FIGURE 1

OVERVIEW OF APPROACH TO "FORTHWITH" STUDIES

Fire Risk Analysis

1. Preparation of plant area/isolatable system matrix
2. Model worst credible fire and explosion scenarios within each area
3. Assess damage levels and identify critical weaknesses

Evacuation, Escape and Rescue

1. Definition and description of existing evacuation system
2. Audit and comparison against existing and proposed standards
3. Base case assessment of system (without effects of accidents)
4. Assessment of system in response to accident scenarios

Emergency Systems Review

1. Identify and agree systems for review
2. Assess failure modes and effects and determine vulnerability
3. Assess impact of accident scenarios (from FRA) on "vulnerable" elements
4. Assess overall consequences for the systems

Smoke and Gas Ingress Review

1. Survey HVAC, doors and penetrations
2. Assess adequacy

COMPARISON OF EVENT TREE, FAULT TREE AND MARKOV METHODS FOR PROBABILISTIC SAFETY ASSESSMENT AND APPLICATION TO ACCIDENT MITIGATION

H James, (ICI FCMO, Blackley, Manchester), MJ Harris (University of Manchester) and SF Hall (SRD, AEA Technology, Warrington)

1. SYNOPSIS

Probabilistic safety assessment (PSA) is used extensively in the nuclear industry. The main stages of PSA and the traditional event tree method are described. Focussing on hydrogen explosions, an event tree model is compared to a novel Markov model and a fault tree, and an unexpected implication for accident mitigation is revealed.

KEYWORDS: Probabilistic safety assessment, event tree, fault tree, Markov, PWR, hydrogen

2. ACRONYMS

CET	Containment Event Tree
LOCA	Loss of Coolant Accident
MCS	Minimal Cut Set
PCSR	Pre-Construction Safety Report
PDS	Plant Damage State
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
RPV	Reactor Pressure Vessel
SRD	Safety and Reliability Directorate (part of AEA Technology, UK)
STPM	Stochastic Transition Probability Matrix
WCAP	WCAP-9991 (pre-construction PSA for Sizewell B)

3. INTRODUCTION TO PSA

PSA tries to assess the whole spectrum of risk presented by a hazardous plant or operation. It does this by systematically modelling a great number of different accident sequences. The main cause of possible public or environmental harm from an accident in a nuclear plant is the radioactive release that may result, so PSA attempts to assess the frequency of occurrence of the whole range of such releases.

The analysis is generally divided into three parts (see Figure 1). Firstly, it models the propagation of an accident through the plant. For each sequence which leads to a state in which the core of the reactor cannot definitely be cooled, the analysis then traces subsequent possible sequences of events in the containment (the building surrounding the reactor and associated equipment) and finally assesses the effects of any radioactive release. The analysis is normally limited to examining only the first twenty-four hours of the accident.

Firstly, a list of so-called Initiating Events which could trigger an accident is compiled. A Plant Event Tree is then used to trace the various possible sequences of plant behaviour that may occur in response to each category of initiating event. The structure of part of an event tree is shown in Figure 2. Every node in the tree represents a question, usually concerning the status of an engineered safety system. By following different paths through the trees, a large number of sequences is developed for each category.

The end of each sequence represents either a safe state, or a damage state in which it would not be certain that the core could be adequately cooled. Sequences which leave the plant in a similar damage state are grouped or binned into a Plant Damage State (PDS).

For each plant damage a Containment Event Tree (CET) is used to analyse the possible progression of the accident in the containment. The questions in this tree mainly relate.the the occurrence of physical phenomena in the containment building. Each accident sequence resulting from this analysis is identified as being either one which would not result in a radioactive release, or one which would give a release of a given magnitude, energy, etc. All those sequences which would give a similar release are grouped into one of a dozen or so Release Categories.

For each release category, the harm that would be inflicted on the population or environment is estimated in the Consequence Analysis using a model of the site (its meteorology, topology, demography etc). This traces the movements of the radioisotopes and their effects on the body and the food chain. The final product is usually a Risk Curve, a graph of frequency of occurrence vs number of deaths, illnesses etc.

