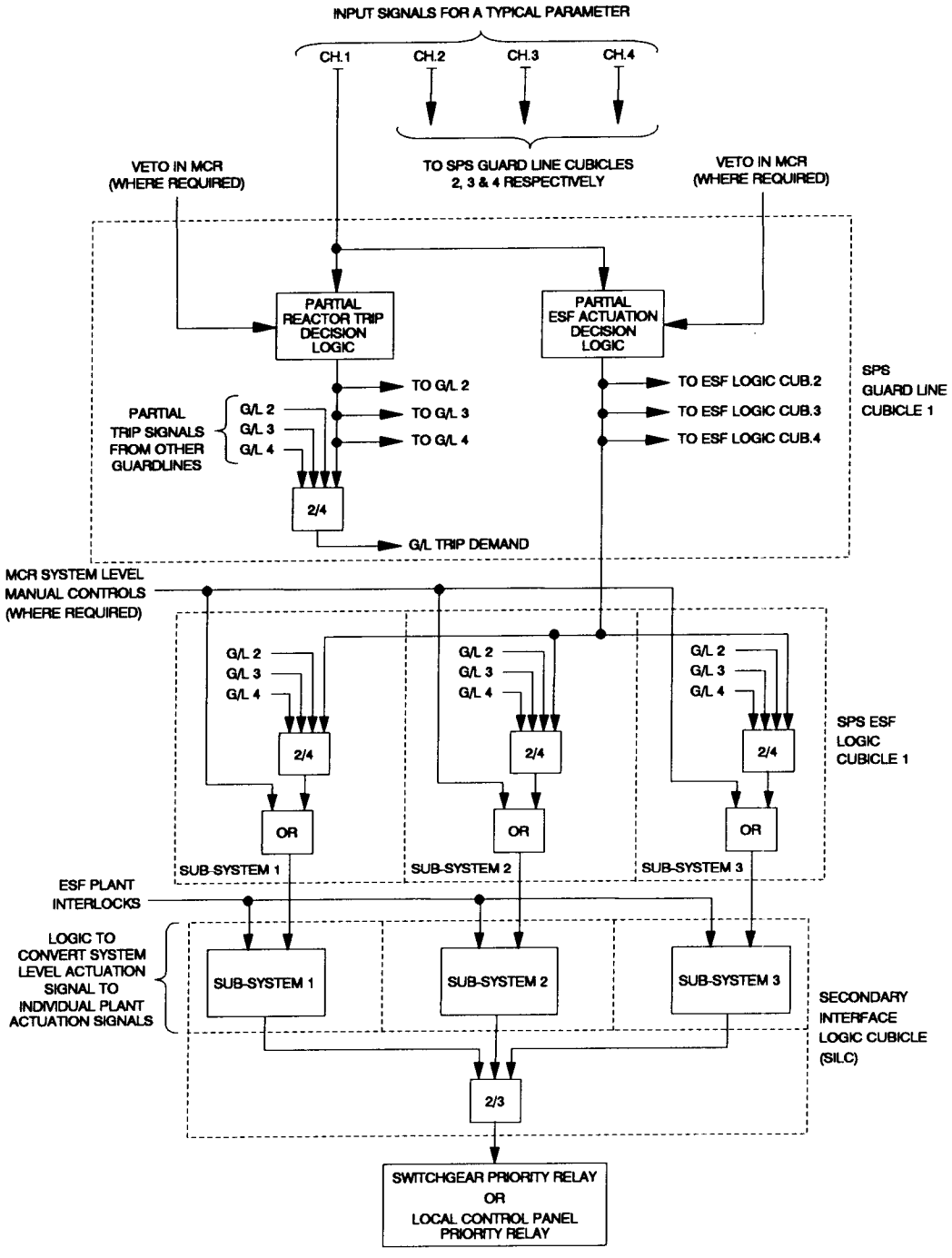


Fig. 4. SPS sub-systems and cubicles - RTS and ESFAS

38. Similarly with integrated circuits the 90%/10% apportionment rule applies. The probability of each pin failing open circuit is 90% of the total failure rate divided by the number of pins. The probability of a short circuit between adjacent pins is 10% of the total failure rate divided by the number of possible short circuit faults. The number of adjacent short circuit pin failures is dependent on whether the package is dual in line or round. For dual in line packages the assumption is that the adjacent pins may fail short circuit and the two end sets may also fail short circuit.