4. SCOPE OF THE STUDY AND SIMPLIFICATIONS

The aim of this project was to develop alternative methods for carrying out the second stage of a nuclear plant PSA, ie containment analysis, which would be more efficient and would impose a more tractable structure.

Containment analysis is the most unsatisfactory and least developed of the three stages of PSA. There are three main areas of difficulty:

1. There is a lack of knowledge of some of the physical phenomena that could occur. Extra nodes are introduced into the tree in an attempt to compensate for this;

2. There is a great deal of uncertainty about the order in which some events could occur in the containment building. The only way to compensate for this is to repeat the relevant nodes at several points in the tree;

3. The resulting event trees are so large as to be unmanageable, often containing many millions of distinct accident progressions. In some cases, this requires the use of binning procedures at several intermediate stages within the event tree. This repeated removal of previously introduced detail is obviously inefficient.

The study was based on Sizewell B, Britain's first pressurised water reactor (PWR) which is currently under construction. It would have been impossible to perform a complete containment analysis in the time available so this 'prototype' study concentrated on hydrogen phenomena. This area seemed to be reasonably self-contained. Also, it was a field in which SRD, the project's sponsors, had considerable experience and expertise.

In a PWR, the main potential sources of hydrogen generation during a severe accident are the oxidation of zirconium and steel by steam and the reaction of molten core materials with the concrete containment floor (1, 2). Hydrogen could accumulate in the containment or on a local scale. This study only considered containment failure due to a global hydrogen deflagration (explosion). Eight categories of loss of coolant accident (LOCA) (five large and three small) were analysed.

The aim of the study was primilarly to develop new methods rather than to analyse the accident phenomena with great rigour, so these simplifications were not expected to affect the usefulness of the overall results. A degree of realism was nevertheless sacrificed.

5. EVENT TREE MODEL

The Sizewell B plant was an obvious choice for this study as the PWR is the most common reactor type in the world and Sizewell B is the newest British reactor. The general arrangement of the Sizewell B containment is shown in Figure 3. A comprehensive pre-construction PSA, referred to as WCAP, was performed for the plant (3) and this formed a natural basis for the event tree developed in this study.

The CET in WCAP contained 30 nodal questions and covered containment failure due to several causes, singly and in combination. However, because, in the present study, it had been decided that the tree would only consider containment failure due to a hydrogen explosion, the WCAP tree could be considerably 'pruned'. The tree was further simplified by eliminating paths which WCAP estimated to be of very low probability.

In the course of these simplifications, the nodes relating to hydrogen phenomena were restructured. It was hoped that these simplifications would make the tree more tractable and easier to comprehend. It produced a quite radical restructuring of the original CET (see Table 1).

Some data was recalculated in this study, either because it was absent from WCAP, or because the method used for its evaluation was judged to be unsatisfactory. The recalculations were of

1. Probability of hydrogen explosion;

2. Pressure rise due to explosion;

3. Probability of containment rupture.

The event trees were analysed on a PC using the MULTIPLET package developed by SRD, UKAEA (4).

6. FAULT TREE MODEL

Fault tree analysis is a well established technique for analysing the reliability of engineering systems. A fault tree was thought to be potentially more compact than an event tree. A fault tree approach might also assist in eliminating some of the detail which is introduced into a CET, only to be removed later on by binning sequences at intermediate stages and at their endpoints.

Fault trees use a 'top-down' logic that is essentially the opposite of that used in event trees. A failure condition or undesirable event, termed the top event, is defined and a tree is constructed to model the various events or plant failures, or combinations of these, that could lead to the top event (see Figure 4). Moving downwards, the first level of branching shows the various general conditions that can, singly or in combination, lead directly to the occurrence of the top event. The second and successively lower levels then show how specific events and plant or component failures, again acting singly or in combination, can lead to the occurrence of the first level conditions. The hierarchy of branching levels is continued downwards to a level at which adequate data is available. The events at this level are termed the basic events.