39. The final section of the Failure Rate Data Base document contains the calculated component together with its failure modes.

3.2 FMEA Methodology

40. The basis of the analysis is as follows:

- Component code allocation. The component types are allocated a code and the codes are subdivided for each component failure mode.
- Failure category allocation. The failure categories for the system being assessed are categorised. For example the category FO is classified as no effect. All other failure modes are categorised by the analyst.
- Analysis. The failure mode of each component and its effect on the system is assessed. For each failure mode, a failure category is assigned.
- Summary table production. The summary table is produced which shows all of

the component codes used against the fault categories.
- Fault frequency determination. The failure frequency of each component code for each failure category is determined using the Reliability Data Base document. All of the contributors to a fault category are summed to produce an overall figure for that fault category.
- Total failure rates and MTBF derivation The total failure rates associated with each category are summated to obtain a total unit failure rate. From this figure the MTBF for the unit is derived.

The summary table is achieved either by using a suitable PC based data base or can be carried out manually.

3.3 Fault Tree Analysis

41. The construction of the SPS fault trees involved the use of an accepted and validated computer based fault tree code. This was a different code to the Westinghouse GRAFTER FTA code. This code is used to produce fault trees for each of the parameters and for each ESF actuation to assess the failure on demand for the initiations and to assess the spurious trip/ESF actuation rate.

42. The fault trees use as input data the individual module failure rates as derived from the FMEAs described above. The probability of failure to initiate a protection action includes the time to detect the particular failure. For a particular protection function the probability of failure on demand is the combination of the individual modules in the functional arrangement of the system. This arrangement takes into account the voting configuration of the system.

43. Similarly the fault trees for the spurious trip/ESF actuation rate are produced using the module failures which could lead to the fault based on the functional arrangement of the system. Once again the failure modes are as identified as a result of the FMEA analysis.

44. The aim of the reliability analysis is to show that the modules which form the system are of adequate reliability and the SPS as a whole meets its reliability targets as stated above. The analysis shows that the overall reliability of the system is limited by Common Mode Failure of the system rather than random failure.

4.0 Common Mode Failure (CMF)

45. The approach to the modelling of CMF is similar for all three systems. The approach adopted for the PPS and the DCPS involved the use of the Multiple Greek Letter (MGL) method, which is described below. In the case of the SPS the beta factor method was used, which produces a more pessimistic result than the MGL method.

46. The PPS is a four redundant train system with two out of four voting being performed on the four redundant trains for protection function actuation. A random failure in a single train will cause a functional failure within that train but because the PPS has 3 other trains which are voted, single train failure does not prevent the PPS from correct operation. If a further train fails then the voting can still be satisfied and it would require three such failures to prevent a protection action from being initiated.

47. The random failures of the PPS have been assessed using the FBA, FMEA and the FTA methods described above. However, the most dominant limiting factor for the claimed reliability of multiple redundant voting systems such as the PPS is not caused by random failures but through common mode failures. Common mode failures are those failures which effect a multiple number of functions across the system. The modelling of CMF is based on the number of multiple trains required to be in the failed state in order to prevent the protection function from operating. In the case of the PPS and certain parts of the DCPS the CMF was modelled using the Multiple Greek Letter (MGL) method.

4.1 Multiple Greek Letter Method of Assessing CMF

48. There are a number of methods by which a contribution from common mode failure can be calculated. For the PPS and the DPCS the MGL method was used to determine the common mode probability of the PPS. This method is a means of quantitatively modelling CMF which addresses the potential for failures that could defeat the intended redundancy or independence of systems sharing identical components or components with similar designs.

49. The CMF contributions are quantitatively modelled using the MGL method by adding the unavailability times its beta, gamma and delta factors for each group of similar or redundant components for a given function within the system. In this way the application of the MGL method to similar or redundant groups of hardware within the system addresses the potential for failures which could defeat the built-in redundancy and voting logic.

50. The three factors used in the modelling of the CMF of the PPS and the DPCS are as follows:

Beta factor:-	this is the probability that the common cause of a component failure will be shared by one or more additional components,
Gamma factor:-	this is the probability that the common cause of a component failure will be shared by two or more additional components (to the first),
Delta factor:-	this is the probability that the common cause of a component failure will be shared by three or more additional failures (to the first).

51. In this way credit can be taken for the full four way redundancy of the PPS and for certain parts of the architecture of the DPCS. In the case of the DPCS, the extent of four way redundancy needed to meet its functional requirements is much less than the PPS and therefore the use of MGL is much more limited.

52. In the cases where four way redundancy is not provided the Beta factor method, a sub-set of the MGL method, was used. The derivation of the Beta factor is based on the method derived from Rolls Royce and Associates (reference 4). The Beta factors for the PPS, DCPS and the SPS were all derived via this method. The Gamma and Delta factors have been extracted from experience from existing electronic systems.

53. CMF is modelled in the fault tree analysis as described previously. The prevention of CMF and hence the minimisation of their frequency of occurrence is based upon defensive measures to avoid their occurrence. The defensive measures required to be taken on board in order to minimise the probability of CMF depends upon the reliability requirements of the system.

54. Some of the methods used in the Sizewell B project to avoid an excessively high frequency of CMF caused by the design/construction process are as follows:

(i) Review of design can be made at the appropriate stages prior to the completion of construction to identify and hence eliminate any sources of CMF.
(ii) The adoption of a comprehensive testing philosophy.
(iii) An important defence against CMF is to carry out a reliability assessment of the design.

55. In addition to the above requirements for the avoidance of CMF it is also necessary to ensure that the design contractor has adequate experience in the design and construction of such systems. It is also important to ensure that the contractor has in place an acceptable quality control regime, uses the most appropriate standards and has acceptable testing/inspection procedures.

5.0 Summary

56. The two constituent components of the Reactor Protection System, the Primary Protection System and the Secondary Protection System, and the Data Processing and Control System have been subjected to separate reliability assessments and have been shown to have an acceptable reliability with respect to the requirements specified at the beginning of the design stage. The modelling of the reliability has included Failure Modes and Effects Analysis for the hardware not containing software, Functional Block Analysis for the computer based parts of the systems and Fault Tree Analysis for the derivation of the quantitative assessment of the reliability of the various functions of the systems. The use of these techniques ensures a comprehensive approach to the assessment of the reliability of each of these systems.

57. It has been shown that the reliability claimed for the systems is not limited by the assessed random failure rates but by the common mode Failure rates assigned to the systems. The quantitative modelling of the CMF has included the Beta factor method and also the Multiple Greek Letter method to model the redundant features of the designs. The reliability assessments of the two systems demonstrates that the Reactor Protection System and the DCPS will deliver an acceptable reliability for its function within the Sizewell B Power station.

REFERENCES

1. IEC-STD-812, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA). International Electromechanical Commission - IEC Standard, Bureau De La Commission Electrotechnique Internationale, 1985.
2. MIL-STD-1629A, Military Standard - Procedures for Performing a Failure Mode, Effects and Criticality Analysis, US Department of Defence, 24 November 1980.
3. MIL -HDBK-217E, Military Handbook; Reliability Prediction of Electronic Equipment, US Department of Defence, 27 October 1986.
4. RAA/7692: Numerical Values for Beta Factor Common Cause Failure Evaluation - STF, Rolls-Royce and Associates Limited Technical Memorandum, February 1986.