At each gate (a branching point, or node) the combinational logic is represented by an appropriate symbol. Boolean algebra can be used to express the tree in a logically equivalent form, in terms of the specific minimal combinations of basic events that would cause the top event to occur. These combinations are called minimal cut sets (MCS's). Various computer codes are available for the identification of MCS's and for quantitative analysis, packages such as ORCHARD (5) and LOGAN (6) being designed to run on a PC.

In addition to WCAP, a Pre-Construction Safety Report (PCSR) (7) for Sizewell B was carried out by EDS Nuclear (8). This was the only example of an apparent containment analysis by a fault tree method that was found in the available literature. However, details of these trees and calculations were not made public (9), so the PCSR trees could not be used in this study.

Fault trees were initially developed using Fullwoods method (10) and the Logic Diagram method (11-1). Each pair of initial trees obtained by these methods was combined to construct a final fault tree. A total of seven trees was enough to adequately define the release categories for all the eight PDS's analysed. The fault trees were judged to be concise and efficient.

The probabilities used in the quantification of the fault tree models were identical to those used in the event tree analysis (11-2). However, any probabilities whose values depended on previous events (so-called conditional probabilities) could not be incorporated, because there are inherent difficulties in using Boolean algebra to handle time-dependent problems (12, 13). The fault trees were analysed on a PC using the LOGAN package (6) developed by RM Consultants Ltd.

7. MARKOV MODEL

Markov methods have proved popular in the field of reliability analysis, particularly when applied to repairable systems. It was felt that a Markov model could overcome the problems of inefficiency associated with event trees and could impose greater structure on the analysis. However, a survey of the available literature failed to reveal any example of their previous use to structure a PSA.

A Markov model begins by defining a manageable set of the possible states that the system could be in at any time. The transitions between these states are represented by a matrix of probabilities, the so-called Stochastic Transition Probability Matrix (STPM). An accident sequence may re-enter previously quitted states, as opposed to the event tree and fault tree approaches in which, for this to occur, the relevant node must be repeated at each time of interest. A Markov model was thus perceived as being relatively compact. Figure 5 shows the structure of the Markov model in simplified form.

Development of the model was essentially an iterative process. An overriding priority was to make the assumptions in the Markov model as consistent as possible with those of the event tree. A summary of the final set of states and the 'skeleton' STPM (the latter showing the transitions that exist and the paths that have probabilities of 0.0 and 1.0) are given in Figures 6 and 7 respectively. The accident evolves in time in a broadly 'downward' direction, although 'upward' transitions to previously entered states are possible. In essence, the model divides into two phases, handling firstly an accident with the reactor pressure vessel (RPV, the vessel containing the core) intact and then with the RPV failed. Each row contains a group of states which deal with related combinations of physical phenomena.

Because the Markov model lacks memory, the combination of phenomena addressed in each state can seem rather obscure. Conditional probabilities can only be incorporated by passing on information on the relevant phenomenon from one state to another and this makes the state definitions bulky. A considerable amount of time and a degree of simplification was required to develop suitable state definitions.

In this study, the time-dependent behaviour was modelled using the "discrete time interval" method (11-3), ie the time behaviour was modelled in steps of t, the transition probabilities p(t) being given time-averaged values p(t) =   t, where   is a transition constant per unit time. The time-averaged model was compact and relatively straightforward to solve. Some transition constants were evaluated from WCAP data or from data that had been recalculated in this study. The remainder were estimated in the light of discussions with experts in degraded core analysis.

Multiplication of the row vector of initial state probabilities by the STPM an appropriate number of times, gave the row vector of state probabilities after twenty-four hours (see (12) for more details). Frequences of release categories could be extracted from the probabilities of containment failure states. Successively smaller values of t were used until the release category frequencies converged. Software was written to perform these calculations on a PC.

8. DISCUSSION OF RESULTS

8.1 Comparison of Methods

The three methods are compared qualitatively in Table 2. It was found that the general trends in sensitivity, of the results of the three models to variations in the modelling assumptions, were similar. The use of Markov and fault tree models for structuring a containment analysis led to the same overall conclusions regarding plant vulnerability as those from using the event tree model, suggesting that the results of all three methods were equally plausible. However, compared with the event tree model, both the Markov and the fault tree models were more compact and more efficiently structure (ie subsequent removal of detail included earlier was avoided) and should therefore be seriously considered as alternatives to the event tree model. It must nevertheless be stressed that it would be necessary to apply the methods to the full range of PDS's and accident phenomena it definitive conclusions about their relative values were to be drawn.

8.2 Sensitivity Studies

The effects on the results of different flammability models and explosion probability distributions were analysed. The conclusions were the same for event trees, fault tree and Markov models. In summary, they were most sensitive to (A) the type of propagation model employed (upward/global), somewhat less so to (B) the deflagration probability model adopted, and least sensitive to (C) the assumed value of minimum steam limit required for inertion against an explosion. This was rather unexpected because B was chosen by judgment alone so is to a great extent arbitrary, whereas C was chosen by judgment <u>and</u> experimental evidence.

8.3 Application to Accident Mitigation

The results of PSA can shed light on the effects of various items of safety equipment on the calculated probability of containment failure. In the containment of a PWR, the most important safety devices are:

1. the spray system, which would be used to lower the temperature and pressure by condensing steam, and remove soluble fission products and entrained solids;

2. the fan coolers, which would cool and mix the atmosphere and prevent the formation of pockets of hydrogen.

As an example, consider a large LOCA with:

1. early failure of emergency core cooling;

2. typical estimates of the amount of hydrogen evolved;

3. a realistic flammability model.

For this particular accident sequence, it was found that the average probability (ie average result of the event tree, fault tree and Markov methods) of containment failure was almost an order of magnitude higher if the fans and sprays were operating, compared to the corresponding accident sequence where both systems had failed. This can be attributed to the increased amount of steam in the containment if the sprays are inactive, which would tend to inert the atmosphere against the occurrence of a hydrogen explosion. If this type of accident were to occur, and if it could be identified at a sufficiently early stage, containment failure due to a hydrogen explosion might therefore be predicted to be less likely if the spray system and fans were actually to be deactivated. This, of course, is a highly simplified example which only considers containment failure due to a hydrogen explosion; realistic conclusions for use in accident mitigation would involve the analysis of a whole range of containment failure mechanisms. Nevertheless, it does illustrate how the results of PSA could have useful implications for accident mitigation planning.

ACKNOWLEDGEMENT

The funding assistance of the Safety and Reliability Directorate of AEA Technology and of the Science and Engineering Research Council is gratefully acknowledged.

REFERENCES

1. PWR Degraded Core Analysis, J.H. Gittus, ND-R-610(S), UKAEA, April 1982.

2. LWR Hydrogen Manual, Allen L. Camp et at., NUREG/CR-2726, USNRC, August 1983.

3. "Sizewell B Probabilistic Safety Study" (WCAP-9991) Rev. 1 Part 2, Westinghouse Electric Corporation, 1982.

4. MULTIPLET - a Program for Calculating Large Event Trees, S.F. Hall, SRD D 300, UKAEA, April 1984.

5. ORCHARD Version 4.0 Fault Tree Analysis Computer Software, SRD, AEA Technology, 1990.

6. LOGAN Version 2.13 User Guide, R87-10, R.M. Consultants Ltd., January 1989.

7. Sizewell B Pre-Construction Safety Report, CEGB, CEGB-10, April 1982.

8. Sizewell B PCSR Reference Report: A Review of the Selected Fault Tree Analysis for Sizewell B Undertaken by EDS Nuclear, R.W. Foden, PWR/RX 560, NNC, June 1982.

9. Sizewell B Public County Council and Suffolk Coastal District Council, Proof of D.C. Leslie, LPA/P/3, CEGB, March 1983, pp 103-105.