2. Improving plant state information for better operational safety

C. GIRARD, CEA, E. OLIVIER, Framatome, and X. GRIMALDI, EDF

Nuclear Power Plant (NPP) safety is strongly dependent on components reliability and particularly on plant state information reliability. This information, used by the plant operators in order to produce appropriate actions, have to be of a high degree of confidence, especially in accidental conditions where safety is threatened.
In this perspective, FRAMATOME, EDF and CEA have started a joint research program to prospect different solutions aiming at a better reliability for critical information needed to safety operate the plant. This paper gives the main results of this program and describes the developments that have been made in order to assess reliability of different information systems used in a Nuclear Power Plant.

1. INTRODUCTION

A major effort to improve the safety of nuclear plants is to make sure that the plant operator has accurate informations on which his actions will be based. A lot of studies have been done, especially using the power of computer-based displays that were introduced in the control rooms following TMI-2 accident.

Various Safety Parameter Display System were developed and the need of validating data has been recognized to be of prime interest. Different techniques were used, providing Fault Detection and Isolation (FDI) modules to deal with faulty sensors that can end to a misleading information.

This techniques are well known and they are presently active in many Nuclear Power Plant control systems. Limit checking, consistency-checks, analytical redundancy are among the most current methods in the signal validation field.

The purpose of our study was, using the above techniques, to understand which kind of default is best treated by each method. Starting from the data of the PRA (Probability Risk Assessment) studies, we identified the most frequent instrumentation failures. Then dealing with those failures we established the way they could lead to a faulty information through different validation systems.

In order to achieve such a goal we had to define what is the generic failure probability of a single data acquisition channel, then of redundant systems. Once defined all these expressions we were then able to give the failure probability of a complex information based on several and different data sources.

An application of these developments was to assess the reliability of the mass inventory information which is one of the most important safety function in accidental operation for pressurized water reactors (PWR).

This information is based on different measurements and particularly on the core vessel water level measurement which is one of the most elaborated data used in the french PWR.

But before presenting this study, we must give the definition of what is an information, an information failure and a reliable information.

2. DEFINITIONS

Dealing with an operator activity, an information must be understood as an element that allows the operator to take a decision or to make a choice. The information is either an indication of a component status or an indication of a physical state of the plant.

The reliability of the first type of information is well defined and based on the classical rules of systems and equipments reliability, while for the second type, very few developments have been made. That is why this study, will deal only with the second type, the physical state information based on sensors datas. The Figure 1 illustrates the way information is generated from sensors.

One must say that in most cases the data processing module is a comparison of the validated value to a setpoint ; the information being for example : "the pressure is above p1".

When considering information reliability, two different approaches can be anticipated.

- The first defines reliability as the consequences it can induce on the safety of the installation.

Then, we consider that an information is reliable when we can guarantee that it will not lead to take a decision threatening plant safety.

- The second definition is somewhat more classical and states that a reliable information is an information that gives an accurate representation of the actual physical state of the plant.

Such a definition is more constraining than the first one but it really places the analysis at the level of the quality of the information (capacity of accurate representation). Our study will be based on this definition.

In fact reliability must be more than defining when the information will be lost (invalidation). It has to take into account more insidious failures such as measurements bias or drifts.

The classical equation of reliability will be used,

$$\text{reliability}(t) = 1 - P\{\text{system failure during } [o, t]\}.$$

P being the probability that the system exihibits a failure during the time internal [o, t].

Here, the failure of the system is that the information (produced from measurements data) does not indicate the accurate physical state of the plant.