10. Systematic Process for Converting Event Trees to Fault Trees, R.W. Fullwood, Nuclear Safety <u>28</u>, No. 4, April-June 1987, pp 170-172.

11. A Study of Containment Analysis in Nuclear Reactor Safety Assessment, H. James, University of Manchester PhD Thesis, 1991.

11-1 p 270
11-2 Tables IV.1 and V.1 and p 203
11-3 pp 216-218

12. Reliability Evaluation of Engineering Systems, R. Billinton and R.A. Allan, Pitman Books, 1983 pp 206-7.

13. Fault Tree Symbols and Methodology, A. Cross, in "Fault Tree Course", SRD, AEA Technology, 12th-16th February 1990. p 5.

TIMEFRAME 1

From initiating event to just before RPV failure

1. Would less than 50% of the core migrate/pour into the lower plenum over this timeframe?

2. Does the hydrogen in the containment become well-mixed and remain well-mixed?

3. Is there no global hydrogen deflagration?

4. Does the containment not fail due to a global hydrogen deflagration?

TIMEFRAME 2

From start of RPV failure to one hour after RPV failure

5. Is the vessel failure mode dispersive?

6. Is water available to quench the discharged debris?

7. Does the majority of the accumulator water discharge into and remain in the lower reactor cavity?

8. Is the debris bed coolable over the first hour after RPV failure?

9. Does the hydrogen in the containment become well-mixed and remain well-mixed?

10. Is there no global hydrogen deflagration?

11. Does the containment not fail due to a global hydrogen deflagration?

TIMEFRAME 3

From one hour after RPV failure to approximately 24 hours after the initiating event

12. Is the debris bed water-covered and coolable over this timeframe?

13. Does the hydrogen in the containment become well-mixed and remain well-mixed?

14. Is there no global hydrogen deflagration?

15. Does the containment not fail due to a global hydrogen deflagration?

TABLE 1 NODAL QUESTIONS IN THE SIMPLIFIED CONTAINMENT EVENT TREE

Criterion	Event tree model	Markov model	Fault tree model
Efficient	No — detail often introduced but later removed	Yes, detail retained	Yes, but closely linked to release category logic diagram
Systematic	No	Yes, but less so than FT	Yes, but closely linked to release category logic diagram
Concise, pictorial representation	No, time-ordering fairly subjective	Yes, time-ordering handled naturally	Yes, but time-ordering could not be handled
Modelling, with adequate resolution, of accident evolution	Limited by coarse timeframe definitions	Yes, straightforward to calculated evolution of probabilities	Not possible, unless fault trees are redefined
Capacity to handle complex sequences	Good but tree could become prohibitively large	Slightly less than ET if set of states is to be manageable, but far more concise	Handled only simplified combination, not sequences, but results not unduly affected by this
Availability of data	Available	Required considerable manipulation and some use of expert judgement	Event tree data used directly (conditional probabilities could not be included)
Software availability	Readily available	None suitable	Readily available
Time to run on PC-AT	Very short (few seconds)	Several hours	Very short
Approximate time to develop and obtain results	4 weeks	7 months (including 4 months for software)	2 weeks