Assuming that P_D is the global failure probability we shall use the following individual failure probabilities :

- P_i probability of invalidation of a measurement (the value is out of scale)
- P_B probability of having a bias or a drift on a measurement (over or under prediction)
- P_{mc} probability of having a common cause failure (producing either an invalidation or a bias or a drift)
- P_{DT} probability of having an electrical supply failure

Fig. 1. Information generation

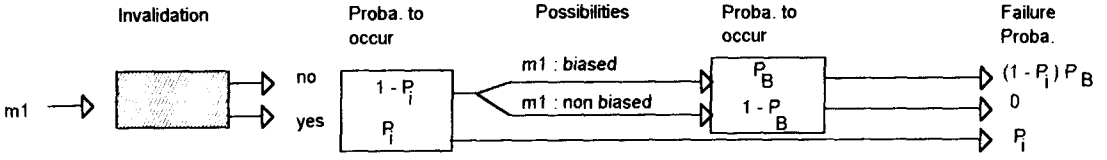


Fig. 2. Failure probability event tree

3. MEASUREMENTS FAILURES

In order to give an information failure probability we must obtain an analytical expression of the failure probability of each component of the generation process and in particular of the data acquisition step.

We will establish formulas for a single data acquisition channel then for redundant system (double and triple).

Failure probability of a single measurement :

The Figure 2 represents the event tree of a single channel probability failure, assuming the data could be invalidated (P_i) or biased or drifted (P_B).

The total failure probability (P_{D1}) of a single channel being the sum : $(1-P_i)P_B + P_i$, then :

$$P_{D1}(m) = P_i + P_B - P_i P_B \qquad (1)$$

In the Figure 2, biased stands for biased or drifted values.

Failure probability of a double redundant measurement :

In this case the event tree diagram (Figure 3), is more complex.

The global failure probability (P_{D2}), sum of the last column, is :

$$P_{D2} = (1-P_i)^2 \cdot \left(P_B + P'_{mc}\right) + 2(1-P_i) P_i P_B + P_i^2 + P''_{mc}(1-P_i)^2$$

P'_{mc} is the probability of having two biased values due to a common cause failure.

P''_{mc} is the probability of common cause failure producing an invalidation.

Putting $P_{mc} = P'_{mc} + P''_{mc}$ and keeping only the second order, we get :

$$P_{D2}(m) \cong P_B + P_{mc}(1-P_i)^2 + P_i^2 \qquad (2)$$

In the diagram, the step "probability to select biased value" has been implemented using a truth table with a "consistency check strategy" that selects the most conservative value in case of inconsistency.

This step is very informative and shows that a biased value is not "filtered" in such a selecting process. The final probability failure expression reflects this statement with a biased probability failure at the first order (Pb) while the invalidation probability is fairly reduced in this double redundant system since being at the second order $\left(P_i^2\right)$. Moreover we can see in this expression that the common cause failure stays at the first order.

Failure probability of a triple redundant measurement :

For seek of clarity we will not present the diagram that is however built on the same approach than for single and double measurements. The selection step is based on the median value (selecting the value between the two others) in case of total inconsistency.

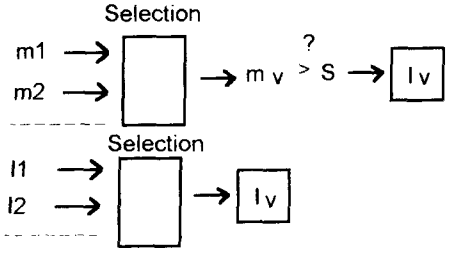
The final reduced expression is :

$$P_{D3}(m) \cong 3/2.P_B^2 + 3 P_i P_B + P_{mc}(1-P_i)^3 \qquad (3)$$

We notice that with a redundancy of three, the probability failure due to biased values is finally decreased.

4. INFORMATIONS FAILURES

We consider two cases : either the information is directly generated from measurements or the information is generated from redundant informations, the figure 4 summarizes the two possibilities.



I_V : validated information
m_V : validated measurement
S : set point

Fig. 4. Two types of information generation

For the first case we assume that :

$$P_{D1}(I_V) = P_{Di}(m_V) \qquad (4)$$

In fact $P_{D1}(I_V)$ is an over-estimated value since in some circumstances, bias or drift have no consequences on the information failure. For instance a positive bias when you are already above the set point will not theoretically induce a false information.

When considering information generated from others redundant informations, we have to stipulate clearly the selection process and the failure definition in order to estimate the failure probability.

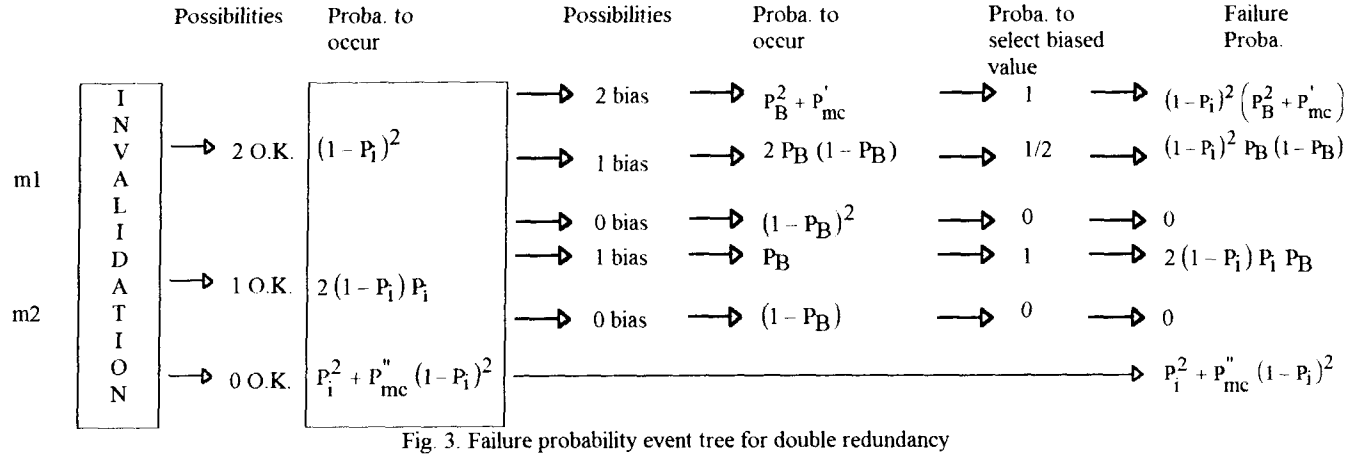
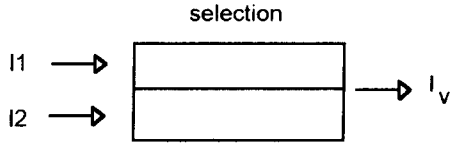


Fig. 3. Failure probability event tree for double redundancy

A selection on information since it is a binary comparison can be very restrictive. One can imagine a selection strategy where a few informations would be validated but with a high degree of confidence. This is the case, for instance, when you do not produce information if any inconsistency is detected and you define that unavailable information is not considered as a system failure. We can see here the strong effect of the selection strategy and the failure definition on the final result. This also shows the link between reliability and availability which are, in this case, antagonist goals.



For example, we can compare the two following selection strategies. In case of inconsistency, first : no information will be generated and there will be a system failure, and second : the worst information will be generated (conservative approach).

In the first case, and assuming I1 and I2 are informations produced with only one measurement, we will have :

$$P_{D2}(I_V) = 2P_B + P_i^2 - P_B^2 + P_{mc} \quad (5)$$

As in the second selection technique, it will be :

$$P_{D2}(I_V) = P_B + P_i^2 + P_iP_B + P_{mc} \quad (6)$$

One can see that the conservative approach is less influenced by a bias failure (P_b instead of $2P_b$), this corresponds to the case where there is inconsistency and where the selected information (the conservative one) is the right information. The first strategy would anyway produce a system failure in this case.