TABLE 2. QUALITATIVE COMPARISON OF METHODS

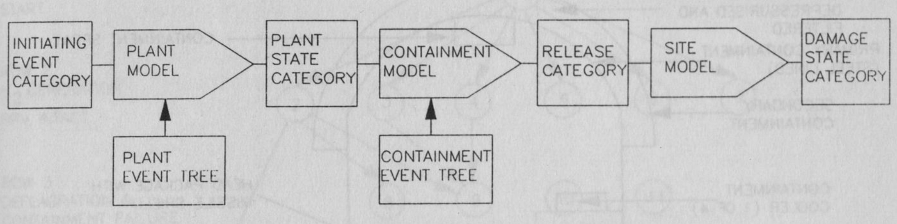

FIGURE 1 : OVERALL STRUCTURE OF PSA

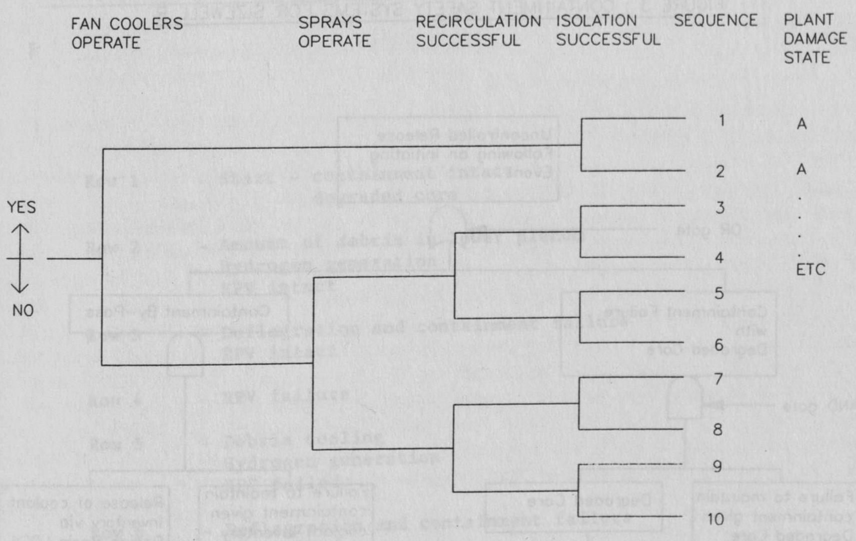

FIGURE 2 : PART OF A PLANT EVENT TREE (FOR SMALL LOCA)

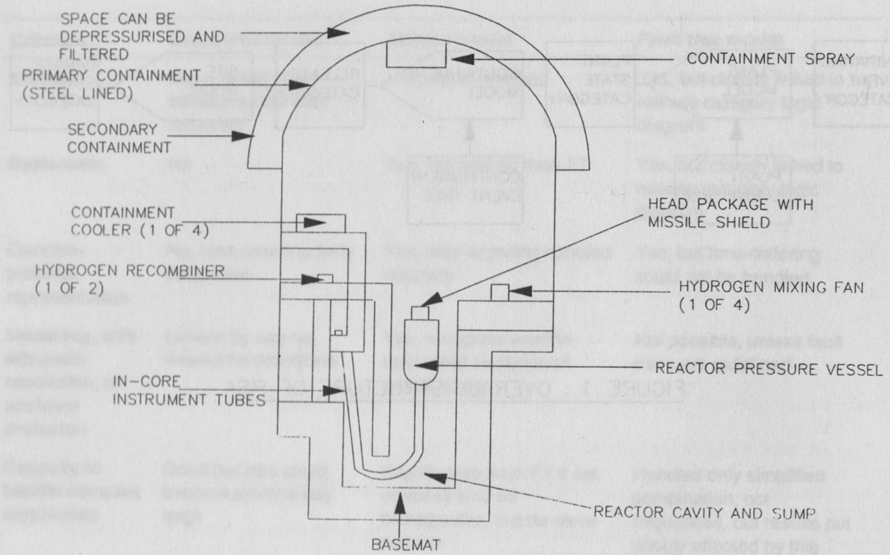
SPACE CAN BE DEPRESSURISED AND FILTERED
PRIMARY CONTAINMENT (STEEL LINED)
SECONDARY CONTAINMENT
CONTAINMENT SPRAY
CONTAINMENT COOLER (1 OF 4)
HEAD PACKAGE WITH MISSILE SHIELD
HYDROGEN RECOMBINER (1 OF 2)
HYDROGEN MIXING FAN (1 OF 4)
REACTOR PRESSURE VESSEL
IN-CORE INSTRUMENT TUBES
REACTOR CAVITY AND SUMP
BASEMAT