We have established the formula for three redundant information, the strategy of selection being based on a 2/3 vote (at least two identical informations to validate it). The analytical expression is, assuming one information is made with a single measurement :

$$P_{D3}(I_V) = 3P_B^2 + 3P_iP_B + P_{mc} \quad (7)$$

5. COMPARISON OF DIFFERENT SOLUTIONS

Once all those formulas established we need some data about invalidation, bias and drift probability. These data were found in the PRA studies developed on the CP 1300 program by Electricité de France (EdF).

The data for instrumentation failure show that among all the causes, 2/3 are bias and drift and 1/3 invalidation, the common cause failure representing 5 % of all these failures.

The influence of the degree of redundancy

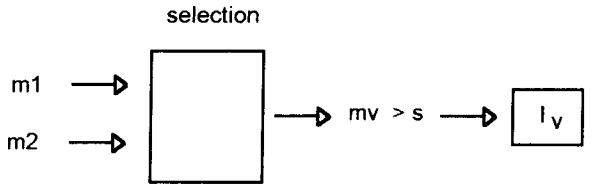
Assuming a sensor having a failure probability rate of 10^{-6}, which is an average, the table I indicates, according to the formulas defined above, the failure rate for different redundancy.

This table illustrates clearly the benefit of redundancy on the failure probability. The bias/drift which are the most important failure sources, are however reduced with a redundancy of the third order. On the other hand, we notice that common cause failure are not treated in this type of redundancy we shall have to go through more sophisticated techniques, like analytical redundancy to see their probability decreased.

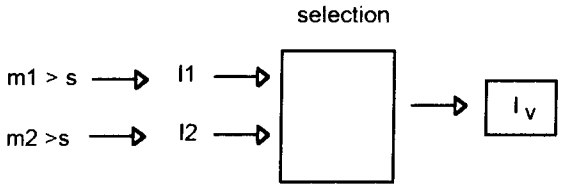
Selection on measurements or informations ?

Using the above formulas, it is easy to answer this question and check, which system gives a better result on failure probability. The two examples are summarized on the schemas below, for double redundant systems.

Selection on measurements :



Selection on informations :



In others words, the question is to understand at which level the selection process must be located in order to get the lowest failure probability.

After comparison, we can say that if the selection expresses the same strategy when applicated either on measurements or on informations, the result is exactly the same. So, no definite trends for a double redundancy are indicated.

On the other hand we must say that double redundant system cannot exihibit powerful consistency check methods either on informations or on measurements as far as bias and drifts are concerned.

Finally, we compared two triple redundant system : one with the consistency checking at the measurements level (based on the choice of the median value) and one with consistency-checking at the informations level (based on a 2/3 vote).

The results showed that consistency-checking on the measurements was slightly better, with a failure probability reduced by a factor of 2 compared to a selection on informations.

6. APPLICATION TO THE MASS INVENTORY INFORMATION

Among the critical safety functions that are challenged during an accident, the primary circuit mass inventory is one of the most sophisticated. Different instrumentations, different type of redundancies with a data processing stage involving different measurements make the reliability analysis relatively complex.

Before presenting the results of this application, one must give a short overview of the mass inventory calculation.

This information is elaborated with two main basic measurements : the core vessel water level (N) and the subcooling margin (ΔTs). These two measurements act in some conditions as physically redundant informations that will allow to implemente some validation procedures.

The signal flow diagram on the figure 5 depicts the information flow that gives the pair : (ΔT_S, N). We have a double redundancy and subscript A stands for the first channel and subscript B for the second one.

	1 measurement	2 redundancies	3 redundancies
Invalidation failure	$0.3.10^{-7}$	$0.09.10^{-14}$	$0.03.10^{-21}$
Bias/drift failure	$0.6.10^{-7}$	$0.6.10^{-7}$	$5.4.10^{-15}$
Common cause	$0.05.10^{-7}$	$0.05.10^{-7}$	$0.05.10^{-7}$

Table I. Failure rates