FIGURE 3 : CONTAINMENT SAFETY SYSTEMS FOR SIZEWELL B

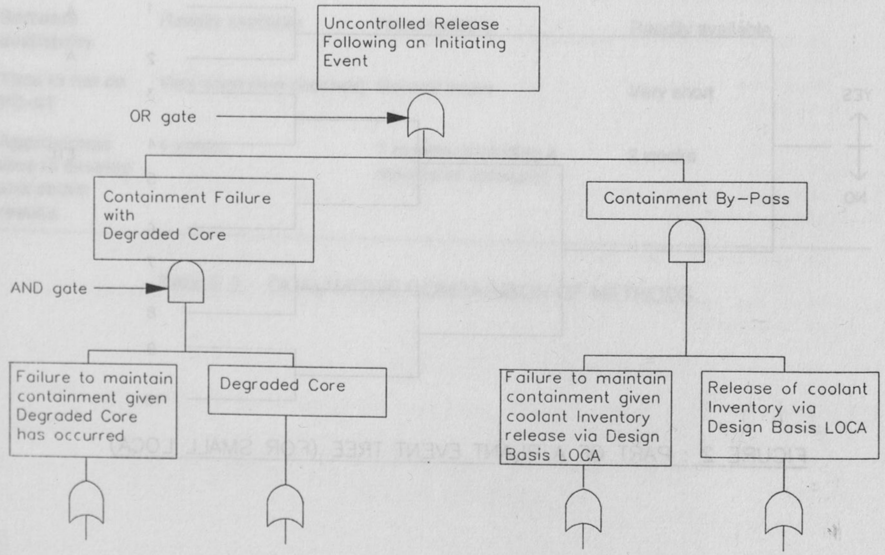
Uncontrolled Release Following an Initiating Event
OR gate
Containment Failure with Degraded Core
Containment By-Pass
AND gate
Failure to maintain containment given Degraded Core has occurred
Degraded Core
Failure to maintain containment given coolant Inventory release via Design Basis LOCA
Release of coolant Inventory via Design Basis LOCA

FIGURE 4 : TOP PART OF A FAULT TREE

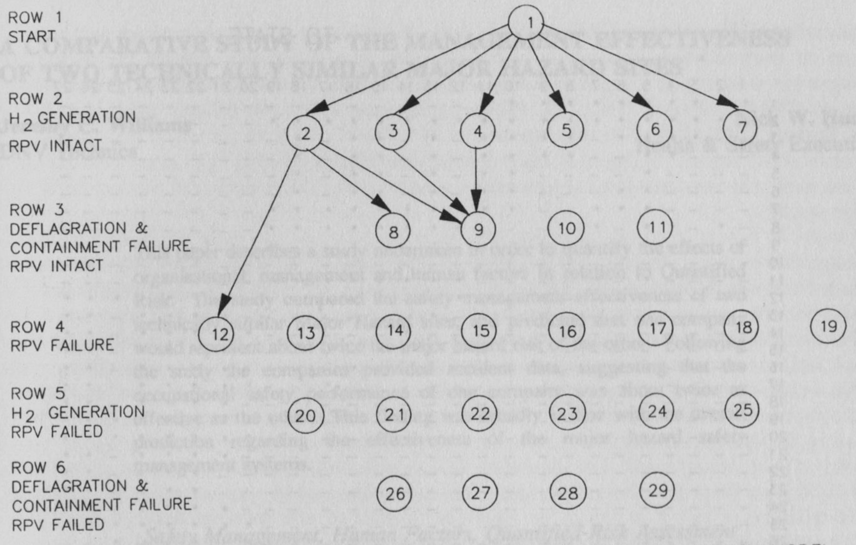

FIGURE 5 : ILLUSTRATION OF SEQUENCE DEVELOPMENT IN THE MARKOV MODEL

Row 1	Start - containment intact degraded core
Row 2	- Amount of debris in lower plenum Hydrogen generation RPV intact
Row 3	- Deflagration and containment failure RPV intact
Row 4	- RPV failure
Row 5	- Debris cooling Hydrogen generation RPV failed
Row 6	- Deflagration and containment failure RPV failed

FIGURE 6 : SUMMARY OF THE SET OF STATES IN THE MARKOV MODEL

TO STATE

FROM STATE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
1	*	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
2	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-
3	-	-	*	*	*	*	-	*	*	*	*	-	*	-	*	*	-	*	-	-	-	-	-	-	-	-	-
4	-	-	-	*	*	-	-	*	*	*	*	-	*	-	*	*	-	*	-	-	-	-	-	-	-	-	-
5	-	-	-	-	*	-	-	-	-	*	*	-	*	-	*	*	-	*	-	-	-	-	-	-	-	-	-
6	-	-	-	-	*	*	-	-	-	*	*	-	*	-	*	*	-	*	-	-	-	-	-	-	-	-	-
7	-	-	-	-	*	*	*	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-
8	-	*	-	*	*	-	*	-	-	-	-	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	*	-	*	-	-	-	-	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*
13	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-	*	*	*	*	-	*	*
14	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	*	*	*	*	*	-	*	*
15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	*	*	*	*	-	*	*
16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	*	*	*	*	-	*	*
17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	*	*	*	*	*	-	*	*
18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	*	*	*	*	-	*	*
19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	*	*	*	*	*	*	*
20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*
21	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	-	*	*
22	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*	*
23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*	*
24	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	-	*	*
25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*
26	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	*	*	-	*	-	-
27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
28	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	*	*	-	*	-	-

KEY

- – transition probability = 0.0
- 1 transition probability = 1.0
- * transition probability in the range 0 < P < 1

FIGURE 7 : 'SKELETON' STPM

A COMPARATIVE STUDY OF THE MANAGEMENT EFFECTIVENESS OF TWO TECHNICALLY SIMILAR MAJOR HAZARD SITES *

Jeremy C. Williams
DNV Technica

Nick W. Hurst
Health & Safety Executive

This paper describes a study undertaken in order to quantify the effects of organisational, management and human factors in relation to Quantified Risk. The study compared the safety management effectiveness of two technically similar Major Hazard sites, and predicted that one company would represent about twice the major hazard risk of the other. Following the study the companies provided accident data, suggesting that the occupational safety performance of one company was about twice as effective as the other. This finding was broadly in line with the overall prediction regarding the effectiveness of the major hazard safety management systems.

Safety Management, Human Factors, Quantified Risk Assessment

INTRODUCTION

The onshore and offshore major hazard industries already apply comprehensive measures to ensure that the levels of safety and availability achieved are of a high order. However, it is apparent that in the onshore and offshore industries, accidents such as those at Flixborough (Health and Safety Executive, 1975 [1]), Bantry Bay (Stationery Office, Dublin, 1980 [2]), and Grangemouth (Health and Safety Executive, 1989 [3]) can be seen to have had strong components of management failure. In addition, many studies have shown that a large proportion of major accidents are associated with human error. Joscheck (1981) [4], for example, suggests that 80-90% of the chemical industry's incidents and accidents involve the human element, and Singleton (1989) [5], reinforces these estimates by suggesting that between 50-80% of system failures can be ascribed to human error. The strength of the human contribution to system failure and hydrocarbon loss has been confirmed by Instone (1989) [6], who observes that, "It can be argued that virtually all causes of loss excluding natural perils are as a result of Human Error". Studies by Rasmussen (1980) [7], Samanta *et al.* (1981) [8], Ghertman and Griffon-Fouco (1985) [9], Institute of Nuclear Power Operations (1985) [10], and Bellamy *et al.* (1989) [11] suggest that it may be possible not only to identify the causes of human failure, but via safety management measures, find ways to reduce their overall likelihood.

Clearly if some techniques can be devised to assess the overall impact of human beings on overall system safety, it should be possible to target resources at the management failures and reduce the

* *The work described in this paper is of an exploratory nature. There is no implication that the findings will have an automatic application for the operational or advice roles of HSE.*